Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application date/ID	2011-11-11 (ITC-1386)
Certification No.	C0378
Sponsor	Konica Minolta Business Technologies, Inc.
Name of the TOE	Japanese: bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Zentai Seigyo Software English: bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software
Version of the TOE	A2XK0Y0-0100-G00-56
PP Conformance	None
Assurance Package	EAL3
Developer	Konica Minolta Business Technologies, 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.
2012-11-15

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3 (Japanese Translation)
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3 (Japanese Translation)

Evaluation Result: Pass

"Japanese: bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Zentai Seigyo Software, English: bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software" 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 "Japanese: bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Zentai Seigyo Software, English: bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software, Version A2XK0Y0-0100-G00-56" (hereinafter referred to as the "TOE") developed by Konica Minolta Business Technologies, Inc., and the evaluation of the TOE was finished on 2012-10 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 Business Technologies, Inc., and provide security information to procurement personnel and consumers who are interested in this TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is the appendix of this report together. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "procurement personnel who purchase this TOE that is commercially available" 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 bizhub C554, bizhub C454, bizhub C364, bizhub C284, bizhub C224, bizhub C7828, bizhub C7822, ineo+ 554, ineo+ 454, ineo+ 364, ineo+ 284, and ineo+ 224, which this TOE is installed, are digital Multi Functional Peripheral (hereinafter referred to as "MFP"), provided by Konica Minolta Business Technologies, Inc., composed by selecting and combining copy, print, scan and FAX functions.

The TOE is the "bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software" that controls the entire operation of MFP, including the operation control processing and the image data management triggered by the panel of the main body of MFP or through the network. The TOE supports the protection function against the exposure of the highly confidential documents stored in the MFP. This TOE includes the audit log function and contributes to the detection of MFP illegal use, such as violation of the protection function.

Moreover, for the danger of illegally bringing out HDD that is a medium to store image data in MFP, the TOE can prevent unauthorized access by encrypting all the data including

image data written in HDD by using ASIC. Besides, the TOE provides the function that deletes all the data of HDD completely by deletion method compliant with various overwrite deletion standards and the function that controls the access from the FAX public line against the danger using Fax function as a steppingstone to access internal network.

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

1.1.2.1 Threats and Security Objectives

This TOE counters each threat with the following security functions.

- It is assumed as threat that information is leaked from MFP after lease-return or discard of MFP. To counter this threat, the TOE has the function to delete the information in storage medium.

- It is assumed as threat that HDD is stolen from MFP and information is leaked from the stolen HDD. To counter this threat, the TOE encrypts and writes information in HDD by using the encryption function of ASIC that is outside the scope of the TOE.

- It is assumed as threat that the unauthorized access is done to the user box files stored in the private user box, the public user box or the group user box. To counter this threat, the TOE identifies and authenticates users and determines the availability of access based on the information of users and user box file that the TOE keeps.

- It is assumed as threat that the unauthorized access is done to the secure print files or ID & print files. To counter this threat, the TOE identifies and authenticates users and permits only the person who stored the secure print files and ID & print files to operate these files.

- It is assumed as threat that information is leaked by the following causes.

  > To transmit the user box file to the different address which the user does not intend, when transmitted it from the TOE.

  > To pretend to be the TOE and exploit the secure print file and ID & print file.

  > To store the user box files to the different user box which the user does not intend, when the TOE received them.

  To counter this threat, the TOE confirms whether a user is an administrator by identification and authentication, and permits only the administrator to operate the setting of the address, the setting to impersonating the TOE, and the setting of the destination.

- It is assumed as threat that the leak of information cannot prevent because the setting of enhanced security function is changed. To counter this threat, the TOE confirms whether a user is an administrator or a service engineer by identification and authentication, and permits only the administrator or the service engineer to change the setting of enhanced security function.

- It is assumed as threat that backup function or restore function is abused, which resulted in a leak of information or a change of setting value. To counter this threat, the

TOE confirms whether a user is an administrator by identification and authentication, and permits only the administrator to use the backup function and the restore function.

(Supplement) The TOE has user authentication function, but it can also perform user authentication by using Active Directory that is outside the scope of the TOE.

1.1.2.2 Configuration and Assumptions

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

It assumes that the MFP including this TOE is installed in an office which is managed by an organisation, such as a company or its section, and is connected to the intra-office LAN.

In this environment, the MFP is managed not to be accessed from an external network (which is outside of the organisation such as internet) even when LAN is connected to an external network, and the communication through the LAN is managed not to be wiretapped.

It assumes that an administrator and a service engineer are reliable, and the other users can also keep the secret about their own passwords.

It assumes that this TOE is used in the condition that the setting of the enhanced security function is enabled.

1.1.3 Disclaimers

- Active Directory function, in case of selecting external server authentication method for the user authentication function, is not assured in this evaluation.

- The encryption function by ASIC installed in MFP is not assured in this evaluation.

- The TOE supports the information deletion function of storage medium for the measure of leaking information when MFP is discarded or returned. However, it is not assured in this evaluation that the information of setting values such as passwords does not remain in the area of SSD, which is unable to be accessed from the TOE (this kind of area might exist by the characteristics of SSD.).

- Fax unit control function is valid only when the Fax unit as an optional part is installed.

- It is necessary to activate the setting of enhanced security function. When it is valid, a part of MFP functions cannot be used. Refer to the description of each settings written in "1.4.3.8 Enhanced Security Function" of the ST.

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 2012-10, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] prepared by the Evaluation Facility as well as evaluation evidential materials, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification 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 the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

Name of the TOE:	Japanese:	bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Zentai Seigyo Software
	English:	bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software
Version of the TOE:	A2XK0Y0-0100-G00-56	
Developer:	Konica Minolta Business Technologies, Inc.	

At the time of TOE installation, etc., a user can ask a service engineer to confirm that the product is the evaluated and certified TOE as follows.

TOE version and checksum are displayed by panel operation of service engineer. A user can confirm that the installed product is the evaluated and certified TOE, by confirming TOE version and that checksum is the same as the one in a service manual.

3. Security Policy

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

The TOE handles the following data.

- Secure Print file
- ID & print file
- User Box file

To protect these data from unintended leak, the TOE identifies and authenticates persons who access these data or the related data, and controls access. Moreover, the TOE provides an encryption function with ASIC and a data deletion function to prevent leaking from storage medium that stores these data or the related data.

This TOE realizes the following for customer's demand.

- A function to prevent the leak from the communication path of these data
- Structure not to permit access from an FAX public line port of MFP to an internal network
- Record of the audit log related to the authentication function and job.

3.1 Roles related to the TOE

The roles related to this TOE are defined as follows.

(1) User
An MFP user who is registered into MFP. In general, an employee in the office is assumed.

(2) Administrator
An MFP user, who manages the operations of MFP, manages MFP's mechanical operations and users. In general, it is assumed that the person elected among the employees in the office plays this role.

(3) Service engineer
A user, who manages the maintenance of MFP, performs the repair and adjustment of MFP. In general, a person-in-charge of the maintenance service of MFP at a sales company in cooperation with Konica Minolta Business Technologies, Inc. is assumed.

