Certification Report

TOMITA Tatsuo, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2020-09-30 (ITC-0769)
Certification Identification	JISEC-C0727
Product Name	RICOH IM C6000/C5500/C4500
Version and Release Numbers	J-2.00
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.
2021-08-17

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 C6000/C5500/C4500 version J-2.00" 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 C6000/C5500/C4500 version J-2.00" (hereinafter referred to as the "TOE") developed by RICOH COMPANY, LTD., and the evaluation of the TOE was finished on 2021-08-04 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 "general consumers and procurement entities who purchase the TOE that is commercially available" 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 digital Multi-Function Product (hereinafter referred to as "MFP"), which provides the functions of copy, scanner, printer, fax and document server.

The TOE provides the security functions required for the conformance PP in order to prevent unauthorised disclosure or alteration of the documents 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 the documents 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 in 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 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
- IP-Fax and Internet Fax Function
- Authentication methods except for Basic Authentication (for Internal Authentication)

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 2021-08, 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] and the Observation Reports 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 C6000/C5500/C4500

TOE Version: J-2.00

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	Fax Unit	SPDF/ARDF/ Exposure Glass Cover
RICOH IM C6000	D0BQ-00	Fax Unit Type M38	Document Feeder DF3110
RICOH IM C6000	D0BQ-00	Fax Unit Type M38	None (*1)
RICOH IM C6000	D0BQ-00	Fax Unit Type M38	Platen Cover PN2000
RICOH IM C5500	D0BP-00	Fax Unit Type M38	Document Feeder DF3110
RICOH IM C5500	D0BP-00	Fax Unit Type M38	Document Feeder DF3120
RICOH IM C5500	D0BP-00	Fax Unit Type M38	Platen Cover PN2000
RICOH IM C4500	D0BN-00	Fax Unit Type M38	Document Feeder DF3110
RICOH IM C4500	D0BN-00	Fax Unit Type M38	Document Feeder DF3120
RICOH IM C4500	D0BN-00	Fax Unit Type M38	Platen Cover PN2000
RICOH IM C5500A	D0BP-04	Fax Unit Type M38	Document Feeder DF3110
RICOH IM C5500A	D0BP-04	Fax Unit Type M38	None (*1)
RICOH IM C5500A	D0BP-04	Fax Unit Type M38	Platen Cover PN2000

MFP		Optional Product	
Product Name	Model Code	Fax Unit	SPDF/ARDF/ Exposure Glass Cover
RICOH IM C4500A	D0BN-04	Fax Unit Type M38	Document Feeder DF3110
RICOH IM C4500A	D0BN-04	Fax Unit Type M38	None (*1)
RICOH IM C4500A	D0BN-04	Fax Unit Type M38	Platen Cover PN2000
RICOH IM C6000F	D0BQ-01	None	Document Feeder DF3110
RICOH IM C6000F	D0BQ-01	None	None (*1)
RICOH IM C6000F	D0BQ-01	None	Platen Cover PN2000
RICOH IM C5500F	D0BP-01	None	None (*2)
RICOH IM C5500F	D0BP-01	None	Document Feeder DF3120
RICOH IM C5500F	D0BP-01	None	Platen Cover PN2000
RICOH IM C4500F	D0BN-01	None	None (*2)
RICOH IM C4500F	D0BN-01	None	Document Feeder DF3120
RICOH IM C4500F	D0BN-01	None	Platen Cover PN2000

(*1) The MFP is equipped with the SPDF by default.
(*2) The MFP is equipped with the ARDF by default.

The TOE version is a combination of multiple software and hardware 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 a fax option matches the fax unit listed in Table 2-1.

- If the product is equipped with an optional ARDF or SPDF, confirm that the name described on the nameplate of the option is "Document Feeder DF3110", "Document Feeder DF3120", respectively. If the product is equipped with an optional exposure glass cover, confirm that the name on the label sticker of the packing box for the option is "Platen Cover PN2000".

