Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2010-02-10 (ITC-0288)
Certification No.	C0279
Sponsor	Konica Minolta Business Technologies, Inc.
TOE Name	Japan: bizhub PRESS C8000 Image Control Program Overseas: bizhub PRESS C8000 Image Control Program
TOE Version	A1RF0Y0-00I1-G00-10
PP Conformance	None
Assurance Package	EAL3
Developer	Konica Minolta Business Technologies, Inc.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
2010-11-16

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

Evaluation Result: Pass
"Japan: bizhub PRESS C8000 Image Control Program, Overseas: bizhub PRESS C8000 Image Control Program" has been evaluated based on the standards required, in accordance with the provisions of the "IT Security Certification Procedure" 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 "Japan: bizhub PRESS C8000 Image Control Program, Overseas: bizhub PRESS C8000 Image Control Program, Version A1RF0Y0-00I1-G00-10" (hereinafter referred to as the "TOE") developed by Konica Minolta Business Technologies, Inc., and the evaluation of the TOE was finished on 2010-10-27 by Mizuho Information & Research Institute, Inc., Center for Evaluation of Information Security (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Konica Minolta Business Technologies, Inc., and provides 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.

1.1.2 TOE and Security Functionality

The TOE is the embedded software installed in the Multi Function Peripheral "bizhub PRESS C8000" (hereinafter referred to as "MFP"), provided by Konica Minolta Business Technologies, Inc. The TOE controls the MFP and provides the functions such as copy, print and scan, etc. This product is utilized for input, storage, and output of the document data in the environment such as offices of general companies where documents are handled.

By identifying and authenticating a general user of the MFP and permitting the general user to manipulate own document data only, the TOE has a function to prevent the document data of other general users, which are stored in the HDD installed in the MFP, from retrieval and unintended exposure by the general user. In addition, the TOE records the information related to the behaviors of security functions and provides the information to the administrator and service engineer (hereinafter referred to as "CE"). Thus, the administrator can detect unauthorized operations.

To manage these security functions, the TOE identifies and authenticates an administrator and CE, and permits the authenticated administrator and CE to use the security management functions. Thus, the document data of other general users stored in the MFP are protected from a threat of taking out and unintended exposure by unauthorized operations of the security management functions by a general user.

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

The TOE counters each threat with the following security functions.

The assumed threats are that a general user uses TOE basic functions and the security functions (including the security management functions) from the operation panel of the MFP to expose the document data of other general users. This TOE limits the document data that can be manipulated and the available security management functions by executing identification and authentication of a general user, the administrator and CE, as well as by checking the role of a person identified and authenticated. In addition, the TOE records the information related to the behaviors of security functions and provides the information to the administrator and CE. Thus, the TOE counters the threats that the document data owned by the other general users is unintentionally exposed by a general user.

1.1.2.2 Configuration and Assumptions

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

It assumes that this TOE is installed in the MFP and used in the environment such as offices of general companies where documents are handled. The TOE shall be installed in the loaded condition in an area where only the administrator, CE, and general users, who are permitted to use the MFP, can enter, and no other than the administrator, CE, and general users can enter the area.

The MFP installed with the TOE can be connected to an intra-network and used to print the document data from a client PC connected to the same network. In order to use the function to print from a client PC via an intra-network, the built-in printer controller device (hereinafter called "printer controller device") designated by the TOE specification should be additionally loaded on the MFP. To connect this intra-network to an external network, a firewall should be connected at the network boundary to block the communication from an external network to the MFP, and appropriate setup to block the communication from the external network to the MFP should be provided.

A person who is reliable and does not misconduct should be assigned to TOE administrator. The CE performs maintenance work for the MFP under the supervision of the administrator. The administrator and CE shall make sure to set the following functions active to maintain and manage the secure state of the TOE; i.e., the identification and authentication function of the administrator and CE, who are needed to actuate the security functions, and the function that sets the TOE to the enhanced security mode.

1.1.3 Disclaimers

This TOE does not assure the security for the following cases.

1) The document data other than those which are stored in the HDD installed in the MFP are out of protection.

- The document data stored temporarily by the TOE in the volatile memory of the MFP in process of document data processing (Sophisticated technology is required to read out the document data stored temporarily in the volatile memory. The document data in the volatile memory are cleared at power off, so that a threat level that a general user reads out such document data is judged as low.)

- The outgoing document data sent from the MFP (the document data sent with the Scan to Email function, Scan to FTP function, or Scan to PC (SMB) function)

- The document data stored in the HDD of the printer controller device (the document data sent from a client PC to the printer controller device, the document data sent from the MFP to the printer controller device)

- The document data that exists on a client PC or the intra-network

- The document data owned as paper media

2) This TOE assures that the HDDs, which are installed in the MFP and have the HDD lock function that conforms to the requirement specification of this TOE, are implemented with the security function that tests the HDD lock function, and they work correctly responding to the operations from the operation panel of the MFP. The safety of the HDD lock function implemented in the HDDs is out of the scope of its assurance. Therefore, this TOE does not counter the threats that a password used to unlock the HDD lock function is stolen after the HDD is taken out from the MFP, and that the document data is read out from the HDD that is taken out from the MFP.

3) If any device other than the printer controller device (model No.: IC-601) is connected to the MFP, it is out of the scope of its assurance.

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 2010-10, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], and "Evaluation Facility Approval Procedure"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report [13] and the Observation Reports 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 oversight reviews were also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body were fully resolved, and 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 Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows;

TOE Name:	Japan: bizhub PRESS C8000 Image Control Program Overseas: bizhub PRESS C8000 Image Control Program
TOE Version:	A1RF0Y0-00I1-G00-10
Developer:	Konica Minolta Business Technologies, Inc.

The administrator can confirm that the product is the evaluated and certificated TOE according to the following method.

The administrator requests the CE, and the CE operates the panel of the MFP installed with the TOE to display the name and version of the TOE. Based on this displayed information, the administrator can confirm that the installed product is the evaluated and certified TOE.

3. Security Policy

This chapter describes the security functions and the security services that this TOE has achieved based on the policies or rules.

This TOE stores the document data in the HDDs of the MFP installed with the TOE through importing the document data from the paper media of general users and receiving the document data from a client PC connected via a network, and outputs the documents by printing and distribution. For those purposes, the TOE provides the security functions for the processing of document data reception, storage, and output. The following paragraphs describe the security functions of the TOE.

