



Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2005-09-13(ITC-5055)
Certification No.	C0085
Sponsor	KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.
Name of TOE	Japan : bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Zentai Seigyo Software English : bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Control Software
Version of TOE	MFP system controller program : 57AA-0100-G00-21-000 MFP image controller program : 57AA-1000-G00-21-000
PP Conformance	None
Conformed Claim	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.

2007-03-22

Haruki Tabuchi, 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 2.1 (ISO/IEC 15408)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations (as of 01 December 2003)

Evaluation Result: Pass

“ Japan:bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Zentai Seigyo Software
English: bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Control Software
version:4037-0100-GM0-11-000” 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
1.1 Introduction	1
1.2 Evaluated Product.....	1
1.2.1 Name of Product.....	1
1.2.2 Product Overview	1
1.2.3 Scope of TOE and Overview of Operation	2
1.2.4 TOE Functionality.....	4
1.3 Conduct of Evaluation	5
1.4 Certificate of Evaluation	6
1.5 Overview of Report.....	6
1.5.1 PP Conformance	6
1.5.2 EAL.....	6
1.5.3 SOF.....	6
1.5.4 Security Functions	7
1.5.5 Threat.....	17
1.5.6 Organisational Security Policy	19
1.5.7 Configuration Requirements.....	19
1.5.8 Assumptions for Operational Environment.....	19
1.5.9 Documents Attached to Product.....	20
2. Conduct and Results of Evaluation by Evaluation Facility.....	21
2.1 Evaluation Methods.....	21
2.2 Overview of Evaluation Conducted	21
2.3 Product Testing	21
2.3.1 Developer Testing.....	21
2.3.2 Evaluator Testing.....	25
2.4 Evaluation Result.....	27
3. Conduct of Certification.....	28
4. Conclusion.....	29
4.1 Certification Result	29
4.2 Recommendations.....	29
5. Glossary	30
6. Bibliography.....	32

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “Japan: bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Zentai Seigyo Software English : bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Control Software Version: MFP system controller program : 57AA-0100-G00-21-000 MFP image controller program : 57AA-1000-G00-21-000” (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.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

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.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:

Japan : bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Zentai Seigyo Software

English : bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Control Software

Version: MFP system controller program : 57AA-0100-G00-21-000

MFP image controller program : 57AA-1000-G00-21-000

Developer: Konica Minolta Business Technologies, Inc.

1.2.2 Product Overview

This TOE is the embedded software that is installed on the Konica Minolta Business Technologies, Inc. digital MFP (bizhub 750 / bizhub 600 / ineo 750 / ineo 600) (Hereinafter referred to as “MFP”). This TOE is on the compact flash memory on the MFP controller carried in MFP, and this controls the whole operation of MFP such as the operation control processing and the image data management received from the panel of MFP body or the network.

This TOE offers the protection from exposure of the highly confidential document

stored in the MFP, and aims at protecting the data which may be exposed against a user's intention. In order to realize it, this offers the functions such as the function that limits the operation to the specific document only to the authorized user, the function that performs the overwrite deletion of the data domain which became unnecessary and the function that deletes the confidential information including a setting value. Moreover, this has the mechanism using the unauthorized access protection function (HDD Lock Function) with which HDD is equipped against the risk of taking out HDD unjustly which is a medium for storing image data in MFP. And this offers the encryption key generation function to encrypt the image data written to the HDD when the encryption board (option part) is installed on the MFP controller. And this also offers the encryption countermeasure and prevention of falsification to the unauthorized operation against compact flash memory which is the media to store various setting data.

1.2.3 Scope of TOE and Overview of Operation

This TOE exists on the compact flash memory on the MFP controller, which built in the body of the MFP, and is loaded on the RAM. Figure 1-1 shows the relationship between this TOE and the MFP. Shaded region on the figure 1-1 indicates the TOE and "*" shows the option parts of MFP.

