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)	2019-07-16 (ITC-9718)
Certification Identification	JISEC-C0670
Product Name	KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517
Version and Release Numbers	G00-45
Product Manufacturer	KONICA MINOLTA, INC.
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile Conformance	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)
Name of IT Security Evaluation Facility	Mizuho Information & Research Institute, Inc. Information Security Evaluation Section, Multimedia Technology Team, Information and Communication Research Division

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

2020-03-17

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

"KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517, Version G00-45" 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 "KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517, Version G00-45" (hereinafter referred to as the "TOE") developed by KONICA MINOLTA, INC., and the evaluation of the TOE was completed on 2020-03 by Mizuho Information & Research Institute, Inc., Information Security Evaluation Section, Multimedia Technology Team, Information and Communication Research Division (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, KONICA MINOLTA, INC., and provide security information to procurement entities and consumers who are interested in the TOE.

Readers of this 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 below. 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").

Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015
(Certification Identification: JISEC-C0553)

1.1.2 TOE and Security Functionality

The TOE is a Multi-Function Printer (hereinafter referred to as "MFP"), which has functions such as copy, scan, print, fax, and document storage and retrieval.

The TOE provides security functions required by the Conformance PP to prevent the data processed by the MFP from unauthorized disclosure and alteration.

For these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance requirements of the Conformance PP.

Threats and assumptions assumed for the TOE are described in the following sections.

1.1.2.1 Threats

The TOE assumes the following threats.

There are threats that user document data and data affecting security functions, which are assets to be protected by the TOE, may be disclosed or altered by unauthorized operation of the TOE or unauthorized access to the network to which the TOE is connected.

There are also threats that security functions of the TOE may be compromised by the failure of the TOE itself or installation of unauthorized software.

1.1.2.2 Configuration and Assumptions

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

The TOE is assumed to be operated in an environment where unauthorized physical access to the TOE is restricted and connected to a LAN protected from the Internet.

The maintenance and management of the TOE during operation must be appropriately performed in accordance with the guidance documents by an administrator trusted by the procurement entities. Also, TOE users must be trained to use the TOE securely.

1.1.3 Disclaimers

In this evaluation, the following operations are outside the scope of assurance.

- Operations under not secure operating environment of TOE described in "4.3 Clarification of Scope"
- TOE operations under conditions other than those described in "7.5 Evaluated Configuration"

The following is not ensured by this evaluation.

- Encryption of user document data etc. stored in this TOE.

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 2020-03, based on functional requirements and assurance requirements of the TOE according to the publicized 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 those concerns pointed out by the Certification Body 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: KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517

TOE Version: G00-45

The TOE components and the identification information are shown in Table 2-1.

Table 2-1 TOE Components

Component	Identification Information
MFP body	- Name: KONICA MINOLTA bizhub C4050i, KONICA MINOLTA bizhub C3350i, DEVELOP ineo+ 4050i, DEVELOP ineo+ 3350i - Version: G00-45
FAX kit (FK-517)	- AA1K

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

Users confirm the following information displayed on the MFP body and FAX kit as described in the guidance document.

- MFP body
  - Name:
    The model number of the label attached to the MFP unit must be one of the names of the identification information of "MFP body" in Table 2-1.
  - Version:
    The version displayed on the operation panel must match the version of the identification information of "MFP body" in Table 2-1.

- FAX kit
  The stamp on the FA kit must be match the identification information of "FAX kit (FK-517) " in Table 2-1.

3. Security Policy

The TOE provides MFP basic functions such as copy, scan, print, fax, and document storage and retrieval functions. The TOE also has the functionalities to store the user document data in the TOE, and to transfer them from/to user terminals and various servers via the network.

The TOE provides the following security functions that satisfy the requirements of the Conformance PP.

1) Identification and Authentication function
2) Access control function
3) Encryption function
4) Trusted communication function
5) Security management function
6) Audit function
7) Trusted operation function
8) FAX separation function

Details of the security functions of the TOE are described in Section 5.1.

Details of user roles, assets, threats and organizational security policies assumed for the TOE are described in Section 3.1 to 3.4.

3.1 Users

For use of the TOE, users shown in Table 3-1 are assumed.

