Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2015-03-09 (ITC-5538)
Certification No.	C0507
Sponsor	KONICA MINOLTA, INC.
TOE Name	bizhub C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS
TOE Version	G0607-999
PP Conformance	IEEE Std 2600.2™-2009
Assurance Package	EAL2 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.
2016-04-25

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 Document."

- 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 C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS" 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 C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS, Version G0607-999" (hereinafter referred to as the "TOE") developed by KONICA MINOLTA, INC., and the evaluation of the TOE was finished on 2016-03 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 entities 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 provided along with this report. 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 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 EAL2 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is a Multi-Function Printer (hereinafter referred to as the "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 scope 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, there are threats of unauthorized disclosure and alteration caused by unauthorized operation of the TOE.

For protected assets such as 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.

This TOE consists of MFP equipped with an optional FAX kit. The FAX kit is not included in the scope of the TOE.

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

The Protection Profile to which the TOE claims conformance does not include user's document data, which are protected assets of this TOE, in the scope of communication data protection on the network.

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 2016-03, 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] and the Observation Reports prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight review was also prepared for those concerns found in the certification process. 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 C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS
TOE Version:	G0607-999
Developer:	KONICA MINOLTA, INC.

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

Table 2-1 Details of the TOE Version

Name	Version	
bizhub C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS	MFP board	A3GNH010-07
	SSD board	A3GNM71A-01
	Firmware	A3GN30G0607-999

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 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 IEEE Std 2600.2™-2009 which is the Protection Profile for the MFP [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.

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.

- TSF Confidential Data
  The data used by security functions, whose integrity and confidentiality are required. For this TOE, this includes login passwords, 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 Section 3.1.1, and to satisfy the organizational security policies shown in Section 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_REST.DIS	User Document Data at rest (stored) in the TOE may be disclosed to unauthorized persons.
T.DOC_REST.ALT	User Document Data at rest (stored) in the TOE may be altered by unauthorized persons.
T.FUNC_REST.ALT	User Function Data at rest (stored) in the TOE 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.

1) Countermeasures against the threats "T.DOC_REST.DIS," "T.DOC_REST.ALT" and "T.FUNC_REST.ALT"

These are the threats of violation (leakage and falsification) to user data (User Document Data and User Function Data) by unauthorized access. The TOE counters the threats with the "Identification and authentication function," "User restriction control function," "Accumulated documents access control function," and "Residual information deletion function."

a. Identification and authentication function

This function of the TOE permits only the users who succeeded at the identification and authentication to use the TOE. The identification and authentication is adopted to all user interfaces of the followings:

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

The authentication methods include the "Device authentication" that uses user ID and login password stored in the TOE, and the "External server authentication" that uses the Kerberos server outside the TOE.

In addition, the following functions are equipped to reinforce the identification and authentication function:

- Login password is required to be 8 digits or more with a specific level of quality.
- If a wrong password is entered three times in a row, the authentication is suspended.
- When no operation is performed for a certain period of time after identification and authentication, the session is terminated.

A quality of login password for the Device authentication is checked when login password setting is changed. In case of the External server authentication, it is checked with logging in, while the login is not permitted when a password registered to the external authentication server does not meet the quality of the TOE.

b. User restriction control function

This is the function to control access for operation of the authorized user and to control access for document data which are generated with using the TOE. However, the access control for stored document data is performed with the "Stored documents access control function."

This 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 Print, Copy, Scan, Fax, and Document storage and retrieval functions.

In case of printing document data, only the owner of the document data is permitted to operate. In case of deleting document data, only the owner of the document data and the administrator are permitted to delete.

c. Stored documents access control function

This function of the TOE performs access control and permits the operation only to the authorized users, when users operate the accumulated document data in the HDD.

The permission for operation request from a user is controlled based on the attribute value such as user identification that is associated with each document data when it is stored on the HDD.

The administrator can delete all stored document data.

d. Residual information deletion function

This function prevents the residual information from being reused to by overwriting and deleting the HDD area where the document data were stored, when deleting the document data. This function is performed when:

- the basic function of the MFP is ended and the document data, including data which is temporarily created because of the TOE processing, become unnecessary,
- the document data are deleted at the direction of a user,

- the MFP is powered on (if the MFP is turned off before the overwrite deletion processing is completed, the processing is restarted when the MFP is powered on), and
- an administrator executes the deletion function of the whole data area on the HDD.

