Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2013-8-14 (ITC-3473)
Certification No.	C0455
Sponsor	KONICA MINOLTA, INC.
TOE Name	bizhub 754e / bizhub 654e / ineo 754e / ineo 654e
TOE Version	G00-60
PP Conformance	IEEE Std 2600.1™-2009
Assurance Package	EAL3 augmented with ALC_FLR.2
Developer	KONICA MINOLTA, INC.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Information Security Evaluation Office

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

2014-12-24

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

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

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

Evaluation Result: Pass

"bizhub 754e / bizhub 654e / ineo 754e / ineo 654e" 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 "bizhub 754e / bizhub 654e / ineo 754e / ineo 654e, Version G00-60" (hereinafter referred to as the "TOE") developed by KONICA MINOLTA, INC., and the evaluation of the TOE was finished on 2014-12-15 by Mizuho Information & Research Institute, Inc., Information Security Evaluation Office (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, KONICA MINOLTA, INC., and provide security information to procurement personnel and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is the appendix of this report together. 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 personnel who purchase this TOE" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

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

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a Multi-Function Printer (hereinafter referred to as "MFP") that offers basic functions such as Copy, Scan, Print, Fax, and Document storage and retrieval functions.

In addition to those MFP basic functions, the TOE provides security functions to prevent the document data used for the basic functions and the setting data relevant to security, from unauthorized disclosure and alteration.

Regarding these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated in the range of the assurance package. Threats and assumptions that this TOE assumes are described in the next clause.

1.1.2.1 Threats and Security Objectives

This TOE assumes the following threats and provides the security functions to counter them.

For protected assets such as the user's document data and the setting data relevant to security, there are threats of unauthorized disclosure and alteration caused by unauthorized operation of the TOE and by unauthorized access to the communication data on the network that the TOE is installed.

To counter those threats, this TOE provides the security functions, such as identification and authentication, access control, and encryption.

1.1.2.2 Configuration and Assumptions

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

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

1.1.3 Disclaimers

Operations and functions indicated below are not included in the assurance of this evaluation.

This TOE claims PP conformance including Fax function. The subject of this evaluation is the configuration that an optional FAX kit is installed in the MFP, which is the TOE. The configuration without Fax kit is not included in the assurance of this evaluation.

In this evaluation, only the configuration which applies the configuration conditions of "7.5 Evaluated Configuration" is evaluated as the TOE. The operations that the TOE is operated with these configuration conditions changed are not included in the assurance provided by this evaluation.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2014-12, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[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 evidential materials, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name: bizhub 754e / bizhub 654e / ineo 754e / ineo 654e

TOE Version: G00-60

Developer: KONICA MINOLTA, INC.

The TOE version is the generic term for the version of MFP board, SSD board, firmware and BIOS. Details of TOE identification are shown in Table 2-1.

Table 2-1 Details of TOE identification

Name (MFP name)	Version	
bizhub 754e, bizhub 654e, ineo 754e, ineo654e	MFP board	A55VH020-01
	SSD board	A161H02C-00
	Firmware	A55V0Y0-F000-G00-60
	BIOS	A55V0Y0-1E00-G00-10

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

The TOE name can be confirmed with the model name printed on the surface of the MFP body. The TOE version can be confirmed with the part number which is the version of MFP board and SSD board, and the version of firmware and BIOS which is displayed on the operation panel, by requesting to a service engineer.

3. Security Policy

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

The TOE provides MFP basic functions such as Copy, Scan, Print, Fax, and Document storage and retrieval functions. The TOE also has the functions to accumulate user's document data in the HDD of the TOE, and to transfer them to and from user's devices and various servers via the network.

When those functions are used, the TOE provides security functions that satisfy security functional requirements required by the Protection Profile for digital multi-function printers, IEEE Std 2600.1™-2009 [14] (hereinafter referred to as the "PP"). Security functions that the TOE provides include identification and authentication of users, access control, encryption of document data accumulated in the HDD, overwrite deletion at the time of deleting document data, and encrypted communication. Those functions prevent user's document data and setting data relevant to security, which are the protected assets, from unauthorized disclosure and alteration.

The TOE assumes the following user roles.

- Normal user
  A user of MFP basic functions, such as Copy, Scan, Print, Fax, and Document storage and retrieval functions, which are provided by the TOE.

- Administrator
  A TOE user who has special authority to configure the settings of the TOE security functions.

- TOE Owner
  A person or organization that has responsibility to protect the TOE assets and to realize security objectives of the TOE operational environment.

The protected assets of the TOE are also defined as follows.

- User Document Data
  Document data of users.

- User Function Data
  Document data of users and information relevant to jobs that are handled by the TOE. For this TOE, this includes various parameters for printing.

- TSF Confidential Data
  The data used by security functions, whose integrity and confidentiality are required. For this TOE, this includes login passwords, passwords for user boxes that store document data, encryption passphrase used for generating encryption key, and audit log.

- TSF Protected Data
  The data used by security functions, whose integrity only are required. For this TOE, this includes various setting values of security functions, such as user ID, user authority, and network settings, excluding TSF Confidential Data.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1, and to satisfy the organizational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functions to counter them. These threats are the same as the ones written in the PP.

Table 3-1 Assumed Threats

Identifier	Threat
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies. The details of each security function are described in Chapter 5.

