Certification Report

SAITO Yutaka, Commissioner
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2023-10-23 (ITC-3865)
Certification Identification	JISEC-C0809
Product Name	RICOH IM 460F/370F with Extended HDD Type M54
Version and Release Numbers	J-1.00
Product Manufacturer	RICOH COMPANY, LTD.
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile 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 by ALC_FLR.2
Name of IT Security Evaluation Facility	ECSEC Laboratory Inc., Evaluation Center

This is to report that the evaluation result for the above TOE has been certified as follows.
2024-03-12

YANO Tatsuro, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

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 5
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

Evaluation Result: Pass

"RICOH IM 460F/370F with Extended HDD Type M54 version J-1.00" 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 IM 460F/370F with Extended HDD Type M54 version J-1.00" (hereinafter referred to as the "TOE") developed by RICOH COMPANY, LTD., and the evaluation of the TOE was completed on 2024-03-01 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 procurement entities and consumers who are interested in the TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") described in Chapter 10. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes procurement entities who purchase the TOE to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the 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 Protection Profile or Assurance Package

The TOE conforms to the following protection profile [14] [15] (hereinafter referred to as the "conformance PP").

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

Assurance Package of the TOE is EAL2 augmented by ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a Multifunction Product (hereinafter referred to as "MFP"), which provides the functions of copy, printer, scanner, fax and document server.

The TOE provides security functions required for the conformance PP in order to prevent unauthorised disclosure or alteration of the document data processed by MFP and the setting information affecting security.

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 the TOE.

1.1.2.1 Threats and Security Objectives

The TOE assumes the following threats.

There are threats of unauthorised disclosure and alteration of assets such as document data processed by the TOE and the setting information relevant to security functions due to unauthorised access to the TOE or the communication data on the network.

To counter such threats, the TOE provides security functions required for the conformance PP such as identification and authentication, access control, encryption, etc.

1.1.2.2 Configuration and Assumptions

The TOE is assumed to be operated under the following assumptions.

It is assumed that the 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

The following operation is not ensured by this evaluation:

- Operational environments and configurations different from those described in "4.2 Environmental Assumptions"

- The TOE with settings different from those described in "7.5 Evaluated Configuration"

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 in 2024-03, based on functional requirements and assurance requirements of the 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] 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 oversight reviews were also prepared for those concerns found in the certification process. The Certification Body confirmed that all the concerns were fully resolved, and 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 and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	RICOH IM 460F/370F with Extended HDD Type M54
TOE Version:	J-1.00
Developer:	RICOH COMPANY, LTD.

The TOE consists of the MFP and optional products. The TOE components are listed in Table 2-1.

Table 2-1 TOE Components

MFP		Optional Product
Product Name	Model Code	
RICOH IM 370F	D0DM-03	Extended HDD Type M54
RICOH IM 460F	D0DN-00	Extended HDD Type M54

The TOE version is a combination of multiple software versions in the TOE. Refer to Chapter 1.2 of the ST for the TOE version in detail.

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

- Confirm that the product name and model code displayed on the product exterior match those listed in Table 2-1.
- Confirm that the name described on the label sticker of the packing box for the optional products (Extended HDD) matches the optional products listed in Table 2-1.
- Operate as described in the product guidance, and confirm that the software names, versions and the part numbers displayed on the operation panel of the product match those listed in Chapter 1.2 of the ST.

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organisational security policies.

The TOE provides the MFP basic functions such as copy, printer, scanner, fax and document server. It has the functionality to store user document data in the TOE and to communicate with user terminals and various servers via a network.

The TOE provides security functions that satisfy the requirements of the Conformance PP, to protect the document data processed by the TOE and setting data etc. affecting security.

Table 3-1 describes users of the TOE. The TOE users are classified into normal user and administrator, and administrators are classified into supervisor and MFP administrator.

Table 3-1 TOE Users

User Definition		Explanation
Normal user		A user who is allowed to use the TOE basic functions.
Administrator	MFP administrator	A user who is allowed to manage the TOE.
	Supervisor	A user who is authorised to modify the login password of the MFP administrator and to release the lockout status of the MFP administrator.