- Operate as described in the product guidance, and confirm that the software and hardware 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 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, to encrypt the stored data in an HDD, and to prevent the unauthorised access through telephone lines via fax I/F.

For each setting that is relevant to the above security functions, only administrators are allowed to set configurations in order to prevent the deactivation and unauthorised use of the security functions.

Table 3-1 shows 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. 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 normal user management, device management, file management, and network management.

Tables 3-2 and 3-3 show the protected assets for the security functions of the TOE.

Table 3-2 TOE Protected Assets (user data)

Type	Asset
Document information	Digitised documents, deleted documents, temporary documents and their fragments under the TOE control.
User job	Jobs specified by users.

Table 3-3 TOE Protected Assets (TSF data)

Type	Asset
TSF protected data	The information that shall be protected from changes by users without edit permission; it includes setting values for the security functions except for TSF confidential data, such as login username, minimum password length, access control related settings, etc.
TSF 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.

3.1 Security Function Policies

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

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE presumes the threats described in Table 3-4 and provides the security functions to counter them. It has been confirmed in the evaluation that these threats are the same as those described in the conformance PP.

Table 3-4 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 allowed to use the TOE.

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 any of the basic MFP functions of copy, printer, scanner, document server and fax, 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 documents or 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 PCs 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 PCs 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. It has been confirmed in the evaluation that these organisational security policies except for P.STORAGE.ENCRYPTION are the same as those described in the conformance PP.

Table 3-5 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 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 any of the basic MFP functions of copy, printer, scanner, document server and fax, 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 "Software Verification Function".

"Software 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 identified and authenticated administrators.

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 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 shows assumptions to operate the TOE. It has been confirmed in the evaluation that these assumptions are the same as those described in the conformance PP.

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)	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.

Note: The responsible manager of MFP is an organisational manager in the operational environment.

4.2 Environmental Assumptions

The TOE is installed in a general office and connected to a local area network (hereinafter referred to as "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 the TOE.

