# Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

**Target of Evaluation**

| | |
|---|---|
| Application date/ID | 2009-06-29 (ITC-9257) |
| Certification No. | C0246 |
| Sponsor | RICOH COMPANY, LTD. |
| Name of TOE | Ricoh imagio MP 5000SP/4000SP with Security Card Type 9 |
| Version of TOE | - Firmware Configuration (System Version V2.16-00)<br>System/Copy :1.11.1 Printer:1.11<br>Network Support:7.26 MSIS:7.15.02<br>Network DocBox:1.10C RPCS Font :1.01<br>Web Support:1.59 Engine:1.04:05<br>Web Uapl:1.15 OpePanel:1.01<br>animation:1.3 LANG0:1.01<br>Scanner:01.24 LANG1:1.01<br>RPDL:7.33 ADF:15.000:15<br>- ASIC Ic Key:1100<br>- Option Data Erase Opt:1.01m |
| PP Conformance | 2600.1, Protection Profile for Hardcopy Devices, Operational Environment A 1.0, dated June 2009 |
| Conformed Claim | 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.
2010-02-25

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

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

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

**Evaluation Result: Pass**

"Ricoh imagio MP 5000SP/4000SP with Security Card Type 9" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

## Table of Contents

# 1. Executive Summary

## 1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of " Ricoh imagio MP 5000SP/4000SP with Security Card Type 9" (hereinafter referred to as "the TOE") conducted by Electronic Commerce Security Technology Laboratory Inc.Evaluation Center (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, RICOH COMPANY, LTD. and provides information to the users and system operators who are interested in this TOE.

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

This certification report assumes "general consumer" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

### 1.1.1 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 augmented with ALC_FLR.2.

### 1.1.2 PP Conformance

The TOE conforms to following PP as demonstrable conformance;

2600.1, Protection Profile for Hardcopy Devices, Operational Environment A 1.0, dated June 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, Version 1.0, dated June 2009
- 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A, Version 1.0, dated June 2009
- 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A, Version 1.0, dated June 2009
- 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval Functions, Operational Environment A, Version 1.0, dated June 2009
- 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A, Version 1.0, dated June 2009

## 1.2 Evaluated Product

### 1.2.1 Name of Product

The target product by this Certificate is as follows;

| | | |
|---|---|---|
| Name of Product: | Ricoh imagio MP 5000SP / 4000SP with Security Card Type 9 | |
| Version: | - Firmware Configuration | |
| | System Version: | V2.16-00 |
| | System/Copy | 1.11.1 |
| | Network Support | 7.26 |
| | Network DocBox | 1.10C |
| | Web Support | 1.59 |
| | Web Uapl | 1.15 |
| | animation | 1.3 |
| | Scanner | 01.24 |
| | RPDL | 7.33 |
| | Printer | 1.11 |
| | MSIS | 7.15.02 |
| | RPCS Font | 1.01 |
| | Engine | 1.04:05 |
| | OpePanel | 1.01 |
| | LANG0 | 1.01 |
| | LANG1 | 1.01 |
| | ADF | 15.000:15 |
| | -ASIC | |
| | Ic Key Version: | 1100 |
| | -Option | |
| | Data Erase OptVersion: | 1.01m |
| Developer: | RICOH COMPANY, LTD. | |

### 1.2.2 Product Overview

The target product in this certification is a digital MFP made by RICOH COMPANY, LTD. (as described below, "MFP"), providing the functions of copier, scanner, printer and etc. for digitizing paper documents, file management, and printing.
This product incorporates each function of scanner and printer with Copy Function. It is generally used to input, store, and output document data with connected to the office LAN. This product protects the MFP from unauthorized operation, the information of the internal stored document data from unauthorized access, and the sending or receiving document data between MFP and the clients from unauthorized access.

### 1.2.3 Scope of TOE and Security Functions

#### 1.2.3.1 Scope of TOE and Usage Environment

The TOE is composed of the "Security Card Type 9" residual data overwrite option installed in the "Ricoh imagio MP5000SP / 4000SP" MFP. The developer installs "Security Card Type 9" into the MFP "Ricoh imagio MP5000SP / 4000SP" on the user's site. After checking the performance, the TOE "Ricoh imagio MP5000SP / 4000SP with Security Card Type 9" is delivered to the users.
The usage environment for the TOE is shown in Figure 1-1.

