# Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

**Target of Evaluation**

| | |
|---|---|
| Application date/ID | 2008-10-30 (ITC-8239) |
| Certification No. | C0223 |
| Sponsor | Konica Minolta Business Technologies, Inc. |
| Name of TOE | Japanese : bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Zentai Seigyo Software<br>English : bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Control Software |
| Version of TOE | A0R50Y0-0100-G00-20 (System Controller)<br>A0R50Y0-1D00-G00-11 (BIOS Controller) |
| PP Conformance | None |
| Conformed Claim | EAL3 |
| Developer | Konica Minolta Business Technologies, Inc. |
| Evaluation Facility | Mizuho Information & Research Institute, Inc.<br>Center for Evaluation of Information Security |

This is to report that the evaluation result for the above TOE is certified as follows.
2009-07-15

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 Revision 2
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2

**Evaluation Result: Pass**

"Japanese：bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Zentai Seigyo Software, English：bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Control Software, Version：A0R50Y0-0100-G00-20 (System Controller), A0R50Y0-1D00-G00-11 (BIOS Controller)" 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

## 1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Japanese：bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622　Zentai Seigyo Software, English：bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Control Software, Version：A0R50Y0-0100-G00-20 (System Controller), A0R50Y0-1D00-G00-11 (BIOS Controller)" (hereinafter referred to as "the TOE") conducted by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"), and 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 corresponding ST. The operational conditions, details of usage assumptions, corresponding security objectives, security functional and assurance requirements needed for its enforcement, their summary of security specifications and rationale of sufficiency are specifically described in ST.

This certification report assumes "general consumer" to be a reader. Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

### 1.1.1 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

### 1.1.2 PP Conformance

There is no PP to be conformed.

## 1.2 Evaluated Product

### 1.2.1 Name of Product

The target product by this Certificate is as follows;

| | | |
|---|---|---|
| Name of Product: | Japanese： | bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 |
| | English： | bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 |
| Version: | Identifiable as above stated. | |
| Developer: | Konica Minolta Business Technologies, Inc. | |

### 1.2.2 Product Overview

bizhub 501, bizhub 421, bizhub 361, ineo 501, ineo 421, ineo 361, VarioLink 5022, VarioLink 4222, VarioLink 3622 is Konica Minolta Business Technologies, Inc. digital MFP (hereinafter referred to as "MFP"), in which this TOE is installed, comprised of

copy, print, scan and FAX functions in their selection and combination.

TOE is the "bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361/ VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Control Software" that controls the entire operation of MFP, including the operation control processing and the image data management that are accepted from the panel of the main body of MFP or through the network. TOE offers the protection function from exposure of the highly confidential document stored in the MFP. Moreover, TOE can prevent the unauthorized access to the image data stored in HDD by using the HDD lock function loaded on the HDD for the danger of taking HDD, the medium that stores the image data in MFP, out illegally. Besides, TOE possesses the deletion method according with the various overwrite deletion standards and it deletes all the data of HDD completely.

### 1.2.3 Scope of TOE and Security Functions

#### 1.2.3.1 Roles related TOE

The roles that relate to the use of the MFP are defined as follows.

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

(2) Administrator
MFP's user who carries out the management of the operation of MFP. An administrator performs the operation management of MFP and the management of user. In general, it is assumed that the person elected from the employees in the office plays this role.

(3) Service Engineer
A user who performs management of maintenance for the MFP. Service Engineer performs the repair and adjustment of MFP. (In general, the person in charge at the sales companies that performs the maintenance service of MFP and is in cooperation with Konica Minolta Business Technologies, Inc. is assumed.)

(4) Person in charge at the Organization that uses the MFP
A person in charge at the organization that manages the office where the MFP is installed. This person assigns an administrator who carries out the management of the operation of the MFP.

(5) Responsible person of the organization that manages the maintenance of the MFP
A responsible person of the organization (In general, the sales companies that performs the maintenance service of MFP) that manages the maintenance of MFP. Assigns service engineers who manage the maintenance for MFP.

Besides this, though not a user of TOE, a person who goes in and out in the office are assumed as an accessible person to TOE.

#### 1.2.3.2 Scope of TOE and Overview of Operation

TOE is the MFP control software and consists of System Controller and BIOS Controller. TOE exists as System Controller being one part of TOE on the compact flash memory (hereafter referred to as "CF") and as BIOS Controller on the flash memory being another part of TOE on the MFP controller which is loaded and run on the RAM when main power is switched ON. The relation between TOE and MFP is

shown in Figure 1-1.

In Figure 1-1, HDD, FAX unit, Encryption protection chip and Image controller marked as * are optional parts of MFP. The equipments of these optional parts are expected for the environment of TOE operation.

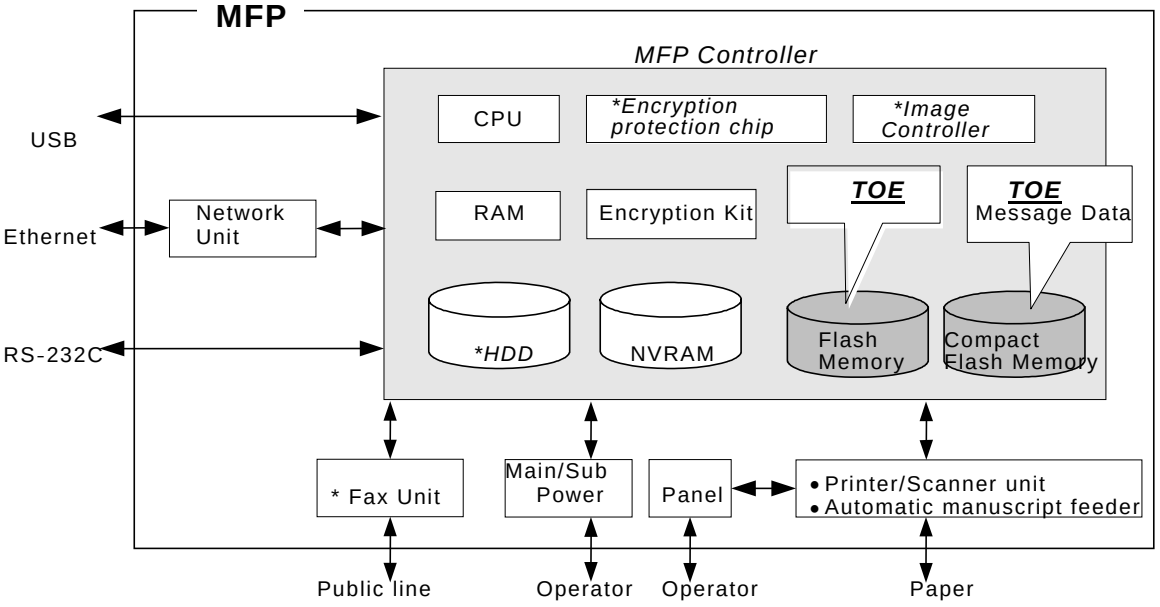


**Figure 1-1 Hardware structure that relates to TOE**

The components related to TOE are shown as follows.

