Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2011-03-24 (ITC-1346)
Certification No.	C0313
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	Japanese : bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo⁺ 360 / ineo⁺ 280 / ineo⁺ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Zentai Seigyo Software English : bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo⁺ 360 / ineo⁺ 280 / ineo⁺ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software
Version of TOE	A0ED0Y0-0100-GM0-24
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.
2011-08-31

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

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria 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

"Japanese: bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo⁺ 360 / ineo⁺ 280 / ineo⁺ 220 / VarioLink 3622c / VarioLink 2822c /

VarioLink 2222c / D407 / D406 / D405 Zentai Seigyo Software,English: bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software Version A0ED0Y0-0100-GM0-24" has been evaluated in accordance with the provision 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 certification result in relation to IT Security Evaluation of "Japanese: bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software Zentai Seigyo Software, English: bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software Control Software Version A0ED0Y0-0100-GM0-24" (hereinafter referred to as "the TOE") developed by Konica Minolta Business Technologies, Inc., and evaluation of the TOE was finished on 2011-08 by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Konica Minolta Business Technologies, Inc. and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is 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 "general consumers" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee individual IT product itself.

1.1 Product Overview

Overview of the TOE functions and operational conditions is 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 C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software, which this TOE is installed, are digital Multi Functional Peripheral, provided by Konica Minolta Business Technologies, Inc., composed by selecting and combining copy, print, scan and FAX functions. (Multi Functional Peripheral, hereinafter all the products are referred to as "MFP".)

The TOE is the "bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software 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. 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 outside of the TOE.

- It is assumed as threat that the unauthorized access is done to the user box file stored in the private user box, the public user box or the group user box. To counter this threat, the TOE identifies and authenticates user 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 file or ID & print file. To counter this threat, the TOE identifies and authenticates user 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 leaks 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 and as a resulted in a leak of information or a change of setting value. To counter this threat, 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 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 the office which is managed by organisations such as a company or the 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 keep the secret about his/her own password.

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.

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

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation and completed on 2011-08 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], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report [13] prepared by Evaluation Facility and evaluation evidential materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure.
The Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and 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:

Name of the TOE:	Japanese：	bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software Zentai Seigyo Software
	English：	bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software Control Software
Version of the TOE:	A0ED0Y0-0100-GM0-24	
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.

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 same as the one in a service manual.

3. Security Policy

This chapter describes the security function policies and the organisational security policies adopted for countering the TOE against the threats.

This TOE operates the following data.

- Secure Print file

- ID & print file

- User Box file

To protect these data from unintended leak, the TOE identifies and authenticates a person who accesses 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 the leak from storage medium that stores these data or the related data.

This TOE realizes the followings for customer's demand.

- A function to prevent the leak from the communication path of these data

- A structure not to permit access from a FAX public line port of MFP to an internal network

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, the 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, the person-in-charge of the sales companies who performs the maintenance service of MFP 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 this, though not a user of TOE, those who go in and out the office are assumed as accessible person to 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 functions to counter them.

<p align="center">**Table 3-1 Assumed Threats**</p>

Identifier	Threat
T.DISCARD-MFP (Lease-return and discard of MFP)	When leased MFPs are returned or discarded MFPs are collected, secure print files, user box files, ID & print files, on-memory image files, stored image files, HDD-remaining image files, image-related files, transmission address data files, and various passwords which were set up can be leaked by the person with malicious intent when he/she analyzes the HDD or NVRAM in the MFP.
T.BRING-OUT-STORAGE (Unauthorized bringing out HDD)	- Secure print files, user box files, ID & print files, on-memory image files, stored image files, HDD-remaining image files, image-related files, transmission address data files, and various passwords which were set up can be leaked by a malicious person or a user illegally when he/she brings out and analyzes HDD in the MFP. - A person or a 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, on-memory image files, stored image files, HDD-remaining image files, image-related files, transmission address data files and various passwords which were set up are accumulated. A person or a user with malicious intent takes 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 which used a user function)	Exposure of the user box file when a person or a user with malicious intent accesses the user box where other user owns and operates the user box file, such as copies, moves, downloads, prints, transmits and so on.
T.ACCESS-PUBLIC-BOX (Unauthorized access to public user box which used a user function)	Exposure of the user box file when a person or a user with malicious intent accesses the public user box which is not permitted to use, and operates the user box file, such as copies, moves, downloads, prints, transmits, and so on.