The data pattern for overwriting can be chosen from multiple patterns in the administrator settings.

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

These are the threats of violation (leakage and falsification) to the data used for the security functions by unauthorized access to the TOE and communication data on the network. The TOE counters the threats with the "Identification and authentication function," "Security management function," and "Network communication protection function."

a. Identification and authentication function

The identification and authentication function stated in 1) verifies whether a user who tries to use the TOE has the authority by using the identification and authentication information obtained from the user, and only the user who is judged as the authorized user is permitted to use the TOE.

b. Security management function

This function is to permit only identified and authenticated administrators to set, browse and change the data used for security functions. General users, however, can change only their own passwords.

c. Network communication protection function

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

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

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.

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

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

The "Identification and authentication function" and "User restriction control function" stated in Section 3.1.1.2 permit only the users who succeeded at the identification and authentication to use the TOE and check the user authority given and permit 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 the "Self-test function."

a. Self-test function

This function is to conduct the following self-tests at the time of startup.

- Verification of encryption passphrases by the TOE-embedded verification data
- Integrity verification of executable codes by checking hash values of the control software

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

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

a. Audit log function

When the audit events relevant to security occurred, this function generates and stores the audit log which consists of date the event occurred, identification information of the event, user identification and the result of the event. Only the identified and authenticated administrators are permitted to read out and delete the generated audit log.

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

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

a. Identification and authentication function

The “Identification and authentication function" stated in Section 3.1.1.2 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 users.

b. External interface separation function

This function is to prevent the data from unauthorized transfer to LAN from the external interfaces, including the telephone line. The TOE must mediate to process the data received from the external interfaces.

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

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

a. HDD encryption function

This function is to encrypt the data stored in the HDD. Encryption algorithm is 256-bit AES. The encryption key is generated by SHA-256 algorithm specified by FIPS180-3 based on 20-digits encryption passphrases set by administrators at the time of introduction.

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.

Incidentally, client PCs can connect to the MFP, which is the TOE, via USB port to use print function of the TOE although it is not shown in Figure 4-1.