(4) Responsible person of the organisation that uses the MFP
A responsible person of the organisation that manages the office where the MFP is installed. An administrator who manages the operation of MFP is assigned.

(5) Responsible person of the organisation that manages the maintenance of the MFP
A responsible person of the organisation that manages the maintenance of MFP. A service engineer who manages the maintenance of MFP is assigned.

Besides these, though not a TOE user, those who go in and out the office are assumed to be accessible persons to the TOE.

3.2 Security Function Policies

The TOE possesses security functions to counter threats shown in 3.2.1 and to fulfill the organisational security policies shown in 3.2.2.

3.2.1 Threats and Security Function Policies

3.2.1.1 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.DISCARD-MFP (Lease-return and discard of MFP)	When leased MFPs are returned or when discarded MFPs are collected, secure print files, user box files, ID & print files, stored image files, HDD-remaining image files, and image-related files can be leaked by a person with malicious intent when he/she analyzes the HDD in the MFP.
T.BRING-OUT-STORAGE (Unauthorized bringing-out of HDD)	- Secure print files, user box files, ID & print files, stored image files, HDD-remaining image files, and image-related files can be leaked by a person or user with malicious intent, who illegally brings them out and analyzes HDD in the MFP. - A person or user with malicious intent illegally replaces the HDD in MFP. In the replaced HDD, newly created files, such as secure print files, user box files, ID & print files, stored image files, HDD-remaining image files, and image-related files, are accumulated. A person or user with malicious intent brings them out to analyze the replaced HDD, so that such image files will be leaked.
T.ACCESS-PRIVATE-BOX (Unauthorized access to the personal user box by using user functions)	User box files are exposed when a person or user with malicious intent accesses the user box that other users own and operates the user box files, such as copies, moves, downloads, prints, and transmits.
T.ACCESS-PUBLIC-BOX (Unauthorized access to the public user box by using user functions)	User box files are exposed when a person or user with malicious intent accesses the public user box which is not permitted to use, and operates the user box files, such as copies, moves, downloads, prints, and transmits.

Identifier	Threat
T.ACCESS-GROUP-BOX (Unauthorized access to the group user box by using user functions)	User box files are exposed when a person or user with malicious intent accesses the group user box which the account where a user does not belong to owns, and operates the user box files, such as copies, moves, downloads, prints, and transmits.
T.ACCESS-SECURE-PRINT (Unauthorized access to the secure print files or ID & print files by using user functions)	- Secure print files are exposed by a person or user with malicious intent when he/she operates (prints, etc.) those files which were not permitted to use. - ID & print files are exposed by a person or user with malicious intent, who operates (prints, etc.) those files which were stored by other users.
T.UNEXPECTED-TRANSMISSION (Transmission to unintended address)	- A person or user with malicious intent changes the network settings that are related to the transmission of user box files. Even if an addressee is set precisely, a user box file is transmitted (the E-mail transmission or the FTP transmission) to the entity which a user does not intend to, so that user box files are exposed. <The network settings which are related to user box file transmission> > Setting related to the SMTP server > Setting related to the DNS server - A person or user with malicious intent changes the network settings which are set in MFP to identify MFP itself where the TOE is installed, by setting the value of MFP (NetBIOS name, AppleTalk printer name, IP address, etc.) that the TOE is originally installed, so that secure print files or ID & print files are exposed. - A person or user with malicious intent changes the TSI reception settings. User box files are stored to the entity which a user does not intend to, so that user box files are exposed. - A person or user with malicious intent changes the PC-FAX reception settings. By changing the setting of the storing for the public user box to the storing to common area for all users, user box files are stored to the entity which a user does not intend to, so that user box files are exposed. *This threat exists only in the case that the setting of PC-FAX reception is meant to work as the operation setting for user box storing.
T.ACCESS-SETTING (Unauthorized change of a function setting condition related to security)	The possibility of leaking user box files, secure print files, or ID & print files rises because a person or user with malicious intent changes the settings related to the enhanced security function.

Identifier	Threat
T.BACKUP-RESTORE (Unauthorized use of backup function and restoration function)	User box files, secure print files, or ID & print files can be leaked by a person or user with malicious intent, using the backup function and the restoration function illegally. Highly confidential data such as passwords can also be exposed, so that settings might be falsified.

3.2.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

(1)Security function to counter the threat [T.DISCARD-MFP (Lease-return and discard of MFP)]

This threat assumes the possibility of leaking information from MFP collected from users.

The TOE provides the function to overwrite the deletion area of HDD when the appropriate file is deleted or when the administrator performs all area deletion, so it prevents the leakage of the protected assets in HDD connected to lease-returned MFPs or discarded MFPs.

(2)Security function to counter the threat [T.BRING-OUT-STORAGE (Unauthorized bringing-out of HDD)]

This threat assumes the possibility of the data in HDD to be leaked by being stolen from the operational environment where MFP is used, or by installing the unauthorized HDD and bringing out with the data accumulated in it.

By using the encryption function of ASIC, which is outside the scope of the TOE, this TOE provides the generation function of encryption key to encrypt the data written in the HDD (referred to as "encryption key generation function") and the supporting function with the ASIC (referred to as "ASIC operation support function") so that the encrypted data are stored in HDD and it makes it difficult to decode the data even if the information is read out from HDD.

(3)Security function to counter the threat [T.ACCESS-PRIVATE-BOX (Unauthorized access to the personal user box by using user functions)]

This threat assumes the possibility that an unauthorized operation is done by using user functions for the personal user box which each user uses to store the image files.

When using various functions of MFP with this TOE, the changes in settings of users and personal user boxes are limited only to administrators and permitted users, and the operation of personal user box is restricted only to normal users, and it prevents from unauthorized operation by using user functions; by maintaining functions such as the identification and authentication function of users and administrators (referred to as "user function" and "administrator function"), the access control function for personal user box (referred to as "user box function"), and the function that limits the changes in

settings of users and personal user box to administrators and users (referred to as "administrator function," "user function," and "user box function").

Furthermore, this TOE provides the function to get the authentication information from the user information management server of Active Directory (referred to as "External server authentication operation support function"), which is outside the scope of this TOE, in the user identification and authentication function.

(4)Security function to counter the threat [T.ACCESS-PUBLIC-BOX (Unauthorized access to the public user box by using user functions)]

This threat assumes the possibility that an unauthorized operation is done by using user functions for the public user box which each user shares to store the image files.

When using various functions of MFP with this TOE, the changes in settings of public user box and the users are limited only to administrators and permitted users, and the operation of public user box is restricted only to normal users, and it prevents from unauthorized operation by using user functions; by maintaining functions such as the identification and authentication function of users and administrators (referred to as "user function" and "administrator function"), the identification and authentication function on the access of public user box, the access control function for public user box, the function that limits the changes in settings of public user box to administrators and permitted users (referred to as "user box function"), and the functions that limits the changes in settings of users to administrators and permitted users (referred to as "administrator function" and "user function").

Furthermore, this TOE provides the function to get the authentication information from the user information management server of Active Directory (referred to as "External server authentication operation support function"), which is outside the scope of this TOE, in the user identification and authentication function.