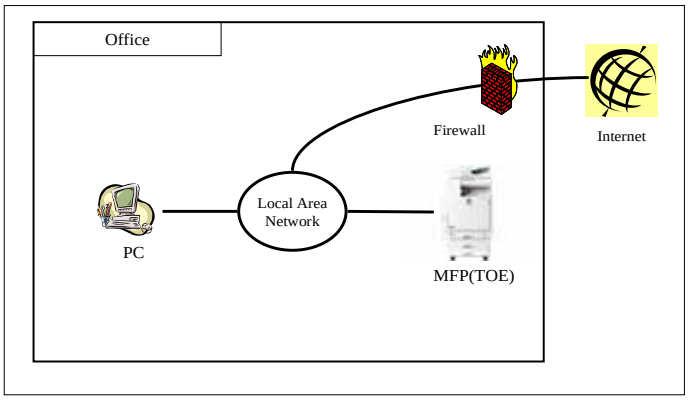


**Figure 1-1 TOE Usage Environment**

As shown in Figure 1-1, it is assumed that the TOE is used in offices.

[Local Area Network]
It indicates Local Area Network (as described below, LAN) used in offices.

[PC]
A client PC communicates with the TOE (MFP) via LAN to;

- Perform operations on the settings for MFP itself and on user documents via Web browser. (Delete / Download)
- Perform operations on user documents via printer driver. (Store / Print)

[Firewall]
It is a device to prevent any attack in the office network from the Internet.

For using the TOE in this environment, the related users are shown in Table 1-1.

**Table 1-1 TOE Users**

| User Definition | | Explanation |
|---|---|---|
| Normal user | | User, who is allowed to use the TOE, is granted login user name and performs normal MFP functions. |
| Administrator | Supervisor | Authorises to delete and register a login password of MFP administrator. |
| | MFP Administrator | User, who is permitted for the TOE management, performs the management operations for user data management of normal users, machine management, file management, and Network management. |

As shown in Table 1-1, the TOE users are categorized as Normal user and Administrator. In addition, administrators are categorized as Supervisor and MFP administrator according to the roles. A user who directly uses the TOE is shown in Table 1-1. An indirect user for the TOE, the MFP chief administrator, is responsible for selecting a supervisor and MFP administrators. The MFP chief administrator is assumed to be an organisational responsible manager for the usage environment.

1.2.3.2 TOE Configuration and Operational Overview

Internal physical configuration for the TOE is shown in Figure 1-2.

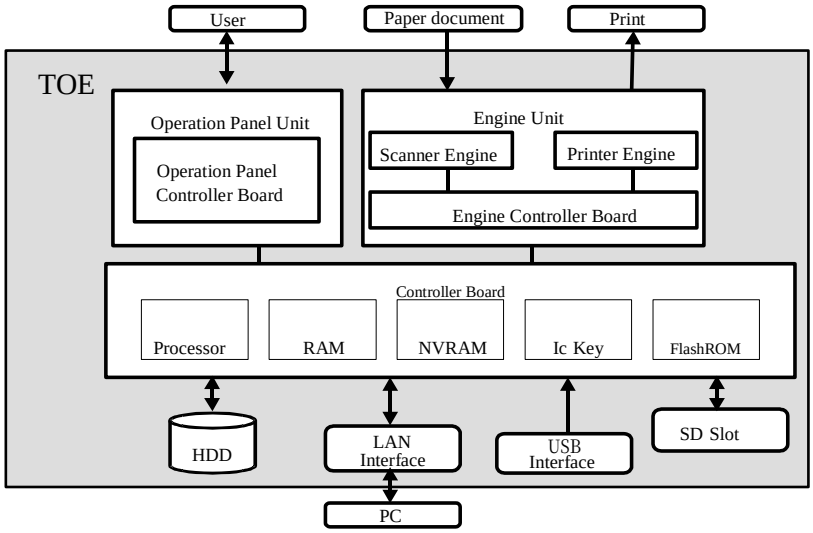


**Figure 1-2 TOE Internal Configuration**

As shown in Figure 1-2, the TOE is composed of hardware of Operation panel unit, Engine unit, Controller board, HDD, LAN interface, USB interface, and SD slot. The overview for each configuration component is shown as follows;

[Operation Panel Unit (as described below, "Operation Panel")]
Operation Panel is a device which has the user interface function installed in the TOE, and consists of key switches, LED indicators, touch screen LCD, and operation panel control board which is connected with these devices. The operation panel control software is installed in the operation panel control board.

[Engine Unit]
Engine Unit is composed of scanner engine that is a device to read paper documents, printer engine that is a device to print and output paper documents, and engine controller board to control each engine.

[Controller Board]
Controller Board is a board equipped with Processor, RAM, NVRAM, Ic Key, and FlashROM. Brief explanations for each component are as follows;

Processor: Semiconductor chip that performs the basic calculation processing for MFP operation.
RAM: Volatile memory which is used as a working area to process the image data for compressing / decompressing the processing information and to temporarily read and write the internal information.
NVRAM: Non-volatile memory to store TSF information which determines the MFP operation.
Ic Key: Security chip which has functions of random number generation, cryptographic key generation, and electronic signature. It provides storage of the signature root key for maintenance when shipping from factories.
FlashROM: Non-volatile memory that installs MFP control software itself.