Tables 3-2 and 3-3 describe assets of the TOE.

Table 3-2 TOE Assets (user data)

Type	Definition
Document data	User's documents under the TOE management.
User job data	Information related to the user's document or document processing job.

Table 3-3 TOE Assets (TSF data)

Type	Definition
TSF confidential data	Data that requires integrity and confidentiality among the data used by security functions. For the TOE, it includes Login password, audit logs and HDD cryptographic key.

TSF protected data	Data that requires only integrity among the data used by security functions. For the TOE, it includes login user name, minimum character number of password, access control related settings, etc., which are setting values for security functions, excluding the TSF confidential data.

3.1 Security Function Policies

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

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats described in Table 3-4 and provides the security functions to counter them.

Table 3-4 Assumed Threats

Identifier	Threat
T.DOC.DIS (Document data disclosure)	Document data under the TOE management may be disclosed by unauthorised persons.
T.DOC.ALT (Document data alteration)	Document data under the TOE management may be altered by unauthorised persons.
T.FUNC.ALT (User job data alteration)	User job data under the TOE management may be altered by unauthorised persons.
T.PROT.ALT (Alteration of TSF protected data)	TSF Protected Data under the TOE management may be altered by unauthorised persons.
T.CONF.DIS (Disclosure of TSF confidential data)	TSF Confidential Data under the TOE management may be disclosed by unauthorised persons.
T.CONF.ALT (Alteration of TSF confidential data)	TSF Confidential Data under the TOE management may be altered by unauthorised persons.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats described in Table 3-4 with the following security function policies. The details of each security function are described in Chapter 5.

1) Countermeasure against the threats "T.DOC.DIS", "T. DOC.ALT" and "T.FUNC.ALT"

These are threats to the user data described in Table 3-2. The TOE counters the threats with "Identification and Authentication Function", "Use-of-Feature Restriction Function", "Document Access Control Function", "Residual Data Overwrite Function" and "Network Protection Function".

"Identification and Authentication Function" allows only users who have succeeded in the identification and authentication to use the TOE.

"Use-of-Feature Restriction Function" checks the permission given to the identified and authenticated users when they try to use the MFP basic functions, and allows only authorised users to use these functions.

"Document Access Control Function" performs access control when users try to access the user data and allows only authorised users to access the user data.

"Residual Data Overwrite Function" overwrites the HDD area where deleted document data and their fragments were stored to prevent the residual data from being reused.

"Network Protection Function" performs encrypted communications to protect communication data when the TOE communicates to client computers and various servers.

With the above functions, the TOE prevents unauthorised disclosure and alteration of the user data due to unauthorised use of the TOE or unauthorised access to the communication data.

2) Countermeasure against the threats "T.PROT.ALT", "T.CONF.DIS" and "T.CONF.ALT"

These are threats to the TSF data described in Table 3-3. The TOE counters the threats with "Identification and Authentication Function", "Security Management Function" and "Network Protection Function".

"Identification and Authentication Function" and "Security Management Function" allow only authorised users to access the TSF data.

"Network Protection Function" performs encrypted communications to protect communication data when the TOE communicates to client computers and various servers.

With the above functions, the TOE prevents unauthorised disclosure and alteration of the TSF data due to unauthorised use of the TOE or unauthorised access to the communication data.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies required for the TOE are described in Table 3-5. P.STORAGE.ENCRYPTION is added to the conformance PP.

Table 3-5 Organisational Security Policies

Identifier	Organisational Security Policy
P.USER.AUTHORIZATION (User identification and authentication)	To maintain operational accountability and security, give users the authority to use the TOE only when authorized by the TOE owner.
P.SOFTWARE.VERIFICAION (Software verification)	To detect corruption of the executable code in TSF, implement procedures to self-test the executable code.
P.AUDIT.LOGGING (Management of audit log records)	To maintain operational accountability and security, create and maintain records that provide audit trail of TOE use and security-relevant events, protect them from unauthorised disclosure and alteration, and make them viewable only by authorised persons.
P.INTERFACE.MANAGEMENT (Management of external interfaces)	To prevent unauthorised use of the external interfaces of the TOE, control the operation of those interfaces by the TOE and its IT environment.
P.STRAGE.ENCRYPTION (Encryption of storage devices)	The data recorded in the TOE's HDD shall be encrypted.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the following security functions to meet the organisational security policies described in Table 3-5. The details of each security function are described in Chapter 5.

