Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2016-10-28 (ITC-6619)
Certification No.	C0564
Sponsor	RICOH COMPANY, LTD.
TOE Name	RICOH Pro 8220S/8210S/8200S
TOE Version	J-1.01
PP Conformance	U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)
Assurance Package	EAL2 Augmented with ALC_FLR.2
Developer	RICOH COMPANY, LTD.
Evaluation Facility	ECSEC Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
2017-07-19

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass
"RICOH Pro 8220S/8210S/8200S J-1.01" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" 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 the certification result in relation to IT Security Evaluation of "RICOH Pro 8220S/8210S/8200S J-1.01" (hereinafter referred to as "this TOE") developed by RICOH COMPANY, LTD., and the evaluation of the TOE was finished on 2017-07 by ECSEC Laboratory Inc. Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, RICOH COMPANY, LTD., and provide security information to consumers and procurement entities who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is provided along with this report. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of this TOE are described in the ST.

This Certification Report assumes "general consumers and procurement entities who purchase this TOE that is commercially available" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which this TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of this TOE is EAL2 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

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

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

This TOE provides Security Functions required for U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009) [14], which is a Protection Profile (hereafter, "conformance PP") for MFPs, and also provides the Security Functions to accomplish the necessary security policy for an organisation which manages the TOE.

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

1.1.2.1 Threats and Security Objectives

This TOE assumes the following threats and provides the Security Functions to counter them.

For protected assets such as the documents that the TOE handles and the setting information relevant to the Security Functions, there are threats of disclosure and tampering caused by unauthorised access to both the TOE and the communication data on the network.

This TOE provides the Security Functions to prevent those protected assets from unauthorised disclosure and tampering.

1.1.2.2 Configuration and Assumptions

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

This TOE is equipped with the Printer and Scanner Option that provides Printer and Scanner Functions for the MFP.

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

1.1.3 Disclaimers

This TOE is assumed to be operated while the following functions are deactivated. The case that the TOE is operated with these settings changed is not included in the assurance provided by this evaluation:

- Maintenance Function
- Authentication methods except for Basic Authentication (when Basic Authentication is applied)

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2017-07, based on functional requirements and assurance requirements of this TOE according to the publicised documents, "IT Security Evaluation and Certification Scheme Document" [1], "Requirements for IT Security Certification" [2], and "Requirements for Approval of IT Security Evaluation Facility" [3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and the Observation Report prepared by the Evaluation Facility, as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

This TOE is identified as follows:

TOE Name: RICOH Pro 8220S/8210S/8200S

TOE Version: J-1.01

Developer: RICOH COMPANY, LTD.

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

After confirming that the name and version of the TOE described in the guidance documents are identical to the aforementioned name and version of the TOE, users can confirm that the installed product is this evaluated TOE by comparing the name that is displayed on the MFP exterior and the version of each component, which constitutes the TOE, displayed on the Operation Panel of the TOE with the applicable descriptions in the list of the TOE configuration items described in the guidance documents.

3. Security Policy

This chapter describes security function policies and organisational security policies.

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

For meeting the organisational security policies, the TOE provides the functions to overwrite the internal stored data and to encrypt the stored data in the HDD.

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

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

Table 3-1 TOE Protected Assets (user data)

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

Table 3-2 TOE Protected Assets (TSF data)

Type	Asset
Protected data	The information that shall be protected from changes by users without edit permission; it includes Login user name, Number of Attempts before Lockout, year/month/day setting, time setting, and Minimum Character No. of password, etc. (Hereafter, referred to as "TSF protected data.")
Confidential data	The information that shall be protected from changes by users without edit permission, and also shall be protected from reading by users without viewing permission; it includes Login password, audit log, and HDD cryptographic key. (Hereafter, referred to as "TSF confidential data.")

3.1 Security Function Policies

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

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

This TOE assumes the threats shown in Table 3-3 and provides the functions as countermeasures against them. Although threats are expressed differently from the conformance PP, the evaluation process confirmed the equivalence of both threats.

Table 3-3 Assumed Threats

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

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

3.1.1.2 Security Function Policies against Threats

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

(1) User identification and authentication

The TOE requires a user to enter the login user name and login password. By confirming that the entered data are identical to the user authentication data managed internally by the TOE, the TOE verifies that the person who attempts to use the TOE is an authorised TOE user. The entry means are the input from Operation Panel of the TOE itself, the input on a Web browser of client computers, the input via drivers when using Printer Function.