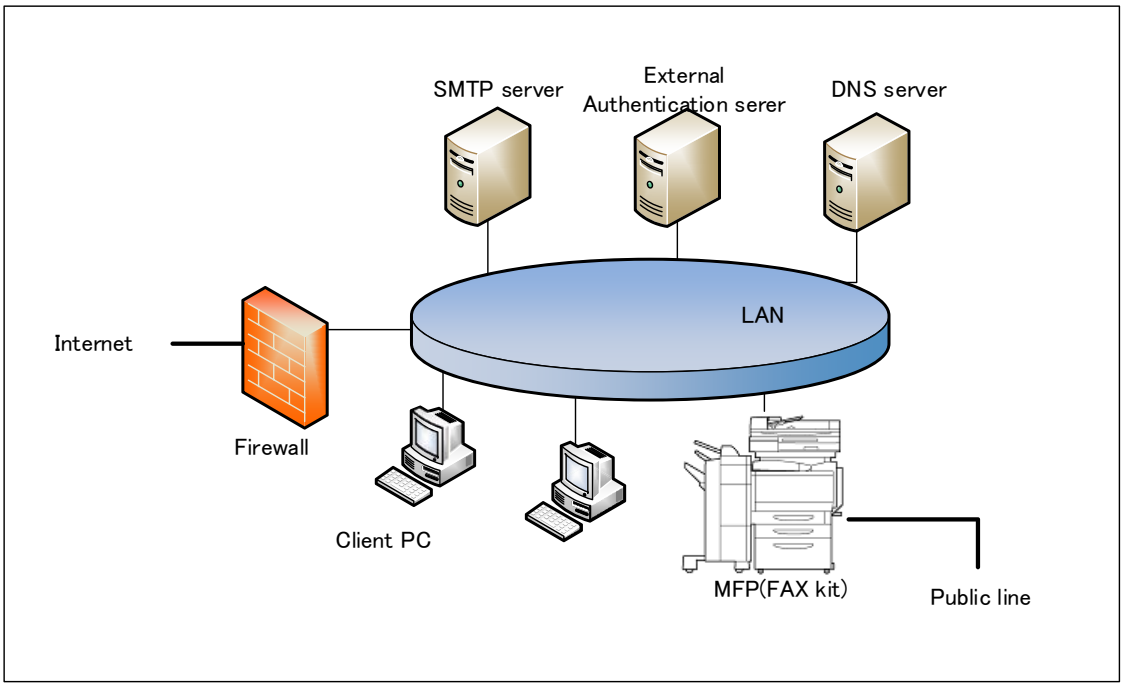

Figure 4-1 Operational environment of the TOE

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

1) FAX kit

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

- KONICA MINOLTA, INC. FK-512

2) Client PC

It is used for users to use the functions provided by the TOE via the LAN or USB port. The software listed in Table 4-2 is necessary.

Table 4-2 Software of Client PC

Type	Name and version
Web browser	- Microsoft Internet Explorer Ver.11 - Mozilla Firefox Ver.36
Printer driver	- KONICA MINOLTA C3850 Series PCL6 Ver. 3.0.1, XPS Ver. 3.0.2
Administrator's tool	- KONICA MINOLTA Data Administrator with Device Set-Up and Utilities Ver. 1.0.06000 - KONICA MINOLTA Data Administrator 4.1.35000)

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.

- DNS server installed in Microsoft Windows Server 2008 R2 Standard Service Pack1

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 scope of the TOE is the whole MFP. Although an optional FAX kit which provides FAX interface is equipped with the TOE, the FAX kit is out of the scope of the TOE.

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. The scope of the TOE is the whole MFP.

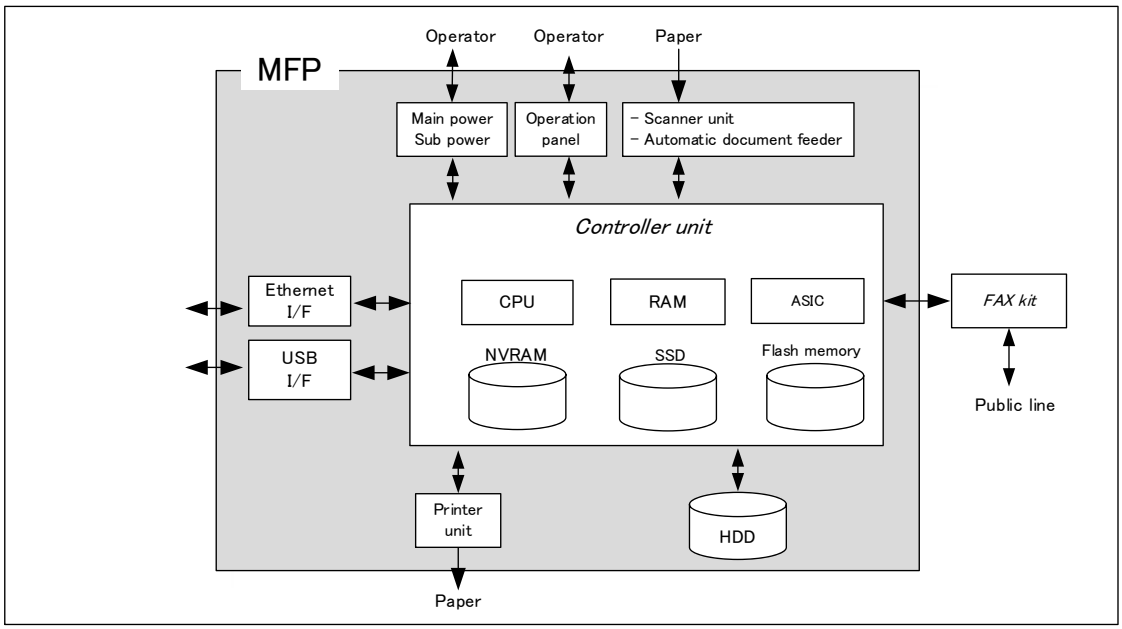

Figure 5-1 TOE boundary

The TOE, as shown in Figure 5-1, is the MFP composed of main/sub power, operation panel, scanner unit, automatic document feeder, MFP controller unit, printer unit and HDD. The overview of each component is described as follows:

(1) Main/sub power supply
Power switches for activating the MFP.

