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)	2020-07-14 (ITC-0761)
Certification Identification	JISEC-C0713
Product Name	KONICA MINOLTA bizhub C287i/bizhub C257i/bizhub C227i with FK-513, DEVELOP ineo+ 287i/ineo+ 257i/ineo+ 227i with FK-513
Version and Release Numbers	G00-16
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	ECSEC Laboratory Inc., Evaluation Center

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

2021-03-10

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 C287i/bizhub C257i/bizhub C227i with FK-513, DEVELOP ineo+ 287i/ineo+ 257i/ineo+ 227i with FK-513, Version G00-16" 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 1
1.1 Product Overview 1
1.1.1 Protection Profile or Assurance Package 1
1.1.2 TOE and Security Functionality 1
1.1.2.1 Threats and Security Objectives 2
1.1.2.2 Configuration and Assumptions 2
1.1.3 Disclaimers 2
1.2 Conduct of Evaluation 3
1.3 Certification 3
2. Identification 4
3. Security Policy 5
3.1 Users 5
3.2 Assets 5
3.3 Threats 6
3.4 Organizational Security Policies 6
4. Assumptions and Clarification of Scope 8
4.1 Usage Assumptions 8
4.2 Environmental Assumptions 8
4.3 Clarification of Scope 11
5. Architectural Information 12
5.1 TOE Boundary and Components 12
5.2 IT Environment 14
6. Documentation 15
7. Evaluation conducted by Evaluation Facility and Results 16
7.1 Evaluation Facility 16
7.2 Evaluation Approach 16
7.3 Overview of Evaluation Activity 16
7.4 IT Product Testing 17
7.4.1 Developer Testing 17
7.4.2 Evaluator Independent Testing 17
7.4.3 Evaluator Penetration Testing 19
7.5 Evaluated Configuration 22
7.6 Evaluation Results 23
7.7 Evaluator Comments/Recommendations 23
8. Certification 24
8.1 Certification Result 24
8.2 Recommendations 24

9. Annexes 25
10. Security Target 25
11. Glossary 26
12. Bibliography 28

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "KONICA MINOLTA bizhub C287i/bizhub C257i/bizhub C227i with FK-513, DEVELOP ineo+ 287i/ineo+ 257i/ineo+ 227i with FK-513, Version G00-16" (hereinafter referred to as the "TOE") developed by KONICA MINOLTA, INC., and the evaluation of the TOE was completed on 2021-03-01 by ECSEC Laboratory Inc., Evaluation Center (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 document data processed by the MFP and the setting data etc. affecting security from unauthorized disclosure and alteration.

For these security functions, 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 and Security Objectives

The following threats are assumed for the TOE.

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.

The TOE provides security functions required by the Conformance PP such as identification and authentication, access control, encryption, and digital signature to counter these threats.

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 separated from the Internet.

The setting, administration and maintenance of the TOE must be performed in accordance with the guidance documents by a trusted administrator. Users of the TOE must have been trained in order to use the TOE securely.

1.1.3 Disclaimers

The following operation is not ensured by this evaluation:

- An environment different from that described in "4.2 Environmental Assumptions"
- TOE with settings different from those described in "7.5 Evaluated Configuration"

The following is not ensured by this evaluation.

- Encryption of user document data etc. stored in the 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 2021-03, 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 C287i/bizhub C257i/bizhub C227i with FK-513, DEVELOP ineo+ 287i/ineo+ 257i/ineo+ 227i with FK-513
TOE Version:	G00-16

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

Users confirm the following information of the model name and version of MFP body and the package of FAX kit as described in the guidance document.

- Model name: One of the following:

  (For Japan)
  KONICA MINOLTA bizhub C287i

  (For other countries)
  KONICA MINOLTA bizhub C287i
  KONICA MINOLTA bizhub C257i
  KONICA MINOLTA bizhub C227i
  DEVELOP ineo+ 287i
  DEVELOP ineo+ 257i
  DEVELOP ineo+ 227i

- Version: "ACM10Y0-F000-G00-16"

- FAX kit: Product name "FK-513", identification information "A879"

3. Security Policy

The TOE provides the basic functions of the MFP such as copy, scan, print, fax, and document storage and retrieval. The TOE also has the functionality to store the user document data in the TOE, and to communicate with user terminals and various servers via a network.

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

As the background of the security functions provided by the TOE, user roles, assets, threats, and organizational security policies assumed for the TOE are described in following Section 3.1 to 3.4. Details of the security functions of the TOE are described in Chapter 5.

3.1 Users

The user roles assumed for the TOE are shown in Table 3-1.