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

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

When the login password is validated and a user is confirmed as an authorized TOE user, the user receives the user privilege that is set in advance in accordance with the role assigned to the user. Accordingly, the user is allowed to use the TOE. As shown in "Table 4-2 TOE Users," the roles specified by the TOE include normal user, MFP administrator, and supervisor.

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

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

(2) Access control (Access control against the user data)

For processing request by users, access control to the document information and the user jobs is performed, based on the login user names and permissions of each user role of the users. Stored documents are associated with specific information (a document user list) that stipulates which user is allowed to perform the operation (deletion, printing, and downloading, etc.). Access control to allow or deny the operation request by normal user is performed, according to the login user names and the information in the document user list. The MFP administrator is permitted to delete any stored documents, but is not permitted to perform any other operation on stored documents.

User jobs are associated with the login user names of the users that create the jobs, and

the normal user who is associated with the login user name is allowed to delete the applicable job. The MFP administrator is allowed to delete all the user jobs. The supervisor is forbidden to perform any operations on the user data.

(3) Overwrite residual data

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

(4) Network protection

In order to prevent information leakage by being monitored via communication paths, TLS encrypted communication is used for communications between the TOE and client computers for the operations via a Web browser and communications using Printer Function. IPsec communication and S/MIME communication are also used for the communications between the TOE and the clients.

(5) Security management

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

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies required in use of this TOE are shown in Table 3-4. The evaluation process has confirmed that the security policies except for P.STORAGE.ENCRYPTION are identical to the security policies in the conformance PP.

P.STORAGE.ENCRYPTION is the security policy that assumes writing data into the HDD not in a directly readable format.

Table 3-4 Organisational Security Policies

Identifier	Organisational Security Policy
P.USER.AUTHORIZATION (User identification and authentication)	Only users with operation permission of the TOE shall be authorised to use the TOE.
P.SOFTWARE.VERIFICATION (Software verification)	Procedures shall exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING (Management of audit log records)	The TOE shall create and maintain a log of TOE use and security-relevant events. The audit log shall be protected from unauthorised disclosure or alteration, and shall be reviewed by authorised persons.
P.INTERFACE.MANAGEMENT (Management of external interfaces)	To prevent unauthorised use of the external interfaces of the TOE, operations of those interfaces shall be controlled by the TOE and its IT environment.
P.STORAGE.ENCRYPTION (Encryption of storage devices)	The data stored on the HDD inside the TOE shall be encrypted.

3.1.2.2 Security Function Policies to Organisational Security Policies

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

(1) Means to support Organisational Security Policy, "P.USER.AUTHORIZATION"

This security policy requires that only officially registered TOE users be allowed to use the TOE.

The TOE implements this policy by the following Security Function:

(a) User identification and authentication

Based on the user identification and authentication described in Section 3.1.1.2, whether a person who attempts to use the TOE is an authorised user will be verified with reference to the identification and authentication information obtained from the

user. A person is provided with the user privileges that are set in advance in accordance with the role assigned to the user, so that the authorised person is allowed to use the TOE only if the person is confirmed as an authorised user.

(2) Means to support Organisational Security Policy, "P.SOFTWARE.VERIFICATION"

This security policy requires the validity of the TOE executable code to be self-verified.

The TOE implements this policy by the following Security Function:

(a) Self test

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

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

(3) Means to support Organisational Security Policy, "P.AUDIT.LOGGING"

This security policy requires audit logs for the security events of the TOE to be acquired, and the audit logs to be appropriately managed.

The TOE implements this policy by the following Security Function:

(a) Security audit

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

In addition, in order to record the occurrence date and time of the audit event log, the date and time information are acquired from the system clock of the TOE.

(4) Means to support Organisational Security Policy, "P.INTERFACE.MANAGEMENT"

This security policy requires that external interfaces (Operation Panel, LAN interface, and USB interface) of the TOE are appropriately managed without being used by unauthorised persons.

The TOE implements this policy by the following Security Functions:

(a) User identification and authentication

Based on the user identification and authentication described in Section 3.1.1.2, whether a person who attempts to use the TOE is an authorised user will be verified with reference to the identification and authentication information obtained from the user. A person is provided with the user privileges that are set in advance in accordance with the role assigned to the user, so that the authorised person is allowed to use the TOE only if the person is confirmed as an authorised user.