Identifier	Threat
T.ACCESS-GROUP-BOX (Unauthorized access to the group user box which used a user function)	Exposure of the user box file when a person or a 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, transmits and so on.
T.ACCESS-SECURE-PRINT (Unauthorized access to the secure print file or ID & print file by utilizing the user function)	- Secure print files are exposed by a malicious person or user when he/she operates (prints etc.) those files which were not permitted to use. - ID & print files are exposed by a malicious person or user when he/she operates (prints etc.) those files which were stored by other users.

T.UNEXPECTED-TRANSMISSION
(Transmission to unintended address)
	- Malicious person or user changes the network settings that are related to the transmission of a user box file. 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 a user box file is exposed.
	
	  <The network settings which are related to user box file transmission>
	   > Setup related to the SMTP server
	   > Setup related to the DNS server
	
	- Malicious person or user 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.
	
	- Malicious person or user changes the TSI reception settings. A user box file is stored to the entity which a user does not intend to, so that a user box file is exposed.
	
	- Malicious person or user 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, a user box file is stored to the entity which a user does not intend to, so that a user box file is 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 (An unauthorized change of a function setting condition	The possibility of leaking user box files, secure print files, or ID & print files rises because a malicious person or user changes the settings related to the enhanced security function.

Identifier	Threat
related to security)	
TBACKUP-RESTORE (Unauthorized use of backup function and restoration function)	User box files, secure print files, or ID & print files can be leaked by a malicious person or user 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

This 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 the user.

The TOE provides the function to overwrite data for the deletion of all area of HDD and initialize the settings like passwords that is set in NVRAM (referred as "All area overwrite deletion function"), so it prevents the leakage of the protected assets and the security settings in HDD and NVRAM connected to the leased MFPs that were returned or discarded MFPs

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

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

This TOE provides the generation function of encryption key to encrypt the data written in the HDD (referred as "encryption key generation function") and the supporting function with the ASIC (referred as "ASIC operation support function") by using the encryption function of ASIC outside of the TOE, so that the encrypted data is 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 personal user box using user function)]

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

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

13

box (referred as "user box function") and the function that limits the changes in settings of users and personal user box to administrators and users (referred 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 as "External server authentication operation support function"), which is out of this TOE, in the user identification authentication function.

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

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

When using various functions of MFP with this TOE, the change in settings of public user box and the users is limited only to administrators and the permitted users, and the operation of public user box is restricted only to the 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 as "user function" and "administrator function"), the identification and authentication function on the access of public user box, 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 as "user box function") and the functions that limits the changes in settings of users to administrators and permitted users (referred 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 as "External server authentication operation support function"), which is out of this TOE, in the user identification authentication function.

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

This threat assumes the possibility that an unauthorized operation is performed by using the user function for the group user box that is a storage area of image file used by user who is permitted the use of the account, or the user box file in it.

When using various functions of MFP with this TOE, the change in settings of group user box and the users is limited only to administrators and the permitted users, and the operation of group user box is restricted only to the 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 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 as "user box function") and the functions that limits the changes in settings of users to administrators and permitted users (referred 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 as "External server authentication operation support function"), which is out of this TOE, in the user

identification authentication function.

(6) Security function to counter the threat [T.ACCESS-SECURE-PRINT (Unauthorized access to a secure print file and ID& Print file using user function)]

This threat assumes the possibility that an unauthorized operation is done to the secure print file and ID & print file using user function.

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 the permitted users, and the operation of secure print files and ID & print files are restricted only to the 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 as "user function" and "administrator function"), the authentication function with secure print password and identification and authentication function of user registered ID & print file, 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 as "secure print function") and the functions that limits the changes in settings of users to administrators and permitted users (referred 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 as "External server authentication operation support function"), which is out of this TOE, in the user identification 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 change of network setting, PC-FAX operation setting and TSI reception setting is restricted only to administrator, 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 administrator (referred 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 change of the specific function setting related to security is restricted only to administrator and service engineer, and as a result, it prevents the possibility of leakage

of the user box file, the secure print file or ID & print file; by maintaining the identification and authentication function of administrator (referred as "administrator function" and "SNMP manager function"), the identification and authentication function of service engineer (referred as "service mode function", and restricting function for setting the specific function related to security only to administrators and service engineer (referred as "administrator function", "SNMP manager function" and "service mode function") with this TOE.