The MFP control software is software installed in the TOE, and among the components of the TOE, corresponds to System / Copy, Network Support, Scanner, Printer, Web Support, Web Uapl, Network Doc Box, animation, RPDL, MSIS, RPDL, MSIS, and RPCS Font.

[HDD]
HDD is a Hard Disk Drive to store user information for image data and identification and authentication.

[LAN Interface]
LAN Interface is an External interface for LAN to support Ethernet (100BASE-TX/10BASE-T).

[USB Interface]
If printing directly from PCs, it is an external interface to connect the TOE with client PCs. This interface is disabled during the installation / setup of the TOE.

[SD slot]
Slot for inserting an SD card, which keeps the residual data overwrite function software (Data Erase Opt). The SD slot is inside of the device, and only a customer engineer is allowed to open the cover and use it for installation.

And the TOE provides as Product Service Function the following basic functions that are realised by the TOE configuration as shown in Figure 1-2.

(1) Copy Function
Copy Function is to scan paper documents and then print the scanned image data according to the chosen number of copies, the printing magnification, and the custom settings.

(2) Printer Function
Printer Function consists of the following 3 functions;

- A function to store as user documents the printing information from client PCs via Network.
- A function to perform the operation of printing the stored user documents.
- A function to directly print the printing information from client PCs via Network.

According to the guidance, normal users shall install first the designated printer driver in their own client PCs, and then use it.

(3) Scanner Function
Scanner Function is to scan paper documents and consists of the following 2 functions;

- A function to scan and store user documents in the device itself.
- A function to download to client PCs the stored user documents.

(4) Document Server Function
Document Server Function is to perform operations on user documents stored in the HDD of the MFP device itself. Printing the user documents which are stored by the above printer function, and downloading to client PCs the user documents stored by the scanner function, are implemented using this document server function.

(5) Management Function
Management Function is to control all of the operation of MFP devices. It is performed by Operation Panel or via Web browser.

(6) Maintenance Function (This function is deactivated.)
Maintenance Function is to implement the maintenance service processing for machines malfunction. Customer Engineer performs to analyse the cause from Operation Panel. This function will be performed only by the procedures which Customer Engineer holds. If MFP administrator sets the service mode lock, Customer Engineer cannot use it.
In this TOE operation, the Service Mode Lock Function is assumed to set to 'ON' in order to deactivate this function.

(7) Web Function
Web Function is a function with which the TOE user operates a remote control for the TOE from a client PC. For the remote control, install the specified Web browser in the client PC according to the guidance, and then connect the TOE via LAN.

1.2.3.3 TOE Security Functions

The TOE provides the security functions in order to prevent unauthorised access (alteration, disclosure) for the document information used in the basic functions shown in 1.2.3.2. The assets to be protected by the security functions (protected assets) and the overview of each security function are shown as follows;

(1) Protected Assets
Protected assets for the TOE are shown in Table 1-2 and 1-3. The following user data and TSF data are included as protected assets of the TOE security functions.

**Table 1-2 TOE Protected Assets (User Data)**

| Type | Assets Content |
|---|---|
| Document Information | Digitalized user documents, deleted documents, temporary documents and fragments under the TOE control. |
| Function Information | Job specified by users (as described below, "User Job".) |

**Table 1-3 TOE Protected Assets (TSF Data)**

| Type | Assets Content |
|---|---|
| Protected Information | Login user name, Status of user job, Number of attempts before lockout, Timer settings of lockout release, Lockout time, Year-month-day settings, Time settings, Service Mode Lock Function (as described below, "TSF Protected Information") |
| Confidential Information | Login password, Audit log (as described below, "TSF Confidential Information") |

(2) Security Functions
The security functions that the TOE provides are shown as follows;

[Audit Function]
Audit Function consists of the following 2 functions; to generate audit log for the occurrence of auditable events in order to check the TOE operation and detect the security intrusion, and to allow MFP administrators only to read and delete the audit log generation. The operations of reading and deleting the audit log data are performed by Web Function.

[Identification and Authentication Function]
Identification and Authentication Function consists of the following 3 functions; Identification and Authentication Function for persons who attempt to use the TOE, Lockout Function for users who consecutively failed in authentication, Authentication Feedback Area Protection Function for entering login password when logging in using the Operation Panel. For using the Printer Function, users enter a user name and a login password in the printer driver.

[Access Control Function]
Access Control Function is used to control based on the authorities given to the roles of the permitted TOE users that the Identification and Authentication Function authorised or based on the operation authorities of user documents given to each user.

[Network Protection Function]
Network Protection Function is used to perform encrypted communication in order to prevent information disclosure from monitoring on Network when using LAN.