(5)Security function to counter the threat [T.ACCESS-GROUP-BOX (Unauthorized access to the group user box by using user functions)]

This threat assumes the possibility that an unauthorized operation is done by using user functions for the group user box that is a storage area of image files used by users who are permitted to use the account or the user box file in it.

When using various functions of MFP with this TOE, the changes in settings of group user box and the users are limited only to administrators and permitted users, and the operation of group user box is restricted only to normal users, and it prevents from unauthorized operation by using user functions; by maintaining functions such as the identification and authentication function of users and administrators (referred to as "user function" and "administrator function"), the access control function for group user box, the function that limits the changes in settings of group user box to administrators and users (referred to as "user box function"), and the functions that limits the changes in settings of users to administrators and permitted users (referred to as "administrator function" and "user function").

Furthermore, this TOE provides the function to get the authentication information from the user information management server of Active Directory (referred to as "External server authentication operation support function"), which is outside the scope of this TOE, in the user identification and authentication function.

(6)Security function to counter the threat [T.ACCESS-SECURE-PRINT (Unauthorized access to the secure print files or ID& Print files by using user functions)]

This threat assumes the possibility that an unauthorized operation is done to the secure print files or ID & print files by using user functions.

When using various functions of MFP with this TOE, the changes in settings of secure print are limited to administrators, and the changes of user settings are limited only to administrators and permitted users, and the operation of secure print files and ID & print files are restricted only to normal users, and it prevents from unauthorized operation by using user functions; by maintaining functions such as the identification and authentication function of users and administrators (referred to as "user function" and "administrator function"), the authentication function with secure print password and identification and authentication function of user registered ID & print files, the access control function for secure print files and ID & print files, the function that limits the changes in settings of secure print files and ID & print files to administrators (referred to as "secure print function"), and the functions that limits the changes in settings of users to administrators and permitted users (referred to as "administrator function" and "user function").

Furthermore, this TOE provides the function to get the authentication information from the user information management server of Active Directory (referred to as "External server authentication operation support function"), which is outside the scope of this TOE, in the user identification and authentication function.

(7)Security function to counter the threat [T.UNEXPECTED-TRANSMISSION (Transmission to unintended address)]

This threat assumes the possibility of sending the information to the address that isn't intended, when the network setting related to the transmission, the network setting related to MFP address, PC-FAX operational setting, or TSI reception setting is illegally changed.

The changes of network setting, PC-FAX operation setting and TSI reception setting are restricted only to administrators, and it prevents the possibility of transmission to the address that isn't intended, by maintaining functions such as the identification and authentication function of administrator and functions to limit the changes of settings, such as network installation, PC-FAX operation setting, and TSI reception setting, only to administrators (referred to as "administrator function") with this TOE.

(8)Security function to counter the threat [T.ACCESS-SETTING (Unauthorized change of function setting condition related to security)]

This threat assumes the possibility of developing consequentially into the leakage of the user box files, the secure print files, and ID & print files, by having been changed the specific function setting which relates to security.

The changes of the specific function setting related to security are restricted only to administrators and service engineers, and as a result, it prevents the possibility of leakage of the user box files, the secure print files, or ID & print files; by maintaining the identification and authentication function of administrator (referred to as

"administrator function" and "SNMP manager function"), the identification and the authentication function of service engineers (referred to as "service mode function"), and the restricting function for setting the specific function related to security only to administrators and service engineers (referred to as "administrator function," "SNMP manager function," and "service mode function") with this TOE.

(9)Security function to counter the threat [T.BACKUP-RESTORE (Unauthorized use of backup function and restoration function)]

This threat has a possibility that user box files, secure print files, and ID & print files may be leaked by unauthorized use of the backup function and the restoration function. Moreover, it assumes the possibility that user box files, secure print files, and ID & print files may be leaked as a result of the leakage of confidential data such as the passwords or of falsifying various setting values.

The use of backup function and restore function is restricted only to administrators, and it prevents the possibility of leakage of user box files, secure print files, ID & print files and confidential data such as passwords; by maintaining the function to restrict the use of the following functions, the identification and authentication function of administrator, backup function and restore function, only to administrators (referred to as "administrator function") with this TOE.

3.2.2 Organisational Security Policies and Security Function Policies

3.2.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE are shown in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.COMMUNICATION-DATA (secure communication of image files)	Highly confidential image files (secure print files, user box files, and ID & print files) which are transmitted or received between IT equipments must be communicated via a trusted path to the correct destination, or encrypted when an organisation or user expects to be protected. (Supplement) The term "between IT equipments" here indicates between client PC and MFP that users use.
P.REJECT-LINE (Access prohibition from public line)	An access to internal network from public line via the Fax public line port must be prohibited.
P.AUDIT-LOGGING (Acquisition and management of audit log)	The generation of the audit log related to all authentication functions and to all jobs necessary to be audited must be maintained. In addition, the audit log must be protected from a person who does not have the authority of disclosure or change, and it must be set to be accessed by a person who has the authority. (Supplement) Jobs necessary to be audited indicate the operation related to the user box files, secure document files, and ID & print files. Jobs unaccompanied by storing to HDD (copy, print without any password protection from client PC, and transmission via network or FAX without storing after scanning) are not considered necessary to be audited.

3.2.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to satisfy the organisational security policies shown in Table 3-2.

(1)Security function to satisfy the organisational security policy
[P.COMMUNICATION-DATA (secure communication of image files)]

This organisational security policy regulates processing via trusted path to a correct destination or encrypting to ensure the confidentiality of the image files which flow on the network, in case an organisation or user expects to be protected. As this corresponds as one's request, there is no need to provide secure communication function for all communication. At least a means needs to be provided between MFP and client PC, which is used by users, when managing the secure print files, ID & print files, and the

user box files.

This TOE provides the functions, such as the function to support the trusted channel to correct destination in the transmission and reception of images between MFP and client PC, for the user box files, the secure print files, and ID & print files (referred to as "trusted channel function"), the encryption key generation function to transmit the user box files by S/MIME, the encryption function of user box files, the encryption function of encrypted key for S/MIME transmission (referred to as "S/MIME encryption processing function"), the identification and authentication function of administrators, and the function to limit the changes in settings related to the trusted channel and S/MIME only to administrators (referred to as "administrator function"), so that it realizes image data on the network to transmit and receive in a confidential fashion and to transmit to the correct destination by restricting the change of settings only to administrators.

(2)Security function to satisfy the organisational security policy [P.REJECT-LINE (Access prohibition from public line)]

This organisational security policy regulates prohibiting the access to the internal network via the Fax public line port on Fax unit installed to MFP. This function is provided when Fax unit is installed in MFP.

This TOE provides the function that prohibits the access to the data existing on the internal network from public line via the Fax public line port (referred to as "Fax unit control function"), so that it realizes the access to the internal network via the Fax public line port to be prohibited.

(3)Security function to satisfy the organisational security policy [P.AUDIT-LOGGING (Acquisition and management of audit log)]

This organisational security policy regulates maintaining the generation of the audit log related to all authentication functions and to all jobs necessary to be audited, protecting the audit log from persons who do not have the authority of disclosure or change, and allowing persons who have the authority to access to the audit log.