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

These are the threats to user data (User Document Data and User Function Data). The TOE counters the threats with "Identification and authentication function," "User restriction control function," "Accumulated documents access control function," "Residual information deletion function" and "Network communication protection function."

"Identification and authentication function" of the TOE permits only the users who succeeded at the identification and authentication to use the TOE.

"User restriction control function" of the TOE checks the operation authority given to the users and permits only the authorized users to perform the basic functions, when

identified and authenticated users use the MFP basic functions such as Copy, Scan, Print, Fax, and Document storage and retrieval functions. In such cases, the access control to user data is also performed, and only those users who have the access authority to user data are permitted to access. However, the following "accumulated documents access control function" is applied to the document data accumulated in the user box.

"Accumulated documents access control function" of the TOE performs access control according to the types of user box and permits the operation only to the authorized users, when users operate the accumulated document data in the user box.

"Residual information deletion function" of the TOE prevents the residual information from being referred to by overwriting and deleting the HDD area where the document data were stored, when deleting the document data.

"Network communication protection function" of the TOE applies the encrypted communication protocol to encrypt the communication data, when the TOE communicates to client PC and various servers.

With the above functions, the TOE prevents the user data to be protected from unauthorized disclosure and alteration by unauthorized use of the TOE and unauthorized access to the communication data.

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

These are the threats to the data used for the security functions. The TOE counters the threats with "Identification and authentication function," "Security management function," and "Network communication protection function."

"Identification and authentication function" and "Security management function" of the TOE permit only the identified and authenticated administrators to set up, refer to, and change the data used for the security functions. However, normal users can change their own login passwords.

"Network communication protection function" of the TOE applies the encrypted communication protocol to encrypt the communication data, when the TOE communicates to client PC and various servers.

With the above functions, the TOE prevents the data to be protected from unauthorized disclosure and alteration by unauthorized use of the TOE and unauthorized access to the communication data.

3.1.2 Organizational Security Policies and Security Function Policies

3.1.2.1 Organizational Security Policies

Organizational security policies required in use of the TOE are shown in Table 3-2. These organizational security policies are the same as the ones written in the PP except for P.HDD.CRYPTO being added.

Table 3-2 Organizational Security Policies

Identifier	Organizational Security Policy
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.HDD.CRYPTO	The Data stored in an HDD must be encrypted to improve the secrecy.

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the following security functions to satisfy the organizational security policies shown in Table 3-2. The details of each security function are described in Chapter 5.

1) Means of the organizational security policy "P.USER.AUTHORIZATION"

The TOE implements this policy by "Identification and authentication function" and "User restriction control function."

"Identification and authentication function" of the TOE permits only the users who succeeded at the identification and authentication to use the TOE.

"User restriction control function" of the TOE checks the user authority given and permits only the identified and authorized users to perform the basic functions, when authenticated users use the MFP basic functions such as Copy, Scan, Print, Fax, and Document storage and retrieval functions.

2) Means of the organizational security policy "P.SOFTWARE.VERIFICATION"

The TOE implements this policy by "Self-test function."

"Self-test function" of the TOE verifies that the HDD encryption function, encryption passphrase and TSF executable code are normal at the time of startup.

3) Means of the organizational security policy "P.AUDIT.LOGGING"

The TOE implements this policy by "Audit log function."

"Audit log function" of the TOE records the events relevant to security functions as the audit log. Only the identified and authenticated administrators are permitted to read out and delete the audit log stored in the TOE. However, audit log cannot be modified.

4) Means of the organizational security policy "P.INTERFACE.MANAGEMENT"

The TOE implements this policy by "Identification and authentication function" and "External interface separation function."

"Identification and authentication function" of the TOE permits only the users who succeeded at the identification and authentication to use the TOE. It also terminates the session after a certain time of no operation by user.

In addition, "External interface separation function" of the TOE prevents the data received from the external interfaces of the TOE, from unauthorized transfer to LAN from the external interfaces, including the telephone line, by means of the TOE processing to mediate.

5) Means of the organizational security policy "P.HDD.CRYPTO"

The TOE implements this policy by "HDD encryption function."

"HDD encryption function" of the TOE encrypts the data stored in the HDD. Encryption algorithm is 256-bit AES.

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 the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. These assumptions are the same as the ones written in the 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	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 Environmental Assumptions

This TOE is installed in general offices and connected to the internal LAN, and it is used from the client PC connected to the internal LAN. The general operational environment of this TOE is shown in Figure 4-1.

Although not shown in Figure 4-1, the client PC can be connected via the USB port to the MFP, which is the TOE, and it is possible to use print function of the TOE.