Table 3-1 User Roles

Designation		Definition
U.USER (Authorized user)		Any identified and authenticated User.
	U.NORMAL (Normal User)	A User who has been identified and authenticated and does not have an administrative role
	U.ADMIN (Administrator)	A User who has been identified and authenticated and has an administrative role

3.2 Assets

Assets to be protected by the TOE can be classified into two categories shown in Table 3-2 below. Two categories of assets are composed of two more types of assets, as shown in Table 3-3 for user data and Table 3-4 for TSF data.

Table 3-2 Assets

Designation	Category	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

Table 3-3 Assets (User Data)

Designation	Type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job

Table 3-4 Assets (TSF Data)

Designation	Type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.3 Threats

The TOE assumes the threats shown in Table 3-5.

Table 3-5 Threats

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4 Organizational Security Policies

The organizational security policies required for the TOE are shown in Table 3-6.

Table 3-6 Organizational Security Policies

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

*) P.STRAGE_ENCRYPTION of the Conformance PP is not applicable to the TOE, because the storage device of the TOE is not field replaceable.

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

Table 4-1 Assumptions

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4.2 Environmental Assumptions

The TOE is installed in an office and connected to the public telephone line and a LAN which is the internal network of the organization, and it is used with a client PC and various servers connected to the LAN. The general operational environment of the TOE is shown in Figure 4-1.

Users use the TOE by operating the operation panel of the TOE or the PC connected to the LAN.

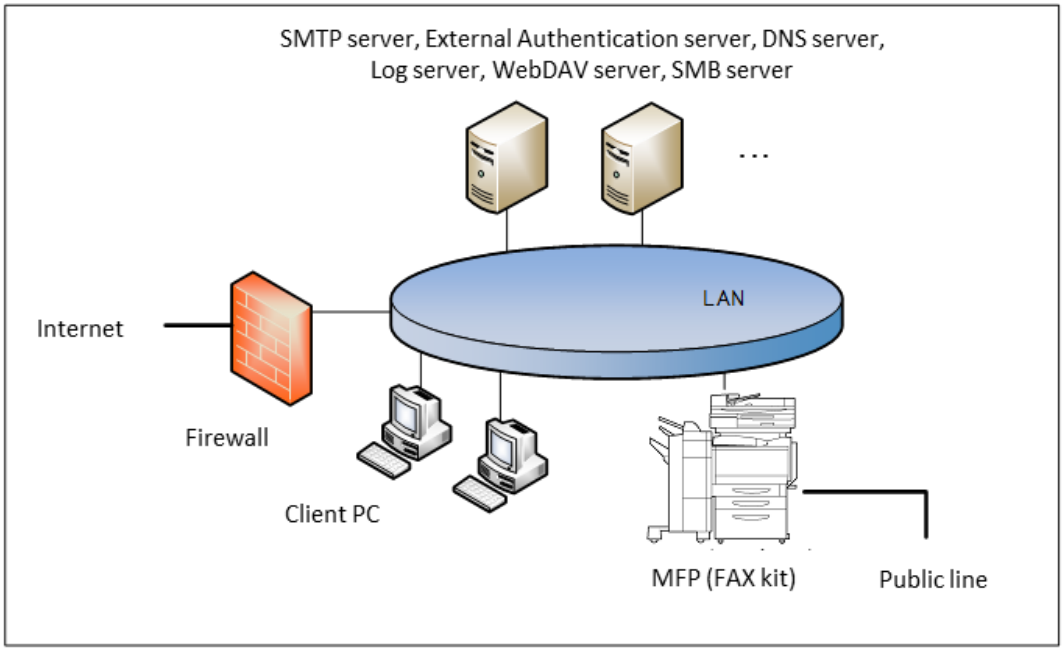

Figure 4-1 Operational Environment of the TOE

The components of the TOE operational environment are as follows.

1) Log server

A server to store the audit log generated by the TOE. Installation of this server is required.

Software that supports the WebDAV protocol is required. In this evaluation, IIS 8.0 included in OS: Microsoft Windows Server 2012 R2 Standard was used.

2) External Authentication server

A server to identify and authenticate TOE users. This server is required when operating with the external server authentication method. In this evaluation, Active Directory installed on Microsoft Windows Server 2012 R2 Standard was used.

3) DNS server

A server to convert domain name to IP address. In this evaluation, Active Directory installed on Microsoft Windows Server 2012 R2 Standard was used.

4) SMTP server, WebDAV server, SMB server

A server to store the data sent from the TOE. The data are the scanned data, or the electronic documents stored in the TOE.

The following was used in this evaluation.