- By identifying and authenticating a general user of the MFP and permitting the general user to manipulate own document data only, the document data of other general users, which are stored in the HDD installed in the MFP, are prevented from retrieval and unintended exposure by a general user.

- To safely manage the identification and authentication information of general users (user identifiers and passwords, etc.) and the use of the security functions, identification and authentication is executed for the administrator and CE of the TOE, and permits the authenticated administrator and CE to use the security management functions, such as the modification function of identification and authentication information of general users and the function to switch ON/OFF of the identification and authentication function of users. Thus, the document data of other general users stored in the MFP are protected from a threat of taking out and unintended exposure by unauthorized operations of the security management functions by impersonating a general user.

- The TOE has the function to manage the quality of character strings for passwords when the general user, administrator, and CE of the MFP set each password, which also counters the threat that a general user impersonates another general user, administrator, or CE, attempting to pass identification and authentication.

- By recording the information related to the behaviors of security functions, the information is provided to the administrator and CE. Thus, the administrator and CE can detect unauthorized operations.

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.

Table 3-1 Assumed Threats

Identifier	Threat
T.ACCESS (Unauthorized operation to document data)	There is a possibility that a general user leaks the document data owned by other general users by using the functions for general users from the operation panel.
T.IMPADMIN (Impersonation to CE or administrator)	There is a possibility that the document data is leaked by unauthorized use of the CE function interface or management function interface by a general user.

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) Countermeasure against threat "T.ACCESS"

The TOE counters the possible threat of "T.ACCESS" that a general user uses the functions for general users from the operation panel to leak the document data owned by other general users by the following countermeasures: identification and authentication of general users, restriction of available functions, management of identification and authentication information, and audit.

The TOE requires a general user who intends to use the function of the TOE to input the user identifier (user No.) and password. The TOE checks whether the input user identifier and password are valid or not. The general user whose input user identifier and password conform to the pre-registered data is permitted to manipulate the document data owned by the general user and also permitted to use the functions for general users from the operation panel, so that the general user can store, print, and distribute the document data. The identified and authenticated general users are also permitted to use the security functions that enable to modify their own passwords.

The TOE has the function to manage the password quality of the MFP general users, and set only the character strings as passwords which satisfy with the quality prescribed in the password rules (number of characters, configuration of character types, and password setting history). Thus, the TOE counters the threat that a general user impersonates another general user and decodes his/her password attempting to pass identification and authentication.

The TOE also records the operations related to the security functions among the operations of the document data for general users to the audit log as the audit information. The TOE provides this audit log to the administrator and CE. The administrator and CE can detect unauthorized operations to the identification and authentication function such as brute-force attack and unauthorized readout and print of the document data by checking the audit information recorded in the audit log.

Thus, the TOE general user cannot manipulate the document data owned by other general users, so that the possible threat of "T.ACCESS" that a general user leaks the document data owned by other general users is countered by identification and

authentication of general users, restriction of available functions, audit, and management of identification and authentication information.

2) Countermeasure against threat "T.IMPADMIN"

The possible threat of "T.IMPADMIN" that a general user uses the administrator functions or the CE functions from the operation panel to leak the document data owned by other general users is countered by the following countermeasures: identification and authentication of administrator and CE, restriction of available functions, management of identification and authentication information, and audit.

The TOE identifies an administrator or CE, and requires the administrator or CE to input a password. The TOE checks whether the input identifier and password are valid or not. The administrator and CE whose input identifier and password conform to the pre-registered password are permitted to use the management functions, maintenance functions, and the security functions for the administrator and CE from the operation panel.

The following paragraphs show the relationship between roles of administrator and CE and security functions that are permitted to use.

a) Security functions for administrator

The authority to use the following security functions is given to the administrator.
- Termination function of the function to set the enhanced security mode
- User identifier (user No.) registration/deletion function
- General user's password new registration/modification function
- Administrator password modification function
- Password modification function for HDD lock function
- Audit log output function

b) Security functions for CE

The authority to use the following security functions is given to the CE.
- CE password new registration/modification function
- Administrator password new registration/modification function
- Audit log output function

The TOE has the function to manage the password quality of the administrator and CE, and accepts only the character strings as passwords which satisfy with the quality prescribed in the password rules (number of characters, configuration of character types, and password setting history). Thus, the TOE counters the threat that a general user impersonates the administrator or CE and decodes his/her password attempting to pass identification and authentication.

The TOE also records the operations that the security functions for administrator and CE were manipulated to the audit log as the audit information. The TOE provides this audit log to the administrator and CE. The administrator and CE can detect unauthorized operations to the identification and authentication function such as brute-force attack and unauthorized operations of the security functions by checking the audit information recorded in the audit log.

Thus, the TOE general user cannot impersonate the administrator or CE, so that the possible threat of "T.IMPADMIN" that a general user abuses the administrator functions or the CE functions from the operation panel to leak the document data owned by other general users is countered by the following countermeasures: identification and authentication of administrator and CE, restriction of available

functions, audit, and management of identification and authentication information.

3.1.2 Organizational Security Policy and Security Function Policy

3.1.2.1 Organizational Security Policy

An organizational security policy required in use of the TOE is shown in Table 3-2.

Table 3-2 Organizational Security Policy

Identifier	Organizational Security Policy
P.CHECK-HDD (Verification of HDD)	The TOE verifies whether the HDD lock function of the HDD mounted on the MFP works correctly. The management function of the passwords for the HDD lock function is permitted only to the administrator. The character strings that satisfy with 8 to 32 digits of half-size uppercase alphabets, half-size lowercase alphabets, and half-size numbers are adopted as the passwords for the HDD lock function.

3.1.2.2 Security Function Policy to Organizational Security Policy

The TOE provides the security function to fulfill the Organizational Security Policy shown in Table 3-2.

1) Means for organizational security policy "P.CHECK-HDD"

The HDDs with the specified HDD lock function are additionally installed in the MFP installed with the TOE. With the security function to test HDD lock function, the TOE checks that the installed HDD lock function is in the active status, the password for the HDD lock function is set, and the status is the locked status that blocks readout of the data stored in the HDD at startup of the MFP.

The TOE identifies an administrator and requires the administrator to input a password. The TOE checks whether the input identifier and password are valid or not. The administrator whose input identifier and password conform to the pre-registered data can use the function that modifies the password for the HDD lockup function from the operation panel.

The password modification function also has the function to manage the password quality. The character strings that satisfy with 8 to 32 digits of half-size uppercase alphabets, half-size lowercase alphabets, and half-size numbers are adopted as the newly modified passwords.