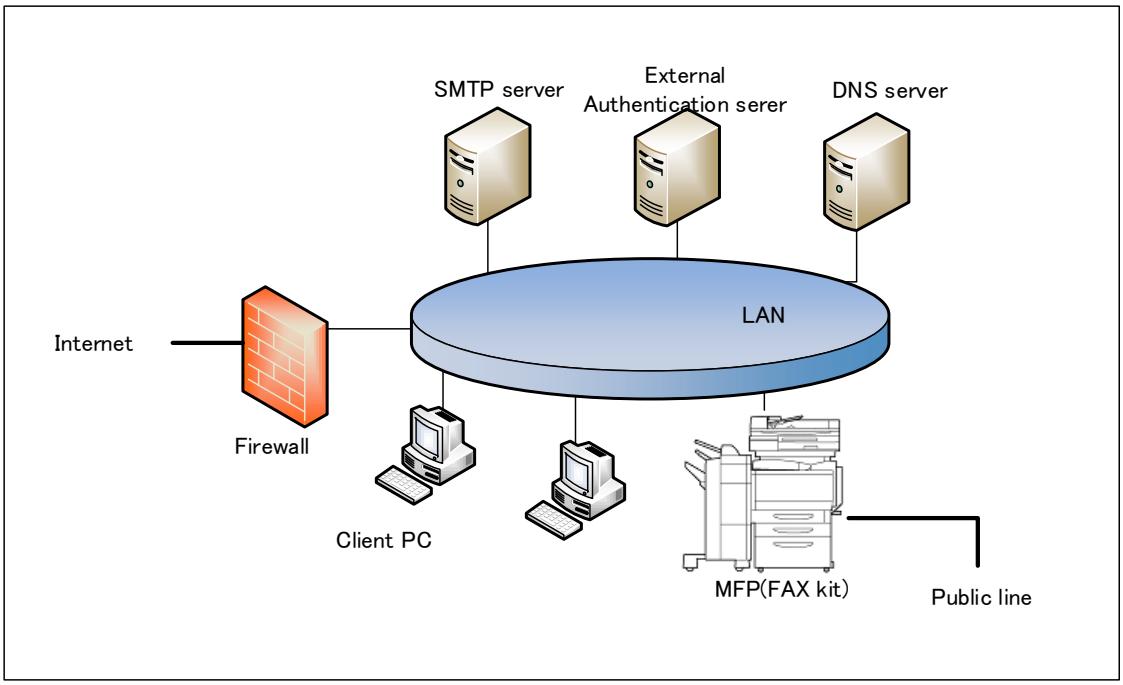

Figure 4-1 Operational environment of the TOE

The MFP is the TOE in Figure 4-1. However, Fax kit installed in the MFP is not included in the TOE. The following show the components other than the MFP, which is the TOE.

1) FAX kit

It performs the sending and receiving of fax data and the communication of the remote diagnostic function via the public line. The following option for the MFP is necessary.

- KONICA MINOLTA, INC. FK-511

2) Client PC

It is used for users to use the functions provided by the TOE via the LAN or USB port. The following software is necessary.

Table 4-2 Software of Client PC

Type	Name and version
Web browser	- Microsoft Internet Explorer 8
Printer driver	- KONICA MINOLTA 754 Series PCL Ver. 3.1.0.0, PS Ver. 3.1.0.0, XPS Ver. 3.1.0.0
Administrator's tool	- Data Administrator with Device Set-Up and Utilities Ver. 1.0.06000.03221 (plugin: Data Administrator 4.1.24000.05011)

3) SMTP server

It is necessary when using the function to send the document data in the TOE by e-mail.

4) External authentication sever

This server identifies and authenticates TOE users by Kerberos protocol. It is necessary when the external server authentication method is selected in the TOE setting. The following software is used in this evaluation.

- Active Directory installed in Microsoft Windows Server 2008 R2 Standard Service Pack 1

5) DNS server

This server converts domain name into IP address. The following software is used in this evaluation.

- Microsoft Windows Server 2003R2 Standard Edition Service Pack2

Note that the reliability of hardware and cooperative software other than the TOE shown in this configuration is outside the scope of this evaluation. (It is assumed to be trustworthy.)

4.3 Clarification of Scope

The TOE provides the function to print the document data stored in the USB flash drive connected to the TOE. Any user from the operation panel can access the document data stored in the USB flash drive. Measures of misplacing USB flash drive, etc., are users' responsibility.

The TOE has the function to terminate the session after a certain time of no operation by user in order to prevent user login status left unattended. On the operation panel of the TOE and the Web browser of the client PC, the value that administrator set is applied to the time to the session termination. However, the tools for administrator of the client PC have the fixed value of 60 minutes, and administrators need to pay attention since it is long.

5. Architectural Information

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

5.1 TOE Boundary and Components

Figure 5-1 shows the composition of the TOE. Fax kit is not included in the TOE.