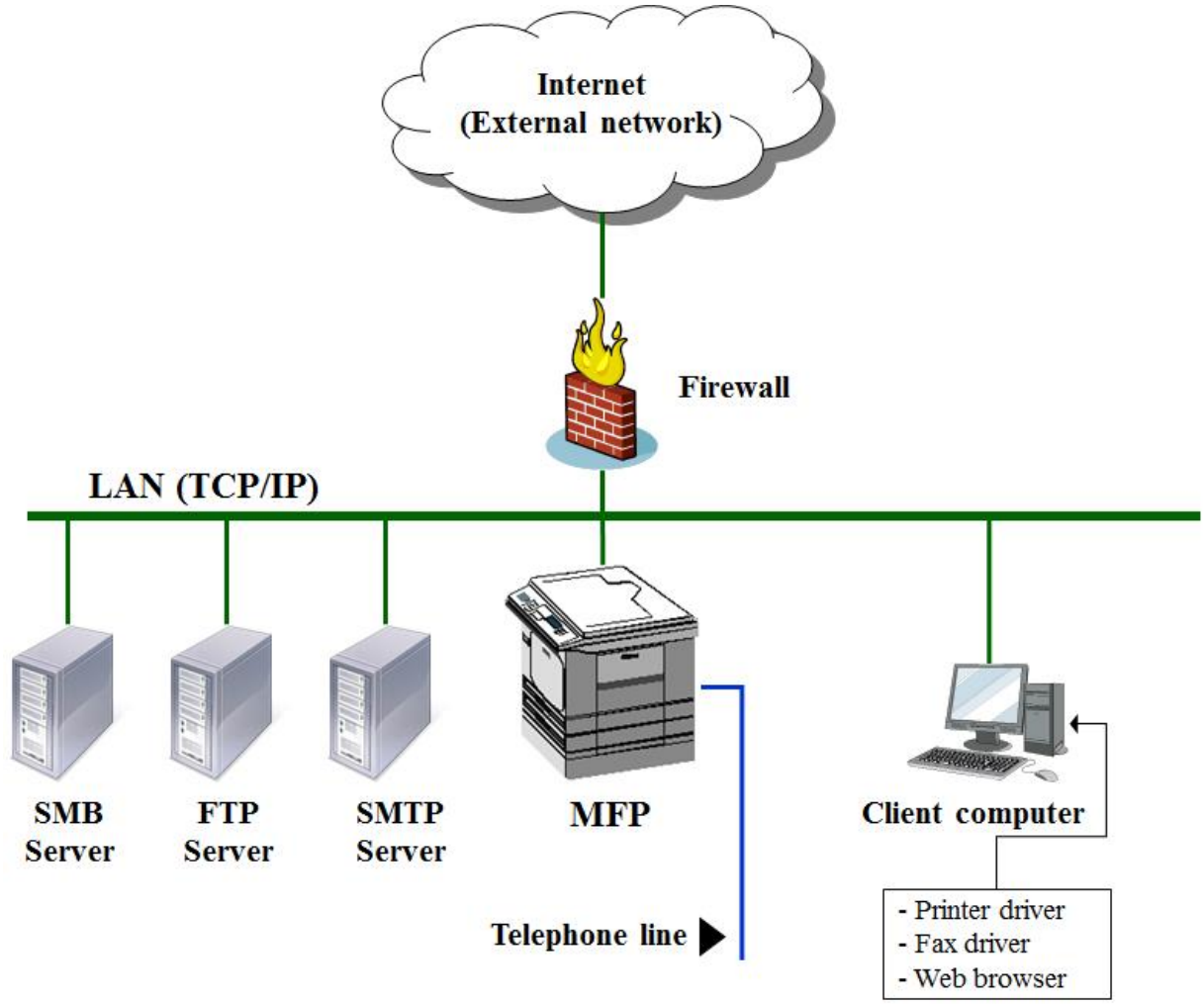

Figure 4-1 Operational Environment of the TOE

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

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 the printer drivers or the fax drivers in client computers enables to process printing via the LAN from the client computers.

The following devices are assumed to be used on the operational environment:

- Client PC
  > OS: Windows 8.1/10
  > Web browser: Internet Explorer11, or Microsoft Edge 44

> Printer driver: RPCS Driver 1.3.0.0
> Fax driver: PC Fax Generic Driver 9.4.0.0

- SMTP server: Windows Server 2012 P-Mail Server Manager

- FTP server: Windows Server 2012 (IIS8), Linux (Fedora20) vsftpd

- SMB server: Windows Server 2012

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

To protect data on communication paths between client computers/each server and the TOE, it is necessary that communication protocols on client computers and each server are operated securely to work properly.

To operate client computers and each server securely is the responsibility of the operator.

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.