[Residual Data Overwrite Function]
Residual Data Overwrite Function is used to completely delete the residual data by overwriting the specific pattern data for user documents, temporary documents and fragments deleted in HDD.

[Security Management Function]
Security Management Function is used to manage all of the functions related to security management performed by administrators.

[Software Verification Function]
Software Verification Function is used to ensure the correctness of MFP control software by verifying the integrity of executable codes for the MFP control software installed in FlashROM.

## 1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follows;

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;

- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "imagio MP 5000SP/4000SP with Security Card Type9 Security Target" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "Ricoh imagio MP 5000SP/4000SP with Security Card Type9 Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

## 1.4 Certification

The Certification Body verified the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2010-02 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

# 2. Summary of TOE

## 2.1 Security Problem and assumptions

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

### 2.1.1 Threat

This TOE assumes such threats presented in Table 2-1 and provides functions for countermeasure to them. These threats are equivalent to those defined in conformance PP, which is an English document translated into the Japanese one. Additionally, the implementation of the TOE and the usage environment are considered and embodied. Attackers in the following threats are assumed to have potential attack capabilities on the basic level and the users are assumed to have knowledge about the public-known information for this TOE operation.

**Table 2-1 Assumed Threats**

| Identifier | Threat |
|---|---|
| T.DOC.DIS<br>(Document Disclosure) | User documents, deleted documents, temporary documents and fragments which the TOE manages may be referenced by persons who have no login user name or by unauthorised persons who have login user names but don't have any access right to their documents. |
| T.DOC.ALT<br>(User Document Alteration) | User documents which the TOE manages may be altered by persons who have no login user name or by unauthorised persons who have login user names but don't have any access right to the user documents. |
| T.FUNC.ALT<br>(User Job Alteration) | User job which the TOE manages may be altered by persons who have no login user name or by unauthorised persons who have login user names but don't have any access right to the user jobs. |
| T.PROT.ALT<br>(TSF Protected Information Alteration) | TSF Protected Information which the TOE manages may be referenced by persons who have no login user name or by unauthorised persons who have login user names but don't have any access right to the TSF Protected Information. |
| T.CONF.DIS<br>(TSF Confidential Information Disclosure) | TSF Confidential Information which the TOE manages may be referenced by persons who have no login user name or by unauthorised persons who have login user names but don't have any access right to the TSF Confidential Information. |
| T.CONF.ALT<br>(TSF Confidential Information Alteration) | TSF Confidential Information which the TOE manages may be altered by persons who have no login user name or by unauthorised persons who have login user names but don't have any access right to the TSF Confidential Information. |

### 2.1.2 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 2-2. These policies are equivalent to those defined in conformance PP, which is an English document translated into the Japanese one. Additionally, the implementation of the TOE and the usage environment are considered and embodied.

**Table 2-2 Organisational Security Policy**

| Identifier | Organisational Security Policy |
|---|---|
| P.USER.AUTHORIZATION (User Authorization) | The person who has a login user name only for the TOE usage shall be able to use the TOE. |
| P.SOFTWARE.VERIFICATION (Software Verification) | The TOE shall provide procedures to self-verify executable codes. |
| P.AUDIT.LOGGING (Audit Log Management) | The TOE shall be able to manage and maintain auditable events logs related to the TOE usage and security in order to prevent unauthorised persons from disclosure or alteration of the audit logs. Additionally, the authorised persons shall be able to reference the logs. |
| P.INTERFACE.MANAGEMENT (External Interface Management) | In order to prevent unauthorised persons from using the external interface of the TOE (Operation Panel, LAN, and USB), those interfaces shall be appropriately controlled by the TOE and the IT environment. |

### 2.1.3 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 2-3.These assumptions are equivalent to those defined in conformance PP, which is an English document translated into the Japanese one. Additionally, the TOE usage environment are considered and embodied.

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

**Table 2-3 Assumptions in Use of the TOE**

| Identifier | Assumptions |
|---|---|
| A.ACCESS.MANAGED (Access Managed) | According to the guidance, the TOE shall be installed in a safe place under control, and physically limit access to unauthorised persons. |
| A.USER.TRAINING (User Training) | MFP chief administrator trains users to be aware of their organisational security policies and procedures in accordance with the guidance. The users are regarded as following their policies and procedures. |
| A.ADMIN.TRAINING (Administrator Training) | Administrators are aware of the organisational security policies and the procedures and can perform the TOE settings and processing in accordance with the guidance. |
| A.ADMIN.TRUST (Trust Administrator) | MFP chief administrator does not use their privileged access rights for malicious purposes. |

### 2.1.4 Documents Attached to Product

The identification of documents attached to the TOE is listed below. TOE users are required full understanding of following documents and compliance with descriptions. (All documents are written in Japanese.)