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

The TOE implements this policy by "Identification and Authentication Function" and "Use-of-Feature Restriction Function".

"Identification and Authentication Function" allows only users who have succeeded in the identification and authentication to use the TOE.

"Use-of-Feature Restriction Function" checks the permission given to the identified and authenticated users when they try to use the MFP basic functions, and allows only authorised users to use these functions.

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

The TOE implements this policy by "Integrity Verification Function".

"Integrity Verification Function" verifies the integrity of the executable codes of security functions at the TOE start up.

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

The TOE implements this policy by "Audit Function".

"Audit Function" records events relevant to security functions as an audit log. The audit log stored in the TOE can be read and deleted only by the identified and authenticated MFP administrator.

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

The TOE implements this policy by "Identification and Authentication Function" and "Fax Line Separation Function".

"Identification and Authentication Function" allows only users who have succeeded in the identification and authentication to use the TOE. It also terminates the session after a certain period of no operation by a user. In addition, it prevents unauthorised transfer of data received from the operation panel or the LAN.

"Fax Line Separation Function" controls the data received from telephone lines and prevents unauthorised data transfer from telephone lines to the LAN.

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

The TOE implements this policy by "Stored Data Protection Function".

"Stored Data Protection Function" encrypts the data stored in the TOE's internal storage (HDD).

4. Assumptions and Clarification of Scope

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

4.1 Usage Assumptions

Table 4-1 describes assumptions to operate the TOE. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ACCESS.MANAGED (Access management)	The TOE is placed in a restricted or monitored environment that is protected from unauthorised access to the physical components of the TOE and data interfaces of the TOE.
A.USER.TRAINING (User training)	Users of the TOE are aware of the security policies and procedures of their organisation, are trained to follow those policies and procedures, and gain competence to follow them.
A.ADMIN.TRAINING (Administrator training)	Administrators are aware of the security policies and procedures of their organisation, are trained to follow the guidance and documents of the manufacturer, gain competence to follow them, and are able to configure and operate the TOE properly according to those policies and procedures.
A.ADMIN.TRUST (Trusted administrator)	Administrators do not use their access rights for malicious purposes.

4.2 Environmental Assumptions

Figure 4-1 shows the assumed operational environment of the TOE. The TOE is installed in a general office and connected to a local area network (hereinafter referred to as "LAN") and the telephone line to use. Users use the TOE through the operation panel of the TOE itself and client computers that are also connected to the LAN.