(2) Operation Panel
An exclusive control device for the operation of the MFP, equipped with a touch panel of a liquid crystal monitor, numeric keypad, start key, stop key, screen switch key, etc.

(3) Scan unit / Automatic document feeder
A device that scans images and photos from paper and converts them into digital data.

(4) MFP Controller unit
A device that controls the MFP.

(5) CPU
Central processing unit.

(6) RAM
A volatile memory used as the working area.

(7) ASIC
An integrated circuit that is designed for performing all image processing as well as performing processing of image expansion and color adjustment when printing images.

(8) NVRAM
A nonvolatile memory that stores TSF data that decide MFP action.

(9) SSD
A storage medium that stores the object code of control software, including message data in supporting languages displayed as responses for access from operation panel and network.

(10) Flash memory
A nonvolatile memory that stores the object code of the TOE (Boot controller).

(11) Printer unit
A device to actually print the image data which were converted for printing when receiving a print request from the MFP controller.

(12) HDD
A hard disk drive. This is used not only for storing electronic documents as files but also for working area.

(13) Ethernet I/F
Interface which supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet.

(14) USB I/F
Interface which can perform TOE update.

(15) FAX kit
A device that is used for fax data transmission and the communication of the remote diagnostic function via the public line. This is not included in 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.

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

6. Documentation

The identification of documents attached to the TOE is listed below. There are Japanese and 2 types of English guidance documents for the TOE, and they are distributed depending on the sales areas.

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

(Japanese)
- bizhub C3850 User's guide 2015.3 Ver. 1.00
- bizhub C3850 User's guide [Security Functions] 2.02

(English)
- bizhub C3850FS/C3850/C3350 user's Guide 2015.4 Ver. 1.00
- bizhub C3850FS/C3850/C3350 user's Guide [Security Operations] 2.02

(English)
- ineo+ 3850FS/3850/3350 User's Guide 2015.4 Ver. 1.00
- ineo+ 3850FS/3850/3350 User's Guide [Security Operations] 2.02

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 joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance 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 2015-02 and concluded upon completion of the Evaluation Technical Report dated 2016-03. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted.

Additionally, the evaluator directly visited the development and manufacturing sites on 2015-10 and examined procedural status conducted in relation to each work unit for configuration management and delivery 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 2016-01.

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

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

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As 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.