This TOE generates the "audit log" in the case of operation of job necessary to be audited or activation of the authentication function, and provides the function to operate audit log. This satisfies this organisational security policy by performing the access control to that function.

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
A.ADMIN (Personnel condition to be administrators)	Administrators, in the role given to them, will not carry out a malicious act during a series of permitted operations.
A.SERVICE (Personnel condition to be service engineers)	Service engineers, in the role given to them, will not carry out a malicious act during a series of permitted operations.
A.NETWORK (Condition for MFP Network connection)	- The intra-office LAN, where the MFP with the TOE installed is placed, will not be intercepted. - When the intra-office LAN, where the MFP with the TOE installed is placed, is connected to an external network, access from the external network to the MFP is not allowed.
A.SECRET (Operating condition on confidential information)	Each password and encryption passphrase will not be leaked from each user in the use of the TOE.

4.2 Environmental Assumptions

This TOE is installed in either bizhub C554, bizhub C454, bizhub C364, bizhub C284, bizhub C224, bizhub C7828, bizhub C7822, ineo+ 554, ineo+ 454, ineo+ 364, ineo+ 284, or ineo+ 224, all of which are MFPs provided by Konica Minolta Business Technologies, Inc.

It assumes that the MFP including this TOE is installed in an office which is managed by an organisation of a company or its section, and is connected to the intra-office LAN.

If the external server authentication method is selected for the user identification and authentication, Active Directory, that is the directory service provided by Windows Server 2000 (or later), is needed to consolidate the user's information under the Windows platform network environment as the external server.

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

4.3 Clarification of Scope

The reliability of ASIC, Active Directory, and SSD below, is not the scope of this evaluation.

- The TOE has the function to encrypt and write the information in HDD. However, the operation of the encryption is a function done by ASIC which is a part of MFP, so that it is outside the scope of the TOE and is not the scope of this evaluation.

- The TOE has the function to authenticate users. If the external server authentication method is selected for the user authentication function, it uses Active Directory, the directory service of an external server, to process the authentication.
  If the external server authentication method is selected, this TOE provides the user identification and authentication function by inquiring the authentication information to an external server and receiving the authentication information. The authentication function done by Active Directory of the external server is outside the scope of the TOE and is not the scope of this evaluation.

- There is a possibility that information on setting values such as passwords might remain in the area of SSD, which is unable to be accessed from the TOE (this kind of area might exist by the characteristics of SSD.). Such remaining information is protected by the difficulty of obtaining the remaining information from SSD. SSD is outside the scope of the TOE, and the difficulty of obtaining the remaining information is not the scope of this evaluation.

5. Architectural Information

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

5.1 TOE Boundary and Components

The TOE is the MFP control software and is installed in the flash memory on the MFP controller in the main body of MFP. It is loaded and run on the RAM when the main power is switched ON. The relation between the TOE and MFP is shown in Figure 5-1.

The device interface kit and FAX unit are optional parts of MFP. For the environment of TOE operation, it assumes that the device interface kit is installed when user uses Bluetooth device, and FAX unit is installed when user uses the FAX function.

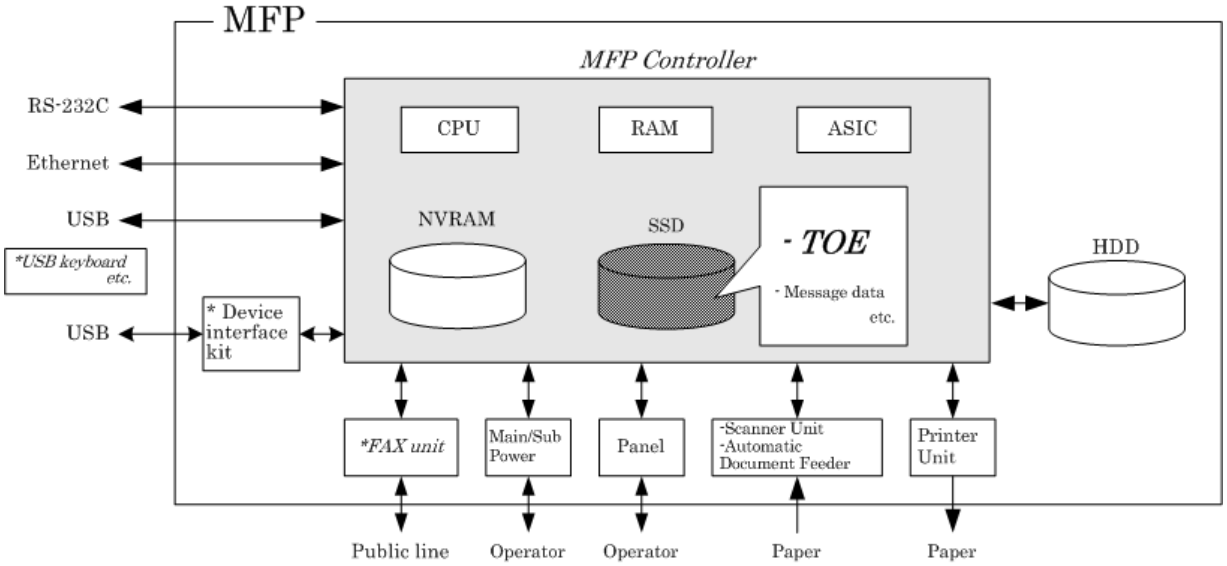

Figure 5-1 Hardware configuration relevant to the TOE

The TOE is composed of the OS part and the application part which controls the MFP. The application part which controls the MFP is composed of the following parts further.

- The part which provides interface through the network
  It controls Ethernet and provides TCP/IP-based communication function. The function of encryption for communication is provided in this part.

- The part which provides interface via the panel
  It has the function which receives the input from the panel as well as the function which draws the screen of the panel.

- The part which controls job
  A job means a unit for managing an execution control and operation order, of copy, print, scan, Fax, user box file operation, and so on.
  When "the part which controls each device" receives the operation from "the part which provides interface through the network" or "the part which provides interface via the panel" and the reception from the Fax unit, the job is generated and registered.
  The execution of the actual job is realized using the following parts, namely, "the part

which executes common management," "the part which handles HDD," and "the part which controls each device."

- The part which executes common management
  This part manages every kind of setting values and provides measure for which another part of the TOE accesses to the setting value. Every kind of setting values includes information used to execute security function, such as the authentication information.
  This part provides the function executing identification and authentication and the function of access control.

- The part which handles HDD
  This part provides the function of the processing image data and of the inputting/outputting to the HDD.
  In input/output function to the HDD, an encryption at the time of writing and a decryption at the time of reading are done by ASIC.

- The part which controls each device
  This part controls scanner unit, printer unit, and Fax unit, and realizes the actual operation of copy, print, scan, and Fax.
  Moreover, the mechanism does not allow an internal network to access from Fax unit.

- The part which provides support function
  This part provides a function used for support of MFP (function for diagnostics of MFP, function for updating the TOE).

5.2 IT Environment

The configuration of IT environment of this TOE in Figure 5-1 is explained as follows.