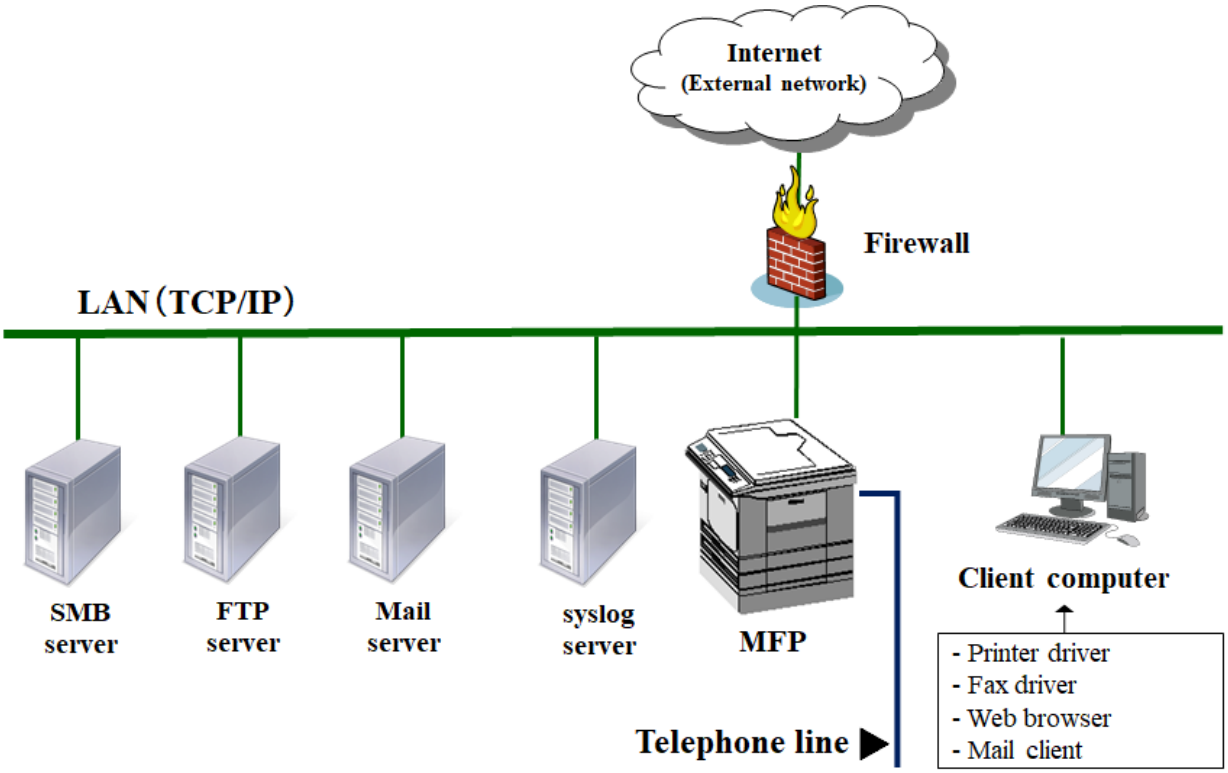

Figure 4-1 Operational Environment of the TOE

The components of the operational environment of the TOE are as follows:

1) Client computer

It is a general-purpose computer used by users. Web browser, mail client that supports S/MIME, RPCS Driver (version 1.0.0.0 or later) and PC FAX Generic Driver (version 13.1.0.0 or later) provided by Ricoh are required. The following software is used in this evaluation.

- OS: Windows 10, Windows 11
- Web browser: Microsoft Edge 107
- Mail client: Thunderbird 102.6.0
- Printer driver: RPCS Driver 1.0.0.0
- Fax driver: PC FAX Generic Driver 13.1.0.0

2) SMB server, FTP server, Mail server

They are servers used to send the user document data scanned by the TOE. Each server requires software that supports IPsec and SMB protocols, IPsec and FTP protocols, or SMTP protocol, respectively. The following software is used in this evaluation.

(SMB server)
- OS: Windows 10
- SMB software: Included in the OS

(FTP server)
- Configuration a:
  - OS: Windows 10
  - FTP software: IIS10 V10.0.19041.804

- Configuration b:
  - OS: Linux (Ubuntu 20.04)
  - FTP software: vsftpd 3.0.3

(Mail server)
  - OS: Windows 10
  - SMTP software: P-Mail Server Manager 1.91

3) syslog server

It is a server to store the audit logs generated by the TOE. It is used when audit log transfer is enabled in the TOE settings. Software that supports syslog protocol with TLS is required. The following software is used in this evaluation.

  - OS: Linux (Ubuntu 20.04)
  - syslog software: rsyslogd 8.2001.0

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

4.3 Clarification of Scope

The functions provided by the TOE or ensured by this evaluation have the following restrictions.

1) Servers and client computers

The secure operation of servers and client computers cooperating with the TOE is the responsibility of the administrators of these devices.

5. Architectural Information

This chapter explains the scope and the main components of the TOE.