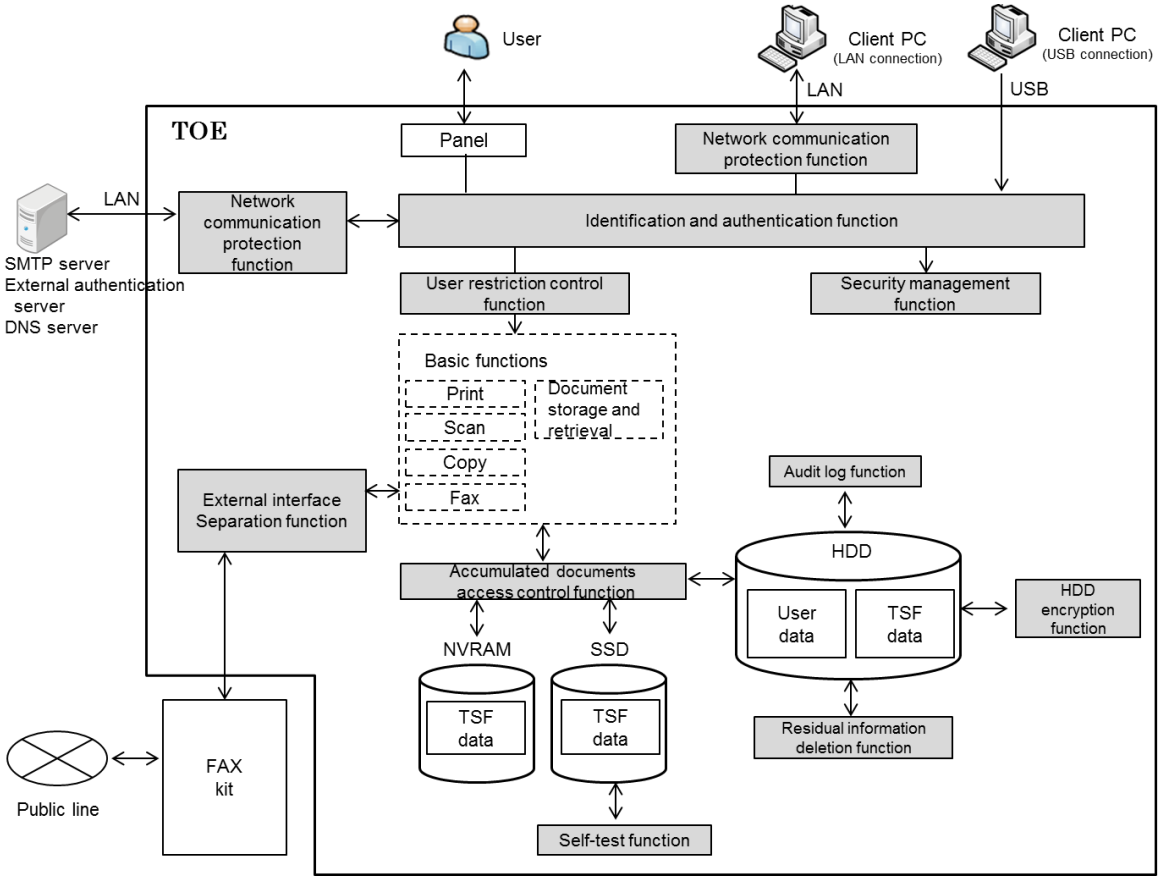

Figure 5-1 Composition of the TOE

The functions of the shaded box in Figure 5-1 are the security functions. TOE security functions are explained below.

1) Identification and authentication function

This function is the function to identify and authenticate TOE users by the user ID and login password. Identification and authentication are applied to all of the user interfaces shown below.

- Operation panel
- Client PC (Web browser, printer driver, various tools)

There are two kinds of authentication methods; "machine authentication" which uses the user ID and login password stored in the TOE, and "external server authentication" which uses Kerberos server outside of the TOE.

In addition, it has the following functions for strengthening identification and authentication function.

- Login passwords of 8 or more characters are required for the specified quality.

- Authentication is suspended when the number of continuous authentication failures reaches the administrator setting value.

- After identification and authentication, the session is terminated when no operation is performed for a certain period of time.

In case of the machine authentication, the quality check of login passwords is performed at the time of changing the setting of login passwords. In case of the external server authentication, it is performed at the time of login, and login is not permitted if the login password, which is registered in the external authentication server, does not satisfy the quality of the TOE.

2) User restriction control function

This function is the function to control the access to the operation of the identified and authenticated users and to the document data generated when using the TOE. However, the access control to the accumulated document data is performed with the "Accumulated document access control function."

When a user uses the MFP basic functions such as print, copy, scan, fax and document storage and retrieval functions, the authority that is set to the user is checked, and it permits the user to perform only the basic functions that have authority.

When a user performs operations such as printing and preview of document data, only the owner of the document data is permitted to perform the operations. When deleting document data, only the owner of the document data and administrators are permitted to delete.

If USB flash drive is connected to the TOE, only the users from the operation panel can access the document data stored in the USB flash drive. It cannot be accessed from the interfaces other than operation panel, like Web browser, etc.

3) Accumulated documents access control function

This function is the function to control the access at the time of retrieving the document data that are accumulated in the user box of the TOE, and it permits only the authorized users to retrieve document data.

The method of access control differs depending on the types of user box that the document data are stored. Either of the followings is used; a user ID and group ID given to the document data, a password set to the user box, or a password set to the document data, etc. That makes users who match the owner, common user, and password, permit the access.

The passwords of user box and document data are required for the specified quality of 8 or more characters at the time of setting, as is the case with the login password.

Note that administrators can delete all the document data accumulated in the user box.

4) Security management function

This function is the function to permit only the identified and authenticated administrators to set up, refer to, and change the data used for the security functions. However, normal users can change their own login passwords as well as the information such as passwords of user boxes permitted to access. The password that is set to the document data cannot be changed by any user including administrators.

5) Audit log function

This function is the function to record the audit events relevant to security functions as the audit log. Only the identified and authenticated administrators can download the audit log stored in the TOE to client PC and delete it. The audit log cannot be modified.

6) HDD encryption function

This function is the function to encrypt the data stored in the HDD. Encryption algorithm is 256-bit AES. An encryption key is generated by KONICA MINOLTA's proprietary algorithm based on the encryption passphrase of 20 characters that an administrator sets at the time of installation.