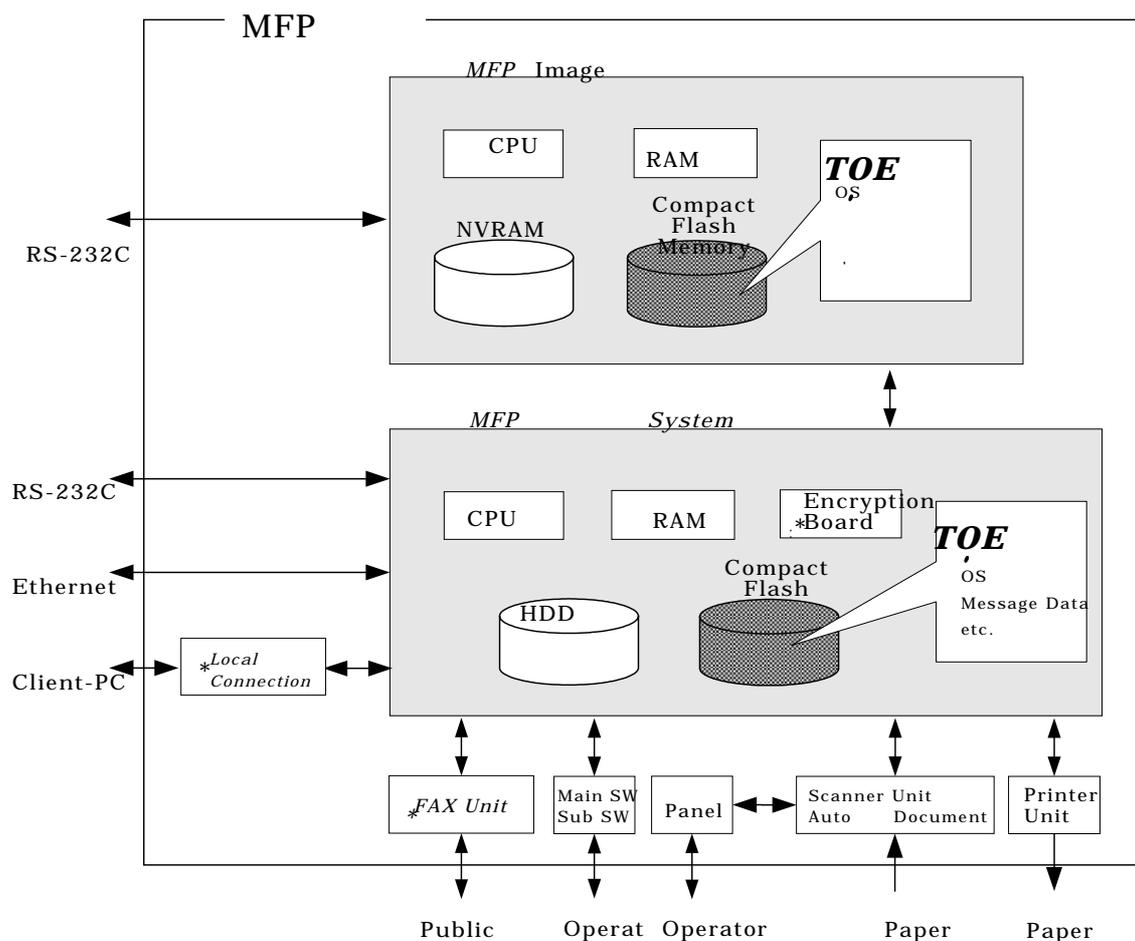


Figure 1-1 : Hardware structure that relates to TOE

Compact flash memory is the storage medium that stores the object code of this TOE and it also stores the message data of each country's language to display the response accessed through the panel and network, OS, setting data (administrator password, image data encryption key, management data encryption key) and so on.

NVRAM is the nonvolatile memory and it stores various setting values (HDD password, image data encryption key, management data encryption key, etc).

HDD stores the image data as the file, and is also used for the storage area for swapping the image data which exceeds the capacity of RAM processing area. Also, this TOE has the HDD lock function that can prohibit the unauthorized reading and unauthorized writing to HDD by setting the password in HDD.