(9) Security function to counter the threat [TBACKUP-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 being used the backup function and the restoration function illegally. Moreover, this assumes the possibility that user box files, secure print files, and ID & print files may be leaked as a result of leaking 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 following functions, the identification and authentication function of administrator, backup function and restore function, only to administrators (referred 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 is presented in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.COMMUNICATION-DATA (secure communication of image file)	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 pass to the correct destination, or encrypted when the organisation or the user expects to be protected.
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.

The term "between IT equipment" here indicates between client PC and MFP that the user uses.

3.2.2.2 Security Function Policies to Organisational Security Policies

16

The TOE provides the functions to fulfill 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 file)]

   This organisational security policy regulates carrying out processing via trusted path to a correct destination or encrypting to ensure the confidentiality about the image files which flow on a network, in case an organisation or a 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 one measure between MFP and client PC, which is used by users, needs to be provided when managing the secure print file, ID & print file and the user box file.

   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 file, the secure print file, and ID & print file (referred as "trusted channel function"), the encryption key generation function to transmit the user box file by S/MIME, the encryption function of user box file, the encryption function of encrypted key for S/MIME transmission (referred as "S/MIME encryption processing function"), the identification and authentication function of administrator, and the function to limit the change in settings related to the trusted channel and S/MIME only to administrator (referred as "administrator function"), so that it realizes to transmit to correct destination by transmitting image data confidentially in the network and restricting the change of settings only to the administrators.

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

   This organisational security policy regulates to prohibit 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 prohibits the access to the data existing in the internal network from public line via the Fax public line port (referred as "Fax unit control function"), so that it realizes to prohibit the access to the internal network via the Fax public line port.

4. Assumptions and Clarification of Scope

In this chapter, it describes the assumptions and the operational environment to operate the TOE as useful information for the judgment before the assumed reader uses the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE.
The effective performance 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 conditions to be an administrator)	Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations.
A.SERVICE (Personnel conditions to be a service engineer)	Service engineers, in the role given to them, will not carry out a malicious act during series of permitted operations.
A.NETWORK (Conditions for MFP Network connection)	- The intra-office LAN where the MFP with the TOE installed is not intercepted. - When the intra-office LAN where the MFP with the TOE installed is connected to an external network, access from the external network to the MFP is not allowed.
A.SECRET (Operating condition on secret information)	Each password and encryption passphrase will not be leaked from each user in the use of the TOE.
A.SETTING (Operational setting condition of enhanced security function)	The enhanced security function is enabled when a user uses the TOE. (Supplement) By enabling the enhanced security function, a part of function can not be used. Please refer to the description of each setting written in "1.4.3.8 Enhanced security function" of this ST.

4.2 Environment Assumptions

This TOE is installed in any one of bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software, which are MFPs provided by Konica Minolta Business Technologies, Inc.

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

If the external server authentication method is selected as 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.

The reliability of hardware, shown in this configuration, and cooperated software is outside the scope of this evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

The reliability of ASIC and Active Directory 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 the outside of 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 as 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 the outside of TOE and is not the scope of this evaluation.

5. Architectural Information

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

5.1 TOE boundary and component

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 main power is switched ON. The relation between the TOE and MFP is shown in Figure 5-1.

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.
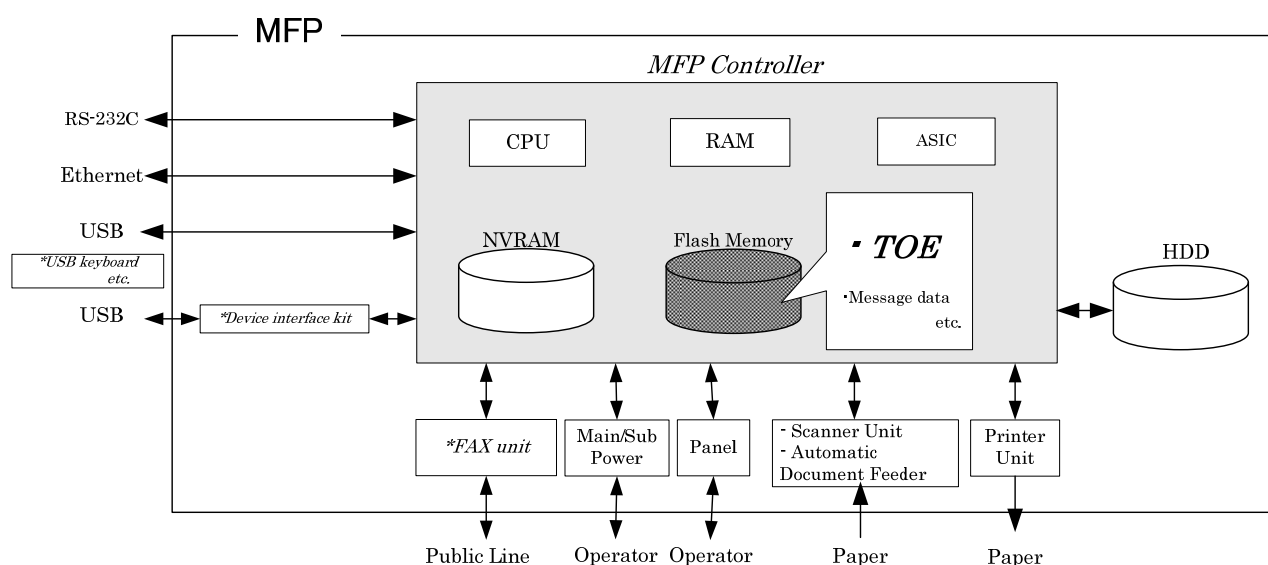
Figure 5-1 Hardware configuration relevant to TOE