Table 3-1 User Roles

Designation	Definition
Normal User	A User who has been identified and authenticated and does not have an administrative role
Administrator	A User who has been identified and authenticated and has an administrative role

3.2 Assets

The assets assumed to be protected by the TOE are shown in Table 3-2, Table 3-3 and Table 3-4. There are two categories of the assets, User Data and TSF Data, as shown in Table 3-2. Furthermore, User Data is classified as shown in Table 3-3 and TSF Data is as shown in Table 3-4.

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 threats assumed for the TOE are 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

Figure 4-1 shows the operational environment assumed for the TOE. The TOE is installed in a general office and used in an environment connected to the public telephone line and a LAN which is the internal network of the organization. Users operate the operation panel of the TOE or a client PC connected to the LAN to use the TOE.

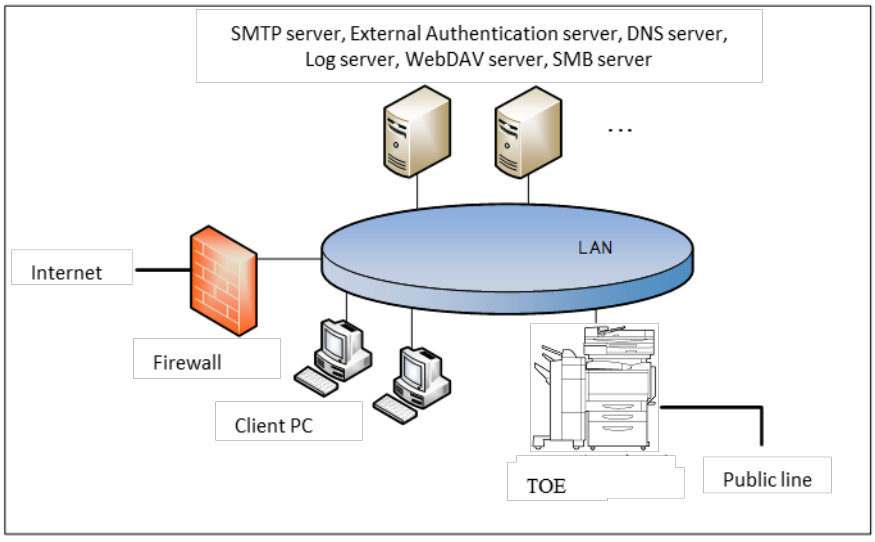

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following components.

1) Client PC

A client PC is a general-purpose PC for users. The following software is required:

- OS: Windows 10 Pro
- Software for IPsec: included in OS
- Web browser: Microsoft Internet Explorer 11
- Printer driver:
  KONICA MINOLTA C287iSeries PCL Version 2.2.2.0 PS Version 2.2.3.0

2) Log Server

A log server is a server to store the audit log generated by the TOE. Software that supports the WebDAV protocol is required. In this evaluation, the following software was used.

- Software for IPsec: strongswan 5.8.0
- Software for WebDAV: apache2 2.4.38

3) External Authentication Server

An external authentication server is a server to identify and authenticate TOE users. This server is required when operating with the external server authentication method. Software that supports the Kerberos is required. In this evaluation, the following software was used.

- OS: Microsoft Windows Server 2012 R2
- Software for IPsec: included in OS
- Software for Kerberos: included in OS (Active Directory)

4) DNS Server

A DNS server is a server to convert domain name to IP address. In this evaluation, the following software was used.

a) For External Authentication server method:
- Same as the external authentication server (Software for DNS is included in OS.)

b) For not External Authentication server method
- Software for IPsec: strongswan 5.8.0
- Software for DNS: bind9 9.11.5

5) SMTP Server, WebDAV Server, SMB Server

An SMTP server, WebDAV server or SMB server is a server to be used when sending the user document data scanned by the TOE or the user document data stored in the TOE by retrieving. The SMAP sever, WebDAV server or SMB server requires the software that supports SMTP, WebDAV or SMB protocol respectively. In this evaluation, the following software was used.

- Software for IPsec: strongswan 5.8.0
- Software for SMTP: Postfix 3.4.5
- Software for WebDAV: apache2 2.4.38

- Software for SMB: samba 4.9.5

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

4.3 Clarification of Scope

There are the following restrictions on the functions provided by the TOE or ensured by this evaluation.

1) Servers and client PCs

Administrators are responsible for operating servers and client PCs cooperating with the TOE securely.

2) Encryption function

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 TOE is the entire MFP with the necessary option.