The encryption board is provided as option parts. The encryption function is installed on the encryption board to encrypt the image file data written to the HDD as the hardware-based function.

Next, the logical structure of this TOE is shown. MFP includes the function that is not associated with the security directly such as basic function and remote diagnosis function other than the function that is indicated in "1.2.4 TOE functionality".

Basic function is a series of function for the office work concerning the image such as copy, print scan and fax and TOE performs the core control in the operation of these functions.

Remote diagnosis function is used for managing the operation status of MFP, setup information, and the device information like the number of prints by using the methods for the connection, such as the modem connection via RS-232C and the E-Mail, etc, and communicating with the support center run by the subsidiaries of the Konica Minolta Business Technologies, Inc.

MFP user who can use these functions uses each function that TOE provides, via the panel or the network.

The roles of the personnel 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) Person in charge at the Organization that manages the Maintenance of the MFP

A person in charge at the organization that carries out management of the maintenance for the MFP. This person assigns service engineers who perform the maintenance management for the 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.

1.2.4 TOE Functionality

This TOE provides the following functions.

1) Secure Print Function

When the secure print password is received with the printing data, the image data is stored as the standby status. And the print command and password input from the panel allows printing.

2) User Box Function

The directory named a use box can be created as an area to store the image file in HDD. The access of user is controlled by using the password set to the user box.

TOE offers the functions to the user box and the image file in a user box such as printing of image file in the user box, moving or copying to the other user box, deleting, and setting of the period to keep (delete automatically by the fixed time passed), and also the change of user box name, the change of the password, the deletion of the user box, from the panel or the network unit. (Upon request via the network from the client PC.)

3) User Authentication Function

TOE can limit the user who uses MFP. Also, when accessing it via the network, TOE identifies and authenticates that the user is permitted to use the MFP by applying the user ID and user password. When the identification and authentication succeeds, TOE permits the user the use of the basic function and the user box function, etc. Two types of user authentication methods exist; one is the "Machine Authentication" that registers the user ID and user password into HDD on MFP controller, and another is the "External Server Authentication" that authenticates the user by using the user ID and the user password that are registered on the user information management server which is connected by the intra-office LAN.

4) Administrator Function

TOE provides the functions such as the management of the user boxes, the management of various settings of the network and image quality, and the management of user information at the time of machine authentication in the administrator mode that only authenticated administrator can operate. Also, it offers the operation setting function related to the behavior of the other function.

5) 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.

6) 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. But the prohibition setting of maintenance function(through serial port) can be changed by service engineer separately. The prohibition setting of maintenance function(through LAN) is set by service engineer separately.

7) HDD Lock Function

HDD has the HDD lock function as measure against the illegal taking out, when the password is set. The administrator function does the operation setting of this function and as for the starting operation of MFP, the access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the MFP. (Even if HDD is taken out, it is impossible to use it excluding the MFP that the concerned HDD installed.)

8) Encryption key generation function and Encryption function

The encoding and decoding are processed on the encryption board due to the reading and writing image data in HDD. However, TOE itself does not process the encryption and decryption. It offers only the function to generate the encryption key. It also generates Encryption key to encrypt and decrypt the setting files stored in compact flash memory, and executes the encryption and decryption process.

The protected assets of this TOE are image files (secure print files) that are registered by the secure print and image files (user box files) that are stored in the user box.

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

a. On Memory Image File

Image file of job in the wait state

b. Stored Image File

Stored image files other than secure print file and user box file

c. 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)

d. 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)

e. File related to the Image

Temporary data file generated in print image file processing

f. Transmission Address Data File

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

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 750 / bizhub 600 / ineo 750 / ineo 600 Zentai Zentai Seigyo Software 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 B of CC Part 1 (either of [5], [8] , [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9] , [12] or [15]) 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], [10] , [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in “bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Zentai Seigyo Software Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”) [22]. Further, evaluation methodology should comply with the CEM (either of [17], [18] or [19]) and Interpretation (either [20] or [21]) is included.