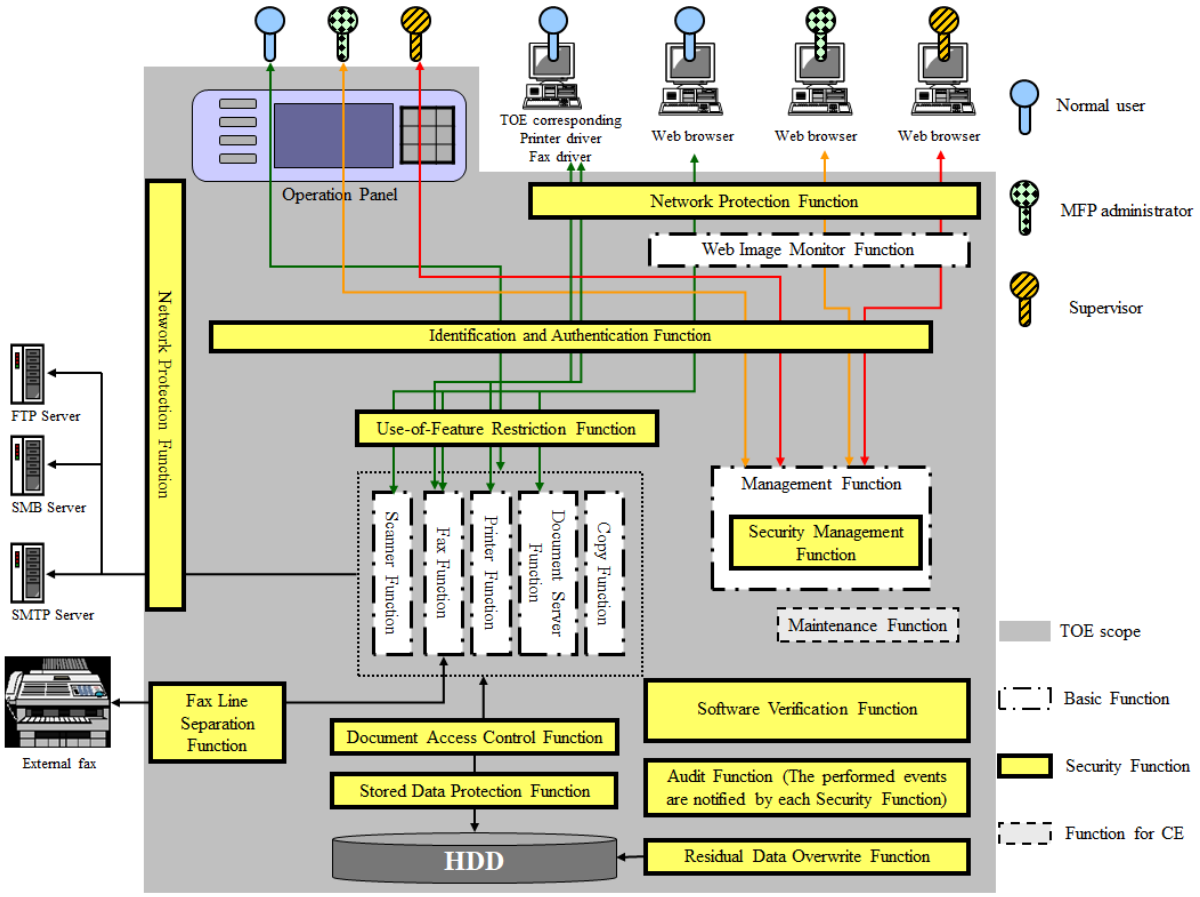

Figure 5-1 TOE Components

The TOE functions consist of security functions and other basic MFP functions. The TOE security functions are described as follows:

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 PC (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 basic MFP functions to authorised users. When a user tries to use any of the basic MFP 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 information and user jobs with any of the basic MFP functions. Access control is performed based on the owner information of the document information and the user jobs, as well as user's identification information and role.

4) Stored Data Protection Function

This function is to encrypt the data stored in the 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 information 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

The MFP administrator can specify an overwriting method. However, in the case of user deletion and user job completion, the data for overwriting are encrypted and written to the HDD. Therefore, the data for the overwriting method specified by the MFP administrator are different from the data actually written to the HDD.

6) Network Protection Function

This function is to perform the following encrypted communications when communicating with IT devices:

- Client PC: HTTP and IPP supporting TLS 1.2
- FTP server: IPsec
- SMB server: IPsec
- SMTP server: S/MIME

7) Fax Line Separation Function

This function is to control data received from telephone lines 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 login password, and the supervisor can change the login password of the MFP administrator.

9) Software 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 certificates of various software programs in the TOE. However, for the fax controller unit in the TOE, this function outputs information for integrity verification and a user compares the output information with the information described in the guidance documents.

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.

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 TOE communicates with fax devices via telephone lines.