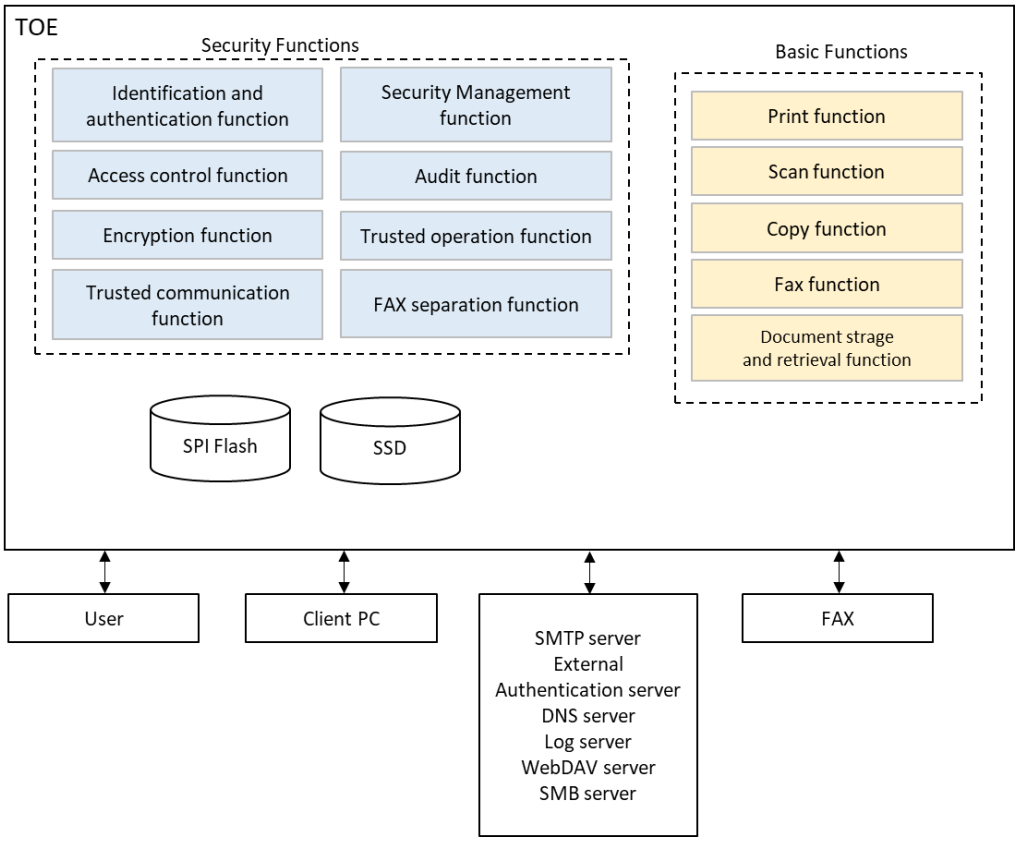

Figure 5-1 Composition of the TOE

Note that the user document data, etc. is stored in the SSD of the TOE, 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 provided by the TOE consist of basic functions and security functions. The security functions of the TOE are described below. Refer to Chapter 11 for the basic functions.

1) Identification and Authentication function

This function is a function to identify and authenticate users with their IDs and passwords, when users use the TOE from the operation panel of the MFP, or the Web browser or the printer driver of the client PC. There are two types of the authentication method: "MFP authentication method" that uses user information stored in the TOE and "External server authentication method" that uses an external authentication server.

This function has the following functionality to reinforce the identification and authentication.

- Restrict the minimum password length.

- Suspend the identification and authentication on continuous unsuccessful authentication attempts.

- Terminate the session if there is no operation for a certain time after the successful authentication.

2) Access Control function

This function is a function to control the access to the user data when users operate the basic functions of the MFP on them. The access control is performed based on the owner information of the user data and on the user's identification information and rights.

3) Encryption function

This function is a function to encrypt the communication data. The encryption of communication data is used in the encryption communication protocol described in "4) Trusted Communication function."

Encryption keys are generated using a random bit generator with enough entropy that is difficult to guess.

4) Trusted Communication function

This function is a function to protect communication data between the TOE and IT devices using encryption communication protocol (IPsec).

5) Security Management function

This function is a function to restrict the setting, etc. of the security functions to administrators. However, normal users can change their passwords.

6) Audit function

This function is a function to generate audit logs on audit events relevant to the security functions and send them to the log server.

7) Trusted Operation function

This function is a function to test the hash value of the firmware and the correct operation of the encryption function at start-up of the TOE, and to verify the digital signature of new firmware when the firmware is updated.

8) FAX Separation function

This function is a function to separate the Public Switched Telephone Network (PSTN) and the LAN. It prevents sending and receiving data from the PSTN to the LAN via the TOE.