(1)Compact Flash Memory (CF)
Storage medium that stores the object code of the System Controller of "MFP Control Software" that is the TOE. Additionally, it stores the message data of each country's language to display the response accessed through the panel and network. Furthermore this medium also stores various setting values which are needed for the operation of the MFP used for processing of TOE.
The security function (CF lock function) is installed, being possible to set the password and not being possible to read and write unless it agrees to the password. Furthermore, when the frequency of uniformity of it becomes unsuccessful in password collation, the function is also ready to lock the password collation function.

(2)Flash Memory
Storage medium that stores the object code of the BIOS Controller being a part of TOE.

(3)HDD (* Option)
Hard disk drive of 60GB in capacity. It is utilized besides the image data is stored as a file, temporarily image data with such as extension conversion, and as an area where the transmission address data kept.
The security function (HDD lock function) is installed, being possible to set the password and not being possible to read and write unless it agrees to the password. Furthermore, when the frequency of uniformity of it becomes unsuccessful in password collation, the function is also ready to lock the password collation function.
It is an optional part., but it is an essential component under this evaluation.

(4)NVRAM
Non-Volatile Memory. The memory medium that stores various setting values needed for the operation of the MFP used for processing of TOE.

(5)Encryption Kit or Encryption Protection Chip (* Option)
The cryptographic function, which is mounted in the Encryption Kit, the hardware on the MFP Controller, is installed in order to encipher image data to be written in HDD or CF. Encryption Protection Chip sold as an optional part is necessary to work encryption function.

(6)Image Controller (* Option)
The controller for image conversion process that be connected to MFP controller with Video bus. It is an optional part., but it is an essential component under this evaluation.

(7)Panel
The exclusive control device for the operation of the MFP equipped with the touch panel of a liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc.

(8)Main / Sub power
The power switch for activating MFP.

(9)Network Unit
The interface device to connect to the Ethernet. It supports 10BASE-T, 100BASE-TX and Gigabit Ethernet.

(10)USB
The Port to print with local connection. It has interface connected directly to MFP controller to backup the setting values, to update the TOE in addition to use Print function.

(11)FAX Unit (* Option)
A device that is used for the communication for sending and receiving FAX and for the remote diagnosis function (described later) via public line. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part.

(12)Scanner Unit / Automatic manuscript feeder
The device that scans images and photos from a paper and converts them into the digital data.

(13)Printer Unit
The device that actually prints the converted image data for printing when demanded to print by the MFP controller.

(14)RS-232C
The serial connection can be done. It can utilize a remote diagnostic function (later description) to connect with the modem connected with the public circuit.

A User (User, Administrator, and Service Engineer) uses a variety of functions of the TOE from the panel and a client PC via the network. The Overview of TOE functions are shown as follows.

(1)Basic Function

In MFP, a series of function for the office work concerning the image such as copy, print, scan, and fax exists as a basic function, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the MFP controller into the image file, and registered in RAM and HDD. (After two or more conversion processing is done, the conversion is done as for the print image file from PC.) The image file which has been converted into data for the print or for the transmission, and is transmitted to the device outside of the MFP controller concerned. Operations of copy, print, scan, and fax are managed by the unit of job, and can be changed the operation order, can be modified the finishing if it's a printing job, and can be cancelled the operation, by the command from the panel.

(2)User Box Function

The directory named "user box" can be created as an area to store the image file in HDD. Three types of user box exist; the first is the personal user box which a user possesses, the second is the public user box which the registered user making a group within a certain number uses jointly and the third is the group box which the users belong to same account uses jointly. As for the personal user box, the operation is limited only for the user who owns it, the public user box performs access control by sharing a password set to the user box among users and group box, the operation is limited only for the user who the use of the account is permitted. TOE processes the required operation, against the user box or the image file in a user box for an operation requests that is transmitted from the panel or the network unit through a network from a client PC.

(3)User Authentication Function

TOE can limit the user who uses MFP. When accessing it through the panel or the network, TOE performs the identification and authentication that the user is permitted to use the MFP by applying the user password and user ID. When the identification and authentication succeeds, TOE permits the user the use of the basic function and the user box function.

The following are supported in the method of the user authentication.

[Machine authentication]

A method to authenticate on MFP by registering a user ID and a user password into HDD on MFP controller.

[External server authentication]

A method to authenticate with processing the authentication on MFP by using the user ID and the user password that are registered on the user information management server which is connected in the office LAN without managing the user ID and user password on the MFP side.

In this evaluation, Machine authentication and External server authentication using Active Directory are the targets for evaluation.

(4)Account Authentication Function

TOE can manage the MFP users by grouping them into Account unit.

The methods of Account Authentication are as follows.

[Method synchronized with User Authentication]

The user is set Account ID which he belongs to beforehand, and the user is related to account ID of belonging account when user is certified.

[Method not synchronized with User Authentication]

When the certification is done by the account password set to each account ID, the user is related to the concerned account ID.

(5)Administrator Function

TOE provides the functions such as the management of user boxes, management of user information at the time of MPF authentication and management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can manipulate.

(6)Service Engineer Function

TOE provides a management function of administrator and a maintenance function, such as adjusting the device for Scan/Print etc, within the service mode that only a service engineer can operate.

(7)Encryption key generation Function

When the encryption protection chip, an optional product, is installed in MFP controller, the encoding and decoding is processed to the reading and writing data in HDD. (TOE does not process the encryption and description itself.)

The operation setting of this function is performed by the administrator function. When it operates, TOE generates the encryption key by the encryption pass phrase that was entered on the panel.

(8)Remote diagnostic Function

Making use of several connected systems such as E-mail, and a modem connection through a FAX public line mouth or a RS-232C, in communication with support center of MFP produced by Konica Minolta business technologies, Inc., it manages the state condition of MFP and the machinery information such as frequency of printing. In addition, if necessary, appropriate service (shipment of an additional toner, the account claim, dispatch of the service engineer due to the failure diagnosis, etc.) is provided.