The TOE is composed of OS part and 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 communication function of TCP/IP base.
    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 and the function which draws the screen of the panel.

- The part which controls job
    Job means the unit 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 "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 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 TOE).

5.2 IT Environment

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

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

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

(3) ASIC
  An integrated circuit for specific applications which implements a 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 users >

- bizhub C360 / C280 / C220 User's Guide Security Functions (Japanese)   Ver.1.02

- bizhub C360 / C280 / C220 User's Guide [Security Operations]   Ver.1.02

- bizhub C7728 / C7722 User's Guide [Security Operations]   Ver.1.02

- ineo⁺ 360 / 280 / 220 User's Guide [Security Operations]   Ver.1.02

- VarioLink 3622c / 2822c / 2222c User's Guide [Security Operations]   Ver.1.02

- D407 / D406 / D405 User's Guide [Security Operations]   Ver.1.02

< For service engineers >

- bizhub C360 / C280 / C220 Service Manual Security Functions (Japanese)   Ver.1.03

- bizhub C360 / C280 / C220 / C7728 / C7722 SERVICE MANUAL SECURITY FUNCTION
          Ver.1.03

- ineo⁺ 360 / 280 / 220 SERVICE MANUAL SECURITY FUNCTION   Ver.1.03

- VarioLink 3622c / 2822c / 2222c SERVICE MANUAL SECURITY FUNCTION   Ver.1.03

- D407 / D406 / D405 SERVICE MANUAL SECURITY FUNCTION   Ver.1.03

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

The history of evaluation conducted was presented in the Evaluation Technical Report as follows.

Evaluation has started on 2011-03 and concluded by completion of the Evaluation Technical Report dated 2011-08. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2011-05 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and interviewing staff.
Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2011-05.