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. 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
ASM.SECMOD (Setting conditions of enhanced security mode)	The administrator keeps the function to set the enhanced security mode of the TOE active during the operation of the TOE.
ASM.PLACE (Installation conditions of the TOE)	The TOE is installed in an area where the general users, administrator, and CE can access in the condition that the MFP has been installed.
ASM.NET (Installation condition of intra-network)	The MFP installed with the TOE is connected to the intra-network, and if the intra-network is connected to an external network, the communication from the external network to the MFP shall be blocked.
ASM.ADMIN (A reliable administrator)	An administrator shall be a person who never misconducts.
ASM.CE (Condition of CE)	A CE shall be a person who never misconducts.
ASM.SECRET (Operational condition about secret information)	The password for administrator and the password for HDD lock function will not be leaked from the administrator. The password for CE will not be leaked from the CE. The password for a general user will not be leaked from the user.
ASM.SETTING (Operational setting condition about security)	- The administrator sets the HDD lock function to be active. - The CE sets the identification and authentication function of CE to be active.

In addition, the function to set the enhanced security mode of the TOE does not become active unless the administrator and CE passwords that satisfy the quality specified by the TOE are set and the identification and authentication function of administrator and CE is set to be active. The administrator and CE shall always maintain the TOE safety by managing the TOE so that the above mentioned conditions are satisfied.

4.2 Environmental Assumptions

This TOE is installed in the MFP "bizhub PRESS C8000" and installed in the office. The TOE is connected to an intra-network and may be used from a client PC connected to the same intra-network. Figure 4-1 shows the typical operational environment of the TOE.

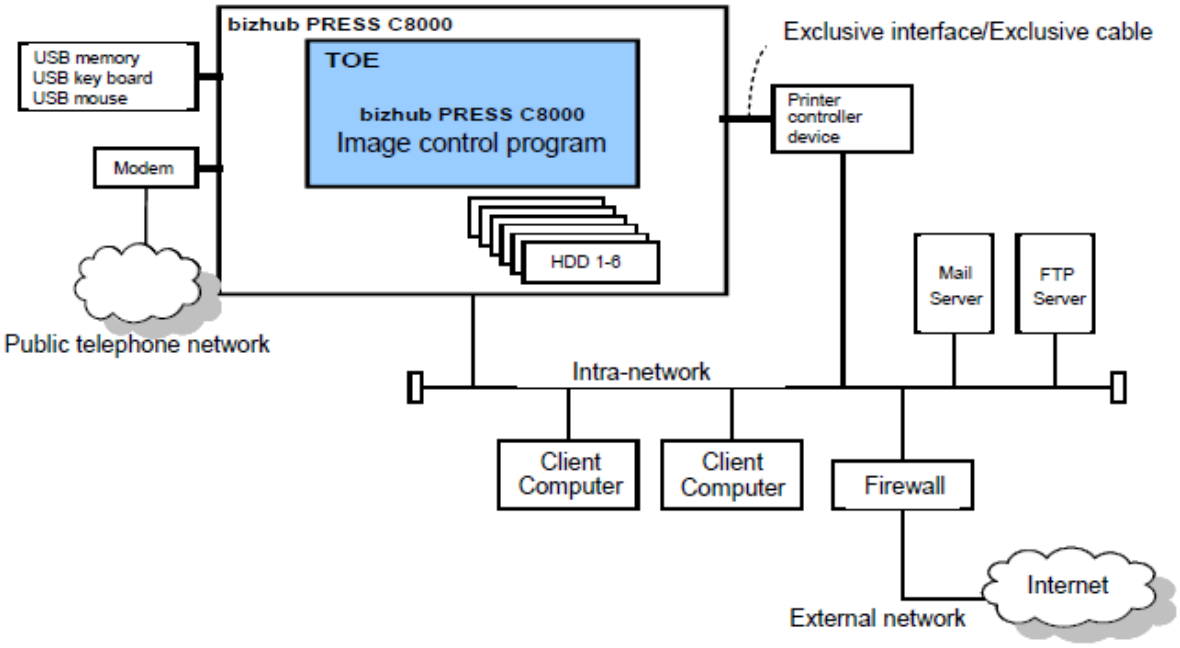

Figure 4-1 Operational Environment

It assumes that the TOE is used in the environment such as offices of general companies where documents are handled as shown in Figure 4-1. The modem, USB devices, and intra-network are connected to the MFP installed with the TOE. If the TOE is installed on the MFP, a manufacturer's optional HDD shall be installed. You can choose whether the printer controller device is loaded or not. If you want to print document data by sending it from a client PC to the MFP, the printer controller device has to be loaded.

If the TOE is connected to the intra-network that is connected to an external network such as the Internet, the intra-network and the TOE shall be protected by installing the firewall at the boundary between the external network and intra-network in order to block the attacks from the external network via the network. The server computers, such as FTP server, Mail server, etc., and client PCs are connected to the intra-network where the document data, etc., are communicated with the TOE.

The TOE is manipulated with the operation panel in the MFP. To print with the printer function, a client PC sends the document data to the printer controller device via the intra-network, and the printer controller device sends the document data to the TOE.

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

4.3 Clarification of Scope

The scope of the TOE covers the basic functions and the security functions of the image control program. The security functions of the TOE counter the threat that a general user abuses the TOE function to take out the document data of another user stored in the HDD and conduct an unintended exposure under the condition that HDDs of the specified specification are installed properly to the MFP.

The TOE sends the specific command to the HDDs installed in the MFP to acquire the information on the operation status of the HDD lock function built in the HDDs, and uses the information protection function mounted on the HDDs. However, since the HDD lock function and the information protection function for the HDD are not the TOE security functions, they are out of the scope of this evaluation. Therefore, the TOE does not counter the threat that unlocks the HDD lock function and reads out the information stored in the HDD after taking out the HDD from the MFP.

Since the printer controller device is also out of the scope of the TOE, the TOE does not counter the threats related to the printer controller device.

5. Architectural Information

This chapter explains the purpose and relationship regarding the scope of the TOE and the main configuration (subsystems).

5.1 TOE Boundary and Components

Figure 5-1 shows the elements that constitute the TOE and the hardware configuration of the MFP required for the TOE to operate. The operating system (OS) and the hardware, such as the MFP main body, printer controller, etc., are not included in the scope of the TOE.