(1) SSD
A storage medium that stores the object code of the "MFP Control Software," which is the TOE. In addition to the TOE, it stores the message data expressed in each country's language to display the response to access through the panel and network, and the information of setting values like password.

(2) NVRAM
A nonvolatile memory. This storage medium stores various settings that MFP needs for the processing of the TOE. These setting values are managed in "the part which executes common management."

(3) ASIC
An integrated circuit for specific applications which implements HDD encryption functions for enciphering the data written in HDD. ASIC is used from "the part which handles HDD."

(4) HDD
A hard disk drive of 250GB in capacity. This is used not only for storing image data as files but also as an area to save image data and destination data temporarily during extension conversion, and so on. It is read and written from "the part which handles HDD."

(5) Main/sub power supply
Power switches for activating MFP

(6) Panel
An exclusive control device for the operation of the MFP, equipped with a touch panel of a liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc. It is controlled by "the part which provides interface via the panel."

(7) Scanner unit/ automatic document feeder
A device that scans images and photos from paper and converts them into digital data. It is controlled by "the part which controls each device."

(8) Printer unit
A device that actually prints the image data which were converted for printing when receiving a print request by the MFP controller. It is controlled by "the part which controls each device."

(9) Ethernet
It supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet. It is controlled by "the part which provides interface through the network."

(10)USB
Copying image file to an external memory, copying or printing image file from an external memory, update of TOE, and so on can be performed through this interface. It is usable as connection interface of the optional parts. The optional parts include the device interface kit which is needed for copying or printing from Bluetooth device and the USB keyboard to complement key entry from the panel, and it needs to be used, including an external memory.

(11)RS-232C
Serial connection using D-sub 9 pins is possible. The maintenance function is usable through this interface in the case of failure. It is also possible to use the remote diagnostic function by connecting with a modem which is connected with the public line. It is controlled by "the part which provides support function."

(12) FAX Unit
A device that has a port of Fax public line that is used for communications for FAX-data transmission and remote diagnostic via the public line. It is controlled by "the part which controls each device."

It is not pre-installed in the MFP as a standard function for selling circumstances, but sold as an optional part. Fax unit is purchased when an organisation needs it, and the installation is not indispensable.

6. Documentation

The identification of documents attached to the TOE is listed below.
TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

< For administrators and general users >

- bizhub C554 / C454 / C364 / C284 / C224 User's Guide Security Functions (Japanese) ver. 1.02
- bizhub C554 / C454 / C364 / C284 / C224 User's Guide [Security Operations] ver. 1.02
- bizhub C7828 / C7822 User's Guide [Security Operations] ver. 1.02
- ineo+ 554 / 454 / 364 / 284 / 224 User's Guide [Security Operations] ver. 1.02

< For service engineers >

- bizhub C554 / C454 / C364 / C284 / C224 Service Manual Security Functions (Japanese) ver. 1.01
- bizhub C554 / C454 / C364 / C284 / C224 / C7828 / C7822 SERVICE MANUAL SECURITY FUNCTION ver. 1.01
- ineo+ 554 / 454 / 364 / 284 / 224 SERVICE MANUAL SECURITY FUNCTION ver. 1.01

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 2011-11 and concluded upon completion of the Evaluation Technical Report dated 2012-10. 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, for site inspections, considering the previous inspections for the same series of the TOE, the evaluator directly visited the development and manufacturing sites on 2012-04, 2012-06 and 2012-07 and examined procedural status of configuration management, delivery, and security measures, focusing on the different parts of those from the same series of the TOE, by investigating records and interviewing staff. Further, 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 2012-07.

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 Technical Report.

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

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

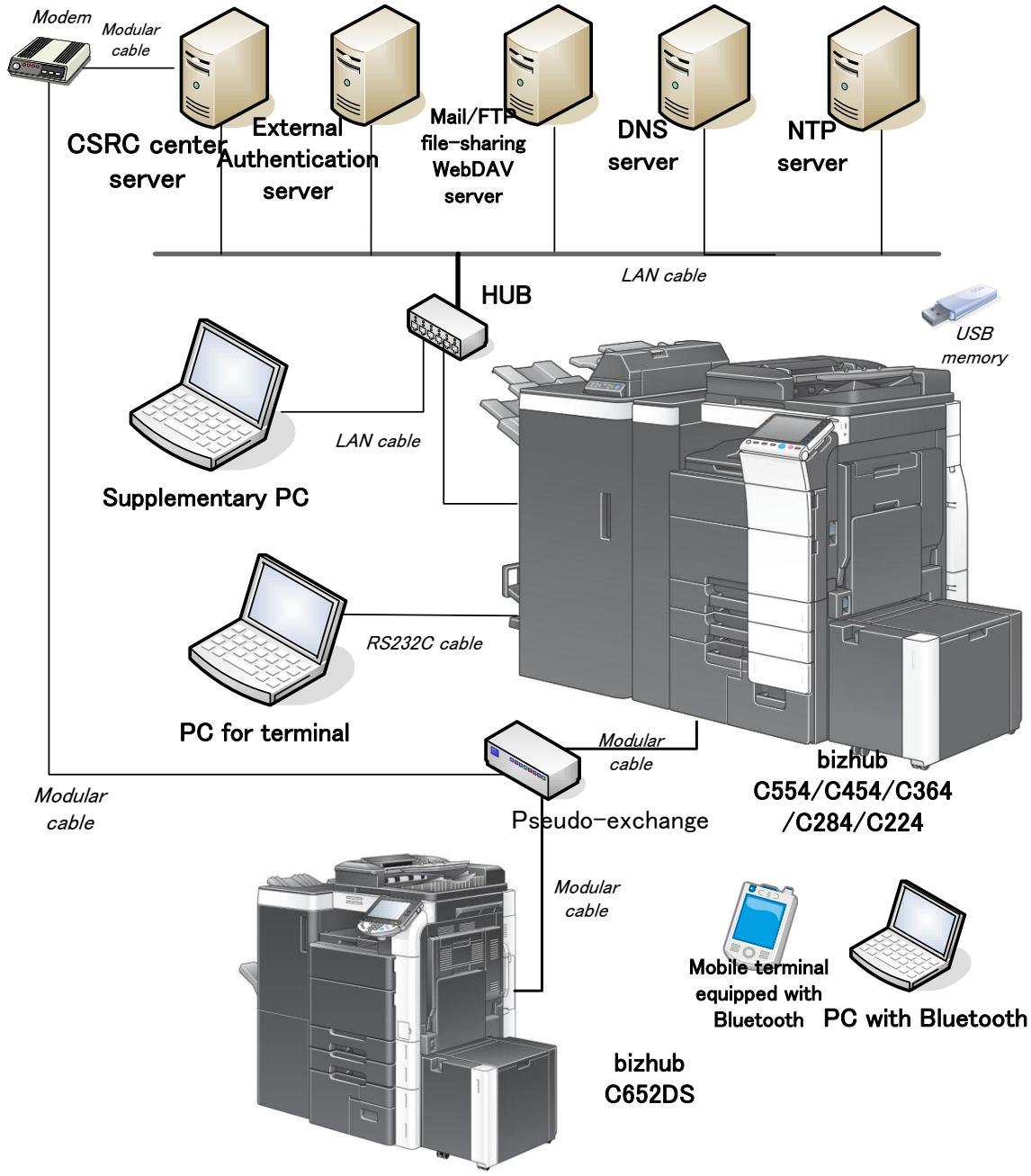

Figure 7-1 Configuration of the Developer Testing

The developer testing was 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 as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

When the functions have the external interfaces that the developer can use, the testing was conducted to execute security functions through the external interface. When the functions do not have the external interfaces that the developer can use, the testing was conducted to obtain and analyze the executed results of security functions through dump tool or capturing tool of communication data.