7) Residual information deletion function

This function is the function to overwrite and delete the HDD area that stores the document data at the time of deleting the document data. This function is performed at the following timing.

- When the MFP basic functions are terminated and the document data became unnecessary; this includes the data temporarily generated in the TOE because of the TOE process.

- When the document data are deleted by the user's command.

- When the power is turned on; in case the process of overwriting is not completed when the power is turned off, it restarts at the time of turning on the power.

The pattern of the data to overwrite can be selected from the multiple patterns by the administrator setting. In addition, there are a method to encrypt the overwrite data and write to the HDD, and a method not to encrypt the overwrite data and directly write to the HDD; this can be selected by the administrator setting.

8) Self-test function

This function is the function to perform the following self-tests at the time of the TOE start-up.

- Verification of the encryption passphrase and encryption function by the data for verifying that are installed in the TOE.

- Verification of the hash value of firmware.

9) Network communication protection function

This function is the function to perform the following encrypted communication on the communications with IT devices.

- Client PC: IPsec, TLS (v1.0, v1.1, v1.2)
- External authentication server: Kerberos v5
- SMTP server: IPsec
- DNS server: IPsec

10) External interface separation function

This function is the function to prevent unauthorized transfer to LAN from external interfaces, including the telephone line. The data received from the external interfaces of the TOE are processed with mediating by the TOE.

5.2 IT Environment

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

Fax function of the TOE performs the sending and receiving of fax data through FAX kit which is not included in the TOE. However, the security functions, such as access control and unauthorized access prevention related to fax function, are realized in the TOE.

6. Documentation

The identification of documents attached to the TOE is listed below. There are English and Japanese guidance documents for this TOE, and they are distributed depending on the sales areas.

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

< Japanese guidance >

- bizhub 754e / 654e User's Guide
  Ver. 1.00

- bizhub 754e / 654e User's Guide [Security Functions]
  Ver. 1.03

< English guidance >

- bizhub 754e / 654e User's Guide
  Ver.1.00

- bizhub 754e / 654e User's Guide [Security Operations]
  Ver.1.03

< English guidance >

- ineo 754e / 654e User's Guide
  Ver.1.00

- ineo 754e / 654e User's Guide [Security Operations]
  Ver.1.03

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Mizuho Information & Research Institute, Inc., Information Security Evaluation Office 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 is agreed on mutual recognition with ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of 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 has started on 2013-08 and concluded upon completion of the Evaluation Technical Report dated 2014-12. 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 directly visited the development and manufacturing sites on 2013-10, 2013-11, 2013-12, 2014-01, 2014-02 and 2014-04, and examined procedural status of configuration management, delivery, and development security by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2014-02, 2014-06 and 2014-11.

7.4 IT Product Testing

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

7.4.1 Developer Testing

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

1) Developer Testing Environment

Figure 7-1 shows the testing configuration performed by the developer.