5.2 IT Environment

The TOE communicates with servers and client PCs via LAN. The function of the TOE described in "4) Trusted Communication function" realizes IPsec communication in cooperation with those IT devices.

6. Documentation

The identification of the guidance documents of the TOE is listed in Table 6-1, Table 6-2 and Table 6-3. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

Table 6-1 Guidance for bizhub (Japanese)

Name[1]	Version
bizhub C287i User's Guide	1.00
bizhub C287i User's Guide Security Functions	1.02

Table 6-2 Guidance for bizhub (English)

Name	Version
bizhub C287i/C227i User's Guide	1.00
bizhub C257i User's Guide	1.00
bizhub C287i/C257i/C227i User's Guide [Security Operations]	1.02

Table 6-3 Guidance for ineo (English)

Name	Version
ineo+ 287i/227i User's Guide	1.00
ineo+ 257i User's Guide	1.00
ineo+ 287i/257i/227i User's Guide [Security Operations]	1.02

[1] The guidance name listed in Table 6-1 is the translation of Japanese name.

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

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 2020-07 and concluded upon completion of the Evaluation Technical Report dated 2021-03. 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 evaluator conducted the evaluator testing at the Evaluation Facility in 2020-08, 2020-10 and 2021-02.

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 evaluator performed the evaluator independent testing to ensure that the security functions of the product are accurately implemented, and the evaluator penetration testing based on vulnerability assessments.

7.4.1 Developer Testing

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

7.4.2 Evaluator Independent Testing

The evaluator 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 evaluator is described below.

1) Independent Testing Environment

The environment for the independent testing is based on the operational environment of the TOE shown in Figure 4-1. The components used in the independent testing environment are listed in Table 7-1.

Table 7-1 Components for the Independent Testing Environment

Components	Description
TOE	KONICA MINOLTA bizhub C287i with FK-513 Version G00-16 (Japanese) KONICA MINOLTA bizhub C257i with FK-513 Version G00-16 (English)
Client PC	- OS: Windows 10 Pro - Web browser: Internet Explorer 11 - Printer Driver: KONICA MINOLTA C287iSeries PCL Version 2.2.2.0 PS Version 2.2.3.0
External authentication server (DNS server)	- OS: Windows Server 2012R2
Servers	- OS: Kali Linux 2019.1 - IPsec: strongswan 5.8.0 - Log server: apache2 2.4.38 - DNS server: bind9 9.11.5 - SMTP server: postfix 3.4.5 - WebDAV server: apache2 2.4.38 - SMB server: samba 4.9.5

There are following differences between the configuration of the independent testing and the TOE configuration identified in the ST. The evaluator determined that there are no problems with those differences and that the security functions of the TOE configuration identified in the ST can be considered properly tested.

(1) Tested models

In the models of the TOE described in Chapter 2 "TOE identification", there are multiple models due to the following differences:

- Difference in brand name
- Difference in printing speed
- Difference in display language

The evaluator determined that the security functions of all the models of the TOE can be considered to have been tested by testing the representative two models considering the above differences, because the security functions of each models are the same. The models with different brand name are the same model except for the difference in name.

(2) Using additional testing tools

In the independent testing, some testing tools were used to confirm and alter the communication data and to confirm the encryption function. The validity of those testing tools was confirmed by the evaluator.

2) Summary of the Independent Testing

A summary of the independent testing performed by the evaluator is described below.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing devised by the evaluator 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 implementation of the cryptographic algorithms is correct.

b. Independent Testing Outline

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

<Independent Testing Approach>
The behavior of the TOE for inputs using the operation panel of the TOE, the client PC and the testing 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 (including audit logs).

- If the behavior cannot be confirmed from the external interfaces of the TOE, the developer interface of the TOE is used.

<Content of the Performed Independent Testing>
The evaluator performed the independent testing of 15 items.

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 functions> Confirm that all security functions work as the specification with the test items created based on the assurance activities of the Conformance PP for each SFR or the requirements of the SFR.
(2)	<Confirmation of implementation of cryptographic algorithms> Confirm the following cryptographic algorithms are implemented as the specification using the test program installed in the TOE. - RSA (key generation, signature verification) - AES-CBC-128, AES-CBC-256 - SHA-1, SHA-256, SHA-384, SHA-512 - HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 - CTR_DRBG (AES)

c. Result

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

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the 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 described below.

1) Summary of the Penetration Testing

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

a. Vulnerability of Concern

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

(1) There is a concern that unintended network ports of the TOE may be open, and known vulnerabilities may exist in the network services running on the TOE.