(b) Restricted forwarding of data to external interfaces

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

As for USB interfaces, unauthorised forwarding of data by using this interface is prevented by deactivating the use of USB interfaces.

(5) Means to support Organisational Security Policy, "P.STORAGE.ENCRYPTION"

This security policy requires that the TOE encrypts the stored contents on the HDD inside the TOE.

The TOE implements this policy by the following Security Functions:

(a) Stored data protection function

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

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate this TOE as useful information for the assumed readers to determine the use of this TOE.

4.1 Usage Assumptions

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

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

Table 4-1 Assumptions in Use of the TOE

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

4.2 Environmental Assumptions

This TOE is installed in general offices and connected to the local area networks (hereafter, "LAN"), and it is used through the Operation Panel of the TOE itself and client computers that are also connected to the LAN. Figure 4-1 shows the general operational environment as assumptions of this TOE.

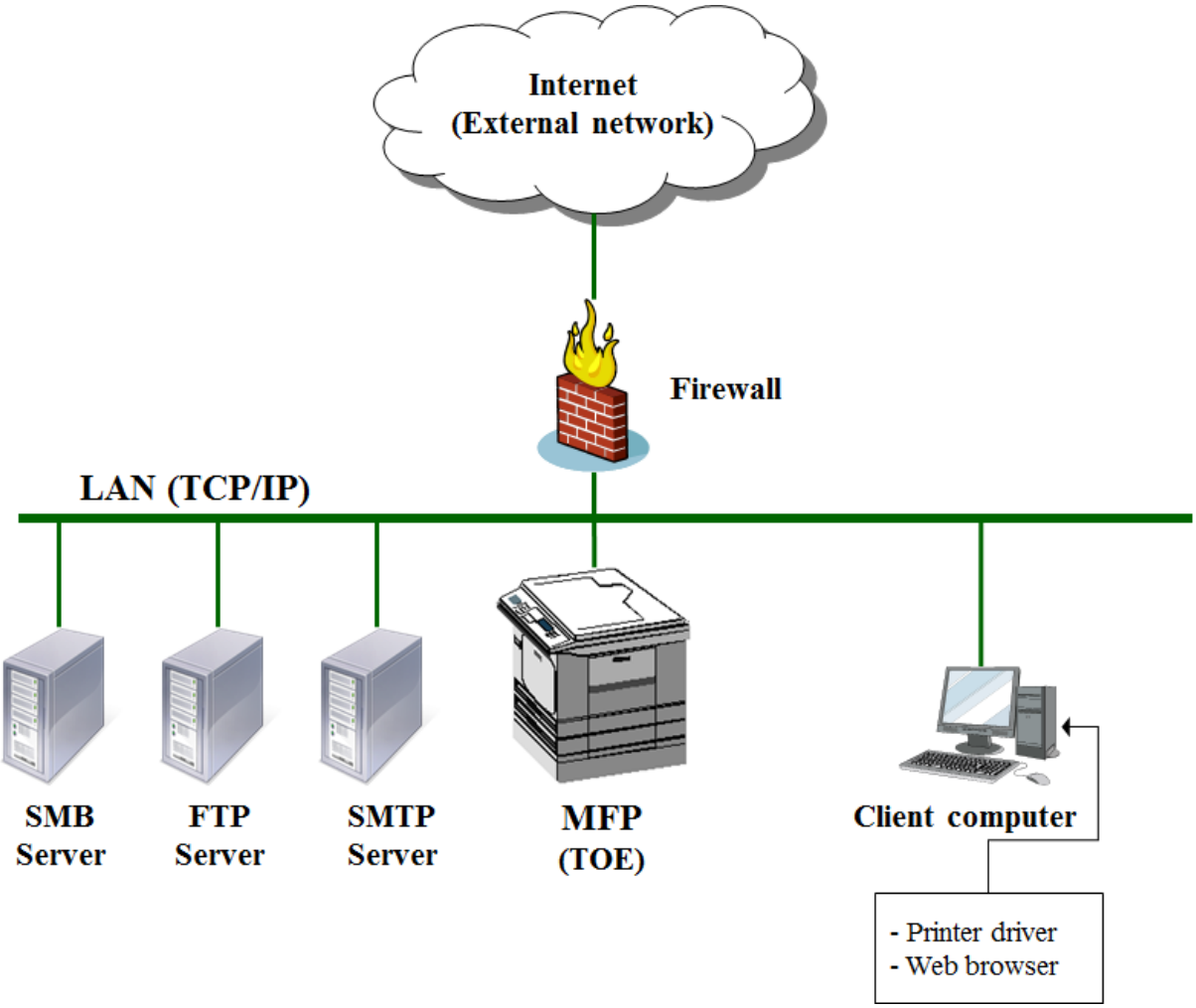

Figure 4-1 Operational Environment of the TOE

Figure 4-1 gives an example environment to handle office documents in general offices where this TOE is assumed to be used. The TOE is connected to the LAN.

When the TOE is connected to the LAN that is connected to an external network such as the Internet, firewalls are installed at the boundaries between the external network and the LAN to protect the LAN and the TOE from attacks that originate from the external network. The LAN is connected to server computers such as an FTP server, an SMB server, and an SMTP server, and is connected to client computers. The LAN performs the communication for the TOE to gather data such as documents and a variety of information.

The operation of the TOE includes both cases of using the Operation Panel of the TOE and using client computers. Installing printer drivers in client computers enables to process printing via the local area network from the client computers.

Although the reliability of hardware and software shown in this configuration is outside the scope of this evaluation, it is assumed to be trustworthy.

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

Table 4-2 TOE Users

User Definition		Explanation
Normal user		A user who is allowed to use the TOE. A normal user is provided with a login user name and can use normal functions of MFP.
Administrator	Supervisor	A user who is authorised to modify the login password of the MFP administrator.
	MFP administrator	A user who is allowed to manage the TOE and performs the management operations such as user data management of normal user, device management, file management, and network management.

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

4.3 Clarification of Scope

The scope of this TOE covers the entire product as sold to users that is equipped with the Printer and Scanner Option which provides the Printer and Scanner Functions to the MFP.