When enhanced security function (later description) is set valid, this function becomes invalid.

(9)Updating function of TOE

TOE facilitated with the function to update itself. As for the update means, there are a method that exists as one of items of remote diagnostic function, a method that downloads from FTP server through Ethernet (TOE update function via Internet), and a method that performs the connection of the memory medium such as USB memory.

When enhanced security function (later description) is set valid, this updating function of TOE through Ethernet becomes invalid.

(10)Encryption Communication Function

TOE can encrypt the data transmitted from client PC to MFP, and the data received by download from MFP by using SSL/TLS. The operation setting of this function is performed by the administrator function.

(11)S/MIME certificate automatic registration Function

It is the function to register the certificate for S/MIME (conforms to ITU-T X.509) with each transmission address automatically. When a certificate is attached in received e-mail, MFP recognizes user ID according to the information of e-mail header, and registers the certificate as certificate of the same user ID.

(12)Enhanced Security Function

Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to

the secure values by the operation settings of the "Enhanced Security Function". Each value set is prohibited changing itself into the vulnerable one individually. As the function that does not have a setting function of the operation individually, there is the reset function of the network setting and the update function of TOE through the network, but the use of these functions is prohibited.

#### 1.2.3.3 Security Functions of TOE

The protected assets are the following image files which are produced as MFP is generally used.

- Secure Print File
  An image file registered by Secure Print.

- ID & Print File
  An image file stored as ID & print file when print data is registered by using ID & print function

- User Box file
  An image file stored in the personal user box, public user box and group user box.

Furthermore, when the stored data have physically been separated from the jurisdiction of a user, such as the use of MFP ended by the lease return or being disposed, or the case of an HDD or CF or NVRAM theft, a user has concerns about leak possibility of every remaining data. Therefore, in this case, the following data files become protected assets.

- Secure Print File

- ID & Print File

- User Box file

- On Memory Image File
  Image file of job in the wait state.

- Stored Image File
  Stored image files other than secure print file, ID & Print file and user box file.

- HDD remaining Image File
  The file which remains in the HDD data area that is not deleted only by general deletion operation (deletion of a file maintenance area).

- CF remaining Image File
  The file which remains in the CF data area that is not deleted only by general deletion operation (deletion of a file maintenance area). The data leak possibility does not exist when HHD is preinstalled as standard. When HDD is not preinstalled and image file happens to be in CF, this leakage possibility exists.

- File related to the Image
  Temporary data file generated in print image file processing.

- Transmission Address Data File
  File including E-mail address and telephone numbers that become the destination to transmit an image.

TOE has the following security functions to protect the above mentioned protected assets.

Firstly, TOE provides the identification authentication function to confirm that the user is permitted and the access control function to limit the access to protected assets for each user, in order to prevent the illegal operation to the secure print file or user box file of the protected assets.

Secondly, TOE provides the verification function the correct HDD or CF at the MFP power ON, all area overwrite deletion function of HDD or CF, the initialization function of set values for NVRAM and the encryption function of data written in HDD by using the lock function for HDD and CF outside of TOE and encryption function of encryption kit in order to prevent the leakage of information from HDD, CF and NVRAM where the protected assets are stored in MFP.

Thirdly, TOE provides the trusted channel function to use for the communication to the correct destination and the encryption transmitting function of image file from MFP to client PC by using S/MIME in order to protect securely the communication between TOE and client PC used by user or administrator.

Fourthly, TOE provides the identification authentication function to confirm the user to be the permitted administrator or service engineer and the management function to limit the access such as the change of set files for each user in order to prevent the illegal operation against the various set files that decide the action of MFP and TOE.

### 1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow;

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Control Software A0R50Y0-0100-G00-20 A0R50Y0-1D00-G00-11 Security Target" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022 / VarioLink 4222 / VarioLink 3622 Zentai Seigyo Software Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with

the CEM (either of [11] or [12]).

### 1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2009-07 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

# 2. Summary of TOE

## 2.1 Security Problem and assumptions

Problems should be solved by TOE and necessary assumptions are as follows;

### 2.1.1 Threat

This TOE assumes such threats presented in Table 2-1 and provides functions for countermeasure to them.

**Table 2-1 Assumed Threats**

| Identifier | Threat |
|---|---|
| T.DISCARD-MFP<br>(Lease-return and disposal of MFP) | When the leaser returned or the discarded MFP were collected, secure print files, ID & print files, user box files, on memory image files, the stored image files, the HDD remaining image files, the CF remaining image files, the image-related files, the transmission address data files, and the set various passwords can leak by the person with malicious intent taking out and analyzing an HDD or CF or NVRAM in MFP. |
| T.BRING-OUT-STORAGE<br>(An unauthorized carrying out of HDD) | - Secure print files, ID & print files, user box files, on memory image files, stored image files, HDD remaining image files, image-related files, transmission address data files, and the set-up various passwords can leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in MFP.<br>- A person or a user with malicious intent illegally replaces an HDD in MFP. In the replaced HDD, new files of the secure print files, ID & print files, user box files, on memory image files, stored image files, HDD remaining image files, image related files, transmission address data files and set various passwords are accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files leak. |
| T.ACCESS-PRIVATE-BOX<br>(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 personal user box where other user owns, and downloads, prints and transmits the user box file (E-mail transmission, FTP transmission, fax transmission, SMB transmission and WebDAV transmission). |
| T.ACCESS-PUBLIC-BOX<br>(Unauthorized access to public box which used a user function) | Exposure of the user box file when a person or the user with malicious intent accesses the public user box which is not permitted |