<Developer Testing Tools>

Table 7-1 Tools for the Developer Testing

Tool Name	Outline and Purpose of Use
KONICA MINOLTA C554 Series PCL PS Ver.1.2.0.0 XPS Ver.1.2.0.0	Exclusive printer driver software included in the bundled CD of bizhub C554 / C454.
KONICA MINOLTA C364 Series PCL Ver.1.1.4.0 PS Ver.1.1.2.0 XPS Ver.1.1.5.0	Exclusive printer driver software included in the bundled CD of bizhub C364 / C284 / C224.
Internet Explorer Ver. 6.0.2800.1106 (Win2000) Ver. 6.0.2900.5512 (WinXP)	General-purpose browser software. It is used to execute PSWC on the supplementary PC, and also used as SSL/TLS confirmation tool.
Fiddler Ver. 2.2.2.0	Monitoring and analyzing software tool of Web access of http, etc. It is used to confirm and test HTTP protocol between MFP and supplementary PC.
Open API test software tool Ver. 7.2.0.5	Exclusive test software tool for the Open API evaluation. For most of the tests for Open API, this tool software is used to confirm functions at the message level.
SocketDebugger Ver. 1.12	It is used as the test software tool for TCP-Socket.
WireShark Ver. 1.2.2	Software tool for monitoring and analyzing the communication on the LAN. It is used for getting communication log.
Mozilla Thunderbird Ver. 2.0.0.21	General-purpose mailer software. It is used as the confirmation tool of S/MIME mail on the supplementary PC.
Open SSL Ver.1.0.0d (8-Feb-2011)	Encryption software tool for SSL and hash function.

Tool Name	Outline and Purpose of Use
MG-SOFT MIB Browser Professional SNMPv3 Edition Ver. 10.0.0.4044	Exclusive browser software for MIB. It is used for tests related to SNMP.
Tera Term Pro Ver. 4.29	Terminal software executed on the terminal PC. It is used to connect with MFP and to operate the terminal software installed in MFP to monitor the state of the TOE.
Disk dump editor Ver. 1.43	Software tool to display the contents in the HDD.
Stirling Ver. 1.31	Binary editor software tool. It is used to confirm the contents of the encryption key and decode S/MIME messages and to edit print files.
FFFTP Ver. 1.92a	It is used as FTP client software.
MIME Base64 Encode/Decode Ver. 1.0	Software tool to encode/decode of MIME Base64. It is used as a tool to confirm encode/decode of S/MIME messages.
PageScope Data Administrator with Device Set-Up and Utilities Ver. 1.0.04000.05241	Device management software tool for administrators corresponding to plural MFPs. (Activation of the following plug-in software is possible.)
HDD Backup Utility (Plug-in) Ver. 1.3.09000.00023	HDD Backup Utility is the utility to backup (store) and restore (recover) the recorded media installed in MFP on the network.
PageScope Box Operator (PSBO) Ver. 3.2.03000	Software tool to acquire and print the image documents stored in the HDD. It is used as a tool to confirm the operation of trusted channel.
sslproxy Ver. 1.2	Proxy software in the supplementary PC operating between the main body of MFP and the browser software of the supplementary PC. By communicating with the main body through SSL and with browser software through non-SSL, it is possible to monitor by Fiddler and SocketDebugger, avoiding SSL encryption by sslproxy.
Blank Jumbo Dog Ver. 4.2.2	Simple server software for intranet. It is used as mailer server and FTP server function.
CSRC center software Ver. 2.6.2	Server software for CSRC center. CSRC is a maintenance service to manage the state of MFP which Konica Minolta business technologies, Inc. offers by remote.
LinuxReader Ver.2.0	Read Software tool of Linux configuration HDD.
WinHex Ver. 16.0 SR-8	Disk editor software tool.
Microsoft Excel 2003 SP3	Microsoft spreadsheet application. It is used for expanding audit log files and storing in Excel format.

b. Scope of the Performed Developer Testing

The developer testing was performed on 259 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested. By the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

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

7.3.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to ensure that security functions are certainly implemented from the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The configuration of the test performed by the evaluator is the same configuration as the developer testing.
The independent testing is performed in the same TOE testing environment as the TOE configuration identified in the ST. KONICAMINOLTA C554 Series PCL / PS / XPS, KONICAMINOLTA C364 Series PCL / PS / XPS and CSRC center software are the ones used for the developer testing, but these specification check, operation test, and calibration, were performed by the evaluator.

Only bizhub C554 / bizhub C284 / bizhub C224 are selected as MFPs, which the TOE is installed; however, it is judged that there is no problem in the result of the following confirmation by the evaluator.

- It was checked by the evidence from the developer that the differences of bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 are the speed of copy/print and the durability guaranteed performance. These differences were judged not to have any effect on the behavior of the performed tests by the evaluator.

- ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 are the products for OEM of bizhub C554/ bizhub C454/ bizhub C364/ bizhub C284/ bizhub C224 respectively.

2) Summary of the Independent Testing

The independent testing performed by the evaluator is as follows.

a. Viewpoints of the Independent Testing

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

<Viewpoints of Testing>
(1) For probabilistic and permutable mechanism, which is important for the security enhancement, the strictness of the developer testing from the point of view of interface type and parameter is supplemented.
(2) For different functions on the products of the same system (functions related to audit log), the strictness of the developer testing from the point of view of interaction with

other functions is supplemented.

(3) For the other functions, tests that are judged to be necessary regarding the variations of settings and parameter and the abnormal input are supplemented.

b. Independent Testing Outline

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

<Independent Testing Approach>

When the functions have the external interfaces that the evaluator can use, the testing was conducted to execute security functions through external interface. When the functions do not have the external interfaces that the evaluator can use, the testing was conducted to obtain and analyze the executed results of security functions through dump tool or capturing tool of transmitted data.

<Independent Testing Tools>

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

<Outline of each Independent Testing viewpoints>

A testing outline for viewpoint of independent testing is shown in Table 7-2.

Table 7-2 Independent Testing Performed

Viewpoints of Independent Testing	Outline of Testing
Viewpoint (1)	In the setup and change function of password, tests were performed to supplement the variations of the operation setting of identification and authentication function, the condition of settable password digit numbers, and the abnormal case of set password digit number. In the identification and authentication function, tests were performed to supplement the variations of the condition of settable password digit numbers, characters types of input password, and the case of wrong user name input.
Viewpoint (2)	Tests were performed to supplement the variations regarding the order of the operation that is for the use of the time setting function and output of audit log as well as the setting of authentication function and the output of audit log.
Viewpoint (3)	Tests were performed to supplement the variations regarding the setting of user setting function, the encryption passphrase of encryption key generation function, the encryption passphrase of ASIC operation support function, the combination of user box No. for user box access control and the user box file, and the expiration date of certificates in S/MIME transmission. Tests were performed to supplement the variations of abnormal case of transmission to the external authentication server, FAX, and Bluetooth.