5.1 TOE Boundary and Components

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

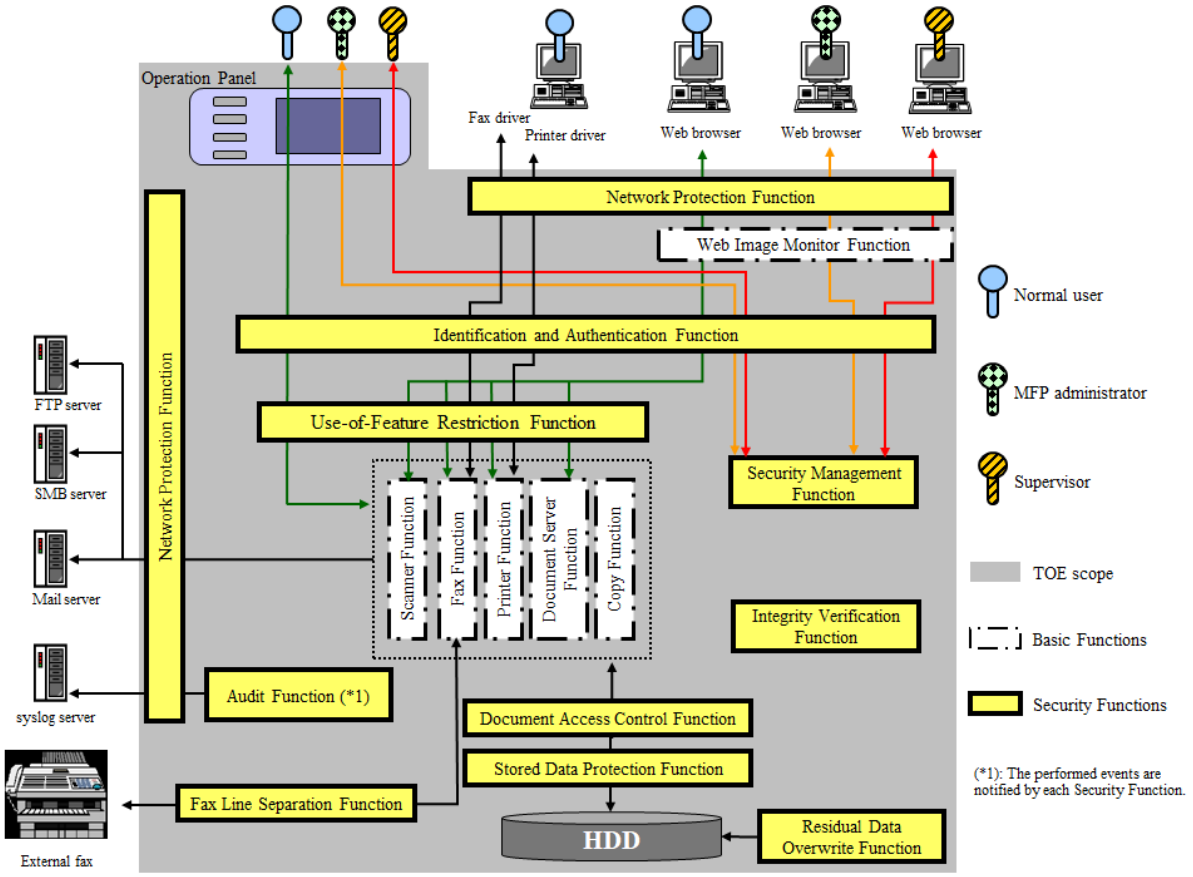

Figure 5-1 TOE Components

The TOE functions consist of security functions and basic functions. The TOE security functions are described below. Refer to Chapter 11 for the basic functions.

1) Identification and Authentication Function

This function is to identify and authenticate a user by the login user name and login password when the user uses the TOE from the TOE operation panel or a client computer (Web browser, printer driver, or fax driver).

In addition, the following functionalities are provided to reinforce the identification and authentication.

- Account lockout after consecutive failed authentication attempts
- Restriction on minimum number of password characters and mandatory character types
- Session termination when no operation is performed for a certain period of time after successful authentication

2) Use-of-Feature Restriction Function

This function is to restrict the use of the MFP basic functions to authorised users. When a user tries to use any of the MFP basic functions, it is determined whether the user is allowed to use the function based on the user's role and permissions set for each user.

3) Document Access Control Function

This function is to control access to data when a user operates document data and user job data with any of the MFP basic functions. Access control is performed based on the owner information of the document data and the user job data, as well as user's identification information and role.

4) Stored Data Protection Function

This function is to encrypt the data stored in the TOE's internal storage (HDD). The encryption algorithm uses AES with a key length of 256 bits.