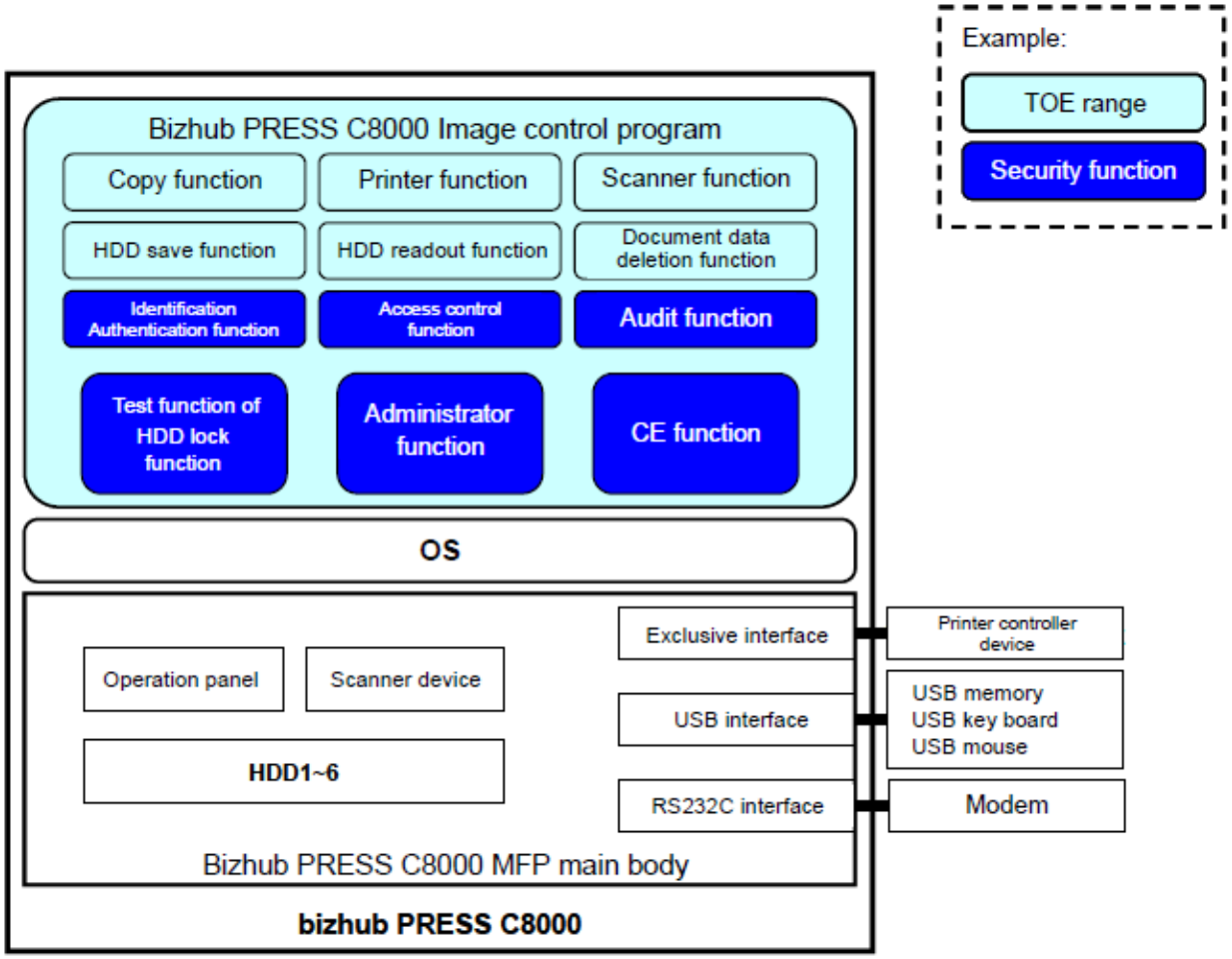

Figure 5-1 TOE Boundary

The following paragraphs explain the elements that constitute the TOE.

1) Basic functions

a) Original read function

This is the function to read out the information on the paper document from a scanner device, to convert the information to document data, and to store the converted data in the volatile memory or the temporary storage area of HDD1 to 6.

b) Image data receiving function

This is the function to receive the document data sent from the printer controller device, and to store the data in the volatile memory or the temporary storage area of HDD1 to 6. This function is effective only when the printer controller device is loaded.

c) Document data storage function

This is the function to re-store the document data stored in the temporary storage area of HDD1 to 6 in the accumulation area of HDD1 to 6.

d) Document data readout function

This is the function to read out the document data from the accumulation area of HDD1 to 6, and to store the data in the temporary storage area of HDD1 to 6.

e) Print function

This is the function to print the document data stored in the volatile memory or the temporary storage area of HDD1 to 6.

f) Image data transmission function

This is the function to send the document data scanned in the scanner device by the original read function to the printer controller device. This function is effective only when the printer controller device is loaded.

g) Deletion function

This is the function to delete the document data stored in the temporary storage area of HDD1 to 6 or the accumulation area of HDD1 to 6.

2) Security functions

a) Identification and authentication function

This is the function to perform identification and authentication of general users, the administrator and CE using the user identifiers and passwords.

b) Access control function

For the general users who are identified and authenticated, this function controls the document data which general users can manipulate by comparing the identification information of the general users (user identifier) with the owner information of the document data (document data user identifier). It permits the general users who were identified and authenticated to use the security functions to change their own passwords.

c) Audit function

This function records the details of date and time (YY:MM:DD:hh:mm:ss) and the operation details when an operation is performed as audit logs when the following operations, which are relevant to the designated security functions, occur: failure/success of identification and authentication of general users, the administrator, and CE; success of modification of the password of a general user, the administrator, and CE; success of modification of the HDD lock password; suspension of the function to set the TOE to the security enhancement state; and success of readout/print of document data by general users.

d) Management function

This function provides the following functions for management to the administrator who is identified and authenticated.

- Termination function of the function to set the enhanced security mode
- User identifier (user No.) registration/deletion function
- General user's password new registration/modification function
- Administrator password modification function
- Password modification function for HDD lock function
- Audit log output function

e) CE function

This function provides the following functions for management to the CE who is identified and authenticated.

- CE password new registration/modification function
- Administrator password new registration/modification function
- Audit log output function

f) Test function of HDD lock system

- This function inspects whether the HDD having the HDD lock function that conforms to the TOE requirement specification is installed in the MFP.
- This function inspects whether the HDD is locked at startup of the MFP.
- This function transmits the password for HDD lock function to confirm that the HDD lock function is released.