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 issued on March 2007 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.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

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

1.5.3 SOF

This ST claims “SOF-basic” as its minimum strength of function.

This TOE assumes the use in the general office environment that is protected from the attack of the external network. The access via the panel or the internal network to TOE is under the management by the administrator and does not assume the complex attack. Therefore, it is reasonable to assume the attacking ability to attacker is “low-level.”

Thus, it is adequate with the SOF-Basic.

1.5.4 Security Functions

Security functions of the TOE are as follow.

1) Administrator Function (F.ADMIN)

This is a series of security function that administrator operates, such as an administrator identification and authentication function in an administrator mode accessing from a panel or through a network, and a security management function that includes a change of an administrator password and a lock cancellation of a locked user box.

a. Administrator Identification and Authentication Function

It identifies and authenticates the accessing user as the administrator in response to the access to the administrator mode.

b. Auto log-off function in Administrator Mode

When no operation is done more than panel auto log-off time during the access from panel in administrator mode, administrator mode is automatically made log-off.

c. Function offered in Administrator Mode

When a user is identified and authenticated as an administrator by the administrator identification authentication function at the accessing request to the administrator mode, the administrator authority is associated with the task substituting the user. And the following operations and the use of the functions are permitted.

Change of the administrator password

When a user is re-authenticated as an administrator, and the new password satisfied the quality, the password is changed.

Administrator password is set with 8-digit by using ASCII code (0x21 to 0x7E, except 0x22 and 0x2B) (A total of 92 characters are selectable.)

It returns "*" for each character as feedback for the entered administrator password if it's the access from the panel.

Also, it shall not be composed of one kind of character.

It resets the number of authentication failure when the authentication is successful.

When the authentication failure that becomes one to three times at total in each authentication function by using the administrator password is detected, it locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)

Lock of authentication function is released with F.RESET function operated.

User Settings

User is registered by setting the user ID and registering the user password. It verifies whether the user password newly set have been satisfied the following qualities. Also, It changes and deletes a user ID and a user password.

User password is set with 8-digit by using ASCII code (0x21 to 0x7E, except 0x22 and 0x2B) (A total of 92 characters are selectable.)

Also, it shall not be composed of one kind of character.

User Box Settings

It registers a user box by setting the user password to the unregistered user box ID. It changes the user box password.

User box password is set with 8 digits by using ASCII code (0x20 to 0x7E, except 0x22 and 0x2B)(A total of 93 characters are selectable.)

Also, it shall not be composed of one kind of character.

Release of Lock

It resets (0 clear) the number of authentication failure for all secure prints, all user boxes, and SNMP password.

If a secure print, user box or MIB object that access locked exists, the lock is released.

Setting of user authentication function

An authentication method in a user authentication function is set to the machine authentication or the external server authentication.

Setting of unauthorized access detection threshold

The unauthorized access detection threshold in the authentication operation prohibition function is set in the range for 1-3 times.

Setting and execution of all area overwrite deletion function

The HDD deletion method is selected and the overwrite deletion at the all data area is performed. (Perform F.OVERWRITE-ALL.) The deletion method is as follows.

Method	Overwritten data type and their order
Mode:1	0x00
Mode:2	Random numbers Random numbers 0x00
Mode:3	0x00 0xFF Random numbers Verification
Mode:4	Random numbers 0x00 0xFF
Mode:5	0x00 0xFF 0x00 0xFF
Mode:6	0x00 0xFF 0x00 0xFF 0x00 0xFF Random numbers
Mode:7	0x00 0xFF 0x00 0xFF 0x00 0xFF 0xAA
Mode:8	0x00 0xFF 0x00 0xFF 0x00 0xFF 0xAA Verification

Setting of auto logoff function

The panel auto logoff time is set in the range for 1-9 minutes.

Network Settings Network Settings

A setup operation of the following setting data is performed.