5. Architectural Information

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

5.1 TOE Boundary and Components

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

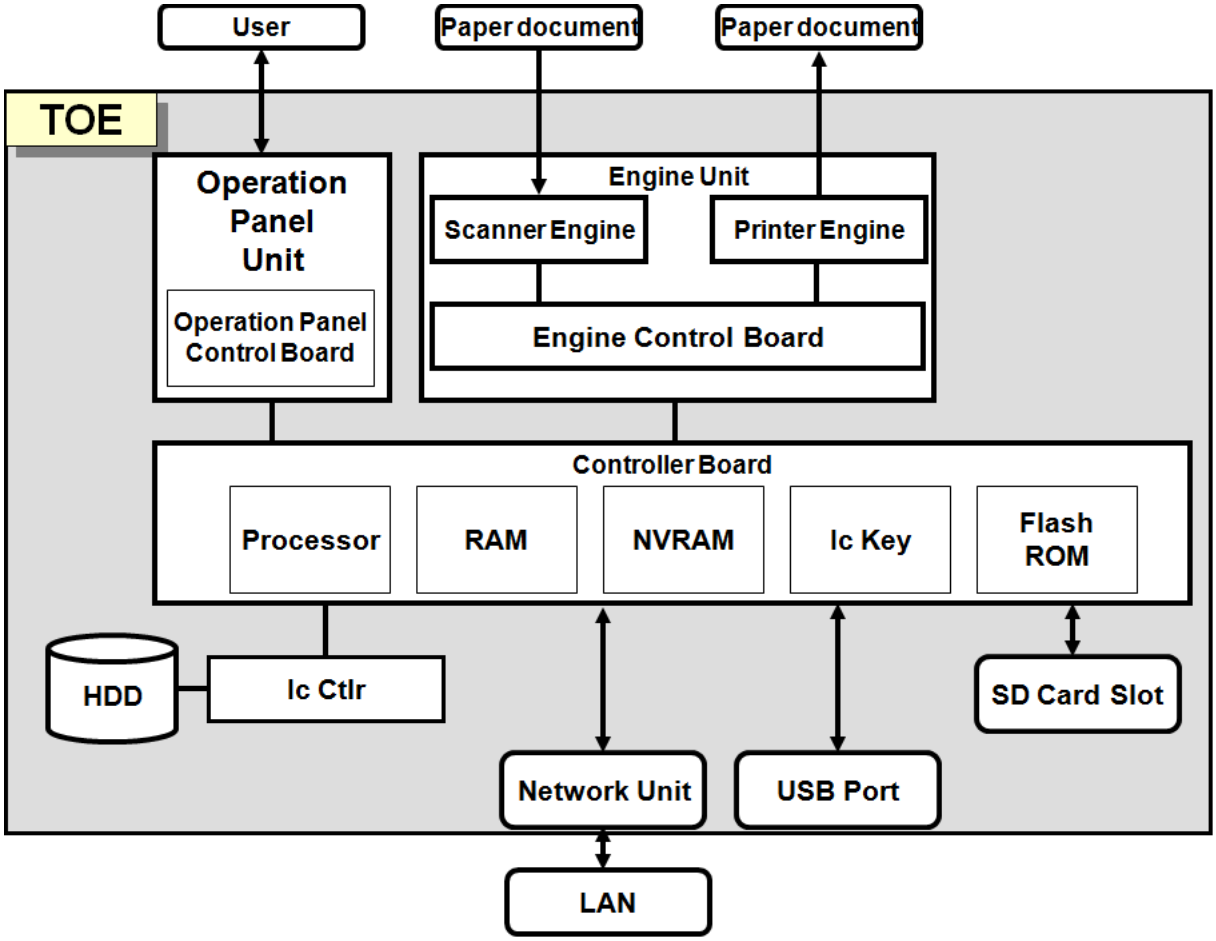

Figure 5-1 TOE Boundary

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

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

[Engine Unit]
The Engine Unit contains a Scanner Engine that is an input device to read paper documents, Printer Engine that is an output device to print and eject paper documents, and Engine Control Board that controls each engine.

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

- Processor
  A semiconductor chip which carries out the basic arithmetic processing of MFP operations.
- RAM
  A volatile memory medium which is used as the image data.
- NVRAM
  A non-volatile memory medium which stores the MFP control data to configure the MFP operation.
- Ic Key
  A security chip which has the function of a random number generation and cryptographic key generation. It is used to detect alteration of the MFP Control Software.
- FlashROM
  A non-volatile memory medium in which the MFP Control Software is installed.

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

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

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

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

[SD Card Slot]
The SD Card Slot is used for inserting an SD Card. The SD Card Slots are located inside and on the front of the MFP. The SD Card Slot on the front of the device is disabled at the time of operation, and the SD Card is not operated by hand in normal operation.

5.2 IT Environment

The TOE is connected to the LAN and communicates with server computers, such as an FTP server, an SMB server, and an SMTP server, as well as with client computers.