5.2 IT Environment

The MFP installed with the TOE is connected to the intra-network via the printer controller device, and the TOE communicates the document data, etc., with the server computers, such as FTP server and Mail server, and with the client PCs. The MFP and the intra-network are directly connected, but when the enhanced security mode of the TOE is activated, the network interface is set to block the communication of the document data, etc. The TOE communicates the information on hardware maintenance, e.g., the number of printed sheets, the number of times of jams, and empty toners, through Konica Minolta Business Technologies, Inc.-specified device and the modem connected via the RS232C interface.

6. Documentation

The identification of documents attached to the TOE is listed below. The documents consist of 3 categories; i.e., user's guide, installation manual, and service manual.

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

Table 6-1 bizhub PRESS C8000 Documents for Japan

No.	Name	ID
User's Guide		
1	bizhub PRESS C8000 User's Guide Copier (Japanese version)	A1RF9550-CO-00
2	bizhub PRESS C8000 User's Guide Main body (Japanese version)	A1RF9550-MB-00
3	bizhub PRESS C8000 User's Guide Network Scanner (Japanese version)	A1RF9550-NS-00
4	bizhub PRESS C8000 User's Guide Security (Japanese version)	A1RF9550-SE-00
INSTALLATION MANUAL		
5	bizhub PRESS C8000 INSTALLATION MANUAL (Japanese version)	A1RF9600-00
SERVICE MANUAL		
6	bizhub PRESS C8000 SERVICE MANUAL (Japanese version)	CCA1RF-M-J1-0000

Table 6-2 bizhub PRESS C8000 Documents for Overseas

No.	Name	ID
User's Guide		
1	bizhub PRESS C8000 User's Guide Copier	A1RF9551-CO-00
2	bizhub PRESS C8000 User's Guide Main body	A1RF9551-MB-00
3	bizhub PRESS C8000 User's Guide Network Scanner	A1RF9551-NS-00
4	bizhub PRESS C8000 User's Guide Security	A1RF9551-SE-00
INSTALLATION MANUAL		
5	bizhub PRESS C8000 INSTALLATION MANUAL	A1RF9601-00
SERVICE MANUAL		
6	bizhub PRESS C8000 SERVICE MANUAL	CCA1RF-M-E1-0000

* Note: Difference between Japanese version and English version
There are two types of documents that are attached to the TOE; the documents for Japan are written in Japanese, while the documents for Overseas are written in English. The English version is the translation of the Japanese version, so their contents are the same.

7. Evaluation conducted by Evaluation Facility and Results

7.1 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.

7.2 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows;

The evaluation has started on 2010-02 and concluded upon completion of the Evaluation Technical Report dated 2010-10. 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 2010-08 and examined procedural status conducted in relation to each work unit for 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 2010-08.

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 reviews, and those were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those concerns were reflected in the evaluation.

7.3 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.

7.3.1 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

The testing configuration performed by the developer is shown in Figure 7-1.

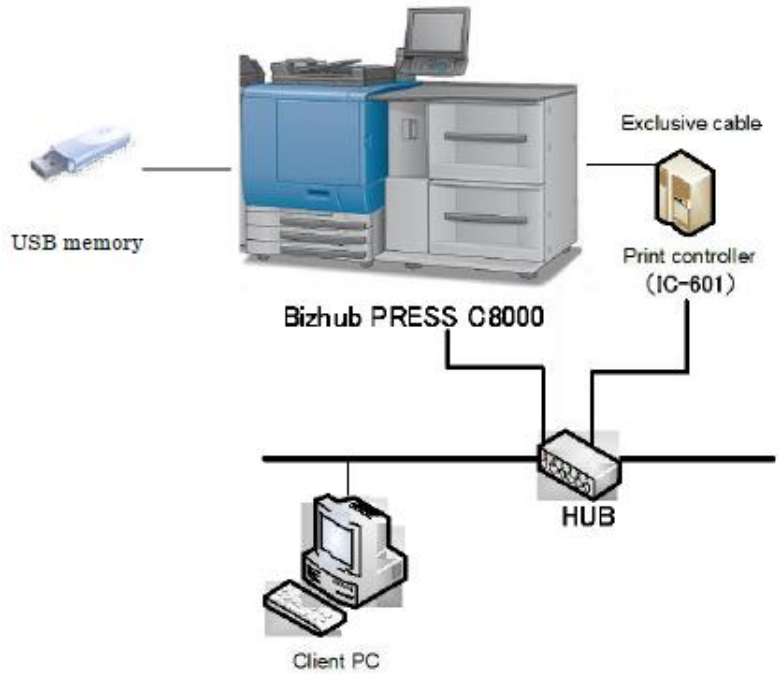

Figure 7-1 Configuration of the Developer Testing

Table 7-1 shows the components other than the TOE in the configuration of the developer testing.

Table 7-1 Configuration Components of the Developer Testing

Configuration Components	Specification
bizhub PRESS C8000 MFP main body	Connection options: - HDD 6 units (manufacturer's option) - Printer controller device (Model No.: IC-601)
Client computer	- OS: Windows XP - Web browser: Internet Explorer 8.0 (IE8) - Printer driver: KONICA MINOLTA C7000/C6000PS (PsPlug-IN) Version 1.0.61 (Compatible with bizhub PRESS C8000/C7000/C6000 Series)
Network	100BASE-T specification

The evaluation target TOE is "bizhub PRESS C8000 Gazo Seigyo Program." "bizhub PRESS C8000 Image Control Program" is the name of "bizhub PRESS C8000 Gazo Seigyo program" for overseas. The same TOE is supplied for both Japan and overseas.

As shown in Figure 7-1 and Table 7-1, the configuration where a HDD is mounted and the printer controller device (IC-601) is loaded on the above model, was tested. In this configuration, all the devices and options are loaded on and connected to the MFP installed with the TOE, which allows tests of all the functions of the TOE.

Therefore, the developer testing is executed in the same TOE testing environment as the TOE configuration identified in the ST.

2) Summary of the Developer Testing

The test performed by the developer is as follows;

a. Developer Testing Outline

An outline of the developer testing is as follows;

<Developer Testing Approach>

In the developer testing, the following approach was adopted; after stimulating the external interface of the TOE, based on the assumed usage of the TOE (operation of the operation panel, and operation of the client computer connected via intra-network), the result was observed visually on the operation panel. However, in case the test result cannot be observed on the operation panel, the following approach was adopted.

- For the audit log function, an audit log was output, and the details of the audit log were checked after an operation that causes an event to be recorded as the audit information.