7.3 IT Product Testing

The evaluator confirmed the validity of the test that the developer had executed. As a result of the evidence shown by the process of the evaluation and those confirmed validity, the evaluator executed the reappearance testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.
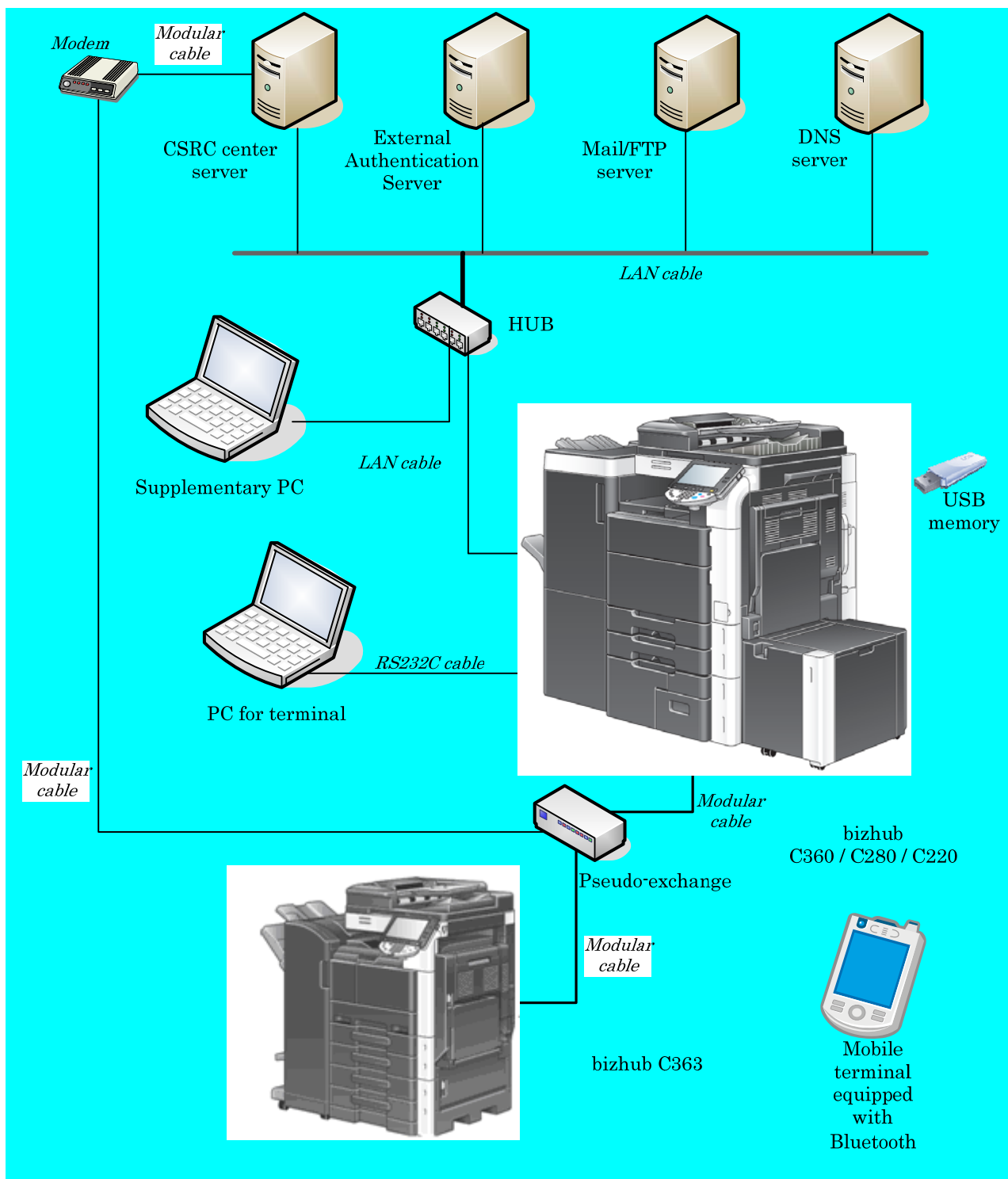
7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer executed and the testing documentation of actual test results. The overview of the developer testing evaluated by the evaluator is shown as follows;

1) Developer Testing Environment

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

Figure 7-1 Configuration of the Developer Testing

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

2) Summary of Developer Testing

Summary of the developer testing is as follows.

25

a. Developer Testing Outline

Outline of the developer testing is as follows;

<Developer Testing Approach>
When the functions have the external interfaces that developer can use, the testing was conducted to execute security functions through the external interface. When 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.

<Tools for the Developer Testing>

Table 7-1 Tools for the Developer Testing

Tool Name	Outline and Purpose of use
KONICA MINOLTA C360 Series PCL/XPS Ver.3.0.16.0	Exclusive printer driver software included in the bundled CD of bizhub C360 / C280 / C220.
Internet Explorer Ver. 6.0.2800.1106 (Win2000) Ver. 6.0.2900.2180 (WinXP)	General-purpose browser software. Used to execute PSWC on the supplementary PC. Also used as SSL/TLS confirmation tool.
Fiddler Ver. 2.2.2.0	Monitoring and analyzing software tool of Web access of http and etc. Use HTTP protocol to confirm and test 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	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. Used for getting communication log.
Mozilla Thunderbird Ver. 2.0.0.21	General purpose mailer software. Used as the confirmation tool of S/MIME mail on the supplementary PC.
Open SSL Ver.0.9.8k (25-Mar-2009)	Encryption software tool for SSL and hash function.
MG-SOFT MIB Browser Professional SNMPv3 Edition Ver. 10.0.0.4044	MIB exclusive browser software. Used for tests related to SNMP.
Tera Term Pro Ver. 4.29	Terminal software executed on the terminal PC. Used to connect with MFP and to operate the terminal software installed in the MFP to monitor the state of TOE.
Disk dump editor Ver. 1.43	Software tool to display the contents in the HDD.
Stirling Ver. 1.31	Binary editor software tool. Used to confirm the contents of the encryption key and decode S/MIME messages and to edit the print file.