- imagio MP 5000/4000 Series Operating Instructions (Security Reference) (D012-7950)
- For Users of Security Functions (D011-7750A)
- For administrators who use IEEE Std. 2600.1-2009 conformant (D011-7755)
- Change the descriptions for operating instructions (D012-7954)
- For customers who use this machine (D015-7103)
- imagio MP5000/4000 Series Included Operating Instructions (D012-7501)
- imagio MP5000/4000 Series Operating Instructions (Copy Function / Document Server Function Reference) (D012-7650)
- imagio MP5000/4000 Series Quick Guide (D012-7658)
- imagio MP5000/4000 Series Operating Instructions (For using this machine) (D012-7750/D012-7751)
- imagio MP5000/4000 Series Operating Instructions (Initialisation) (D012-7900)
- imagio MP5000/4000 Series Operating Instructions (Printer Reference) (D381-7000)
- imagio MP5000/4000 Series Operating Instructions (Scanner Reference) (D381-7100)
- imagio MP5000/4000 Series Operating Instructions (Network Guide) (D381-7200)
- imagio MP5000/4000 Series Operating Instructions (Q&A) (D012-7800/D012-7801)
- imagio Security Card Type 7 imagio Security Card Type 9 Operating Instructions (D377-7902)

### 2.1.5 Configuration Requirements

For using the printer function of the TOE from client PCs, it is necessary to install the proprietary printer driver in client PCs. The evaluation confirmed the operation of the following printer drivers;

- imagio MP5000/4000 For Windows XP RPCS Driver Ver.7.69
- imagio MP5000/4000 For Windows Vista RPCS Driver Ver.7.69

And for the Web browser used by client PCs, the evaluation environment confirmed the operation of the following browser;

- Internet Explorer 6.0/7.0

## 2.2 Security Objectives

TOE counters threats described in 2.1.1 as follows by implemented security functions and fulfills the organisational security policies in 2.1.2.

### 2.2.1 Counter to Threats

All threats defined in ST are assumed intrusion (disclosure and alteration) to user data and TSF data by the person other than TOE proper user or the person who has no access right.

These threats are countered by the following security functions;

(1) User Identification and Authentication
For the person who attempts to use a TOE, it is required to enter login username and login password and to check matching the user data managed internally by the TOE. There are 3 entry ways; from Operation Panel of the TOE itself, on the Web browser of client PCs, and via driver for using the printer function.
The following functions are included as measures to ensure the required function strength;

- Consecutively failing authentication at a certain times set by MFP administrator, the user account will be locked out (the user account will not be able to be used until released).
- The length (number of characters) and character types for login passwords managed by the TOE require higher level of certain quality at installation (for the quality details, depending on the settings for the MFP administrators, it is required to set more than 8 characters for number of characters).

Verifying the appropriate login username and password, the user is permitted to use the TOE corresponding to the authorisation for the TOE usage specified in advance by each role of the users.
The specific roles of users for the TOE are as follows;

- Normal user
- MFP administrator
- Supervisor

And the following functions are included as measures to support the identification and authentication function;

- Display dummy letters for login passwords entered in the entry screen.
- In case of not performing operations on the TOE for some interval of time, the user will be automatically logged out.

(2) Access Control (Access Control for User Data)
Access control to document information and user job operation is enforced based on authorising each login username and each role of the user. The user documents stored in the TOE are associated with the setting information (user list of document data) to determine whether or not to permit the operation for which user will (delete, print, and download), and the TOE performs the control of permission or denial to the operation that normal user requests by the information for the login usernames and for the user list of document data. For operation of the user documents by MFP administrators, the deletion authorisation is only allowed to all user documents.
The user job is associated with the login username that creates the job, and normal users matching the login usernames are allowed to delete the applicable jobs. MFP administrators are authorised to delete all user jobs. Supervisor is prohibited to perform all operations for user data.

(3) Residual Data Deletion
In order to prevent unauthorised access to deleted user documents,

temporarily used documents and fragments (remained in HDD), the specific data are overwritten when deleting the document data.

(4) Network Protection
In order to prevent the information disclosure monitored by communication paths, use the SSL encrypted communications for the communication related to the operation via Web browser between the TOE and clients, and for the communication with using the printer function.

(5) Security Management
In order to prevent the unauthorised access to TSF data beyond the user authorisation, access control is enforced for reference / alteration of the TOE setting information based on the role of the TOE user, and it is enforced for registration and alteration of user information and so on. As an authorisation policy about altering (modifying) the information, normal users are authorised only to alter their own login passwords, a supervisor and MFP administrators are to alter their own ones. MFP administrators are allowed only to alter except for the above mentioned.