<Developer Testing Tools>

There were no tools used other than the configuration of the developer testing environment shown in Figure 7-1.

<Content of the Performed Developer Testing>

The prospected values in the testing plan, listed in the evidential materials "bizhub PRESS C8000 Series test specification" provided by the developer, and the values in the developer testing result were compared. Thereby, it was confirmed that there was no inconsistency between the prospected test values and the actual test results listed in the testing evidential materials.

b. Scope of the Performed Developer Testing

The developer testing was performed on 34 items (111 subjects) by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been sufficiently 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 consistencies between the testing results expected by the developer and the actual testing results performed by the developer. The evaluator confirmed the approach of the performed developer testing and the legitimacy of tested items, and confirmed consistencies with the testing approach and its results described in the testing plan.

7.3.2 Evaluator Independent Testing

The evaluator performed the evaluator independent testing to reconfirm that the security functions are certainly implemented from the evidence shown in the process of the evaluation. The overview of the evaluator independent testing performed by the evaluator is shown as follows.

1) Evaluator Independent Testing Environment

The evaluation target TOE is "bizhub PRESS C8000 image control program." For the MFP installed with the TOE, "bizhub PRESS C8000" is selected with the configuration on which the printer controller device (IC-601) and a HDD are loaded. In this configuration, all the devices and options are loaded on and connected to the MFP installed with the TOE, which allows tests of all the functions of the TOE, and no influence is given on the behaviors of the TOE security functions. Therefore, the evaluator judged that there was no problem as the configuration for the evaluator independent testing.

2) Summary of the Evaluator Independent Testing

A summary of the Evaluator Independent Testing performed by the evaluator is as follows;

a. Viewpoints of the Evaluator Independent Testing

<Devising Testing Items>

Based on the following viewpoints, the evaluator devised 9 items for the evaluator devising testing from the developer testing and the provided evaluation evidential materials.

* Viewpoints of Security Functions

- Tests that overlap the sampling testing are excluded.

- Functions of which behaviors were fully confirmed by the developer testing are excluded.

- Functions that can be manipulated only from the operation panel and of which parameters are fixed are excluded.

From the above consideration, the following functions are included as testing targets which were judged that additional confirmation of behaviors should be conducted by the devising testing, such as "password modification function," "access rules for users and control function," "audit information recording function," "audit area management function," "management support function (administrator)," and "HDD lock password function," while "administrator registration/CE registration function," "CE identification and authentication function," "administrator identification and authentication function," "HDD lock function testing function," and "enhanced security mode setting function," are excluded from the testing targets.

* Evaluator Focused Viewpoints

- Viewpoint 1
  Functions that give critical influences on the security are targeted.

- Viewpoint 2

Security functions using the probabilistic and permutable mechanism (authentication mechanism and HDD lock password collating mechanism) are targeted.

- Viewpoint 3
  Security functions related to domains (general user, administrator, and CE) are targeted, taking account of possible differences depending on different domains.

Based on the above viewpoints, abnormal behavior tests that cover from the identification and authentication function that has critical influences on the security up to the password modification function, and tests depending on domain difference that stands the different viewpoints from the developer testing were implemented.

<Sampling Testing Items>

As the sampling testing from the developer testing, 13 items were selected, which cover the tests of target security functions and interfaces, and also include the following viewpoints.

- Comprehensiveness of security functions
  All the security functions are included in the test targets.

- Comprehensiveness of input devices
  All activation targets of TSFI, such as the operation panel, power supply, via-controller, etc., are included in the test targets.

- Comprehensiveness of testing approaches
  All the testing approaches, such as panel operation, HDD attachment/detachment, output audit log check, etc., are included in the test targets.

b. Evaluator Independent Testing Outline

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

<Evaluator Independent Testing Approach>

The evaluator prepared the devising testing procedure based on the same testing approaches as the developer testing, and implemented the independent testing by the following methods.

- Testing with the operation panel only
  For example, in a case of the developer testing that unspecified character types are input from the operation panel, the testing result is checked from the display of the operation panel after inputting the character string omitted in the developer testing from the operation panel.

- Testing to confirm the test result from other than the operation panel
  For example, the operation is conducted to cause events that the audit information is recorded from the operation panel, and the audit log containing audit information is output to USB memory, and the record details are checked.

The sampling testing was implemented in the same approach as the developer testing.

<Independent Testing Tools>

As with the developer testing environment, there were no tools other than the configuration of the evaluator independent testing.

<Content of the Performed Independent Testing>

Table 7-2 and Table 7-3 show the details of 9 items from the devising testing and 13 items from the sampling testing.

Table 7-2 Content of the Performed Devising Testing

Item No.	Name	Description of Testing
E-1	Testing of CE password modification function (Viewpoint 2)	Only the CE can modify the CE password. Only the character strings that satisfy the specified quality shall be set as passwords.
E-2	Testing of administrator password modification function by CE (Viewpoint 2)	Only the CE can modify the administrator password.
E-3	Testing of administrator password modification function by administrator (Viewpoint 2)	Only the administrator can modify the administrator password. Only the character strings that satisfy the specified quality shall be set as passwords.
E-4	Testing of general users' password modification function by administrator (Viewpoint 2)	Only the administrator can modify the general users' passwords. Only the character strings that satisfy the specified quality shall be set as passwords.
E-5	Testing of general users' password modification function by general users themselves (Viewpoint 2)	General users can modify their own passwords. Only the character strings that satisfy the specified quality shall be set as passwords.
E-6	Testing of password modification function for HDD lock function (Viewpoint 2)	Only the administrator can modify the password for HDD lock function. Only the character strings that satisfy the specified quality shall be set as passwords.
E-7	Testing of audit log output function by administrator (Viewpoint 3)	Only the administrator and CE can output audit logs.
E-8	Testing of printer job storage (Viewpoint 3)	General users can store their own printer jobs.

Item No.	Name	Description of Testing
E-9	Testing to confirm the setting of the enhanced function at the enhanced security mode (Viewpoint 1)	In the state that the TOE is set to the enhanced security mode, the setting to enhance the security of the TOE cannot be modified, including the closing of the network port and banning the use of backup/restore function to USB memory, etc.