(2) There is a concern that known vulnerabilities may exist in the Web interface of the TOE.

(3) There is a concern that known vulnerabilities may exist in the print processing of the TOE.

b. Penetration Testing Outline

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

<Penetration Testing Environment>
The penetration testing was performed in the environment where tools for penetration testing are added to the independent testing environment. The tools used in the penetration testing are listed in Table 7-3.

Table 7-3 Penetration Testing Tools

Name	Outline and Purpose of Use
Nmap 7.80	A tool to detect available network service ports.
OWASP ZAP 2.8.0	A tool to detect known vulnerabilities in Web applications. The tool is also used to refer to and alter the communication data between Web browser and Web server (TOE).
PRET 0.35	A tool to inspect various vulnerabilities in print processing.

<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 unexpected network ports of the TOE are not open using Nmap. - Confirm that there are no known vulnerabilities by retrieving the name and version of software etc. used by the TOE using the developer interface.
(2)	- Confirm that there are no known vulnerabilities in the Web interface of the TOE using OWASP ZAP. - Confirm that the identification and authentication function and the access control function cannot be bypassed even if the data from Web browser to the TOE are altered using OWASP ZAP.
(3)	- Confirm that there are no known vulnerabilities in print processing of the TOE using PRET and exploit codes obtained on the Internet. - Confirm that unexpected behaviour is not observed even if the data that may cause unauthrised processing are input to the printer driver interface of the TOE.

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

7.6 Evaluation Results

The evaluator 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
  - Treatment regarding FCS_IPSEC_EXT.1.1

- 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 evaluator presented in the Evaluation Technical Report shall be adequate.

3. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM 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 "4.3 Clarification of Scope" and "7.5 Evaluated Configuration" to make sure the scope of the evaluation and the operational requirements of the TOE meet the operational conditions assumed by each user.

As described in Chapter 2, to confirm the TOE identification, it is necessary to check the information printed on the package of FAX kit in addition to the TOE display, etc. Note that it is necessary to keep the information of FAX kit package even after the start of the operation in order to confirm the TOE identification.

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 C287i/bizhub C257i/bizhub C227i with FK-513, DEVELOP ineo+ 287i/ineo+ 257i/ineo+ 227i with FK-513 Security Target
Version:	2.00
Publication Date:	February 25, 2021
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.

MFP	Multi-Function Printer
PSTN	Public Switched Telephone Network
SSD	Solid State Drive

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

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CTR_DRBG	Counter (CTR) mode block cipher algorithm DRBG
DRBG	Deterministic Random Bit Generator
HMAC	Keyed-Hash Message Authentication Code
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
WebDAV	Web-based Distributed Authoring and Versioning

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

Copy Function	A function to scan paper documents by the operation of the MFP operation panel and duplicate them.
Document storage and retrieval Function	A function to store user document data in the MFP and retrieve them. The document storage functionality can store the following user document data: - User document data that is scanned paper documents by the operation of the MFP operation panel. - User document data sent from the printer driver or the Web browser of the client PC. - User document data received by "Fax function." The document retrieval functionality enables the following operations to the stored user document data: - Operation of the MFP operation panel: print, send by "Fax function" or send to the SMTP server, WebDAV server or SMB server. - Operation of Web browser of the client PC: download or send to the SMTP server, WebDAV server or SMB server.
Fax Function (fax send, fax receive)	A function to send and receive fax data via Public Switched Telephone Network. Fax send functionality is to scan paper documents by the operation of the MFP operation panel and send the scanned user document data using the standard facsimile protocol. It is also possible to send the user document data stored in the MFP. Fax receive functionality is to receive user document data using the standard facsimile protocol and store them with "Document storage and retrieval function".
Print Function	A function to receive user document data sent from the printer driver or the web browser of the client PC, and then print out them by the operation of the MFP operation panel.
Scan Function	A function to scan paper documents by the operation of the MFP operation panel and send the scanned user document data to the SMTP server, WebDAV server or SMB server.
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 C287i/bizhub C257i/bizhub C227i with FK-513, DEVELOP ineo+ 287i/ineo+ 257i/ineo+ 227i with FK-513 Security Target, Version 2.00, February 25, 2021, KONICA MINOLTA, INC.

[13] KONICA MINOLTA bizhub C287i/bizhub C257i/bizhub C227i with FK-513, DEVELOP ineo+ 287i/ineo+ 257i/ineo+ 227i with FK-513 Evaluation Technical Report, Version 2.0, March 1, 2021, ECSEC Laboratory Inc., Evaluation Center

[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 1.7, July 1, 2020, Information-technology Promotion Agency, Japan, JISEC-CERT-2020-A17