- SMTP server: Black Jumbo Dos Ver. 5.9.5
- WebDAV server: IIS 8.0 included in Microsoft Windows Server 2012 R2 Standard
- SMB server: File sharing by Microsoft Windows Server 2012 R2 Standard

5) Client PC

A general PC used by users.

The following software are required for use of the TOE.

- Printer driver: KONICA MINOLTA C4050i Series PCL/PS
- Web browser: Microsoft Internet Explorer 11

It should be noted that the reliability of the hardware and the cooperating software shown in this configuration is outside the scope of this evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

In the TOE, a server such as an external authentication server may be installed in addition to the log server that must be installed. Also, a firewall is required to connect to the internet which is an external network. It is the operator's responsibility to operate these severs and firewalls securely.

The encryption function of the TOE is used for encrypting the communication data. The encryption of the data stored in the TOE is not included.

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 beige-colored area surrounded by the frame in Figure 5-1 is the TOE. User(U.USER), log server, external authentication server, DNS server, SMTP server, WebDAV server, SMB server, client PC and FAX are not included.

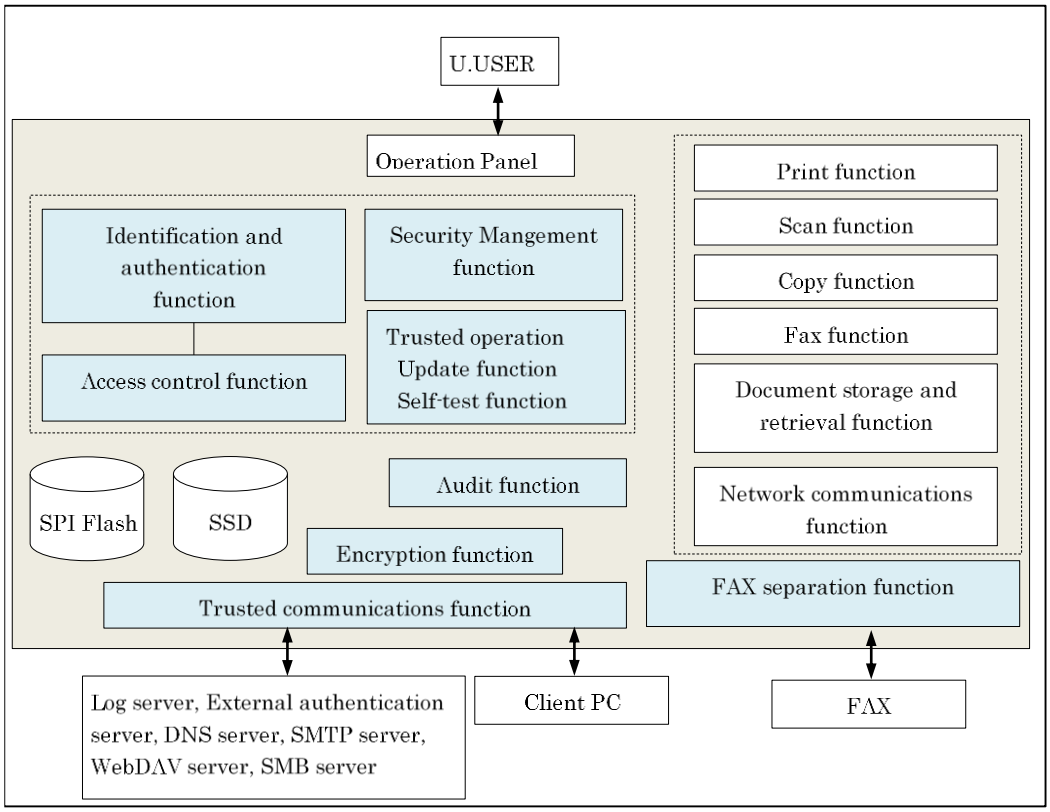

Figure 5-1 TOE boundary

Note that the user document data, etc. is stored in the SSD, but it cannot be removed by the SSD alone. Therefore, it does not correspond to "Field replaceable non-volatile storage device" of the Conformance PP.

The functions of the TOE consist of security functions (shaded square box in Figure 5-1) and basic functions (white square box).

The security functions are described below. Refer to Chapter 11 for the basic functions.

5.1.1 Security Functions

1) Identification and authentication function

This function identifies and authenticates the TOE user by the user login name and password, in the operation panel, Web browser and printer driver of the client PC.