### 2.2.2 Realization of Organisational Security Policies

#### 2.2.2.1 Realization of P.USER.AUTHORIZATION (User Authorisation)

This security policy requires to allow the official users only registered in the TOE to use the TOE.
In the TOE, this policy is implemented by the following security functions;

(1) User Identification and Authentication
According to the identification and authentication described in 2.2.1, it is required to enter login username and login password for person who attempts to use the TOE and confirmed to be the authorised user registered for the TOE, and to relate the corresponding role to the login username.
Only authorised users who are confirmed by the TOE are allowed to use the functions that the TOE provides.

(2) Security Management
In order to prevent the unauthorised access beyond the user authorisation for TSF data, access control is enforced for reference / alteration of the TOE setting information by the role of the TOE user.
Only MFP administrators are allowed to alter the list of available functions.

#### 2.2.2.2 Realization of P.SOFTWARE.VERIFICATION (Software Verification)

This security policy requires to self-verify the integrity of the TOE executable codes.
In the TOE, this policy is implemented by the following security functions;

(1) Self Testing
The TOE executes the self testing during initialisation after turning on the power and confirms the integrity and validity of executable codes in the MFP control software. The self testing verifies hash values of firmware and confirms the integrity of executable codes. Each application performs verification of executable codes based on PKI and confirms the correctness of executable codes.
In case of recognising unusual events during the self testing, the TOE displays an error message on Operation panel and stops the processing with the TOE unavailable for normal user. In case of recognising no unusual events during the self testing, the TOE continues the start-up processing with the TOE

available for the user.

#### 2.2.2.3 P.AUDIT.LOGGING (Audit Log Management)

This security policy is required to obtain and to appropriately manage the audit log related to the TOE security events.
In the TOE, this policy is implemented by the following security functions;

(1) Security Audit
The TOE generates audit log consisting of event type, user identifier, date and time of occurrence, and results, it adds and stores audit log files. Only MFP administrators who succeed in identification and authentication are allowed to read out and delete the generated audit log files. Reading out the audit log files is performed in text forms via Web browser in client PCs.
And in order to record the occurrence date and time of auditable events logs, the date and time information is obtained from the TOE system clock.

#### 2.2.2.4 P.INTERFACE.MANAGEMENT (External Interface Management)

This security policy requires that external interfaces (Operation Panel, LAN Interface, and USB Interface) are appropriately managed not to be used by the unauthorised users.
In the TOE, this policy is implemented by the following security functions;

(1) User Identification and Authentication
According to the descriptions of identification and authentication in 2.2.1, it is required to enter login username and login password for person who attempts to use the TOE and it is confirmed to be the authorised users registered in the TOE who are allowed to use the TOE.

(2) Restricted forwarding of data to external interfaces
This function is not the implementation of active mechanisms, but the compliant to the architectural design of external interfaces. The purpose is to prevent the restricted forwarding of unauthorised data to external interfaces by ensuring the TOE is involved in processing the data entered from the one external interface before sending data to an external interface (especially LAN interfaces).
USB interfaces prevent forwarding of the unauthorised data by means of operating the settings of deactivating the use of this interface.

# 3. Conduct and Results of Evaluation by Evaluation Facility

## 3.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

## 3.2 Overview of Evaluation Conducted

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

Evaluation has started on 2009-07 and concluded by completion the Evaluation Technical Report dated 2010-02. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2009-08,2009-09 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-10.

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

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

## 3.3 Product Testing

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

### 3.3.1 Developer Testing

The evaluator evaluated the integrity of developer testing that the developer executed and the test documentation of actual test results
The overview of evaluated tests performed by the developer is shown as follows;

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 3-1, and the major configuration components are shown in Table 3-1.