- A series of setup data that relates to SMTP server (IP address, Port Number, etc)
- A series of setup data that relates to DNS server(IP address, Port Number, etc)
- A series of setup data that relates to MFP address (IP address, NetBIOS Name, AppleTalk Printer Name, etc.)

Execution of back-up and restoration function

The setting data (except administrator password and CE password) stored in NVRAM and HDD is backed-up (refer) and restored (change).

Operation setting function of HDD lock function

When turning HDD lock function ON from OFF, it verifies that the newly set HDD lock password satisfies the following qualities.

Change the HDD lock password. By using the HDD lock password currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.

HDD lock password is composed of 20-digits by using ASCII code. (0x21 to 0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, and 0x5D) (A total of 83 characters are selectable)

Return "*" for each character as feedback for the entered HDD lock password in verification.

Also, it shall not be composed of one kind of character.

Operation setting of Image data encryption function

When turning the image data encryption function ON from OFF, it verifies that the image data encryption passphrase newly set satisfies the qualities, and F.CRYPT-IMAGE is performed.

Change the image data encryption passphrase. By using the image data encryption passphrase currently set, when it is re-authenticated as an administrator, and the new encryption passphrase satisfies the quality, it is changed and F.CRYPT-IMAGE is performed.

Image data encryption passphrase is composed of 20-digits by using ASCII code. (0x21 to 0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, and 0x5D) (A total of 83 characters are selectable)

Return "*" for each character as feedback for the entered image data encryption passphrase in verification.

Also, it shall not be composed of one kind of character.

Operation setting of Management data encryption function

When turning the management data encryption function ON from OFF, it verifies that the management data encryption passphrase newly set satisfies the qualities, and F.CRYPT-DATA is performed.

Change the management data encryption passphrase. By using the management data encryption passphrase currently set, when it is re-authenticated as an administrator, and the new encryption passphrase satisfies the quality, it is changed and F.CRYPT-DATA is performed.

Management data encryption passphrase is composed of 20-digits by using ASCII code. (0x21 to 0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, and 0x5D) (A total of 83 characters are selectable)

Return "*" for each character as feedback for the entered management data encryption passphrase in verification.

Also, it shall not be composed of one kind of character.

Function related to Enhanced Security function

The function that influences the setting of the Enhanced Security function that the administrator operates is as follows.

- Operation setting of Enhanced security function
Function to set valid or invalid of Enhanced Security function.

- HDD Logical Format Function

Function to re-write system file of OS in HDD. Along with the execution of this logical format, the setting of security function is invalidated.

- Overwrite Deletion Function for all area

The settings of enhanced security function are invalidated by executing the overwrite deletion of all area.

Change of SNMP password

SNMP password is changed. Verify that SNMP password newly set satisfies the following qualities.

SNMP password is composed of 8 or more digits by using ASCII code (0x20 to 0x7E) that is selectable in total of 95 characters.

Setting of SNMP password authentication function

The authentication method in the SNMP password authentication function is set to "Only Authentication password" or the "Authentication password and Privacy password."

2)SNMP Administrator Function (F.ADMIN-SNMP)

This is a security function, which identifies and authenticates the administrator in the access through the network by SNMP from PC, and then permits the operation of setting function of the network only to the administrator whose identification and authentication was succeeded.

a. Identification and authentication function by SNMP password

It identifies and authenticates by the SNMP password, that the user who accesses the MIB object through the network with the use of SNMP is an administrator.

SNMP password is composed of 8 or more digits by using ASCII code. (0x20 to 0x7E) (A total of 95 characters is selectable.)

SNMP password includes "Authentication password" and "Privacy password" and all authentication function to user SNMP password is locked when the authentication failure in total of 1 to 3 times is detected in the authentication function that uses these. (Deny the access to MIB object.)

The lock of authentication function is released with the operation of the lock release function to MIB object of F.ADMIN or the operation of the F.RESET function.