5) Residual Data Overwrite Function

This function is to overwrite the HDD area where document data was stored, with specified data. This function is executed at the following timing:

- When a user deletes document information
- When a user job is complete
- When the MFP administrator specifies batch overwriting

In the case of batch overwriting, its overwriting method can be set by the MFP administrator. On the other hand, in the case of deletion by user or user job completion, the HDD is overwritten with random numbers.

6) Network Protection Function

This function is to protect communication data between the TOE and IT devices with the cryptographic communication protocol.

7) Fax Line Separation Function

This function is to restrict data received from telephone lines to fax data and prevent unauthorized data transfer from telephone lines to the LAN.

8) Security Management Function

This function is to restrict the settings, etc. of the security functions to the MFP administrator. However, all users can change their own login password, and the supervisor can change the login password of the MFP administrator.

9) Integrity Verification Function

This function is to verify the integrity of the executable codes of the security functions at the time of TOE start-up. The verification uses hash values or digital signatures of various software in the TOE.

10) Audit Function

This function is to record audit events relevant to security functions as an audit log. The audit log stored in the TOE can be read or deleted only by the identified and authenticated MFP administrator. The audit log can be sent to the syslog server by the TOE settings.

5.2 IT Environment

The TOE communicates with servers and client computers via the LAN. The network protection function of the TOE works in cooperation with those IT devices and uses the following protocols:

- Client computer (Web browser): HTTP over TLS (TLS 1.2, TLS 1.3)
- Client computer (Printer driver, Fax driver): IPP over TLS (TLS 1.2, TLS 1.3)
- SMB server: IPsec
- FTP server: IPsec
- Mail server: S/MIME
- syslog server: Syslog over TLS (TLS 1.2, TLS 1.3)

6. Documentation

The identification of documents attached to the TOE is listed in Table 6-1. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

Table 6-1 Product-attached documents (Japanese)

Document Name	Version
かんたん操作ガイド	D0DM-7002
本機を安全にご利用いただくために	D0DM-7013
安全上のご注意	D0DM-7300
使用説明書 RICOH IM 460F/370F	D0DM7302
セキュリティーリファレンス	D0E37515
使用説明書〈IEEE Std 2600.2™-2009 準拠でお使いになる管理者の方へ〉	D0DM-7306 2024.02.08
セキュリティー機能をお使いになるお客様へ	D0E3-7510 2023.09.28
ヘルプ	83NHEZ- JAR1.00 v281

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 requirements in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the 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 started in 2023-10 and concluded upon completion of the Evaluation Technical Report dated 2024-03. 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.

Additionally, the evaluator examined the implementation of the requirements for each work unit of configuration management and delivery by visiting the development site and remote inspection to the manufacturing sites in 2023-11. For some manufacturing sites, the Evaluation Facility determined that the site examination could be omitted and the examination results in the past CC certification 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 Evaluation Facility or the developer site from 2023-11 to 2023-12.

Concerns in the evaluation process that the Certification Body found were described as the certification oversight reviews, and they were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As the verification results of the evidence shown in the evaluation process and 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 had performed and the documentation of actual test 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 lists the main configuration items.