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 (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 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.

<Vulnerability requiring the penetration testing>

(1) There is a possibility that the unexpected service related to the components used for the TOE is activated.
(2) The existence of the vulnerabilities within the public domain related to the components used for the TOE is concerned.
(3) Parameters to be input through the network are determined with the functional specification, but the unexpected input by the functional specification is available depending on the input method, and it is concerned to affect the TOE behavior.
(4) It makes it difficult to confirm that there is no concern when searching for the developer's documentation whether takeover of session is easily done or not, which is generally considered as the concern for Web interface, since it is known that it has Web interface from the functional specification.
(5) When retrieving the development documentation, concerns were detected that security functions are bypassed or falsified, depending on the timing of the power ON/OFF.
(6) As it is known from the ST, several types of interface supporting the authentication function exist. From the developer documentation, considering cases when authentication from different types of interface competes with each other, it is concerned that there is a possibility of being operated by an operator with different authority
(7) It is known from the development documentation that the setting of the enhanced security function is not on the HDD, but it is not confirmed of the testing that the exchange of HDD does not affect the enhanced security function.
(8) It is concerned that there are possibilities of hiding the unauthorized access by filling the audit log area up.

b. Penetration Testing Outline

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

<Penetration Testing Environment>

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

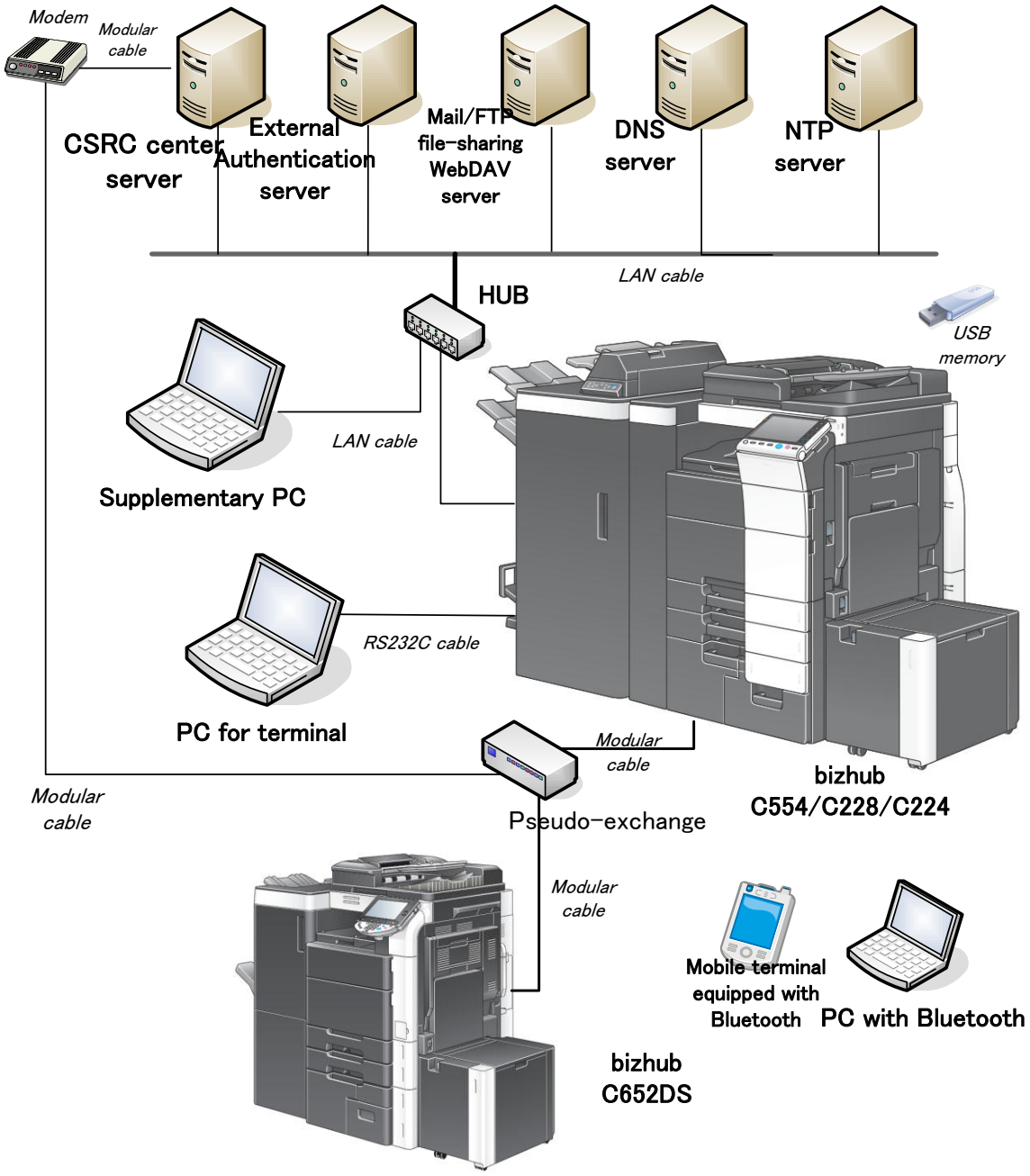

Figure 7-2 Configuration of Penetration Testing

<Penetration Testing Approach>

Penetration testing was done by the following methods.

- Method to check by the visual observation of the behavior after stimulating the TOE with operating from the operational panel.
- Method to check by the visual observation of the behavior after accessing the TOE through the network with operating the supplementary PC.
- Method to check the behavior by the testing tool after tampering parameters by using testing tool.
- Method to scan the publicly-known vulnerabilities by the vulnerability checking tool with operating the inspection PC.

<Tools, etc., used at Penetration Testing>

Test Configuration Environment	Details
Inspection object (TOE)	- The TOE installed in bizhub C554 / bizhub C284 / bizhub C224 (Version: A2XK0Y0-0100-G00-56) - Network configuration Penetration Testing was done by connecting each MFP with hub or cross-cable.
Supplementary PC	- PC with network terminal operated on Windows XP (SP2) or Windows 2000 (SP4). - Using the tools shown in Table 7-1. (Fiddler, OpenAPI test tool, SocketDebugger, etc.) - By accessing MFP using PSWC (abbreviation of "PageScope Web Connection"), HTTPS, TCPSocket, OpenAPI, and SNMP, etc., it can setup the network, etc. Furthermore, it is also possible to use TamperIE.
Inspection PC	- Inspection PC is a PC with network terminal operated on Windows XP SP3, and is connected to MFP with cross-cable to perform vulnerability tests. - Explanation of testing tools (The latest versions of plug-in and vulnerability database as of July 3, 2012, are applied.) (1)snmpwalk Version 3.6.1 MIB information acquiring tool (2)openSSL Version 0.9.8x Encryption tool of SSL and hash function (3)Nessus 4.4.1.(build 15078) Security scanner to inspect the vulnerabilities existing on the System (4)TamperIE 1.0.1.13 Web proxy tool to tamper the transmitted data from general Web browser such as Internet Explorer to arbitrary data (5)sslproxy v 1.2 2000/01/29 SSL proxy server software (6)Fiddler 2.4.0.0 Web debugger to monitor HTTP operation offered by MS (7)WireShark 1.8.0 Packet analyzer software that can analyze more than 800 protocols (8)Nikto Version 2.1.4 Publicly-known vulnerability inspection tool of CGI (9)extrstr 0.01 Binary analyze tool developed by the Evaluation facility. By using GNU binutils, the printable character string are extracted from binary to compile (10)Nmap 6.0.1 Security scanner to inspect the port on the system