Reset the authentication failure frequency if it succeeds in authentication. But if both Privacy password and Authentication password is used, both authentications need to succeed to reset the authentication failure frequency.

b. Management function using SNMP

When it is identified and authenticated that the user is an administrator by the SNMP password, the access to the MIB object is permitted, and then the operation of the setting data shown as followings is permitted to be done.

Network Settings

Setting operation of the following setting data is performed.

- Setting data that relates to SMTP server (IP address, port number, etc.)
- Setting data that relates to DNS server (IP address, port number, etc.)
- A series of setting data that relates to MFP address (IP address, NetBIOS name, AppleTalk printer name, etc.

Change of SNMP password

SNMP password (Privacy password, Authentication password) is changed. SNMP password newly set is composed of 8 or more digits using ASCII code. (0x20 to 0x7E)) (A total of 95 characters is selectable)

Setting of SNMP password authentication function

The authentication method in the SNMP password authentication

function is set to “Only Authentication password” or the “Authentication password and Privacy password.”

3)Service mode function (F.SERVICE)

This is a series of security function that the service engineer operates, such as the service engineer identification authentication function in service mode accessing from the panel, and a security management function that includes a change in the CE password and the administrator password.

a. Service engineer identification authentication function

It identifies and authenticates the accessing user as the service engineer in response to the access request to the service mode from the panel.

b. Function offered in service mode

When a user is identified and authenticated as a service engineer by the service engineer identification authentication function at the access request to the service mode, the use of the following functions is permitted.

Change of CE password

When a user is re-authentication as a service engineer and the new password satisfies the quality, it is changed.

CE password is composed of 8-digits using ASCII code. (0x21 to 0x7E, except 0x22 and 0x2B) (A total of 92 characters is selectable)

Return “*” for each character as feedback for the entered CE password.

When the access is from panel, if the authentication is failed, the input from the panel does not be accepted for 5 seconds.

Reset the number of authentication failure when succeeding in the authentication.

It locks all the authentication functions to use the CE password when the authentication failure that becomes 1-3 times at total in each authentication function by using the CE password is detected. (Deny the access to service mode.)

F.RESET function operates and then the lock of the authentication function is released.

Also, it shall not be composed of one kind of character.

Change of administrator password

Change the administrator password. Administrator password newly set is composed of 8-digits using ASCII code. (0x21 to 0x7E, except 0x22 and 0x2B) (A total of 92 characters is selectable)

Function that relates to Enhanced Security function

The functions that influence the setting of the Enhanced Security function that the service engineer operates are as follows.

- HDD logical format function

The function to re-write system file of OS in HDD. The setting of the Enhanced Security function is invalidated along with the execution of this logical format.

- HDD physical format function

The function to rewrite the entire disk in HDD with a regulated pattern including the signal rows such as the track and sector information. The setting of the Enhanced Security function is invalidated along with the execution of this physical format.

- Initialization function(Network setting)

Function to reset every setting value written in NVRAM to the factory default. The setting of the Enhanced Security function is

invalidated by executing this initialization function.

Operational setting Function of maintenance function(through LAN, through serial port)

The function that sets the operation of maintenance function working in the access(through LAN, through serial port). (Available to change operation from halting-state to activated-state)

Function that relates to password initialization function

The function that relates to the initialization of the password that the service engineer operates is as follows.

- Initialization function(Network setting)
Function to reset various setting values written in NVRAM to the factory default. The SNMP password are set to an initial value of the factory shipment by executing this initialization function.
- HDD physical format function

The function to rewrite the entire disk to a regulated pattern in HDD including the signal rows such as the track and sector information. The HDD lock function is turned OFF along with the execution of this physical format. (The HDD lock password that is set cannot be used again by turning OFF the operation setting.)

4)User Function (F.USER)

It identifies and authenticates the user of the use of MFP various function. To the identified and authentication user, it offers the management function of the user password that is managed in the MFP at the time of machine authentication, besides the permission of the use of functions such as F.BOX and F.PRINT.

a. User identification and authentication

It identifies and authenticates to be a user for the access request to the user box and the registration request of secure print file. The use of F.BOX and F.PRINT is permitted to the user who is identified and authenticated.