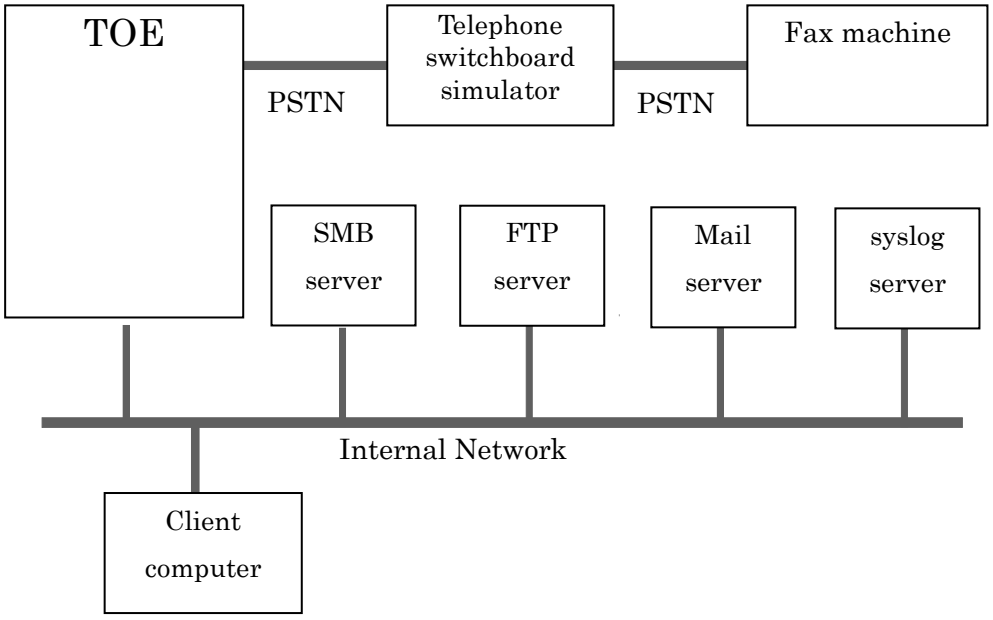

Figure 7-1 Configuration of the Developer Testing

Table 7-1 Test Configurations

Configuration Item	Detail
TOE	- RICOH IM 370F with Extended HDD Type M54 J-1.00 (D0DM-03) - RICOH IM 460F with Extended HDD Type M54 J-1.00 (D0DN-00)
Client computer	OS: Windows 10, Windows 11 Web browser: Microsoft Edge 107 Mail client: Thunderbird 102.6.0 Printer driver: RPCS Driver 1.0.0.0 Fax driver: PC FAX Generic Driver 13.1.0.0
SMB server	OS: Windows 10 SMB software: Included in the OS
FTP server	- Configuration a: OS: Windows 10 V10.0.19041.804 FTP software: IIS10 (Included in the OS) - Configuration b: OS: Linux (Ubuntu 20.04) FTP software: vsftpd 3.0.3
Mail server	OS: Windows 10 SMTP software: P-Mail Server Manager 1.91
syslog server	OS: Linux (Ubuntu 20.04) syslog software: rsyslogd 8.2001.0
Telephone switchboard simulator	XF-A150 (Panasonic Corporation)
Fax machine	RICOH IM C6000F, MFC-J877N (Brother Industries)

The TOE items tested by the developer are all the models included in the TOE.

The developer testing was performed in the TOE testing environment consistent with 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 external interfaces of the TOE are stimulated by operating the operation panel of the TOE or the client computer, and the response, the behaviour of the TOE, the communication data and the audit log are confirmed. For behaviours that cannot be confirmed on the external interface of the TOE, the developer interface of the TOE and the TOE software modified for the testing are used to confirm the internal operation of the TOE.

<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 500 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 the approach of the performed developer testing and the validity 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 expected test results by the developer and the actual test results performed by the developer.

7.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the implementation of security functions using the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further confidence 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 as follows.

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.

2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing are described below, which are devised by the evaluator based on the analysis of developer testing and the evaluation documentation provided.

<Independent Testing Viewpoints>

1. Confirm variations of input data and operations that are different from the developer testing.

2. Confirm execution timing of several TSFs and execution combinations that are not tested by the developer.

3. Select the testing items for the sampling testing from the following viewpoints:

- The testing items are selected to include all of security functions and TSF interfaces.
- The testing items are selected to cover the different testing approaches and testing environments.
- The testing items that contribute to the vulnerability evaluation are selected.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

The independent testing was performed using the same testing approach as the developer testing.

<Content of the Performed Independent Testing>

Based on the viewpoints of the independent testing, 12 items for the independent testing and 42 items for the sampling testing were performed.

The outline of the main independent testing corresponding to the viewpoints is described in Table 7-2.

Table 7-2 Outline of the Performed Independent Testing

Viewpoints for the Independent Testing	Outline of the Independent Testing
1	- Confirm that the user account lock, access control, password length limit etc. are as specified under the changed conditions. - Confirm that the disabled functions and interfaces are actually disabled. - Confirm the behaviour of IPsec and TLS with expired certificates.
2	- Confirm that the behaviour of the auto logout for multiple logins and for changing its settings during login is as specified. - Confirm that the behaviour when operating the same data from multiple interfaces is as specified.