Tool Name	Outline and Purpose of use
FFFTP Ver. 1.92a	Used as FTP client software.
MIME Base64 Encode/Decode Ver. 1.0	Software tool to encode/decode of MIME Base64. Used as a tool to confirm encode/decode of S/MIME messages.
Pagescope Data Administrator with Device Set-Up and Utilities Ver. 1.003200.10051	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. 1.3.03000 781	HDD Backup Utility is the utility to backup (store) and restore (recover) the recorded media installed in the MFP on the network.
PageScope Box Operator (PSBO) Ver. 3.2.03000	Software tool to acquire and print the image document stored in the HDD. Used as the confirmation tool of trusted channel.
sslproxy Ver. 1.2	Proxy software in the supplementary PC operating between MFP main body and the browser software of the supplementary PC. By communicating with 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. Used as mailer server and FTP server function.
CSRC center software Ver. 2.6.1	Server software for CSRC center. CSRC is maintenance service to manage the state of MFP which Konica Minolta business technologies, Inc. offers by remote.

b. Scope of Execution of the Developer Testing

The developer testing is executed on 348 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 tested enough.

c. Result

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

7.3.2 Evaluator Independent Testing

The evaluator executed the sample testing to reconfirm the executing of the security function by the test items extracted from the developer testing. The evaluator executed the evaluator independent testing (hereinafter referred to as "the Independent Testing") to

reconfirm that security functions are certainly implemented from the evidence shown by the process of the evaluation.

It explains the independent testing executed by the evaluator as follows.

1) Independent Testing Environment

The configuration of the test performed by the evaluator is the same configuration as the developer testing.

Independent Testing is performed in the same TOE testing environment as the TOE configuration identified in the ST.

Only bizhub C280 is selected as MFPs which TOE is installed, however it is judged not to have any problems in the result of the following confirmation by the evaluator.

- C7728 corresponds to C280. C7722 corresponds to C220. The name differs depending on the destination.

- ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 are the products for OEM of bizhub C360 / bizhub C280 / bizhub C220.

- It was confirmed by documents offered from developer that the difference of bizhub C360 / bizhub C280 / bizhub C220 lies only copy / print speed and the durability guarantee value.

2) Outline of Independent Testing

Independent testing performed by the evaluator is as follows.

a. Viewpoints of Independent Testing

The viewpoint of the independent testing devised by evaluator from the developer testing and the provided evaluation evidence are shown as follows.

<Viewpoints of Testing>
(1) Based on the situation of the developer testing, it applies to all security functions.
(2) Test targets are all probabilistic and permutable mechanism.
(3) Test the behaviors depending on the differences of password input methods to TSFI for the test of the probabilistic and permutable mechanism.
(4) Based on the strictness of the developer testing, test the necessary variations.
(5) Based on the complexity of interfaces, test the necessary variations.
(6) For the interfaces with innovative and unusual characters, test the necessary variations.
(7) Extracting the parameter which affects a lot to the security function, set the testing items by changing the input data variation, etc.

b. Outline of Independent Testing

Outline of independent testing performed by the evaluator is as follows;

<Independent Testing Approach>
When the functions have the external interfaces that evaluator can use, the testing was conducted to execute security functions through external interface. When

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.

<Tools for the Independent Testing>
The tools, etc., are the same as those used at the developer test.

<Outline of each Independent Testing viewpoints>
Testing outline for viewpoint of independent test is shown in Table 7-2.

Table 7-2 Independent Testing performed

Viewpoints of Independent Testing	Outline of Testing
(1) Viewpoint	Testing was performed, which were judged to be necessary in addition to the developer testing.
(2) Viewpoint	Testing was performed with changing the digit number of characters and the types of characters by paying attention to the probabilistic and permutable mechanism at identification and authentication, etc., by the user.
(3) Viewpoint	Testing was performed to confirm the behavior depending on the differences of password input method, with considering the operated interfaces.
(4) Viewpoint	Testing was performed to confirm the WebDAV server password modification function, based on the strictness of the test done by the developer.
(5) Viewpoint	Testing was performed to confirm the action at changing the types of user boxes by considering the complexity of various user boxes combination.
(6) Viewpoint	Testing was performed to confirm the action by judging the behavior of Fax unit control function and the abnormal behavior of Bluetooth device to be innovative or not general.
(7) Viewpoint	Related to the function improvement, the parameter which affects a lot to the security function is extracted, and the testing items by changing the input data variation, etc., were set.

c.　Result

All the executed independent testing 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 executed the necessary evaluator penetration testing (hereinafter referred to as "the penetration testing") for the possibility of exploitable concern at assumed environment of use and attack level. It explains the penetration testing executed by the evaluator as follows.