The client computer connected via the LAN uses the TOE through the printer driver and the Web browser. The client computer performs not only communication of document data to the TOE, but also an operation of some management functions and status checking of the TOE via the Web browser.

6. Documentation

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

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

Document Name	Version
Notes on Using Multi Function Printers Safely	D181-2585
Read This First	D270-7402
User Guide	D270-7465
RICOH Pro 8220S/8210S/8200S RICOH Pro 8220Y/8220HT/8210Y/8210HT Operating Instructions Driver Installation Guide	D270-7467
RICOH Pro 8220S/8210S/8200S RICOH Pro 8220Y/8220HT/8210Y/8210HT Operating Instructions Guide of Paper	D270-7468
RICOH Pro 8220S/8210S/8200S RICOH Pro 8220Y/8220HT/8210Y/8210HT Operating Instructions Security Guide	D270-7469
About Open Source Software License	D270-7470
Notes for Users	D270-7472
Copy/Document Server	D270-7473
Printer	D270-7474
Scanner	D270-7475
Troubleshooting	D270-7476
Connecting the Machine/System Settings	D270-7477
Paper Settings	D270-7478
Extended Feature Initial Settings	D270-7479
Emulation	D270-7480
Notes on Security Functions	D181-2584
RICOH Pro 8220S/8210S/8200S RICOH Pro 8220Y/8220HT/8210Y/8210HT Operating Instructions Notes for Administrators: Using This Machine in a Network Environment Compliant with IEEE Std 2600.2™-2009	D270-7463

Help	83NHDPJAR1.00 v147

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

ECSEC Laboratory Inc., Evaluation Center that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of this TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2016-10 and concluded upon completion of the Evaluation Technical Report dated 2017-07. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. For the development sites, site visits have been omitted, and the Evaluation Facility determined with its responsibility that the examination details on those of the past CC-certified products could be reused.

Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2017-04.

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed.
As a result of the evidence shown in the process of the evaluation and the verification results of the testing performed by the developer, the evaluator performed the reproducibility testing, additional testing, and penetration testing based on vulnerability assessments judged to be necessary.

7.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

(1) Developer Testing Environment

Figure 7-1 shows the testing configuration performed by the developer, and Table 7-1 shows the main configuration items.

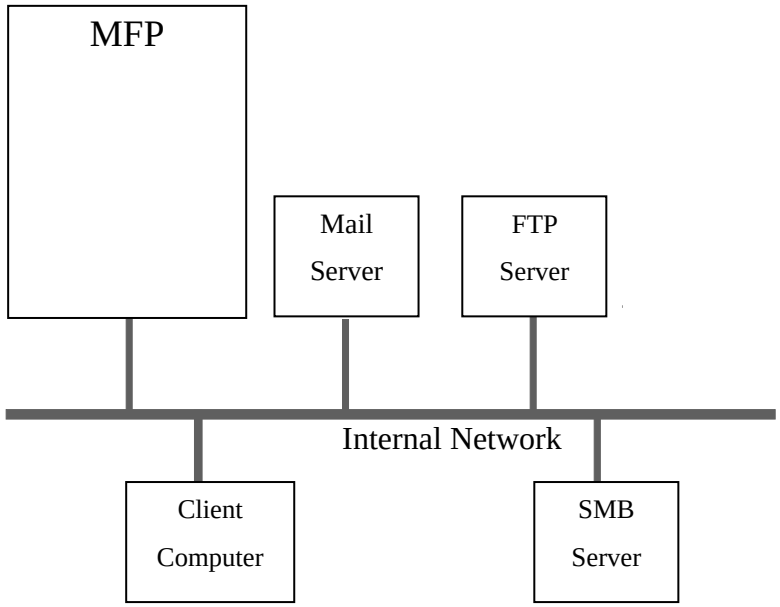

Figure 7-1 Configuration of the Developer Testing

Table 7-1 Test Configurations

Configuration Item	Detail
TOE	RICOH Pro 8200S version J-1.01 RICOH Pro 8220S version J-1.01
Client Computer	OS: Windows Vista/7/8.1/10 Web browser: Internet Explorer 9/11 Printer driver: RPCS Driver Ver. 1.0.0.0
SMTP Server	Windows Server 2012 P-Mail Server Manager version 1.91
FTP Server	Windows Server 2012 IIS8 V8.0.9200.16384 Linux (Fedora20) vsftpd 3.0.2
SMB Server	Windows Server 2012

The TOE used in the developer testing is a part of multiple MFPs that are identified in the ST with different print speed, and the evaluator has confirmed that the difference of print speed does not affect the security function.

As mentioned above, the evaluator judged that the models selected as the target for the developer testing are consistent with the descriptions in the ST and cover the TOE configuration identified in the ST. The evaluator also judged that the developer testing was performed in the same TOE testing environment as the TOE configuration identified in the ST.

(2) Summary of the Developer Testing

A summary of the developer testing is as follows.

(a) Developer Testing Outline
An outline of the developer testing is as follows.

<Developer Testing Approach>
The testing approaches consisted of:
- stimulating the assumed external interfaces (Operation Panel, Web browser, and so on) in normal use of the TOE, and visually observing the results;
- analysing the generated audit log and the logging data for debug;
- checking the communication protocols between client computers/each server and the TOE with packet capture; and
- executing anomaly simulation tests to generate abnormal events by altering a part of the TSF implementation, and so on.

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

(b) Scope of the Performed Developer Testing
The developer testing was performed on about 460 items by the developer.

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

(c) Result

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

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

7.4.2 Evaluator Independent Testing

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

The independent testing performed by the evaluator is explained below.

(1) Independent Testing Environment

The configuration of the independent testing performed by the evaluator was the same as the configuration of the developer testing as shown in Figure 7-1. However, for the TOE, models with different print speed from the ones used for the developer testing were used for the independent testing to cover all models that are identified in the ST.