- Requires a password consisting of uppercase letters, lowercase letters, numbers, and special characters, that are longer than the number of characters set by the administrator.

- Supports "MFP authentication method" that uses user information stored in the TOE and "External server authentication method" that uses an external authentication server.

- When entering a password, display dummy characters instead of the entered characters.

- In the MFP authentication method, if the password authentication fails the number of times specified by the administrator, the user is locked out. The lockout can be released by an administrator who is not in the lockout state.

- Terminate the session if the user does not operate for the time set by the administrator after identification and authentication, in the operation panel and the Web browser of the client PC.

2) Access control function

This function controls the access to the user data when operating the user data with the TOE basic functions.

- Access control is performed based on the owner information of user data and identification information and roles of user.

3) Encryption function

This function encrypts assets on the LAN when TOE communicates with the client PC and log server etc.

- Encryption key is stored on the RAM (volatile memory) and SSD.

4) Trusted communication function

This function assures the communication is performed with known terminal.

- Protects by verifying the validity of the connection destination and encrypting the assets on the network by the "3) encryption function", when communicating with log server, external authentication server, DNS server, SMTP server, WebDAV server, SMB server and client PC.

5) Security management function

This function restricts the setting of the security function to system administrator. Normal user can change own password.

6) Audit function

This function records the log of events related to the use of the TOE and security with the time of events occurrence, etc. as a log file, and provides it in the auditable format.

- The log file is sent to the log serer using "4) Trusted communication function" and can be viewed from the log server. Log files are stored in the TOE until the transmission to

the log server is successful.

7) Trusted operation function

This function verifies the authenticity of the firmware to be updated and confirm that it is the legitimate one before starting the firmware update of the TOE and perform the self-test.

8) FAX separation function

This function prevents that the TOE fax I/F is used to create the network bridge between the PSTN and the network that the TOE is connected.

5.2 IT Environment

The TOE communicates with various servers and client PCs via the LAN.

The TOE sends the generated audit data to the log server. The administrator reads the audit data from the log server.

The TOE identifies and authenticates users by using the external authentication server in case of the external server authentication method.

The TOE can store the scanned user document data in the WebDAV server and the SMB server, or send them by e-mail using the SMTP server.

6. Documentation

The identification of the guidance 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 Attached Documents

Type	Name	Version	Language
FULL	bizhub C4050i User's Guide	1.00	Japanese
	bizhub C4050i/C3350i User's Guide	1.00	English
	ineo+ 4050i/3350i User's Guide	1.00	English
Security Functions	bizhub C4050i User's Guide Security Functions	1.02	Japanese
	bizhub C4050i/C3350i User's Guide [Security Operations]	1.02	English
	ineo+ 4050i/3350i User's Guide [Security Operations]	1.02	English

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Mizuho Information & Research Institute, Inc., Information Security Evaluation Section, Multimedia Technology Team, Information and Communication Research Division 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

The evaluation was conducted in accordance with the assurance requirements in the CC Part 3 required by the Conformance PP using the evaluation methods prescribed in the CEM and the assurance activities of the Conformance PP.

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 for each work unit in the CEM and assurance activity of the Conformance PP.

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 2019-07 and concluded upon completion of the Evaluation Technical Report dated 2020-03. 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. Furthermore, the evaluators conducted the evaluator testing at the Evaluation Facility and the developer site in 2019-07 to 2020-02.

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

7.4 IT Product Testing

As the verification results of the evidence shown in the evaluation process, the evaluators performed the evaluator independent testing to ensure that the security functions of the product are accurately implemented, and the evaluator penetration testing based on the vulnerability assessments.

7.4.1 Developer Testing

The developer testing is not included in the assurance requirements of this evaluation.

7.4.2 Evaluator Independent Testing

The evaluators performed the evaluator independent testing (hereinafter referred to as the "independent testing") based on the evidence shown in the evaluation process to ensure that the security functions of the product are accurately implemented. The independent testing performed by the evaluators is described below.

1) Independent Testing Environment

Configurations for the independent testing are based on the operational environment of the TOE shown in Figure 4-1, and the components are as shown in Table 7-1. Although there are differences in the following points, the evaluators evaluate that these configurations are also equivalent to the configuration identified in the ST, and there are no problems in confirming the functions of the TOE.

- A firewall does not exist in the testing environment, because it is installed to protect the TOE against unauthorized access from the external network and does not affect the operation of the TOE.