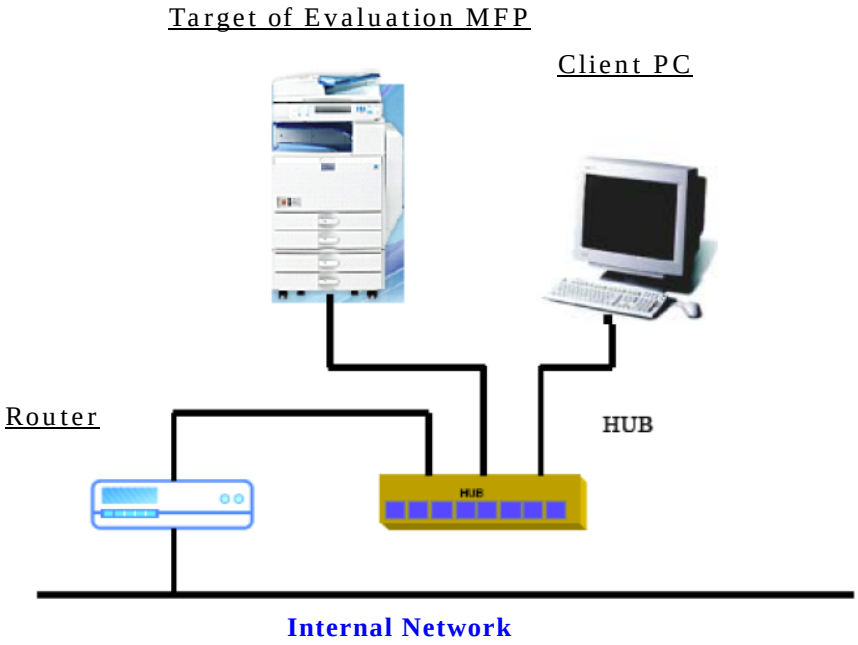


**Figure 3-1 Configuration Figure of Developer Testing**

**Table 3-1 Testing Configuration Components**

| | |
|---|---|
| TOE | imagio MP 5000SP/4000SP with Security Card Type 9<br>- Firmware Configuration<br>System Version: V2.16-00<br>System/Copy 1.11.1<br>Network Support 7.26<br>Network DocBox 1.10C<br>Web Support 1.59<br>Web Uapl 1.15<br>animation 1.3<br>Scanner 01.24<br>RPDL 7.33<br>Printer 1.11<br>MSIS 7.15.02<br>RPCS Font 1.01<br>Engine 1.04:05<br>OpePanel 1.01<br>LANG0 1.01<br>LANG1 1.01<br>ADF 15.000:15<br>- ASIC<br>Ic Key Version: 1100<br>- Option<br>Data Erase Opt Version: 1.01m |
| Client PC | OS: Windows XP Pro SP2 / Windows Vista Business |

| | |
|---|---|
| | SP1<br>Web browser: Internet Explorer 6.0/7.0<br>Printer Driver:<br>imagio MP5000/4000 for Windows XP RPCS Driver Ver.7.69<br>imagio MP5000/4000 for Windows Vista RPCS Driver Ver.7.69 |

The developer testing is executed the same TOE test environment as TOE configuration identified in ST.

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follows;

a. Test outline

The testing configuration which the developer conducted is shown in Figure 3-1, and the major configuration components are shown in Table 3-1. The developer testing is executed the same TOE test environment as TOE configuration identified in ST.
The testing stimulated external interfaces (Panel, Web browser and etc.) that are assumed for usually using the TOE and other than the way to eye-check and observe the results, the generated audit log, the log data analysis for debug, communication protocols between MFP and client PCs by packet capture, and the unusual testing by using the implementation of the unauthorised TSF are also performed.

b. Scope of Testing Performed

Testing is performed 339 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

c. Result

The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

### 3.3.2 Evaluator Independent Testing

Evaluator executed the independent testing to reconfirm that Security functions are certainly implemented from the evidence shown by the process of the evaluation.
Outlining of the independent testing performed by the developer is as follows;

1) Evaluator Independent Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.
Test configuration performed by the evaluator is showed in the Figure 3-1.
Test configuration performed by the evaluator shall be the same configuration with TOE configuration identified in ST.

2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. In terms of Evaluator Independent Testing

Evaluator devised the independent testing from the developer testing and the provided documentation in terms of followings.

(1) For TSFI to be considered that the developer testing is insufficient from the perspectives of the completeness due to many kinds of input parameters, add testing items such as combination of parameters, boundary values, and aberrant values.
(2) For the implementation timing of multiple TSF and the combination of the implementation, conduct the testing items which are added to the conditions.
(3) Sampling tests select the testing items from the following perspectives;

- From the perspectives of the completeness, select the items for including all of TSF and TSFI.
- Select the testing items related to TSFI that has many kinds of the input parameters specifically.
- Select specifically the items related to TSFI that conducts the efficient testing with corresponding to many SFRs.

b. Outlining of Evaluator Independent Testing

Considering the above perspectives, the evaluator testing is conducted by 36 sampling tests and 18 independent tests. The tools and testing approach are used in the same way as the developer testing used in the independent testing conducted by the evaluators.

c. Result

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

### 3.3.3 Evaluator Penetration Testing

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

1) Outlining of Evaluator Penetration Testing

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

a. Vulnerability of concern

Evaluator searched the potential vulnerability from information which is within the public domain and provided evidence to identify the following vulnerability that requires penetration testing.

- There is the potential unauthorised access to the TOE by the existing unintentional network port interface.
- There is the public-known, potential vulnerability existing in Web application used by the operation of client PCs.
- The security function is potentially bypassed by the unauthorised access to external interfaces of the TOE.
- The security function is potentially bypassed by operating the TOE in the overloading status.

b. Scope of Test Performed

Evaluator conducted the following penetration testing to determine the exploitable potential vulnerability.