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 test 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 as follows.

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 unexpected 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.

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 lists key tools used in the penetration testing.

Table 7-3 Penetration Testing Tools

Name (Version)	Outline
ZAP (2.14.0)	Inspection tool of Web vulnerabilities with Proxy traffic
nmap (7.92)	Port Scanning Tool
Burp Suite Professional (1.7.37)	Inspection tool of Web vulnerabilities with Proxy traffic
Wireshark (3.6.2)	Packet Capture Tool
PRET (0.40)	A tool to inspect various vulnerabilities in print processing.

<Content of the Performed Penetration Testing>

Table 7-4 describes outline of the penetration testing corresponding to the vulnerabilities of concern.

Table 7-4 Outline of the Performed Penetration Testing

Vulnerability	Outline of the Penetration Testing
1	- Confirm that there are no unexpected available interfaces by using the port scanning tool, etc.
2	- Confirm that there are no known vulnerabilities on Web interfaces of the TOE by using Web browser and proxy tool. - Confirm that there are no known vulnerabilities in the print processing of the TOE using the inspection tool for the print processing. - Confirm that unintended behaviour is not observed even if character strings that may cause unauthorized processing are entered into the operation panel of the TOE.
3	- Confirm that there are no implementation-specific vulnerabilities in the IPsec and TLS processing of the TOE. - Confirm that parameters are not easily predicted by verifying the randomness of numbers as parameters used in Web interfaces.
4	- Confirm that the TOE is not unsecured when the fax reception capacity is full or when all TOE functions are used simultaneously.

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

The configuration conditions of the TOE, which are the prerequisites for this evaluation, are described in the guidance documents listed in Chapter 6. In order to use the TOE securely as ensured by the evaluation, the TOE must be set as described in the guidance documents. Different settings from those described in the guidance documents are not subject to the assurance of this evaluation.

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM as per 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-FAX, SFR Package for Hardcopy Device Fax 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 procurement entities.

8. Certification

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

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

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

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

Concerns found in the certification process were prepared as the certification oversight reviews, and they were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the Evaluation Technical Report and related evaluation documentation submitted by the Evaluation Facility, the Certification Body determined that the TOE evaluation satisfies all assurance requirements for EAL2 augmented by ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

Procurement entities who are interested in the TOE are advised to refer to the description of "4.2 Environmental Assumptions" and "7.5 Evaluated Configuration" and to see whether or not the evaluated scope of the TOE and the operational requirements meet the operational conditions assumed by each individual.

To make sure of the TOE identification, checking the sticker on the surface of package as well as display of the TOE should be required, as described in Chapter 2. Be sure to keep the information described on this sticker to certainly identify the TOE.

9. Annexes

There is no annex.

10. Security Target

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

RICOH IM 460F/370F with Extended HDD Type M54 Security Target, Version 1.00, February 26, 2024, 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.

MFP	Multifunction Product

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

Copy function	A function to scan paper documents by the operation of the TOE operation panel and duplicate them.
Document Server function	A function to store or retrieve document data.
Fax function	A function to send and receive faxes using the telephone line.
Printer function	A function to receive user document data sent from the printer driver of a client computer and print them by operating the TOE operation panel.
Scanner function	A function to scan paper documents by the operation of the TOE operation panel and send the scanned data to an external server.
Web Image Monitor function	A function to operate the TOE from a Web browser of a client computer.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, December 2023, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, December 2023, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2021, 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 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001, (Japanese Version 1.0, July 2017)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002, (Japanese Version 1.0, July 2017)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003, (Japanese Version 1.0, July 2017)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004, (Japanese Version 1.0, July 2017)

[12] RICOH IM 460F/370F with Extended HDD Type M54 Security Target, Version 1.00, February 26, 2024, RICOH COMPANY, LTD.

[13] RICOH IM 460F/370F with Extended HDD Type M54 Evaluation Technical Report, Version 1.2, March 1, 2024, 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