- Instead of the public telephone line, a telephone line pseudo-switch that can emulate the same fax communication protocol as the public telephone line is used.

- For some tests such as cryptographic tests, a developer interface is used to stimulate and observe the internal behavior of the TOE.

Table 7-1 Components for the Independent Testing

components	Description
TOE	KONICA MINOLTA bizhub C4050i/ bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ ineo+ 3350i with FK-517 Version: G00-45
Log server	- OS: Microsoft Windows Server 2012 R2 Standard - Log server software: IIS (included in OS)
External Authentication server	- OS: Microsoft Windows Server 2012 R2 Standard - Kerberos software: Active Directory (included in OS)
DNS server	- OS: Microsoft Windows Server 2012 R2 Standard - DNS server software: Microsoft DNS (included in OS)

SMTP server	- OS: Microsoft Windows Server 2012 R2 Standard - SMTP server software: Black Jumbo Dog 5.9.5
WebDAV server	- OS: Microsoft Windows Server 2012 R2 Standard - WebDAV server software: IIS (included in OS)
SMB server	- OS: Microsoft Windows Server 2012 R2 Standard - SMB server software: File sharing function (included in OS)
Client PC	- OS: Microsoft Windows7 Professional Service Pack1 - Web browser: Internet Explorer 11 - Printer Driver: KONICA MINOLTA C4050i Series PCL Ver. 1.1.28.0 PS Ver. 1.1.28.0

2) Summary of the Independent Testing

A summary of the independent testing performed by the evaluators are described below.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing devised by the evaluators based on the requirements of the Conformance PP and on the provided evaluation documentation are as follows.

<Viewpoints of the Independent Testing>

(1) Confirm security functions for each Security Functional Requirement (SFR).

(2) Confirm that the cryptographic implementation is correct.

b. Independent Testing Outline

An outline of the independent testing performed by the evaluators is as follows.

<Independent Testing Approach>
The behavior of the TOE external interfaces by inputting using the operation panel, the client PC, and the test tools was confirmed by following means.

- If the behavior can be confirmed from the external interfaces of the TOE, the external interfaces of the TOE are used.

- If the behavior cannot be confirmed from the external interfaces of the TOE, the developer interfaces, the network analyzer and the log investigation in the log server is used.

<Content of the Performed Independent Testing>
The evaluators performed 39 items of independent testing.

Table 7-2 shows contents of the independent testing corresponding to the viewpoints.

Table 7-2 Performed Independent Testing

Viewpoint	Outline of the Independent Testing
(1)	Confirmation of security function - Confirm that all security functions are as specified for each SFR by the test items created from the assurance activities of the Conformance PP or the specification of SFR.
(2)	Confirmation of cryptographic implementation - Confirm the implementation of the following cryptographic algorithm to be tested by using the developer interfaces of the TOE. - RSA (key generation, signature generation/verification) - AES-CBC-128, AES-CBC-256, AES-ECB-256 - SHA-1, SHA-256, SHA-384, SHA-512 - HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 - CTR_DRBG

c. Result

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

7.4.3 Evaluator Penetration Testing

The evaluators 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 evaluators is explained below.

1) Summary of the Penetration Testing

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

a. Vulnerability of Concern

The evaluators 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) There is a concern that known vulnerabilities may exist in the network service running on the TOE.

(2) There is a concern that known vulnerabilities such as XSS and bypassing the identification and authentication function by directly specifying the URL may exist in the Web interface of the TOE.

(3) There is a concern that manipulation of print job, buffer overflows or arbitrary code execution may occur due to unauthorized print data input to the TOE.

(4) There is a concern that the identification and authentication function may be bypassed by unauthorized input from the Web interface.

(5) There is a concern that Konica Minolta's remote diagnosis service may be abused due to unintended operation on the TOE.

b. Penetration Testing Outline

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

<Penetration Testing Environment>
The penetration testing was performed by adding the testing tools shown in Table 7-3 to the independent testing environment.

Table 7-3 Penetration Testing Tools

Tool Name	Outline and Purpose of Use
Vulnerability scan Tool Nessus 8.5.1	A tool used for detecting known vulnerabilities.
Web vulnerability scan tool OWASP ZAP 2.8.0	A tool used for detecting general vulnerabilities of Web.
Web application analyzing tool Fiddler 5.0. 20192.25091	A tool used for capture or publish communication data transmitted from or to Web application.
Printer security test tool PRET 0.40	A tool used for detecting vulnerabilities of print device using printer language.
TCP/UDP data communication tool nc 1.10	A tool used for detecting vulnerabilities of identification and authentication.
Penetration testing tool Metasploit Framework v5.0.2	A tool used for creating unauthorized print files.