User password is composed of 8 or more digits using ASCII code. (0x21 to 0x7E, except 0x22 and 0x2B)(A total of 92 characters is selectable)

It uses the session information more than 10^{10} for the access from the network.

Return "*" for each character as feedback for the entered user password.

Also, it shall not be composed of one kind of character.

Reset the number of authentication failure when succeeding in the authentication.

It locks all the authentication functions to the user when the authentication failure that becomes 1-3 times at total for the concerned use is detected.

The lock of authentication function is released with the operation of the lock release function to the user authentication of F.ADMIN or the operation of the F.RESET function.

In the case of the "External server authentication" has been selected as the user authentication method, when the user who is identified and authenticated with the above-mentioned function is not registered in the MFP, this user ID is registered.

b. Auto logoff function in user identification and authentication domain

While the user who is identified and authenticated is accessing from a panel, if it does not accept any operations for more than the "panel automatic logoff time," it logs off from a user identification and authentication domain automatically.

c. Modification function of user password

When the identification and authentication are succeeded, and the access to

the user identification and authentication domain is permitted, the user is permitted to change its own password. When the external server authentication is effective, this function cannot be applied.

5) User Box Function (F.BOX)

This is a series of security function related to the user box to the user who is identified and authenticated that you are the registered user, such as the permission of the operation and management of the personal user box of the user, the authentication to the user who is permitted the utilization of the user box in the access to the public box, and the access control function to permit various operations of the concerned user box and the user box file after the authentication.

a. Registration of user box

By selecting the user attribute to the non-registration user box ID selected, this registers a personal user box or a public user box.

In the case of the personal user box, the arbitrary user ID registered is specified.

When the designated box is not registered as in the box storing operation at copying job and printing job, this user box, which is set user ID to operate such jobs, is automatically registered as user attribute.

In the case of the public use box, verify that a user box password registered satisfies the qualities.

Public user box password is composed of 8-digits using ASCII code. (0x20 to 0x7E, except 0x22 and 0x2B) (A total of 93 characters is selectable)

Also, it shall not be composed of one kind of character.

b. Personal User Box Function

The task to act for the identified and authenticated user has "User ID" of the user who is identified and authenticated for the user attribute. This task is permitted the display of the list of the personal user box which has a corresponding user attribute with this user attribute.

When the user box to operate is selected, "User Box ID" of the user box is related to the task as a user box attribute in addition to the user attribute. This task is permitted, to the user box file with the user attribute and the user box attribute corresponding to the user attribute and the user box attribute of itself, the printing, the E-mail transmission, the FTP transmission, the FAX transmission, the SMB transmission, download, the removing to other user boxes, and the copy operations to other user boxes.

The user attribute of a personal user box can be changed. If another registered user is specified, it becomes a personal user box that another user manages. If public is specified, it becomes a public user box. In this case, it is necessary to register the user box password.

c. Public User Box Function

The task to act for the identified and authenticated user has "User ID" of the user who is identified and authenticated for the user attribute. This task is permitted the display of the list of the public user box which is set the public as the user attribute.

For the access request to each public user box, it authenticates that a user is permitted to use each concerned user box.

It utilizes the 10¹⁰ session information or more for the access from the network.

Return "*" for each character as feedback for the entered user box password.

Reset the number of authentication failure when succeeding in the authentication.

In case of the access from the panel, when it fails in the authentication, an input from the panel is not accepted for five seconds.

When the authentication failure that becomes the 1-3 times in total is detected for the public user box concerned, the authentication function to the public user box concerned is locked.

The lock of the authentication function is released with the operation of the lock release function to the public user box of F.ADMIN or the operation of F.RESET function.