| | |
|---|---|
| | to use, and downloads, prints, transmits (E-mail transmission, FTP transmission, FAX transmission, SMB transmission and WebDAV transmission) and removes and copies to the other user box the user box file. |
| 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 the user with malicious intent accesses the group user box which the account where a user does not belong to owns, and downloads, prints, transmits (E-mail transmission, FTP transmission, FAX transmission, SMB transmission and WebDAV transmission) and removes and copies to the other user box the user box file. |
| 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 those malicious including users when he/she prints ones to which access is not allowed.<br>- ID & print files are exposed by those malicious including users when he/she prints ones which were registered 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 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.<br><br><The network setting which is related to user box file transmission><br>- Setting related to the SMTP server<br>- Setting related to the DNS server<br><br>- Malicious person or user changes the network setting which set in MFP to identify MFP itself where TOE installed, by setting to the value of the entity such as another illegal MFP from the value of MFP (NetBIOS name, AppleTalk printer name, IP address etc) that TOE is originally installed, so that secure print files or ID & print files are exposed.<br>- Malicious person or user changes the TSI receiving 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.<br>- Malicious person or user changes the PC-FAX operation settings. By changing the setting of the storing for the public user box to store 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.<br><br>*This threat exists only in the case that the operation setting of PC-FAX is meant to work as the operation setting for box storing. |
| T.ACCESS-SETTING<br>(An 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 those malicious including users change the settings related to the enhanced security function. |
| T.BACKUP-RESTORE<br>(Unauthorized use of Backup function and restoration function) | User box files, secure print files, or ID & print files can leak by those malicious including users using the backup function and the restoration function illegally. Also highly confidential data such as passwords can be exposed, so that settings might be falsified. |
| T.BRING-OUT-CF<br>(An unauthorized carrying out of CF) | The possibility of the following rises because a malicious person or a user with malicious intent illegally taking out and analyzing a CF in MFP.<br>- Leak of setting value (SNMP password, WebDAV server password).<br>- Operation by a falsified password (SNMP password, other operation setting values of various functions).<br>- Operation under falsified TOE.<br>- Leak of image information existed in the CF through remaining CF image file. |

### 2.1.2 Organizational Security Policy

Organizational security policy required in use of the TOE is presented in Table 2-2.

**Table 2-2 Organizational Security Policy**

| Identifier | Organizational Security Policy |
|---|---|
| P.COMMUNICATION-DATA<br>(secure communication of image file) | Highly confidential image files (secure print files, ID & print files and user box files) which transmitted or received between IT equipment is communicated via trusted pass to the correct destination, or has to be encrypted in the case of the organization or the user expect to be protected. |

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

### 2.1.3 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 2-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

**Table 2-3 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 given to them. |
| 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 the series of permitted operations given to them. |
| A.NETWORK (Network Connection Conditions for the MFP) | - The intra-office LAN where the MFP with the TOE will be installed is not intercepted.<br>- When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed. |
| A.SECRET (Operating condition concerning confidential information) | Each password and encryption pass phrase does not leak from each user in the use of TOE. |
| A.SETTING (Enhanced Security Function Operational Settings Condition) | MFP with the TOE is used after enabling the enhanced security function. |

### 2.1.4 Documents Attached to Product

The identification of documents attached to the TOE is listed below. TOE users are required full understanding of following documents and compliance with descriptions.

<Documents for administrator and user>

- bizhub 501 / 421 / 361 User's Guide [Security Operations] (Ver.103) (Japanese)
- bizhub 501 / 421 / 361 User's Guide [Security Operations] (Ver.103) (English)
- ineo 501 / 421 / 361 User's Guide [Security Operations] (Ver.103) (English)

- VarioLink 5022 / 4222 / 3622 User's Guide [Security Operations] (Ver.103) (English)

<Documents for service engineer>

- bizhub 501 / 421 / 361 Service Manual [Security Function] (Ver.1.01) (Japanese)
- bizhub 501 / 421 / 361 ineo 501 / 421 / 361 VarioLink 5022 / 4222 / 3622 Service Manual [Security Function] (Ver.1.01) (English)

### 2.1.5 Configuration Requirements

The TOE is software. This evaluation targets at the behavior on the following hardware and software. However the reliability of hardware and software described in the configuration is outside the scope of this evaluation.

- The configuration of Konica Minolta Business Technologies, Inc provided digital MFP, bizhub 501, bizhub 421, bizhub 361, ineo 501, ineo 421, ineo 361, VarioLink 5022, VarioLink 4222 and VarioLink 3622 equipped with the options such as HDD with HDD lock function, FAX unit, Encryption protection chip and Image controller.
- If the external server authentication is selected as for identification authentication of user, Active Directory, 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 authentication server.

## 2.2 Security Objectives

TOE counters threats described in 2.1.1 as follows by implemented security functions and fulfills the organizational security policies in 2.1.2.

(1)Security function to cope with T.DISCARD-MFP (Lease return and disposal of MFP)
This threat assumes the possibility of leaking information from MFP collected from the user.

TOE offers the function to overwrite data for the deletion to all area of HDD and initializes the information such as passwords of NVRAM and CF (referred as "All area overwrite deletion function"), so that it prevents the leakage of the protected assets and the security setting values in HDD, CF and NVRAM connected to the MFP that is returned by the leaser or the discarded.

(2)Security function to cope with T.BRING-OUT-STORAGE (Unauthorized taking out of HDD)
This threat assumes the possibility that the image data in HDD leaks by being stolen from the operational environment under MFP used or by installing the unauthorized HDD and taking away with the data accumulated in it.

By using HDD lock function that the HDD outside of TOE is not permitted to write before the authentication of HDD lock password, this TOE offers the function working with HDD with HDD lock function (referred as "HDD lock operation support function"), so that it requests the HDD lock password at reading the information form HDD and it prevents the leakage of the protected assets and the security setting values in HDD connected to the MFP that is illegally brought out and analyzed. Furthermore, by using the Encryption function of the encryption kit outside of TOE, this TOE offers the generation function of encryption key to encrypt the image data written on HDD (referred as "Encryption key generation function") and supporting function with the Encryption kit (referred as "Encryption kit operation support function"), so that it makes it difficult to decode the image data that is encrypted in HDD.

This TOE offers the verifying function that HDD is correct and has HDD lock function (referred as "HDD verification function"), so that information is stored only in the correct HDD with HDD lock function and it prevents the leakage of image data from HDD connected to MFP by taking out the HDD and replacing another HDD without the HDD lock function.

(3)Security function to cope with 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 MFP functions, this TOE offers the identification and authentication function of user and administrator (referred as "User function" and "Administrator function"), the access control function for personal user box (referred as "User box function") and restricting function for changing the setting of a personal user box and the user to administrator and the user (referred as "Administrator function", "User function" and "User box function"), so that the change of setting for a personal user box and the user is restricted to the permitted user, and the operation of the personal user box is restricted to the qualified user, and it prevents unauthorized access to the personal user box using user function.

Furthermore, this TOE offers 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 cope with 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 file.

When using various MFP functions, this TOE offers the identification and authentication function of user and administrator (referred as "User function" and "Administrator function"), the access control function for public user box, restricting function for changing the setting of public user box to Administrator and the user (referred as "User box function") and restricting function for changing the setting of user to Administrator and the user (referred as "Administrator function" and "User function"), so that the change of setting for public user box and the user is restricted only to administrator and the permitted user, and the operation of public user box is restricted only to the qualified user, and it prevents unauthorized access to the public user box using user function.