<Content of the Performed Penetration Testing>
Table 7-4 shows contents of the penetration testing corresponding to the vulnerabilities of concern.

Table 7-4 Outline of the Penetration Testing

Vulnerability	Penetration Testing Outline
(1)	Confirm that the unexpected ports are not open and there are no known vulnerabilities on available ports by using the vulnerability scanning tool.
(2)	Confirm that there are no known vulnerabilities in the Web interface by using the Web vulnerability scan tool and the Web application analyzing tool.
(3)	Confirm that the unintended behavior does not occur by using print data of Postscript, PJL language, and PDF format, which are intended to cause unauthorized behavior.
(4)	Confirm that the character string entered in the identification and authentication function does not cause unauthorized behavior.
(5)	Confirm that unintended behavior does not occur for Konica Minolta's remote diagnosis service.

c. Result

In the penetration testing performed by the evaluators, the evaluators 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 evaluators had concluded that the TOE satisfies all work units prescribed in the CEM and all assurance activities in the Conformance PP as per the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance:

  Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015

  Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

  Guideline for Certification Application with HCD-PP Conformance [16]
  - Treatment regarding FCS_RBG_EXT.1 Test

- 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 required by the Conformance PP.

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1,
ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1,
ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in the 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 in the CEM and assurance activities of the Conformance PP shall be evaluated as presented in the Evaluation Technical Report.

2. Rationale of the evaluation verdict by the evaluators 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 and the assurance activities of the Conformance PP.

Concerns found in the certification process were prepared as the certification oversight reviews, and those 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 the assurance requirements required by the Conformance PP.

8.2 Recommendations

Procurement entities who are interested in the TOE are advised to refer to "4.3 Clarification of Scope" and "7.5 Evaluated Configuration" to make sure that the scope of the evaluation and the operational requirements of the TOE meet the operational conditions assumed by each user.

9. Annexes

There is no annex.

10. Security Target

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

Title:	KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 Security Target
Version:	2.00
Publication Date:	2020-02-27
Author:	KONICA MINOLTA, INC.

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
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
HMAC	Keyed-Hash Message Authentication Code
MFP	Multifunction Printer, Multifunction Peripheral
PSTN	Public Switched Telephone Network
SHA	Secure Hash Algorithm
SMB	Server Message Block
WebDAV	Web-based Distributed Authoring and Versioning
XSS	Cross Site Scripting

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

Copy function	A function to scan a paper document and print the scanned image by user's operation from the operation panel.
Document storage and retrieval function	A function to store electronic documents in Personal user box, Memory RX user box and Password Encrypted PDF user box or retrieve the stored electronic documents.
FAX function	A function to send and receive documents through the public switched telephone network (PSTN) by using standard facsimile protocol.
Field Replaceable (Unit)	The smallest subassembly that can be swapped in the field to repair a fault.
Hardcopy Device	A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, MFPs (multifunction peripherals), MFDs (multifunction devices), "all-in-ones" and other similar products.
Network communication function	A function to send and receive documents via local area network (LAN).
Print function	A function to store temporarily the print data received via LAN by using a printer driver of client PC or Web browser in the ID & Print user box or the password encrypted PDF user box and print.
Scan function	A function to scan a paper document by user's operation from operation panel and generates a document file, and sends (E-mail, WebDAV, SMB).
Assurance Activity	Evaluation work to be performed by an evaluator in order to conform to a PP. It is a supplement of the CEM. In the case of the Conformance PP [14], it is described in the Conformance PP.

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] KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 Security Target, Version 2.00, February 27, 2020, KONICA MINOLTA, INC.

[13] KONICA MINOLTA bizhub C4050i/bizhub C3350i with FK-517, DEVELOP ineo+ 4050i/ineo+ 3350i with FK-517 Evaluation Technical Report, Version 7, March 2, 2020, Mizuho Information & Research Institute, Inc. Information Security Evaluation Section, Multimedia Technology Team, Information and Communication Research Division

[14] Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)

[15] Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

[16] Guideline for Certification Application with HCD-PP Conformance, Version 1.6, August 1, 2019, Information-technology Promotion Agency, Japan