<Content of the Performed Penetration Testing>

Table 7-3 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-3 Concerned Vulnerabilities and Overview of Testing

Concerned Vulnerabilities	Overview of Testing
Vulnerability (1)	Testing was performed to confirm a possibility of abusing by using the tool such as Nessus and behavior inspection.
Vulnerability (2)	Testing was performed to confirm a possibility of abusing by using the tool such as Nessus and result analysis.
Vulnerability (3)	Testing was performed to confirm that there is no influence on the behavior of security functions (domain separation, by-pass, interference, etc.) by transmitting edited parameters input through the network.
Vulnerability (4)	Testing was performed to confirm that the mechanism for holding session has a unique identification.
Vulnerability (5)	Testing was performed to confirm that the forced power ON/OFF does not affect the security functions of initialization process, screen display, and so on.
Vulnerability (6)	Testing was performed to confirm the exclusive control by accessing from operational panel and network simultaneously.
Vulnerability (7)	Testing was performed to confirm that the exchange of HDD does not affect the setting of the enhanced security function.
Vulnerability (8)	Testing was performed to measure the time to fill the audit log area up.

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

(1) Operating model

It is assumed that this TOE is installed either bizhub C554, bizhub C454, bizhub C364, bizhub C284, bizhub C224, bizhub C7828, bizhub C7822, ineo+ 554, ineo+ 454, ineo+ 364, ineo+ 284, or ineo+ 224, all of which are MFPs provided by Konica Minolta Business Technologies, Inc.

Because of the reason shown in 7.3.2, the evaluation is considered to be conducted with all models though the evaluation was not conducted with these all models.

(2) Setting of the TOE

The evaluation was conducted in the following setting.

- The enhanced security function is "valid"
- The user authentication method is either of the followings;
  "Machine authentication"
  "External server authentication" with Active Directory use

These settings are the settings as shown in the ST.

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 Extended
- Security assurance requirements: Common Criteria Part 3 Conformant

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

- All assurance components of EAL3 package

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

The evaluator recommendations for procurement personnel are not mentioned.

8. Certification

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

1. The submitted evidential materials were sampled, the contents were examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

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

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

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report 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

- This TOE depends on the following functions to counter threats (Refer to 4.3).
  > ASIC installed in MFP
  > Active Directory (In case the external server authentication method is selected for the user authentication function)
  > Difficulty of obtaining the information of setting values such as password which remains in SSD

  The reliability of these functions is not assured in this evaluation, and it depends on procurement personnel's judgment.

- If FAX unit as an optional part is not installed, FAX unit control function as a security function is invalid. (It does not affect the operation of other security functions.)

- By enabling the enhanced security function, a part of function cannot be used. It is recommended to check carefully the description of each setting written in "1.4.3.8 Enhanced security function" of the ST.

- Administrators should manage to register valid certificates for the validity of S/MIME certificates (collation with the certificate revocation list).

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 C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software A2XK0Y0-0100-G00-56 Security Target Version 1.01 (August 24, 2012) Konica Minolta Business Technologies, Inc.

11. Glossary

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

API	Application Programming Interface
DNS	Domain Name System
FTP	File Transfer Protocol
HDD	Hard Disk Drive
HTTPS	HyperText Transfer Protocol Security
MFP	Multiple Function Peripheral
MIB	Management Information Base
NVRAM	Non-Volatile Random Access Memory
RAM	Random Access Memory
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL/TLS	Secure Socket Layer/Transport Layer Security
S/MIME	Secure Multipurpose Internet Mail Extensions
TSI	Transmitting Subscriber Identification
USB	Universal Serial Bus

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

Administrator mode:
State possible for administrators to conduct the permitted operation to the MFP

Bluetooth: One of the short distance wireless communication technology used for connection between the devices, such as mobile device, in several meters

DNS: Protocol to manage the relationship of the domain name and IP address through the internet

Encryption passphrase:
Original information to generate the encryption key to encrypt and decrypt on ASIC

External network:
Network that access is restricted with intra-office LAN, which the TOE is connected, and with firewall, etc.

FTP: File Transfer Protocol used at TCP/IP network

HDD remaining image file:
File that remains in the HDD data area and is not deleted only by normal deletion operation (deletion of file management area)

HTTPS: Protocol adding the encryption function of SSL to hold a secure communication between Web server and client PC

Intra-office LAN:
Network which the TOE is connected being secured by using switching hub and eavesdropping detection device in the office environment, and being securely connected to the external network through firewall.

MIB: Various setting information, which the various devices managed by SNMP, open publicly

NVRAM: Random access memory that has a non-volatile and memory keeping character at the power OFF

PageScope Web Connection:
Tool installed in the main body of MFP to confirm and set the state of MFP by using browser

PC-FAX operation:
Operation to process sorting the received image data into user boxes based on the information specified at the time of FAX reception

Secure Print: Printing method that restricts by the password authentication. After specifying the password by the printer driver, printing by MFP is allowed only when the password is authenticated.

Secure Print file:
Image file registered by Secure Print

Secure Print password:
Password to confirm whether it is a permitted user or not before the operation to the secure print file

Service Mode: State possible for service engineers to conduct the permitted operation to MFP

S/MIME: Standard of e-mail encryption method. Transmitting and receiving the encrypted messages using RSA public key encryption system. Electric certificates published by the Certification Body are necessary.

SMTP: Protocol to transfer e-mail in TCP/IP

SNMP: Protocol to manage various devices through the network

SNMP password:
Generic term of password (Privacy password and Authentication password) to confirm users in use of SNMP v3, which is used in the TOE

SSL/TLS: Protocol to transmit by encrypting information through the internet

TSI reception: Function to designate the storing user box for each sender

User Box file: Image file stored in the user box, public user box, and group user box

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, March 2012, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, March 2012, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of Evaluation Facility, March 2012, 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 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: 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 C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software A2XK0Y0-0100-G00-56 Security Target Version 1.01 (August 24, 2012) Konica Minolta Business Technologies, Inc.

[13] bizhub C554 / bizhub C454 / bizhub C364 / bizhub C284 / bizhub C224 / bizhub C7828 / bizhub C7822 / ineo+ 554 / ineo+ 454 / ineo+ 364 / ineo+ 284 / ineo+ 224 Control Software Evaluation Technical Report, Version 2, October 25, 2012, Mizuho Information & Research Institute, Inc. Information Security Evaluation Office