1) Summary of the Penetration Testing

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 public domain 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 component 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 documentations 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) Concerns were detected to be bypassed or falsified the security functions, depending on the timing of the power ON/OFF, when it is retrieved it to the documentations.
(6) Several types of interface supporting the authentication function exist, as it is known from the ST. It is concerned that the possibility to be operated by an operator with different authority by considering the case it competes with the authentication from different types of interfaces, from the documentations.
(7) It is known that the setting of the enhanced security function is not on the HDD from the development documentations, but it is not confirmed of the testing that the exchange of HDD does not affect the enhanced security function.

b. Outline of Penetration Testing

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

<Penetration Testing Environment>
Figure 7-2 shows the penetration testing configuration used by evaluator.
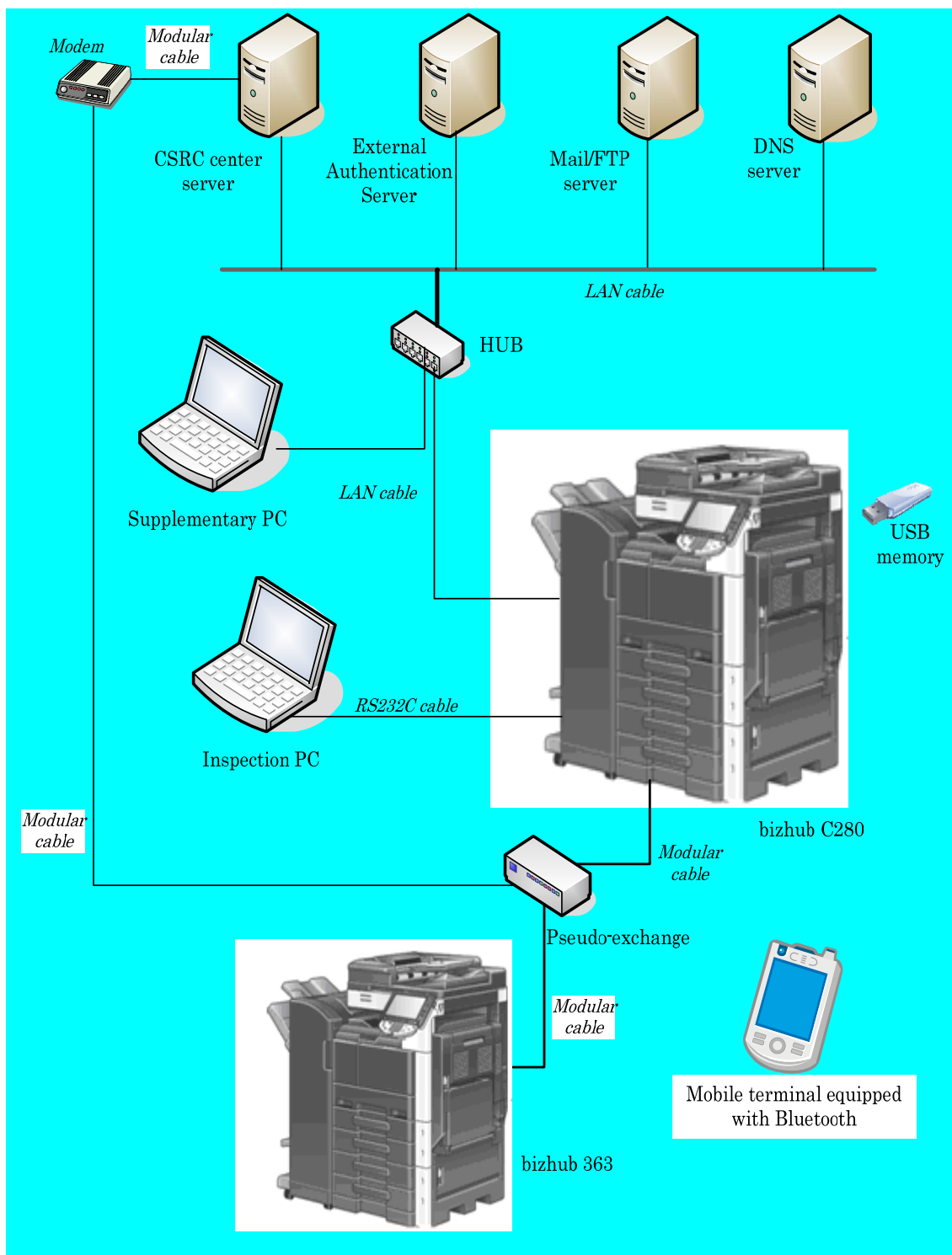
Figure 7-2 Configuration of Penetration Testing