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

6. Documentation

The identification of documents attached to the TOE is listed 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

Document Name	Version
かんたん操作ガイド	D0BQ-7003B
本機を安全にご利用いただくために	D0BQ-7028
本製品をお使いのお客様へ	D0BQ-7035A
本機をお使いのお客様へ	D0BQ-7037A
本製品をお使いのお客様へ（正誤表）	D0BQ-7091
安全上のご注意	D0BQ-7590
セキュリティーリファレンス	D0BQ-7588
セットアップ	D0BQ-7586
本機の紹介と基本操作	D0BQ-7573
コピー	D0BQ-7574
ドキュメントボックス	D0BQ-7575
ファクス	D0BQ-7576
スキャナー	D0BQ-7577
プリンター	D0BQ-7578
メンテナンス	D0BQ-7579
こまったときには	D0BQ-7580
設定（従来）	D0BQ-7581
設定（標準）	D0BQ-7582
設定項目対応表（従来：標準）	D0BQ-7583
仕様	D0BQ-7584
セキュリティー	D0BQ-7585
ドライバーインストールガイド	D0BQ-7587
セキュリティー機能をお使いになるお客様へ	D0C9-7025
IEEE Std 2600.2™-2009準拠でお使いになる管理者の方へ	D0BQ-7571
ヘルプ	83NHEEJAR1.10 v242

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 2020-09 and concluded upon completion of the Evaluation Technical Report dated 2021-08. 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 procedural status implemented for each work unit of configuration management and delivery by visiting the development site and remote inspection to the manufacturing sites in 2020-11, 2021-01, 2021-02, 2021-03, 2021-04 and 2021-05.

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 in 2021-04 and 2021-05.

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

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 shows the main configuration items.

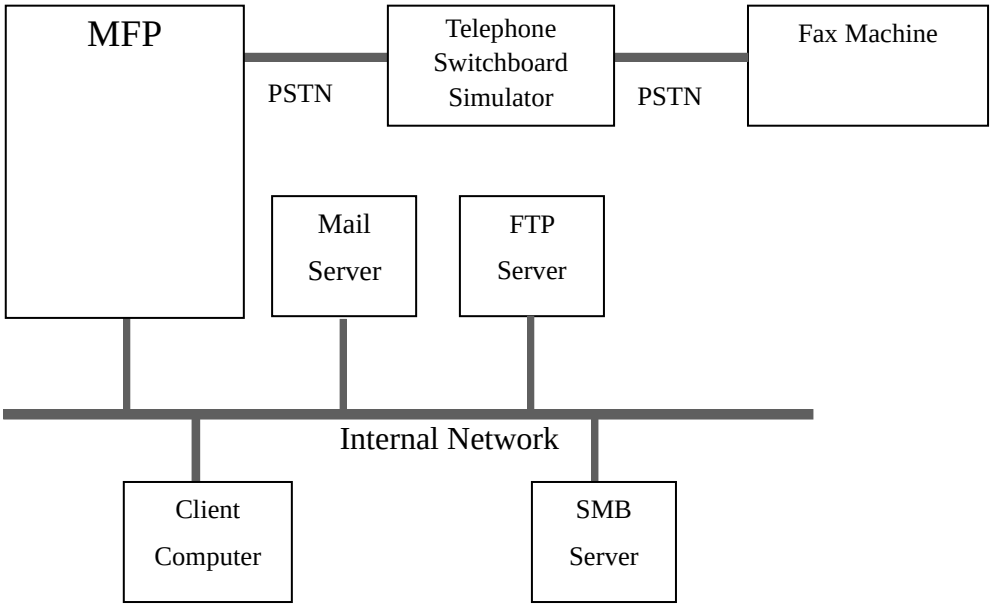

Figure 7-1 Configuration of the Developer Testing

Table 7-1 Test Configurations

Configuration Item	Detail
TOE	- RICOH IM C4500F (D0BN-01) - RICOH IM C4500F (D0BN-01), Document Feeder DF3120 - RICOH IM C4500F (D0BN-01), Platen Cover PN2000 - RICOH IM C5500 (D0BP-00), FAX Unit Type M38, Document Feeder DF3110 - RICOH IM C6000F (D0BQ-01)

Configuration Item	Detail
Client Computer	OS: Windows 8.1/10 Web browser: Internet Explorer 11, Microsoft Edge 44 Printer driver: RPCS Driver 1.3.0.0 FAX driver: PC Fax Generic Driver 9.4.0.0
Mail Server (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
Telephone Switchboard Simulator	XF-A150 (Panasonic Corporation)
Fax Machine	MP C6503

The TOE items tested by the developer are part of the multiple models included in the TOE. The evaluator judged that the security functions of the all TOE models could be deemed to have been tested by testing the representative models considering differences in printing speed and options.