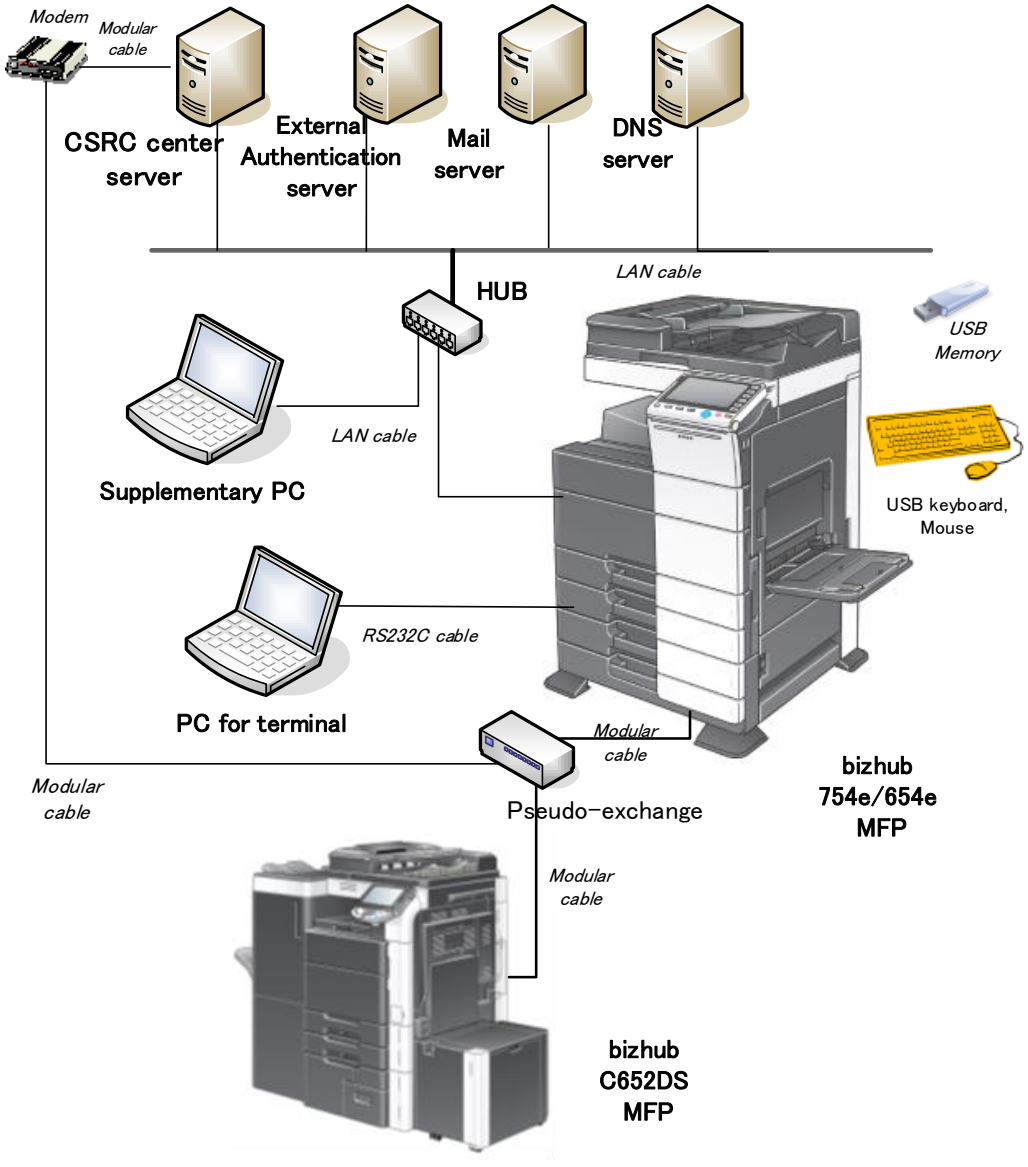

Figure 7-1 Configuration of the Developer Testing

Table 7-1 shows the components of the developer testing.

Table 7-1 Components of the Developer Testing

Name	Detail
MFP (TOE)	bizhub 754e, bizhub 654e (Version G00-60)
MFP built-in FAX kit	KONICA MINOLTA　FK-511
Supplementary PC (Client PC)	- Windows Vista SP2 PC (Web browser: Internet Explorer Ver.8) * Various drivers and tools shown in the above Table 4-2, are installed on the above PCs.
External Authentication Server	- Windows Server 2008 R2 Standard SP2 PC - Kerberos software: Active Directory (OS attached)
Mail server (SMTP server)	- Windows Server 2003R2 Standard SP2 PC - SMTP software: Black Jumbo Dog
DNS server	- Windows Server 2003R2 Standard SP2 PC - DNS software : OS attached
CSRC center server	A server to provide the same function as the remote diagnostic service of KONICA MINOLTA, INC. - Windows Server 2003R2 Standard SP2 PC - CSRC center software Ver.2.7.0
bizhub C652DS MFP	It is used as the other device of Fax TX/RX of the TOE.
Pseudo-exchange (public line)	Line-exchange to realize pseudo-public line - CE-97 by Neix, Inc.
USB memory (USB flash drive)	It is used to register the document data with the TOE - Sony USM1GJX, USM2GJ-3C
USB keyboard, mouse	The operation panel of the TOE can be used with the USB keyboard as an option, but not with the mouse. It is used for the tests of that function.
PC for terminal	It is connected with the interface for the TOE developer via RS232C. - Windows XP SP3 PC - Terminal software: Tera Term Pro Ver.4.29

The TOEs tested by the developer are all models of bizhub series among the TOE models. ineo series of the TOE are the same products as the bizhub series, which only names are different. It can be considered that the configuration of the developer testing includes all the identified TOEs.

The developer testing was performed in the same TOE testing environment as the TOE configuration identified in this ST.

2) Summary of the Developer Testing

A summary of the developer testing is described as follows.

a. Developer Testing Outline

An outline of the developer testing is described as follows.

<Developer Testing Approach>

For the external interfaces of the TOE, the developer confirmed its behavior by using the TOE operation panel, PC and the testing tools to input. The following approach was used for the confirmation of the behavior.

- For the behavior that can be checked by the interface provided by the TOE, the response to the input, the operation of the TOE, the audit log, and the communication data are checked by using the interface.

- For the data inside the TOE and the data on the HDD that cannot be checked by the interface provided by the TOE, those are checked by using the developer interface.

It is confirmed that the encryption algorithm is implemented to specification by comparing the data that were obtained by the above method, with the data encrypted by Open SSL. On the other hand, for the hash algorithm which is used for the self-test inside the TOE and for Web session information generation, it is confirmed that it is implemented to specification by reviewing the source codes.

<Developer Testing Tools>

Table 7-2 shows the tools used in the developer testing.

Table 7-2 Developer Testing Tools

Tool Name	Outline and Purpose of Use
Fiddler Ver.2.2.2.0	It mediates the communications between Web browser and Web server (TOE), and refers to and changes the communication data between them.
Open API testing tool Ver. 7.2.0.5	A testing tool for the Open API of KONICA MINOLTA, INC. Open API is the network interface of the TOE used by Data Administrator, which is the tool on the client PC.
SocketDebugger Ver. 1.12	The debug supporting tool for socket communications of TCP/IP. It is used for testing the network interfaces of the TOE.
Open SSL Ver.1.0.0d	It is used for testing SSL/TLS, encryption algorithm, and hash function.
Open SSL Ver.1.0.1e	It is used for testing TLS v1.2.
PC for terminal	By using the developer interfaces, it refers to the HDD data and the memory contents inside the TOE, such as encryption key.