Furthermore, this TOE offers 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 cope with T.ACCESS-GROUP-BOX (Unauthorized access to a group 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 file.

When using various MFP functions, this TOE offers the identification and authentication function of user and administrator (referred as "User function" and "Administrator function"), the access control function for group user box, restricting function for changing the setting of group user box to Administrator and the user (referred as "User box function") and restricting function for changing the setting of user to Administrator and the user (referred as "Administrator function" and "User function"), so that the change of setting for group user box and the user is

restricted only to administrator and the permitted user, and the operation of group user box is restricted only to the qualified user, and it prevents unauthorized access to the group user box using user function.

Furthermore, this TOE offers 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 cope with T.ACCESS-SECURE-PRINT (Unauthorized access to secure print files and ID & print files using user function)
This threat assumes the possibility that an unauthorized operation is done to the secure print files and ID & print files using user function.

When using various MFP functions, this TOE offers the identification and authentication function of user and administrator (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 and ID & print files, the function that limits the changes in settings of secure print files and ID & print files to administrator (referred as "secure print function") and the functions that limits the changes in settings of users to administrator and permitted users (referred as "Administrator function" and "User function"), so that change of setting for secure print is restricted only to administrator, and change of setting for the user is restricted only to administrator and the permitted user, and the operation of secure print files and ID & print files are restricted only to the qualified user, and it prevents unauthorized access to the secure print files and ID & print files using user function.

Furthermore, this TOE offers 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 cope with T.UNEXPECTEC-TRANSMISSION (Transmission to unintended address)
This threat assumes the possibility of sending the user box file to the address that isn't intended, when the network setting that relates to the transmission or to the MFP address, PC-FAX operational setting or TSI receiving setting is illegally changed.

This TOE offers the identification and authentication function of administrator and restricting function for changing network setting, PC-FAX operation setting and TSI receiving setting only to administrator (referred as "Administrator function"), so that the change of network setting, PC-FAX operation setting and TSI receiving setting is restricted only to administrator, and it prevents the possibility of transmission to the address that isn't intended.

(8)Security function to cope with 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.

This TOE offers 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 administrator and service engineer (referred as "Administrator function", "SNMP manager function" and "Service mode function"), so that the change of the specific function related to security only to Administrator and Service engineer, and as a result, it prevents the possibility of leakage of the user box files, secure print files or ID & print files.

(9)Security function to cope with T.BACKUP-RESTORE (Unauthorized use of back-up function and restoration function)
This threat assumes a possibility that user box files, secure print files and ID & print files may leak since the back-up function or the restoration function being illegally used. Moreover, this assumes that because of a leak of confidential data such as the password, the various setting values are falsified and there is a similar possibility that user box files, secure print files or ID & print files may leak.

This TOE offers the identification and authentication function, and restricting function for the use of back-up function and restore function only to administrator (referred as "Administrator function"), so that the use of back-up function and restore function is restricted only to administrator, and as a result, it prevents the possibility of leakage of user box files, secure print files, ID & print files or secure data such as passwords.

(10)Security function to cope with T.BRING-OUT-CF (Unauthorized taking out of CF)
This threat assumes the possibility that the leak of the information data in CF by being taken away or the unauthorized operation by installing the CF with falsified information or TOE.

By using CF lock function that the CF outside of TOE is not permitted to write before the authentication of CF lock password, this TOE offers the function working with CF with CF lock function (referred as "CF lock operation support function"), so that it requests the CF lock password at reading the information form CF and it prevents the leakage of the protected assets and the security setting values in CF connected to the MFP that is illegally brought out and analyzed.

This TOE offers the verifying function that CF is correct and has CF lock function (referred as "CF verification function"), so that information is stored only in the correct CF with CF lock function and MFP works on the correct TOE, therefore it prevents the leakage of information from CF connected to MFP or the illegal operation by taking out the CF and replacing another CF without the CF lock function.

(11)Security function to satisfy P.COMMUNICATION-DATA (secure communication of image file)
This organizational security policy prescribes carrying out processing via trusted pass to a correct destination or encrypting to ensure the confidentiality about the image file which flows on a network in the case of the organization or the user expect 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 secure communication method between MFP and client PC needs to be provided when transmitting the secure print files, ID & print files or user box files.

This TOE offers the Trusted Channel to a correct destination in the transition and reception of an image such as from MFP to client PC or from client PC to MFP, for user box files, secure print files and ID & print files (referred as "Trusted channel function"), the encryption key generation function to transmit by encrypting the

user box file including the confidential image data in S/MIME (referred as "S/MIME encryption processing function"), the identification authentication function of administrator and restricting function of the change of the setting for trusted channel and S/MIME only to Administrator (referred as "Administrator function"), so that it makes it possible to transmit to a correct destination by transmitting image data confidentially in the network and restricting the change of setting only to the administrator.

# 3. Conduct and Results of Evaluation by Evaluation Facility

## 3.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

## 3.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows;

Evaluation has started on 2008-11 and concluded by completion the Evaluation Technical Report dated 2009-07. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on 2009-02 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-02.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

## 3.3 Product Testing

The evaluator confirmed the validity of the test that the developer had executed.
The evaluator executed reappearance tests, additional tests and penetration tests based on vulnerability assessments judged to be necessary from the evidence shown by the process of the evaluation and results by the verification of the developer testing.

### 3.3.1 Developer Testing

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

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 3-1.