Therefore, the evaluator judged that 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 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 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 TSFs and TSFIs.
   - The testing items are selected to cover the different testing approaches and testing environments.

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, 21 items for the independent testing and 19 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, the access control, etc. are as specified under the changed conditions. - Confirm that the input character limit and display customisation of the Operation Panel are as specified. - Confirm that the disabled functions and interfaces are actually disabled. - Confirm that the IPsec processing with expired certificates is as specified. - Confirm that the behaviour of the fax function is as specified when an error occurs in the fax function and when the transmission standby queue is full.
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 shows key tools used in the penetration testing.

Table 7-3 Penetration Testing Tools

Name (Version)	Outline
ZAP (2.7.0)	Inspection tool of Web vulnerabilities with Proxy traffic
nmap (7.70)	Port Scanning Tool
Netcat (1.12)	Packet Communication Tool
Nessus (8.8.0) Plugin 202105130021	Vulnerability Scanning Tool
Burp Suite Professional (1.7.37)	Inspection tool of Web vulnerabilities with Proxy traffic

Name (Version)	Outline
Wireshark (2.2.5, 3.0.11)	Packet Capture Tool
OpenSSL (1.0.1j)	Software library that provides the SSL/TLS protocol
PRET (0.40)	PJL and PostScript test tools
Android Debug Bridge (1.0.41)	Debugging tool for Android OS devices. (Used for the TOE components operated by Android OS.)

<Content of the Performed Penetration Testing>

Table 7-4 shows 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	Confirmed that the unexpected available interfaces were not exist by using the port scanning tool, the vulnerability scanning tool, and debug tool.
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. Checked no implementation-specific vulnerabilities regarding PJL, PostScript, and SQL.
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 insufficient resources.

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 enable the security functions of the TOE and use them securely, 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

Based on the evidence submitted by the Evaluation Facility during the evaluation process, the Certification Body has performed certification by checking that the following requirements are satisfied:

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

2. Contents pointed out in the Observation Reports 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.

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, Observation Reports 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

Any influences on the security functions of the 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 "4.2 Environmental Assumptions" and "7.5 Evaluated Configuration" and to see whether or not the evaluated scope of the TOE and the operational requirements can be handled in the actual operating environment of the TOE.

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 C6000/C5500/C4500 Security Target, Version 2.02, August 2, 2021, 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.

ARDF	An abbreviation of Automatic Reversing Document Feeder; Auto Document Feeder equipped with Auto Reverse Document Feeder.
HDD	An abbreviation of Hard Disk Drive; in this document, it indicates the HDD installed in the TOE if simply described as "HDD."
IPsec	Security 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.
SPDF	An abbreviation of Single Pass Document Feeder; Auto Document Feeder equipped with one-pass duplex scanning ADF.

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

Internet Fax	A function to perform fax communications with the system of sending or receiving e-mails. It also uses the Internet lines.
IP-Fax	A generic term of Realtime-Internet Fax of RICOH, conformant with the International Standard ITU-T T.38. It assigns IP address to a fax that is connected to a telephone line, instead of Fax number.
Maintenance Function	A function to perform maintenance service for machine malfunctions. In the operation of the TOE, the Service Mode Lock Function is set to "ON" for deactivating this function.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, July 2018, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, September 2018, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, September 2018, 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 C6000/C5500/C4500 Security Target, Version 2.02, August 2, 2021, RICOH COMPANY, LTD.

[13] RICOH IM C6000/C5500/C4500 Evaluation Technical Report, Version 1.1, August 4, 2021, 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