Tool Name	Outline and Purpose of Use
WireShark Ver. 1.2.2	It monitors and analyzes the communication data on the LAN.

<Content of the Performed Developer Testing>

By operating MFP basic functions and security management functions with various interfaces, it was confirmed that the security functions applied to various input parameters perform to specification.

The variations of the input parameters include the rewrite of communication data between Web browser and the TOE, and power OFF/ON during the overwrite deletion. Also, it is confirmed that the number of authentication failures until the account is locked is totaled when using different interfaces.

Regarding the security functions, the cases where the behavior differs depending on the TOE settings, such as authentication method, IPv4, and IPv6, are also confirmed.

Note that the combination of the Web browser and the Windows of the supplementary PC, which is used by the developer as the client PC, does not support the TLS v1.2 protocol, but the developer used Open SSL for substituting the test of TLS v1.2.

b. Scope of the Performed Developer Testing

The developer testing was performed on 287 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. By the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

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

7.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by 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 ensure that security functions are certainly implemented from 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 environment of the independent testing performed by the evaluator is the same configuration as the developer testing shown in Figure 7-1 except for the following:

- Adding the inspection PC, which installs Windows 7 and Internet Explorer 8.

The independent testing was performed in the same environment with the TOE configuration identified in this ST.

The configuration and testing tools of the independent testing are those which used for the developer testing. Although those include the ones independently developed by the developer, their validity and operation tests were performed by the evaluator.

2) Summary of the Independent Testing

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

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluator designed from the developer testing and the provided evaluation evidential materials are shown below.

<Viewpoints of the Independent Testing>

(1) To confirm the behavior of the threshold limit value that is not tested by the developer.

(2) To confirm the behavior of combining the multiple interfaces and operations that are not tested by the developer.

(3) To confirm the variations of input data and operation environments to supplement the developer testing.

(4) In the sampling testing, to select the items of the developer testing from the following viewpoints:

- To confirm all the security functions and the external interfaces.
- To confirm all the different testing approaches, such as testing tools.
- To confirm the content of source code review performed by the developer.
- To confirm those which contribute to the vulnerability measures, such as the rewrite of the communication data.

b. Independent Testing Outline

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

<Independent Testing Approach>

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

<Independent Testing Tools>

The tools used at the independent testing are the same as those used at the developer testing.

<Content of the Performed Independent Testing>

The evaluator performed 49 items of sampling testing and 12 items of additional independent testing, based on the viewpoints of the independent testing.

Table 7-3 shows viewpoints of the independent testing and the content of the main tests corresponding to them.

Table 7-3 Viewpoints of Independent Testing Performed

Viewpoints of Independent Testing	Overview of Testing
Viewpoint (1)	- For login passwords, user box passwords, and encryption passphrases, confirm the behavior when inputting one long character string than the maximum number of characters at the time of changing.
Viewpoint (2)	- Confirm the behavior when changing the password of the public user box in a state where multiple users access the public user box. - Confirm that the access is controlled just like the changed multiple authorities when changing the multiple authorities of a user by one operation.
Viewpoint (3)	- Regarding the remote diagnostic function to use FAX data, confirm that the unauthorized data are denied if the data are different from the developer testing. - Confirm that TLS 1.2 protocol can be used properly, by using Internet Explorer 8 on Windows 7.

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 testing results.

7.4.3 Evaluator Penetration Testing

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

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is described 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 concern that known vulnerabilities may exist in the network interfaces.

(2) There is concern that known vulnerabilities may exist in the processing of print job command and the PDF files.

(3) If confidential information such as secret login accounts is included in the TOE, there is concern that it may be exploited.

(4) When the power of the TOE is turned off during the operation of the TOE from Web browser, there is concern that it may be exploited while keeping the authentication status.

(5) When the TOE is operated from USB keyboard, there is concern that the TOE may be exploited by interrupting the start-up process of the TOE.

(6) There is concern that the attacks, such as buffer over-flow or bypass of identification and authentication and of the access control, may succeed by transferring the unauthorized communication data to 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 same environment as the independent testing environment by installing the penetration testing tools in the inspection PC. Table 7-4 shows the tools used for the penetration testing.

Table 7-4 Penetration Testing Tools

Tool Name	Outline / Purpose
Nessus Version 5.2.5	Security scanner of various communication protocols. (The latest vulnerability database as of February 12, 2014, is referred.)
Nikto Version 2.1.5	Security scanner for the Web. (The latest vulnerability database as of October 28, 2013, is referred.)
nmap Version 6.40, 6.47	A tool for detecting available network port. * The evaluator used the ver. 6.40 for UDP and the ver. 6.47 for TCP, because of the difference in the performed timing of the tests.
Fiddler Version 2.4.5.9	Web debugger that mediates the communications between Web browser and Web server (TOE), and refers to and change the communication data between them. * The evaluator uses any of the three types of tools for the concerned test items.
TamperIE Version 1.0.1.13	
Burp Suite Version 1.5.0	
extrstr Version 0.2	A binary analysis tool developed by the Evaluation Facility. It is used for extracting character strings that are included in the binary files.

Metasploit Version 4.9.2	It is used for creating the inspection data for inspecting vulnerabilities in the PDF.