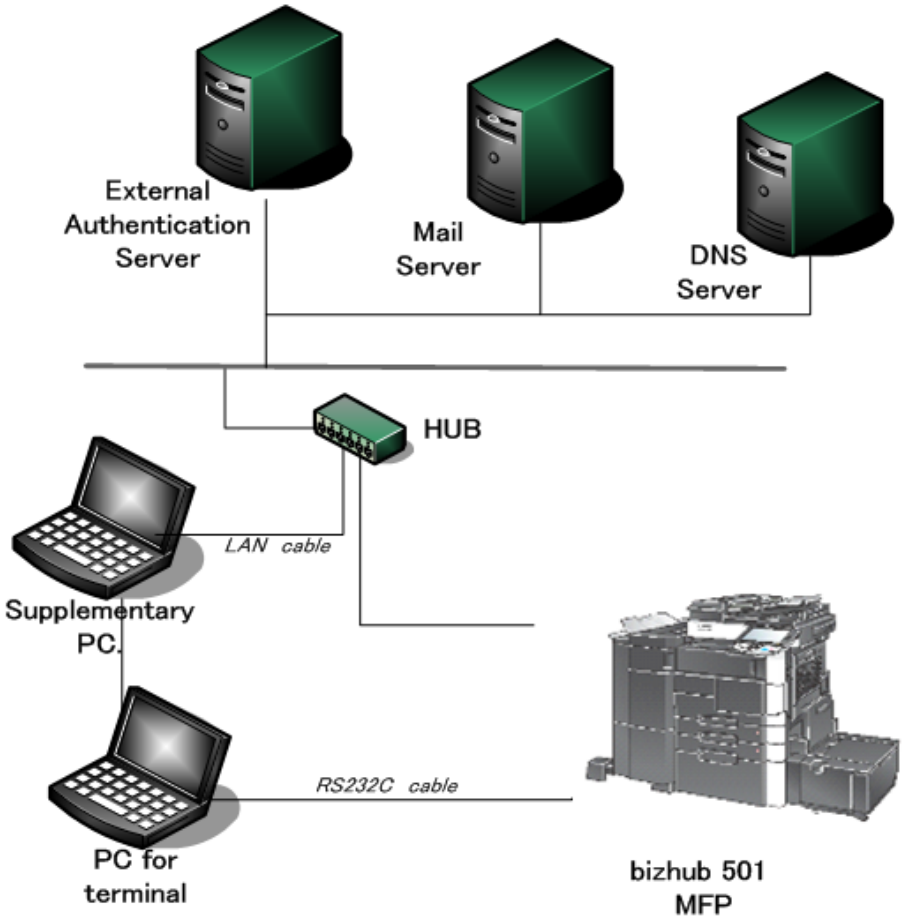


**Figure 3-1 Configuration of Developer Testing**

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

Only bizhub 501 is selected as the MFP installed with TOE, but evaluator judged there is no problem as the results of the following confirmation.

- Confirmed that the difference among bizhub 501, bizhub 421 and bizhub 361 is only in their copy/print speed and guaranteed value of durability according to the provided documents from developer.
- Confirmed that the test results are the same and no affection to the security functions under the partial sampling tests for bizhub 361 that are extracted from bizhub 501 developers testing.

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow;

a. Test outline

Outlining of the testing performed by the developer is as follows;

<Testing Approach>
Test was done to execute security functions through external interface when the functions have the external interfaces that developer can use, and was done to get and analyze the executed results of security functions through dump tool or capturing tool of transmitted data when functions do not have the external interfaces that developer can use.

<Tools and others used at Testing>
The tools and others are shown in Table 3-1.

**Table 3-1 Tools and others used in developer testing**

| Name of hardware and software | Outline and Purpose of use |
|---|---|
| Pseudo-exchange | Device for FAX communication. Using this pseudo-exchange, MFP can connect with the opposed machine in FAX communication. |
| Opposed FAX | Opposed FAX machine to send FAX to the MFP in FAX communication. |
| KONICA MINOLTA 501 Series PCL Driver Ver. 2.0.1.0 | Exclusive printer driver software included in the bundled CD of bizhub 501. |
| KONICA MINOLTA 501 Series XPS+ Driver Ver. 2.0.1.0 | Exclusive printer driver software included in the bundled CD of bizhub 501. |
| Internet Explorer Ver. 6.0.2900.2180 | General purpose browser software. Used to execute PSWC in the supplementary PC. Also used as SSL/TLS confirmation tool. |
| Fiddler Ver. 1.2.0.0 | Monitor and analyzing tool for web access of http and etc. Used to test HTTPS protocol between MFP and supplementary PC. |
| Open API test tool Ver. 7.2.0.5 | Exclusive test tool for the Open AP evaluation. Most of the tests for Open API are to confirm the functions at the communication level by this tool. |
| SocketDebugger Ver. 1.12 | Used as the test tool for TCP-Socket. |
| WireShark Ver. 0.99.5 | Tool for monitoring and analyzing of the communication on the LAN. Used to get communication log. |
| Mozilla Thunderbird Ver. 2.0.0.12 | General purpose mailer software. Used as the confirmation tool of S/MIME mail on the supplementary PC. |
| Open SSL Ver. 0.9.8.g | Encryption tool software for SSL and hash function. |
| MG-SOFT MIB Browser Professional SNMPv3 Edition (hereafter referred and abbreviated as "MIB Browser") Ver. 10.0.0.4044 | MIB exclusive browser software. Used for tests related to SNMP. |
| Tera Term Pro Ver. 4.10 | Terminal software executed in the terminal PC. Used to connect MFP and to operate the terminal software installed in the MFP to monitor the state of TOE. |
| Disk dump editor | Tool software to display the contents in the HDD. |

| Name of hardware and software | Outline and Purpose of use |
|---|---|
| Ver. 1.33 | |
| TamperIE Ver. 1.0.1.13 | Software to change POST parameters at the login by public user using Web browser. |
| Stirling Ver. 1.31 | Binary editor to confirm the contents of the encryption key and decode S/MIME message and to edit the print file. |
| FFFTP Ver. 1.92a | FTP client software. |
| Microsoft Office Excel 2007 12.0.6123.1000 | Used to confirm the contents of export file. |
| MIME Base64 Encode/Decode v1.0 | Tool used to confirm Encode/Decode of S/MIME message. |
| PageScope Data Administrator (PSDA) with Device Set-up and Utilities Ver. 1.0.2000.21092 | Device management tool for administrator of plural MFPs.<br>(Activation of the following 2 plug-in software is possible.) |
| HDD Backup Utility Ver. 1.3.01000.1050 | HDD Backup Utility is the utility installed in the MFP on the network to backup and to restore the recorded media. |
| PageScope Data Administrator (PSDA) Ver. 4.1.2000.12051 | Tool to register the address information of Email, Fax or etc. in the MFP and to restrict the use by user.<br>Used as the Open API Interface confirmation tool. |
| PageScope Box Operator (PSBO) Ver. 3.2.01000 | Tool to acquire and to print or other the image document reserved in the HDD.<br>Used as the TCP Socket Interface confirmation tool. |
| Pagescope Web Connection (PSWC) Ver. 3.2.1 | Tool installed in the MFP main body to set and confirm the state of the main body.<br>Used as the HTTP Interface confirmation tool. |
| sslproxy Ver. 2.0 | Proxy software in the supplementary PC operating between MFP main body and the browser software of the supplementary PC.<br>By communicating with main body through SSL and with browser software through non-SSL, it makes Fiddler and Socket Debugger possible to monitor avoiding SSL encryption by sslproxy. |
| Blank Jumbo Dog Ver. 4.1.3 | Simple server software for intranet.<br>Used as the Web and mailer server function at the S/MIME tests. |

b. Scope of Testing Performed

Testing is performed about 199 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the TOE design and the subsystem interfaces.

c. Result

The evaluator confirmed consistencies between the expected test results and the

actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

### 3.3.2 Evaluator Independent Testing

Evaluator executed the independent testing to reconfirm that Security functions are certainly implemented from the evidence shown by the process of the evaluation.
Outlining of the independent testing performed by the developer is as follow;

1) Evaluator Independent Test Environment

Test configuration performed by the evaluator shall be the same configuration with developer testing.
Test configuration performed by the evaluator shall be the same configuration with TOE configuration identified in ST.