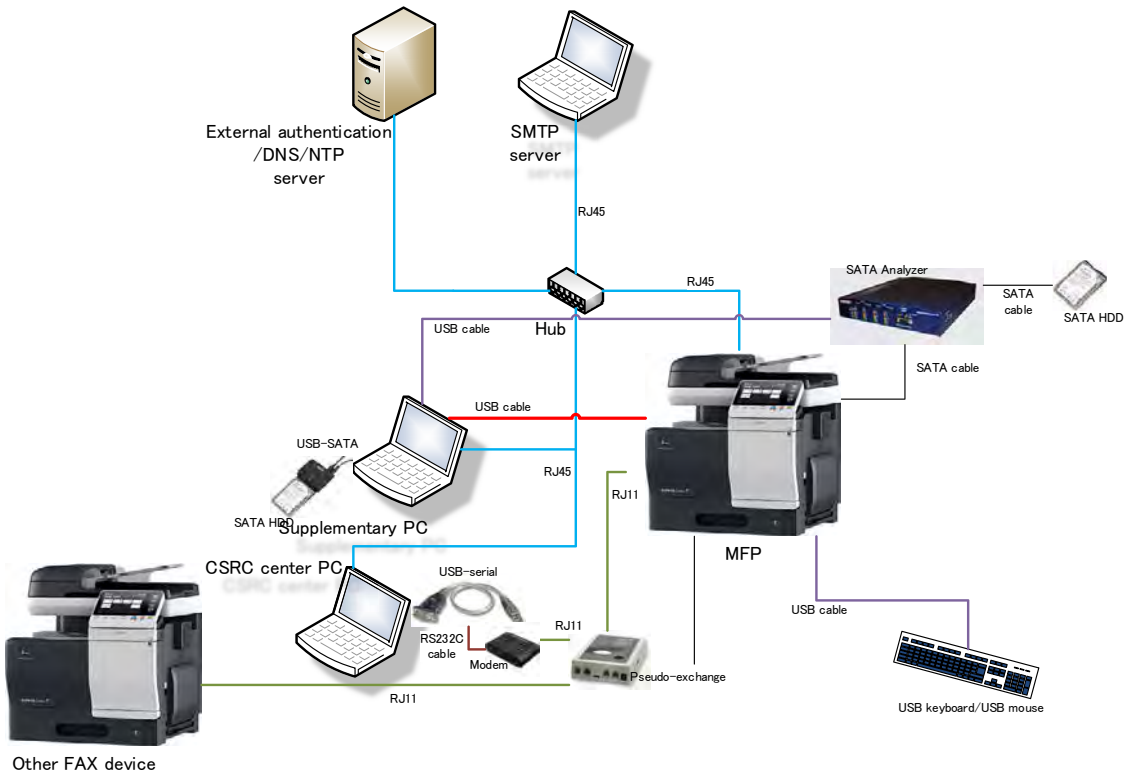

Figure 7-1 Configuration of the Developer Testing

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

Table 7-1 Components of the Developer Testing

Name	Detail
MFP (TOE)	bizhub C3850/C3350/C3850FS
MFP built-in FAX kit	KONICA MINOLTA　FK-512
Supplementary PC (Client PC)	- Windows 7 SP1 PC * 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 SP1 PC - Kerberos software: Active Directory (OS attached)
SMTP server	- Windows 7 SP1 PC
DNS server	- Windows Server 2008 R2 Standard SP1 PC - DNS software : OS attached
CSRC center PC	A server to provide the same function as the remote diagnostic service of KONICA MINOLTA, INC. - Windows 7 SP1 PC - CSRC center software Ver.2.8.1
Other FAX device	bizhub C3850/C3350/C3850FS
Pseudo-exchange (public line)	Line-exchange to realize pseudo-public line
USB memory	It is used for Firmware update test and check test of usage restriction.
USB keyboard, mouse	It is used for operation check test of USB port.
SATA Analyzer	It is used to capture HDD writing processing.
PC for terminal	It is connected with the interface for the TOE developer via RS232C. - Windows 7 SP1 PC - Terminal software: Tera Term Ver.4.86

The TOEs used for the developer testing are some models of multiple MFPs identified in the ST, however, other models are the OEM products of the MFP used for the testing; although the products name are different, they are the same product.

Therefore, "bizhub C3850," "bizhub C3350" and "bizhub C3850FS," the target models of the developer testing, were determined in the evaluation that they are consistent with the description in the ST and that they include the TOE configurations identified by the ST. The developer testing was determined to be performed in the same TOE testing environment as the TOE configuration identified in the 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.

<Content of the Performed Developer Testing>

The expected values of the testing results stated in the specification, which was offered by the developer, were compared with the values of the developer testing results included in the testing report, which was offered by the developer. As a result, it was confirmed that the values of the actual testing results were consistent with the expected values of the testing results.

b. Scope of the Performed Developer Testing

The developer testing was performed on 184 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested.

c. Result

The evaluator confirmed the approach of the performed developer testing and the 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 gain further assurance that security functions are certainly implemented, based on the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The environment of the independent testing performed by the evaluator is the same configuration as the developer testing shown in Figure 7-1.

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 documentation are shown below.

<Viewpoints of the Independent Testing>

(1) To add test items such as boundary values and combinations of parameters that the developer testing seems to be insufficient from the viewpoint of completeness.

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

(3) To conduct test items for exception processing by adding the variations being different from the developer testing.

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

- To select items including all the security functions and the external interfaces from the viewpoints of completeness.
- To select items including all the different testing approaches and testing environments.

b. Independent Testing Outline

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

<Independent Testing Approach>

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

<Content of the Performed Independent Testing>

The evaluator performed 11 items for the independent testing and 58 items for the sampling testing, based on the viewpoints of the independent testing.

Table 7-2 shows viewpoints of the independent testing and the content of the main tests corresponding to them.

Table 7-2 Viewpoints of Independent Testing Performed

Viewpoints of Independent Testing	Overview of Testing
Viewpoint (1)	• For login passwords and encryption passphrases, it was confirmed that the TOE behaved to the specification when inputting a string with one-character longer than the maximum number of characters at the time of changing.
Viewpoint (2)	• It was confirmed that the behavior of account lock was the same as that stated in the specification when being accessed via different interfaces. • The behavior of account lock was confirmed with the different authentication modes from the developer testing. • It was confirmed that the access was controlled as specified even when multiple authorities of a user were changed by one operation.
Viewpoint (3)	• Concerning the behavior of data control from the public line, it was confirmed that unauthorized data were denied even if those were different data from the developer testing.