<List of the Performed Penetration Testing>

Table 7-5 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-5 Outline of the Penetration Testing

Vulnerabilities	Outline of Testing
Vulnerability (1)	- By performing nmap, Nessus, and Nikto to the TOE, it was confirmed that there is no known vulnerability.
Vulnerability (2)	- It was confirmed that the processing is not performed even if the print job command that can be exploited and the PDF files that include illegal processing are input to the TOE.
Vulnerability (3)	- By analyzing the binary that is stored in the updated media of the TOE using extrstr, it was confirmed that the secret character strings that can be exploited, such as secret login accounts, are not included.
Vulnerability (4)	- While operating the TOE by the TOE operation panel, Web browser on PC, and various tools, even if the power of the TOE is turned OFF/ON, it was confirmed that the authentication status is not maintained and the re-login is required to use.
Vulnerability (5)	- It was confirmed that there is no effect on the start-up process of the TOE even if USB keyboard is operated during the TOE start-up.
Vulnerability (6)	- It was confirmed that unexpected operations cannot be performed, such as bypass of the identification and authentication or access control, and the buffer over-flow, even if the communication data from Web browser to the TOE is altered by using Web debugger. - Regarding the individual interfaces besides the Web, the equivalent confirmation was performed by using the developer testing tools, as is the case with the Web.

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 assumptions of this evaluation, are described in the guidance documents shown in Chapter 6. TOE administrators need to activate the security functions of this TOE and to configure the TOE as described in the appropriate guidance documents for secure use. If these setting values are changed to the different values from those described in the guidance documents, such cases are not included in the assurance of this evaluation.

Among the configuration conditions of the TOE, in addition to the "Enhanced Security Setting" that configures secure values collectively to the various settings of the security functions, there are also setting values that need to configure individually. Note that the configuration conditions of the TOE also include those settings which prohibit the use of the functions provided by the TOE. For example, the following setting values are also included:

- Invalidation of Internet Fax function
- Invalidation of print protocol other than IPP
- Invalidation of SNMP
- Invalidation of TCPsocket
  (Notice: By this setting, a scanner driver for the client PC and tools such as Box Operator and HDD BackUp Utility cannot be used.)

The guidance also describes a method to restore the changed configuration to the evaluated configuration which is assured in this evaluation.

7.6 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance:

  2600.1, Protection Profile for Hardcopy Devices, Operational Environment A (IEEE Std 2600.1™-2009)

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

  - 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
  - 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
  - 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
  - 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
  - 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
  - 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

- 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 EAL3 package

- Additional assurance component ALC_FLR.2

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

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to consumers.

8. Certification

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

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

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

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

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report and related evaluation deliverables, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

It should be noted that the procurement personnel who are interested in this TOE need to refer to the descriptions of "1.1.3 Disclaimers," "4.3 Clarification of Scope," and "7.5 Evaluated Configuration" and to see whether or not the evaluated scope of this TOE and the operational requirements are consistent with the operational conditions that they assume.

In the print function of this TOE, the print data from the client PC is accumulated in the TOE, and it is necessary to be operated from the operation panel for printing on paper. However, the document data stored in the user box of the TOE can be printed on paper by the operation from the client PC. It should be noted that there is a possibility that it does not satisfy the needs of the procurement personnel who expect to restrict the printing on paper only from the operation panel in order to ensure the security of the output paper.

9. Annexes

There is no annex.

10. Security Target

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

bizhub 754e / bizhub 654e / ineo 754e / ineo 654e Security Target, Version 1.10, December 8, 2014, 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
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviation relating to the TOE used in this report is listed below.

MFP	Multi-Function Printer

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

Copy function:
A function to read paper documents and to print the copy by the operation of the operation panel.

Document storage and retrieval function:
A function to accumulate document data in the TOE and retrieve the accumulated document data.

Encryption passphrase:
A string of 20 characters used for generating the encryption key of HDD encryption.

Fax function:
Fax TX function is a function to send paper documents or the document data accumulated in the TOE to the external fax device via the telephone line. The transmission of the paper documents is operated from the operation panel, while the transmission of accumulated document data is operated from the operation panel and the Web browser of the client PC.
Fax RX function is a function to receive the document data via the telephone line from the external fax device. The received data are retrieved with the Document storage and retrieval function.

Print function:
A function to print the document data received by the TOE from the client PC via the LAN or USB interface. The received document data by the TOE is once accumulated in the TOE, and it is output with the command

from the operation panel.

Remote diagnostic function:

A function to connect to Konica Minolta support center via the public line for the maintenance of the MFP and to communicate the device information, such as MFP operation status and the number of printings, etc.

Scan function:

A function to read the paper documents and to generate the document data by the operation of the operation panel. The generated document data are retrieved with the Document storage and retrieval function.

User box:

A directory to accumulate document data in the TOE. There are several types of user box, such as personal user box and public user box, etc.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, March 2014, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, April 2014, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, April 2013, Information-technology Promotion Agency, Japan, CCM-03

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

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

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

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

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

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

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

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

[12] bizhub 754e / bizhub 654e / ineo 754e / ineo 654e Security Target Version 1.10, December 8, 2014, KONICA MINOLTA, INC.

[13] bizhub 754e / bizhub 654e / ineo 754e / ineo 654e Evaluation Technical Report, Version 3, December 15, 2014, Mizuho Information & Research Institute, Inc. Information Security Evaluation Office

[14] IEEE Std 2600.1™-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009