(2) Summary of Independent Testing

A summary of the independent testing is as follows.

(a) Independent Testing Viewpoints

The viewpoints for the independent testing that the evaluator designed from the developer testing and the provided evaluation documentation are shown below.

<Independent Testing Viewpoints>

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

   - The testing items are selected to include all of TSFs and TSFIs in terms of completeness.
   - The testing items are selected to cover the different testing approaches and testing environments.
   - The testing items involving TSFI that meet many of the SFRs are mainly selected in order to conduct tests efficiently.
   - Considering the functionality difference from the similar products that have

been CC-certified, the testing items for TSFs which are newly added in this TOE are preferably selected.

(b) Independent Testing Outline
An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>
In setting the different initialisation and the different parameters from the developer testing, the independent testing approaches consisted of:

- stimulating the assumed external interfaces (Operation Panel, Web browser, and so on) in normal use of the TOE, and visually observing the results;
- analysing the generated audit log; and
- checking the communication protocols between client computers/each server and the TOE with packet capture, and so on.

<Content of the Performed Independent Testing >
Based on the viewpoints of the independent testing, 14 items for the independent testing and 16 items for the sampling testing were performed.

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

Table 7-2 Viewpoints for the Independent Testing

Viewpoints for the Independent Testing	Outline of the Independent Testing
1	- By changing conditions, etc., confirmed that the behaviours concerning the user account lock were as specified. - Confirmed that the access control was performed as specified when operating the internally stored documents from several interfaces.
2	- Confirmed that the lockout process of accounts was performed as specified while normal users and administrators simultaneously log on. - Confirmed that the behaviours were as specified when user accounts were deleted while login status was maintained or when user privileges were changed.
3	- Confirmed that the S/MIME and IPsec procedures were performed as specified when using the expired certificates. - Regarding the operational function for the internally stored documents, confirmed that the exception procedures were performed as specified when unexpected parameters were specified or when a process

	was interrupted. - Confirmed that the exception procedures were performed as specified when entering unauthorised inputs from the printer driver. - Confirmed that the procedures for abnormal operations or process interruption were performed as specified when editing stored documents using Document Server Function.

(c) Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behaviour of the TOE. The evaluator confirmed consistencies between the expected behaviour and all the testing results.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation.

The penetration testing performed by the evaluator is explained below.

(1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

(a) Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

1. Unauthorised access to the TOE may be caused by unintentional network port interfaces.
2. Security Functions may be bypassed in case of entering data, for interfaces, which have the values and formats that are unintended by the TOE.
3. There may be some vulnerabilities when implementing secure channels, and consequently the Security Functions of the TOE may be bypassed.
4. Security Functions may be bypassed by maintaining the TOE overloaded.
5. Security Functions may be bypassed if operation conflicts by multiple interfaces occur.

(b) Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

< Penetration Testing Environment>

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

Table 7-3 shows key tools used in the penetration testing.

Table 7-3 Penetration Testing Tools

Name(Version)	Outline
ZAP (2.4.3/2.5.0)	Inspection tool of Web vulnerabilities with Proxy traffic
nmap (7.01/7.40)	Port Scanning Tool
Netcat (1.11)	Packet Communication Tool
Nessus (6.10.4) Plugin 201703312215	Vulnerability Scanning Tool
Burp Suite Professional (1.7.12/1.7.15)	Inspection tool of Web vulnerabilities with Proxy traffic
Wireshark (2.2.5/2.2.4)	Packet Capture Tool
OpenSSL 1.0.1j	Software library that provides the SSL/TLS protocol

<List of the Performed Penetration Testing>
Table 7-4 shows vulnerabilities concerned and the content of the related penetration testing. The evaluator performed 11 test cases in the following penetration testing to identify possibly exploitable vulnerabilities:

Table 7-4 Outline of the Performed Penetration Testing

Vulnerability	Outline of the Penetration Testing
1	Confirmed that the unintended network ports were not opened using the port scanning tool and the vulnerability scanning tool. Also checked no vulnerabilities to unauthorised inputs for available ports.
2	Checked no publicly-known vulnerabilities on Web interfaces to access the TOE. Confirmed that the Security Functions may not be bypassed by the specified URL at the time of connecting to the TOE via a Web browser.
3	Checked no implementation-specific vulnerabilities regarding the encryption communication with TLS and IPsec. Confirmed that parameters were not easily predicted by verifying the randomness of numbers as parameters used in Web interfaces.
4	Confirmed that the TOE was not unsecured due to the overloaded CPU and insufficient resources.