2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. In terms of Evaluator Independent Testing

Evaluator devised the independent testing from the developer testing and the provided documentation in terms of followings.

<Viewpoints of Test>
(1)Based on the situation of developer test, test as many security functions as possible.
(2)Test targets are all probabilistic and permutable mechanism.
(3)Test the behavior depending on the differences of TSFI password input methods in the probabilistic and permutable mechanism.
(4)Based on the strictness of the developer test, test the necessary variations.
(5)Based on the complexity of interfaces, test the necessary variations.
(6)For the interfaces with innovative and unusual character, test the necessary variations.

b. Outlining of Evaluator Independent Testing

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

<Testing Approach>
Test was done to execute security functions through external interface when the functions have the external interfaces that evaluator can use, and was done to get and analyze the executed results of security functions through dump tool or capturing tool of transmitted data when functions do not have the external interfaces that evaluator can use.

<Tools and others used at Testing>
The tools and others are the same as used ones at the developer test.

<Test viewpoints and testing outline>
Test outline for each independent test viewpoint is shown in Table 3-2.

**Table 3-2 Viewpoints of Independent Test and Overview of Testing**

| Viewpoints of Independent Test | Overview of Testing |
|---|---|
| (1) Viewpoint | Test was performed that was judged to be necessary in addition to developer test. |
| (2) Viewpoint | Test was performed with changing the number of letters and the kinds of letters by paying attention to the probabilistic and permutable mechanism at identification authentication or etc. by the user. |
| (3) Viewpoint | Test was performed with considering the operated interfaces to confirm the behavior depending on the difference of password input method. |
| (4) Viewpoint | Test was performed with considering the detailed level of developer test to confirm the HDD verifying function, CF lock verifying function, WebDAV server password modification function and the state of encryption. |
| (5) Viewpoint | Test was performed with considering the complexity of interfaces to confirm the action at changing the kind of box. |
| (6) Viewpoint | Test was performed with considering the interface with innovative and unusual character to confirm the action of the HDD verifying function and CF lock verifying function. |

c. Result

All evaluator independent tests conducted were complete correctly and could confirm the behavior of the TOE. The evaluator also confirmed that all the test results are consistent with the behavior.

### 3.3.3 Evaluator Penetration Testing

Evaluator devised and conducted the necessary penetration testing about the possibility of exploitable concern at assumed environment of use and attack level.
Outlining of f Evaluator penetration testing is as follows;

1) Outlining of Evaluator Penetration Testing

Outlining of penetration testing performed by the evaluator is as follows;

a. Vulnerability of concern

Evaluator searched the potential vulnerability from information which is within the public domain and provided evidence to identify the following vulnerability that requires penetration testing.

<Vulnerability requiring the penetration tests>

(1)Possibility of the unexpected service activation.
(2)Possibility of the detection of the publicly known vulnerability found by the vulnerability checking tool.
(3)Possibility to affect the behavior of the TOE through the variation of input data.
(4)Possibility of the easy speculation of session information.
(5)Possibility to affect the security functions by the power ON/OFF.
(6)Possibility of the inappropriate exclusive access control.
(7)Possibility to affect the security function through the setting status of CF lock password.

b. Scope of Test Performed

Evaluator conducted the following penetration testing to determine the exploitable potential vulnerability.

<Testing Environment>
Figure 3-2 shows the penetration test configuration used by evaluator.

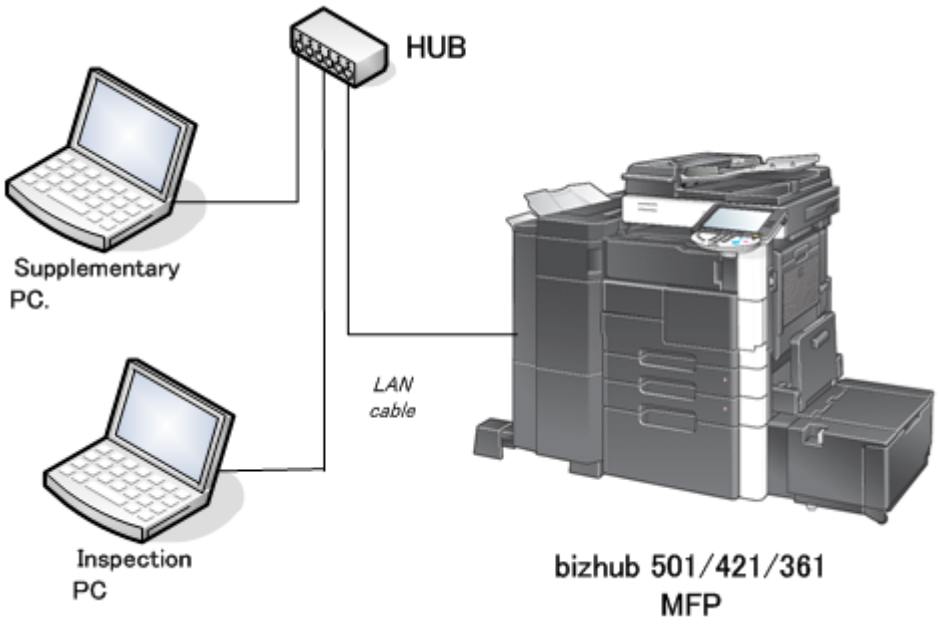


**Figure 3-2 Configuration of Penetration Testing**

<Testing Approach>
Test was done to use the following methods; a method to check by the visual observation of the behavior after stimulating TOE with operating from the operational panel, a method to check by the visual observation of the behavior after accessing TOE through network with operating from supplementary PC, a method to check by the test tool of the behavior after tampering parameters by using test tool, a method to scan the publicly known vulnerability by the vulnerability checking tool with operating from inspection PC.