- Confirm that the tool for port scan is used and unnecessary network ports are not open.
- Confirm that the proxy tool is used and the public-known vulnerability does not exist in the Web application.
- Confirm that the unauthorised USB devices and SD cards are used and that the security functions of the TOE are not bypassed.
- Confirm that the TOE is not unsecure by the overloading status of CPU and the insufficient resource.

c. Result

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

## 3.4 Evaluation Result

### 3.4.1 Evaluation Result

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

### 3.4.2 Evaluator comments/Recommendations

The following recommendations for users are described in the ETR by the evaluator.
The following functions described in the guidance (Operating instructions (Security reference)) for this TOE are outside of the scope.

- Copy Prevention Function

- Confidential print
- Access control for each administrator role (Machine administrator, User administrator, Network administrator, and File administrator)

And the following functions related to deactivating the maintenance function in this TOE are deactivated by the installation procedure, according to the guidance included in the TOE.

- @Remote
- RFU (Remote Firmware Update)

## 4. Conduct of Certification

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

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

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

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

# 5. Conclusion

## 5.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body determined the TOE is satisfied the assurance requirements of EAL3 augmented with ALC_FLR.2 components prescribed in CC Part 3.

## 5.2 Recommendations

For discarding the TOE, MFP administrator needs to explicitly perform the data overwrite function on HDD in order to prevent the data disclosure in HDD.

As shown in 1.2.3.2, it is assumed to deactivate the maintenance function that is the basic function as the evaluation environment for this TOE. In case of activating the maintenance function, it may not be the TOE later. Users should make sure whether or not the expected functions are deactivated for use.

# 6. Glossary

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

| | |
|---|---|
| CC: | Common Criteria for Information Technology Security Evaluation |
| CEM: | Common Methodology for Information Technology Security Evaluation |
| EAL: | Evaluation Assurance Level |
| PP: | Protection Profile |
| SOF: | Strength of Function |
| ST: | Security Target |
| TOE: | Target of Evaluation |
| TSF: | TOE Security Functions |

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

| | |
|---|---|
| HDD | An abbreviation for Hard Disk Drive. If simply describing 'HDD' in this ST, it indicates the HDD installed in the TOE. |
| RFU | An abbreviation for Remote Firmware Update.<br>A function to update the firmware remotely connected to the TOE. (This function is not the target of evaluation.) |
| @Remote | A function to remote control the TOE via Internet. Remote failure diagnosis, Counter information collection, Toner information collection are the target of remote control. (This function is not the target of evaluation.) |
| Copy Prevention Function | A function to prevent the information disclosure of document copy by verifying special print in the document background and by performing the corresponding processing. (This function is not the target of evaluation.) |

| | |
|---|---|
| Confidential Print | A function to require the password entry set in advance for printing the stored documents.<br>(This function is not the target of evaluation.) |
| Administrator role | Defined roles in advance which are assigned to MFP administrators.<br>The following 4 administrator roles are defined and allowed to assign each individual administrator. In this TOE, it is assumed to assign all roles to MFP administrators.<br>(Access control for each categorised administrator role is not the target of evaluation.)<br>- Machine administrator<br>(performs machine management and conducts audit.)<br>- User administrator<br>(performs the management of normal user.)<br>- Network administrator<br>(performs the network connection management of the TOE.)<br>- File administrator<br>(performs user documents and the available document user list.) |
| Document | Digital image data under the TOE control generated by using Copy Function, Printer Function, and Scanner Function.<br>The stored documents in HDD of the device itself are explicitly called as user document in this ST.<br>If simply describing 'document', this means the deleted documents, the temporary documents and fragments for copying and printing. |
| User job | A job that user requires the operation of the TOE, which is regarded as 1 job that is continuing from start to end. The target operations are to store, print, download, and delete user documents. |
| Login password | A password corresponds to each login username. |
| Number of | The number of consecutive unsuccessful |

| | |
|---|---|
| Attempts before Lockout | authentication times until locked out user account for identification and authentication.<br>The setting values are set to between 1 and 5 for the initial settings of the TOE by MFP administrator and the values must not be changed after the settings. |
| Login username | An identifier given to a user. The TOE specifies the user with the identifier. |
| Lockout | A status of making user accounts unavailable |
| Lockout time | Time of automatically releasing user accounts from the lockout status<br>This TOE is set to 60 minutes and operated by MFP administrators. |

## 7. Bibliography

[1] imagio MP 5000SP/4000SP with Security Card Type9 Security Target Version 1.00 (Feb 18, 2010) RICOH COMPANY, LTD.

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

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

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

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

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

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

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

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

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

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

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

[13] Ricoh imagio MP 5000SP/4000SP with Security Card Type9 Evaluation Technical Report Version 3.0, Feb 18, 2010, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center