5	Confirmed that Security Functions were not bypassed when user login was performed using multiple interfaces and user privileges were changed on various occasions.

(c) Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

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

7.6 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance:

  U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

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

  - 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
  - 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
  - 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
  - 2600.2-DSR, SFR Package for Hardcopy Document Storage and Retrieval Functions, Operational Environment B
  - 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

- Security functional requirements: Common Criteria Part 2 extended
- Security assurance requirements: Common Criteria Part 3 conformant

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

- All assurance components of EAL2 package
- Additional assurance component ALC_FLR.2

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

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to consumers.

8. Certification

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

1. Contents pointed out in the Observation Report shall be adequate.

2. Contents pointed out in the Observation Report shall properly be solved.

3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

4 Rationale of the 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 the submitted Evaluation Technical Report, Observation Report, and related evaluation documentation, the Certification Body determined that this TOE satisfies all assurance requirements for EAL2 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

Any influences on the security functions of this TOE in the operation, in the case the Maintenance Functions are activated, are out of the scope of the assurance provided by this evaluation. Therefore, it is advised to make a judgment at the administrator's responsibility about the acceptance of maintenance.

It should be noted that the TOE users need to refer to the description of "4.3 Clarification of Scope" and to see whether or not the evaluated scope of this TOE and the operational requirement items can be handled in the actual operating environment of the TOE.

9. Annexes

There is no annex.

10. Security Target

The Security Target [12] of this TOE is provided as a separate document along with this Certification Report.

RICOH Pro 8220S/8210S/8200S Security Target, Version 1.00,
June 16, 2017, RICOH COMPANY, LTD.

11. Glossary

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

HDD	An abbreviation of Hard Disk Drive; in this document, it indicates the HDD installed in the TOE if simply described as "HDD."
IPsec	Secure Architecture for Internet Protocol; a protocol that provides the functions of data tampering prevention and data confidentiality with IP packets traffic using cryptographic technology.
MFP	An abbreviation of a digital multifunctional product.
S/MIME	Secure / Multipurpose Internet Mail Extensions; a standard for e-mail encryption and digital signatures with a public key system.

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

Administrative role	Pre-defined roles that enable administrators to be given. Although the following four types of administrative roles are defined and can be assigned to respective administrators, this TOE assumes the MFP administrator who is assigned to all the roles. (The access control for each subcategorised administrative role is excluded from this evaluation.) - Device administrator (executes device administration and audit) - User administrator (executes the management of normal users) - Network administrator (executes the network connection management of the TOE) - File administrator (executes the management of stored documents and document user list)

Documents	General term for paper documents and electronic documents operated by the TOE.
Lockout	The state of making the user accounts unavailable.
Lockout time	The time from being locked out to automatically releasing the user accounts.
Login password	A password corresponding to each login user name.
Login user name	An identifier assigned to normal users, an MFP administrator, and a supervisor. The TOE identifies users by this identifier.
Maintenance Function	A function to perform maintenance service for machine malfunctions. In the operation of this TOE, the Service Mode Lock Function is set to "ON" for deactivating this function.
Number of Attempts before Lockout	The number of consecutive failed attempts to identify and authenticate users, which is allowable until locking out the user accounts. The MFP administrator can assign 1 to 5 as a setting value.
Stored Documents	Documents stored in the TOE so that they can be used with Document Server Function, Printer Function, and Scanner Function.
User job	A work, from beginning to end, for each of the following TOE functions: Copy, Document Server, Scanner, and Printer. A user job may be paused or cancelled during the process by a user. If a user job is cancelled, the user job will end.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001, (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002, (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003, (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004, (Japanese Version 1.0, November 2012)

[12] RICOH Pro 8220S/8210S/8200S Security Target, Version 1.00, June 16, 2017, RICOH COMPANY, LTD.

[13] RICOH Pro 8220S/8210S/8200S Evaluation Technical Report, Version 2.0, July 7, 2017, ECSEC Laboratory Inc. Evaluation Center

[14] U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

[15] CCEVS Policy Letter #20, 15 November 2010, National Information Assurance Partnership