Table 7-3 Content of the Performed Sampling Testing

Item No.	Name of Testing Item
1	Testing of interface for identification and authentication function of CE
2	Testing of interface for administrator password setting by CE
3	Testing of interface for identification and authentication function of administrator
4	Testing of interface for user password modification by user
5	Testing of interface for identification and authentication function of users
6	Testing of interface for HDD testing
7	Testing of interface for HDD lock password modification
8	Testing of interface for the enhanced security mode setting modification (from ON to OFF)
9	Testing of interface for audit log data output by administrator
10	Testing to confirm the closing of network port for Web connection under the condition that the TOE is set in the enhanced security mode
11	Testing of the limit of USB memory function
12	Testing of interface for printer job storage method
13	Testing of interface for temporary storage job operation

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.

7.3.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator 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 Evaluator Penetration Testing

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

a. Vulnerability of Concern

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

Table 7-4 Vulnerability of Concern

Item No.	Details of Vulnerability of Concern	Viewpoint of Vulnerability
VLA-T1	There is a network port that is not used for the TOE network interface.	Penetration inspection
VLA-T2	There is a network port for communication service having the interface for manual input available for a command, such as telnet, in the TOE network interface, which can execute a command.	Penetration inspection
VLA-T3	If there is an unused network port in the TOE network interface, which receives the communication from other than the TOE and processes responding to the communicated contents, the vulnerability related to the processing of the communication is exploited.	Penetration inspection Known vulnerability
VLA-T4	Known vulnerability found by examining the vulnerability information (CVN, JVN, etc.) (including OS, library, etc.)	Known vulnerability
VLA-T5	Passwords written in other character types than those specified as character strings for passwords can be set.	Bypass Direct attack
VLA-T6	By the unintended operations while the security functions work, TOE security functions are either bypassed or falsified to reach a malfunction state.	Bypass Falsification Misuse
VLA-T7	The TOE update function using the USB is exploited.	Falsification

Item No.	Details of Vulnerability of Concern	Viewpoint of Vulnerability
VLA-T8	TOE security functions are damaged by the unintended behavior of the TOE when the TOE receives the unauthorized data via the printer controller device.	Falsification

b. Evaluator Penetration Testing Outline

The evaluator conducted the following evaluator penetration testing to determine the potentially exploitable vulnerability.

<Evaluator Penetration Testing Environment>

Figure 7-2 shows the penetration testing configuration used by the evaluator.

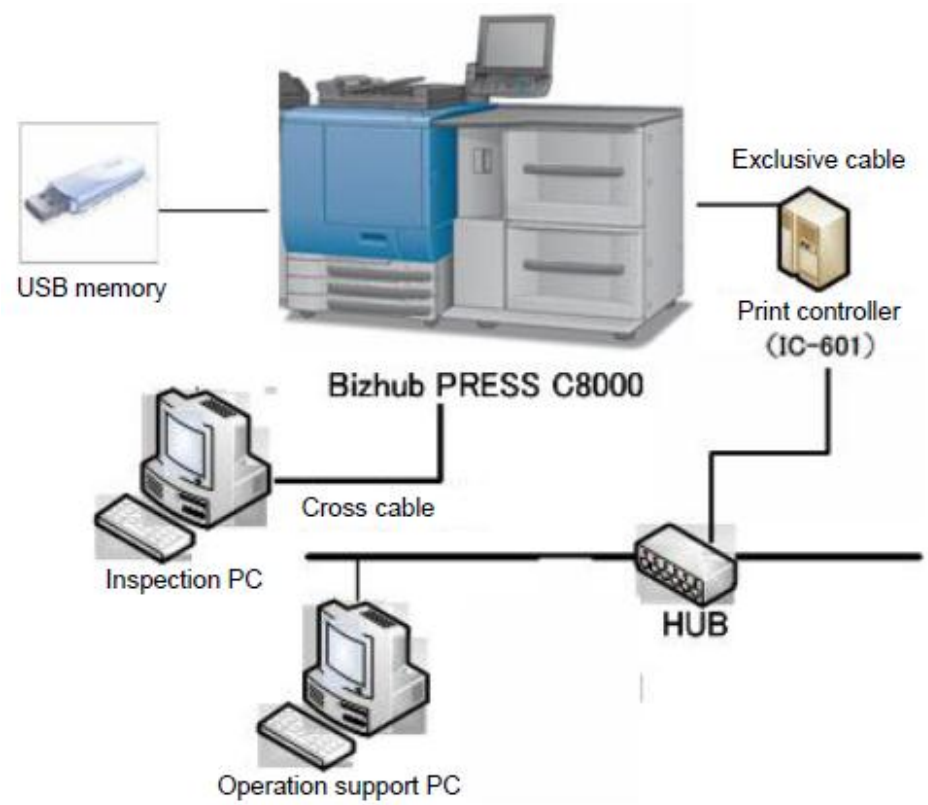

Figure 7-2 Configuration of the Evaluator Penetration Testing

In the configuration of evaluator penetration testing (Figure 7-2), the MFP model and the inspection PC-related parts are different from the configuration of the developer testing (Figure 7-1). Since the inspection PC is provided to use the inspection tools for the vulnerability testing, there is no difference in the TOE behaviors between the configuration of the developer testing and the configuration of the evaluator independent testing.

As with the configuration of the evaluator independent testing, the configuration of the evaluator penetration testing is the configuration where all the devices are

connected to the MFP installed with the TOE, which allows tests of all the functions of the TOE, and no influence is given on the behaviors of TOE security functions. Therefore, the evaluator judged that there is no problem as the configuration for the evaluator penetration testing.

Table 7-5 shows the differences from the configuration components in the developer testing among the configuration components in the evaluator penetration testing.

Table 7-5 Configuration Components in the Evaluator Penetration Testing

Configuration Components	Details
Operation support PC	- OS: Windows XP - Web browser: Internet Explorer 8.0 (IE8) - Printer driver: KONICA MINOLTA C7000/C6000PS (PsPlug-IN) Version 1.0.61 (Compatible with bizhub PRESS C8000/C7000/C6000 Series) * Equivalent to the client computer in Table 7-1
Inspection PC	- OS: Windows XP - Web browser: Internet Explorer 8.0 (IE8) - Inspection tools: Nessus, BZ

Table 7-6 shows the tools used in the environment of the evaluator penetration testing.

Table 7-6 Evaluator Penetration Testing Tools

Tool name	Outline and Purpose of Use
Nessus	- Version: 4.2.2　build 9219 - It is used for the examination of network ports.
BZ	- Version: 1.62 - Binary editor; it is used to create the TOE for penetration testing, which is different from the standard version.