<Tools and others used at Testing>
The tools and others used at tests are shown in Table 3-3

**Table 3-3 Tools and others used at Penetration Testing**

| Test Configuration Environment | Details |
|---|---|
| Inspection object (TOE) | - TOE installed in bizhub 501/421/361<br>(System Controller：A0R50Y0-0100-G00-20<br>BIOS Controller ：A0R50Y0-1D00-G00-11)<br>- Network configuration<br>Penetration testing was done by connecting each MFP with hub or cross-cable. |
| Supplementary PC | - PC with network terminal operated on Windows XP SP2.<br>- Using the tools shown in table 3-1.<br>(Fiddler, OpenAPI test tool, SocketDebugger and etc.)<br>- Using PSWC (abbreviated word of "PageScope Web Connection"), Https, TCPSocket, OpenAPI, SNMP and etc., this PC is possible to access the MFP and to set network setting. Furthermore it can use TamperIE. |
| Inspection PC | - Inspection PC is a PC with network terminal operated on Windows XP SP2, and is connected to MFP with cross-cable to perform penetration test.<br>- Explanation of test tools<br>(1)Snmpwalk Version 3.6.1<br>MIB information acquiring tool<br>(2)openSSL Version 0.9.8d<br>encryption too of SSL and hash function<br>(3)Nesuss 3.2.1.1<br>Security scanner to inspect the vulnerability on the System<br>(4)TamperIE 1.0.1.13<br>Web proxy tool to tamper the transmitted data from general Web browser such as Internet Explorer to arbitrary data.<br>(5)sslproxy Version 2.0<br>SSL proxy server software<br>(6)Fiddler 2.2.0.7<br>Web debugger to monitor HTTP operation<br>(7)Wireshark 1.06<br>Packet analyzer software<br>(8)Nikto Version 2.03<br>CGI and publicly known vulnerability inspection tool |

<Concerned vulnerabilities and Test outline>
The concerned vulnerability and the corresponding test outline are shown in Table 3-4

**Table 3-4 Concerned vulnerabilities and Overview of Testing**

| Viewpoints of Independent Test | Overview of Testing |
|---|---|
| (1) Vulnerability | Test was performed to confirm possibility of abusing by using the tool such as Nessus and behavior inspection. |
| (2) Vulnerability | Test was performed to confirm possibility of abusing by using the tool such as Nessus and result analysis. |
| (3) Vulnerability | Test was performed to confirm that there is no influence on the security behavior (domain separation, by-pass, interference and etc.) by transmitting of edited parameters through network. |
| (4) Vulnerability | Test was performed to confirm that the mechanism for holding session has a unique identification. |
| (5) Vulnerability | Test was performed to confirm that the forced power ON/OFF does not affect the security function of initialization process, screen display and etc. |
| (6) Vulnerability | Test was performed to confirm the exclusive control being done by the access from operational panel and network simultaneously. |
| (7) Vulnerability | Test was performed to confirm that the setting state of CF lock password does not affect the behavior of the security function. |

c. Result

In the conducted evaluator penetration testing, the exploitable vulnerability that attackers who have the assumed attack potential could not be found.

## 3.4 Evaluation Result

### 3.4.1 Evaluation Result

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

### 3.4.2 Evaluator comments/Recommendations

- According to the guidance, CF lock password of CF lock function needs to be uniquely identified for each machine.

- The analysis for direct reading of lock password from HDD or CF is judged to be a residual vulnerability because it needs to use the specific devices. But it's quite possible of each lock password to be easily analyzed because the specific devices and decoding services are provided at a low-price and abused. Therefore for the consumers who take this issue as a threat, it's preferable to consider the encryption of image data using optional encryption function.

## 4. Conduct of Certification

The certification body conducted the following certification based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification review and were sent to evaluation facility.

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

# 5. Conclusion

## 5.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body determined the TOE is satisfied the assurance requirements of EAL3 prescribed in CC Part 3.

## 5.2 Recommendations

- If the external server authentication method is selected as for the user authentication function, the external server authentication method using Active Directory is required and TOE accepts the identification and authentication information managed with Active Directory that is outside of TOE with assuming that it is correct and, operates.

- If FAX unit which is option is not installed, security functions related to FAX transmissions are not usable, but it does not affect the operation of other security functions.

# 6. 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 Functions |

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

| | |
|---|---|
| API: | Application Programming Interface |
| BIOS: | Basic Input/Output System |
| CF: | Compact Flash |
| 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 |
| SMB: | Server Message Block |
| 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 definition of terms used in this report is listed below.

BIOS: A group of program to control the peripherals connected to a computer.

CF lock function:
Function that the password other than coinciding with the password set in CF stops to read and write.

CF lock password:
Password that releases the forbidden state to read and write on CF.

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

FTP: File Transfer Protocol used at TCP/IP network.

HDD lock function:
Function that the password other than coinciding with the password set in HDD stops to read and write.

HDD lock password:
Password that releases the forbidden state to read and write on HDD.

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

MIB: Various setting information that the various devices managed using SNMP opened 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.

SMB: Protocol to realize the sharing of files and printers on Windows.

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 in TOE.

SSL/TLS: Protocol to transmit encrypted data in the Internet.

S/MIME: Standard of e-mail encryption method.
Transmitting the encrypted message using RSA public key cryptosystem and needs electric certificate published from certification organization.

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

WebDAV: Protocol to manage files on the Web server.
Expanded specification of HTTP1.1.

Encryption word:
Original information to generate the encryption key to encrypt and decrypt on the encryption kit.

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

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

External network:
Access restricted Network from TOE connected office LAN by firewall or other.

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

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

Secure Print file:
Image file registered by secure print.

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

Flash Memory: Memory device that performs the high speed and high integration of EEPROM and carries the batch deletion mechanism.

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

## 7. Bibliography

[1] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022/ VarioLink 4222 / VarioLink 3622 Control Software A0R50Y0-0100-G00-20 A0R50Y0-1D00-G00-11 Security Target Version 1.07 (Apr 20, 2009) Konica Minolta Business Technologies, Inc.

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

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

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

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001 (Translation Version 1.2, March 2007)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-002 (Translation Version 2.0, March 2008)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-003 (Translation Version 2.0, March 2008)

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004

[12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004 (Translation Version 2.0, March 2008)

[13] bizhub 501 / bizhub 421 / bizhub 361 / ineo 501 / ineo 421 / ineo 361 / VarioLink 5022/ VarioLink 4222 / VarioLink 3622 Zentai Seigyo Software Evaluation Technical Report Version 2, Jun 8, 2009, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security