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 the security functions may be bypassed if data of unexpected value or format by the TOE are entered.

(3) There is concern that the security functions may be bypassed if the TOE is operated with overloading.

(4) There is concern that the security functions may be violated by unauthorized information collection from the TOE firmware or unauthorized rewriting of firmware.

(5) There is concern that the security functions may be bypassed by unexpected power-on/off operation.

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 evaluator independent testing and the developer testing shown in Figure 7-1.

Table 7-3 shows the tools used for the penetration testing.

Table 7-3 Penetration Testing Tools

Tool Name/Version	Outline
Nessus Version 6.5.4	A vulnerability scanning tool
nmap Version 7.01	A port scanning tool
Nikto Version 2.1.5	A vulnerability scanning tool
Metasploit Version 4.11.4	A framework of establishing/executing Exploit
TamperIE Version 1.0.1.13	A Web debugger

<List of the Performed Penetration Testing>

Table 7-4 shows vulnerabilities of concern and the content of the penetration testing corresponding to them. The evaluator performed 12 items of penetration testing to evaluate the possibility of potential vulnerabilities being exploited.

Table 7-4 Outline of the Penetration Testing

Vulnerabilities	Outline of Testing
Vulnerability (1)	• It was confirmed that unnecessary network port was not open or that there was no known vulnerability with open port using port scanning tools and vulnerability scanning tools.
Vulnerability (2)	• It was confirmed that there was no vulnerability for input data from USB keyboard.

	• It was confirmed that the processing was not performed even if the print job command that could be exploited and the PDF files that include unauthorized processing were input to the TOE. • It was confirmed that the security functions were not bypassed even if communication data from Web browser to the TOE were rewritten by using a Web debugger. • Concerning unique interfaces other than the Web, it was confirmed that the security functions were not bypassed by unexpected input data.
Vulnerability (3)	• It was confirmed that the TOE would not become unsecured with its resource depletion.
Vulnerability (4)	• It was confirmed that there was no confidential information which could be easily extracted by binary analysis of the TOE. • It was confirmed that the update function could not be performed using illegally falsified firmware.
Vulnerability (5)	• It was confirmed that the security functions were not bypassed even if the TOE was powered off while the security functions were running.

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 evaluation was performed with the configuration shown in Figure 7-1. IPv4 was used for the network. The TOE is never operated with the configuration which consists of extremely different components from the above. Therefore, the evaluator judged that the above evaluated configuration is appropriate.

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:

  2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B (IEEE Std 2600.2™-2009)

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

  - 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
  - 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
  - 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
  - 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
  - 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B
  - 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

  - Security functional requirements: Common Criteria Part 2 Extended
  - Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL2 package

- Additional assurance component ALC_FLR.2

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

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to consumers.

8. Certification

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

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

2. Contents pointed out in the Observation Reports shall properly be solved.

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

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

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

Concerns found in the certification process were prepared as the certification oversight review, and it was sent to the Evaluation Facility. The Certification Body confirmed that such concerns pointed out in the certification oversight review 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 submitted Evaluation Technical Report, Observation Reports, and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL2 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

It should be noted that the procurement entities 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.

9. Annexes

There is no annex.

10. Security Target

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

bizhub C3850 / bizhub C3350 / bizhub C3850FS /ineo+ 3850 / ineo+ 3350 /
ineo+ 3850FS Security Target
Version 1.16, March 11, 2016, 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.

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

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.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, 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 C3850 / bizhub C3350 / bizhub C3850FS /ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS Security Target, Version 1.16, March 11, 2016, KONICA MINOLTA, INC.

[13] bizhub C3850 / bizhub C3350 / bizhub C3850FS /ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS Evaluation Technical Report, Version 1, March 11, 2016, Mizuho Information & Research Institute, Inc. Information Security Evaluation Office

[14] IEEE Std 2600.2™-2009, IEEE Standard for a Protection Profile in Operational Environment B, Version 1.0, March 2009