<Content of the Performed Penetration Testing>

For the concerned vulnerabilities shown in Table 7-4 identified in the search of potential vulnerabilities, the evaluator penetration testing corresponding to those vulnerabilities is described in Table 7-7. The evaluator conducted the following evaluator penetration testing to determine the possibility that potential vulnerabilities might be exploited.

Table 7-7 Content of the Evaluator Penetration Testing

Item No.	Overview of Testing	Item No. of Concerned Vulnerability
1	With Nessus, the network ports used by the TOE from the inspection PC are examined.	VLA-T1
2	By executing a typical command for the network service from the inspection PC, it is examined that the document data cannot be taken out.	VLA-T2
3	With Nessus, the known vulnerabilities from the inspection PC are examined.	VLA-T3
4	It is confirmed that the character strings, which do not satisfy with the quality of character strings for passwords, cannot be set when modifying passwords.	VLA-T5
5	It is confirmed that TOE security functions work properly when the TOE is restarted, even though unintended operations are executed while the security functions are working.	VLA-T6
6	The TOE created for the penetration testing via USB is updated.	VLA-T7
7	The document data, including unauthorized data, are printed from the operation support PC.	VLA-T8

* Note: "VLA-T4" in "Table 7-4 Vulnerability of Concern"
It was confirmed that the known vulnerabilities related to OS, library, etc., were not included in the TOE body and the OS needed for the operation of the TOE by the examination on June 11, 2010. Therefore, those were excluded from the testing items.

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.

7.4 Evaluated Configuration

This evaluation was conducted with the configuration shown in "7.3.2 Evaluator Independent Testing," and "Figure 7-2." This TOE is not operated in a configuration where its components are significantly different from the above.

However, the TOE shall be operated in an active status of the enhanced security mode setting function (enhanced security mode). Therefore, in this evaluation, the tests were conducted under the condition that the following settings are kept active.

- To set the characters that satisfy with the specified quality for the passwords used for the identification and authentication of CE and administrator.
- To set the CE identification and authentication function to be active.
- To set the administrator identification and authentication function to be active.
- To set the enhanced security mode setting function (enhanced security mode) to be active.
- To set the characters that satisfy with the specified quality for the passwords used for the HDD lock function.
- To set the HDD lock function to be active.

7.5 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: None
- Security functional requirements: Common Criteria Part 2 Conformant
- 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

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

7.6 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 reflected.
3. The submitted evidential materials were sampled, the contents were examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the Observation Reports and certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

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

8.2 Recommendations

* Setting timing of the password for the HDD lock function in the TOE installation procedure

  The TOE installation procedure of the guidance specifies that the password for the HDD lock function shall be set after the registration of the general users. Since it might take a long time for the registration of general users in the TOE installation procedure if many general users shall be registered, there is a risk of operating error and break-in of unauthorized operations, such as shutdown of the MFP power supply. In such case, the TOE does not reach a secure condition assured by the evaluation because the setting of passwords for the HDD lock function and the HDD lock function are not yet activated.

  Therefore, it is required to complete the TOE installation procedure by shortening the time for general user registration by minimizing the number of general users to be registered, and restart the MFP. After the restart of the MFP, the registration of general users is to be resumed under the enhanced security mode of the TOE.

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 PRESS C8000 Series Security Target Version 1.17, October 7, 2010, Konica Minolta Business Technologies, 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 abbreviations relating to the TOE used in this report are listed below.

CE	Customer service Engineer
FTP	File Transfer Protocol
HDD	Abbreviation of Hard Disk Drive that is installed in TOE
MFP	Abbreviation of Multi Function Peripheral
USB	Abbreviation of Universal Serial Bus that is one of the serial bus standards to connect various peripheral devices to a computer

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

Audit log:	Record of audit information.
Copy function:	TOE function that imports the information on the paper documents via the scanner device, converts the data to the document data, and then prints the data.
Document data:	The data that paper document information is imported from the scanner and converted to be stored in the MFP, and the data of the document transmitted from a client computer.
Document data user identifier:	Information to identify the owner of the document data added in the document data. A user identifier is added.

Enhanced Security Mode:	Status that the security for the TOE is enhanced. This is set by the function that enhances the security for the TOE.
External network:	Network that the MFP is installed in but the organization cannot control; the general-purpose Internet is indicated in general.
FTP server:	Server to exchange files with clients using the File Transfer Protocol.
HDD lookout function:	One of the HDD security functions specified in ATA Standards.
Intra-network:	Network that the MFP is installed in and the organization can control. In general, the intra-office LAN environment built as the intra-net.
Nessus:	Tool referred to the vulnerability scanner, which examines vulnerabilities existing on the examination target by examining the network ports existing in the network interfaces of the examination target and using those ports.
Network port:	Number used to identify the services and programs of transmission destination and transmission source when conducting the network communication.
Network service:	Services available from a remote location via a network, such as Web services, Email services, and remote login service.
Operation panel:	Display and input device used for the operation of the MFP by users, which consists of LCD display with touch panel, physical keys/buttons, and indication lamps, etc.

Printer controller device:	Device to receive the document data sent from a client computer once, and then transfer to the MFP.
Scanner function:	Function that imports the information on the paper documents via the scanner device and converts the data to the document data.
Scan to Email function:	TOE function that imports the information on the paper documents via the scanner device, converts the document data, and then transmits the data by Email.
Scan to FTP function:	TOE function that imports the information on the paper documents via the scanner device, converts the document data, and then transmits the data by FTP.
Scan to PC (SMB) function:	TOE function that imports the information on the paper documents via the scanner device, converts the document data, and then transmits the data by SMB to a client computer.
SMB server:	Server that shares files with a client using the Server Message Block protocol.
SMTP server:	Server that transmits the Email using the Simple Mail Transfer Protocol.
User identifier:	Information for identifying general users (No.).

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[2] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[3] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 3 July 2009 CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 3 July 2009 CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 3 July 2009 CCMB-2009-07-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 3, July 2009, CCMB-2009-07-001 (Japanese Version 1.0, December 2009)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 3, July 2009, CCMB-2009-07-002 (Japanese Version 1.0, December 2009)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 3, July 2009, CCMB-2009-07-003 (Japanese Version 1.0, December 2009)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 3, July 2009, CCMB-2009-07-004 (Japanese Version 1.0, December 2009)

[12] bizhub PRESS C8000 Series Security Target Version 1.17, October 7, 2010, Konica Minolta Business Technologies, Inc.

[13] bizhub PRESS C8000 Image Control Program Technical Report Version 1, October 16, 2010, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security