<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 test 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)	- TOE installed in bizhub C280 (Version: A0ED0Y0-0100-GM0-24) - 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.) - Access the MFP by using PSWC (abbreviation of "PageScope Web Connection"), HTTPS, TCPSocket, OpenAPI, SNMP, etc., and it can setup the network, etc., Furthermore, 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 May 4, 2011 are applied.)
	(1)snmpwalk Version 3.6.1
	    MIB information acquiring tool
	(2)openSSL Version 0.9.8r
	    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 2.3.3.5
	    Web debugger to monitor HTTP operation offered by MS.
	(7)WireShark 1.4.6
	    Packet analyzer software that can analyze protocols more than 800
	(8)Nikto Version 2.1.4
	    Publicly-known vulnerability inspection tool of CGI

<Implementation items of Penetration Testing>
The concerned vulnerabilities and the corresponding penetration testing are shown in Table 7-3.

Table 7-3 Concerned Vulnerabilities and Overview of Testing

Concerned vulnerabilities	Overview of Testing
(1) Vulnerability	Testing was performed to confirm a possibility of abusing by

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

   c. Result

      In the conducted evaluator penetration testing, the exploitable vulnerabilities that
      attackers who have the assumed attack potential could exploit were not found.

7.4 Evaluated Configuration

   (1) Operating model
   It is assumed that this TOE is installed in any one of bizhub C360 / bizhub C280 / bizhub
   C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c /
   VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software 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 in all
   models though the evaluation was not conducted in 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 the conclusion that the TOE satisfies all work units prescribed in CEM by

submitting the Evaluation Technical Report.

In the evaluation, the followings 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 applied to the composed by the corresponding TOE to the identification described in Chapter 2.

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

The certification body conducted the following certification based on the materials submitted by Evaluation Facility in the evaluation process.

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

2. Rationale of 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.

The Certification Body confirmed no concerns found in the ST and the Evaluation Technical Report and issued this certification report.

8.1 Certification Result

As a result of verification of submitted Evaluation Technical Report and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the 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 that the external server authentication method is selected as for the user authentication function)

    The reliability of these functions is not assured in this evaluation, and it depends on operator'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 can not be used. It is recommended to check carefully the description of each setting written in "1.4.3.8 Enhanced security function" of this ST.

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

9. Annexes

There is no annex.

10. Security Target

Security Target[12] of the TOE is provided within a separate document of this certification report.

bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software Control Software A0ED0Y0-0100-GM0-24 Security Target Version 1.01 (April 20, 2011) 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
WebDAV	Web-based Distributed Authoring and Versioning

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

Administrator mode
State possible for administrator 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.

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 MFP to confirm and set the MFP state by using browser

PC-FAX operation
> Operation to process sorting the received image data into storage user boxes based on the information specified at the FAX receiving

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 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 the MFP

S/MIME
> Standard of e-mail encryption method. Transmitting and receiving the encrypted message using RSA public key encryption system. Electric certification published by certification body is necessary.

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

SNMP
> Protocol to manage various devices through network

SNMP password
> Generic term of password (Privacy password, Authentication password) to confirm the user at the use of SNMP v3 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.

WebDAV   Protocol to manage files on the Web server with expanded specification of HTTP1.1

12. Bibliography

[1]   IT Security Evaluation and Certification Scheme, February 2011, Information-technology Promotion Agency, Japan, CCS-01

[2]   IT Security Certification Procedure, February 2011, Information-technology Promotion Agency, Japan, CCM-02

[3]   Evaluation Facility Approval Procedure, February 2011, 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 C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software Control Software A0ED0Y0-0100-GM0-24 Security Target Version 1.01 (April 20, 2011) Konica Minolta Business Technologies, Inc.

[13]   bizhub C360 / bizhub C280 / bizhub C220 / bizhub C7728 / bizhub C7722 / ineo+ 360 / ineo+ 280 / ineo+ 220 / VarioLink 3622c / VarioLink 2822c / VarioLink 2222c / D407 / D406 / D405 Control Software Zentai Seigyo Software Evaluation Technical Report First Version (August 11, 2011) Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security