The task to act for the user is related the "User Box ID" of the user box as a user box attribute in addition to the user attribute. This task is permitted the user box file, which have been set the public to the user attribute and have a corresponding user box attribute to the user box attribute of the subject attribute, to do the printing, the E-mail transmission, the FTP transmission, the FAX transmission, the SMB transmission, download, the movement to other user boxes, and the copy operations to other user boxes.

The user attribute of the public user box can be changed. Specify the registered user and change to a personal user box for the registered user.

Change the public user box password.

6) Secure Print Function (F.PRINT)

This is a series of security function related to the secure print such as the access control function that allows the printing the secure print file after authenticating if a user is the authorized user to use the secure print file for the access to the secure print file from the panel to the identified and authenticated user as a registered user.

a. Authentication function by the secure print password

When the user is identified and authenticated as the registered user, it authenticates that the accessing user is a user to whom the user of the secure print file concerned is permitted, in response to the access request to each secure print file.

Secure print password is composed of 8-digits using ASCII code. (0x20 to 0x7E, except 0x22 and 0x2B)(A total of 93 characters is selectable)

The access from the panel is not accepted for five seconds when the authentication is failed.

Return "*" for each character as feedback for the entered secure print password.

When the authentication failure that becomes the 1-3 times in total for the secure print file concerned is detected, the authentication function to the secure print file is locked.

The lock status is released with the operation of the lock release function to secure print file of F.ADMIN or the operation of F.RESET function.

b. Access control function to secure print file

The task to act for the user who is permitted to use the secure print file has the secure print internal control ID of the authenticated secure print file for the file attribute.

This task is permitted the printing to the secure print file with a corresponding file attribute to the file attribute of this task.

c. Registration function of a secure print file

Verification of the secure print password

For the registration request of secure print file, the registered secure print password is verified to satisfy the following requirements.

- Secure print password is composed of 8-digits using ASCII code.

(0x20 to 0x7E, except 0x22 and 0x2B)(A total of 93 characters is selectable)

- Also, it shall not be composed of one kind of character.

Giving of the secure print internal control ID

For the registration request of secure print file, when the verification of the secure print password is completed, the secure print internal control ID uniquely identified is set to the concerned secure print file.

7) All area overwrite deletion function (F.OVERWRITE-ALL)

This executes the overwrite deletion in the data area of HDD and initializes the setting value of the password that is set to Compact Flash Memory and NVRAM as well. The object for the deletion or the initialization is as follows.

< Object for the deletion : HDD >

- Secure print file
- User box file
- On memory image file
- Stored image file
- HDD remaining image file
- Transmission address data file
- User ID
- User password
- User box password
- Secure print password
- HDD remaining TSF data

< Object for the initialization : NVRAM >

- Operation setting of HDD lock function (OFF)
- Operation setting of Image data Encryption function (OFF)
- Operation setting of Management data Encryption function (OFF)

< Object for the initialization : Compact Flash Memory >

- Administrator password
- CE password
- SNMP password

The deletion methods such as the data written in HDD and the written frequency is executed according to the deletion method of all area overwrite deletion function set in F.ADMIN. The HDD lock password, Image data encryption Passphrase and Management data encryption Passphrase cannot be used for being turned off the operation setting of the HDD lock function, the Image data encryption function and the Management data encryption function.

The setting of the Enhanced Security function becomes invalid in the execution of this function.

8) CF remaining data deletion function (F.OVERWRITE-CF)

This deletes the remaining data in CF by using overwriting all data.

- CF remaining image data

- CF remaining TSF data

9) Encryption key generation function (F.CRYPT)

This generates the encryption key to encrypt image data written in HDD by using KonicaMinolta HDD encryption key generation algorithm (SHA-1) that is regulated by the KonicaMinolta encryption specification standard. KonicaMinolta HDD encryption key generation algorithm (SHA-1) is the algorithm to generate the encryption key by using the SHA-1 regulated by FIPS 180-1.

10) Management data Encryption function (F.CRYPT-DATA)

This generates the encryption key to encrypt setting files in CF and store after encryption. The object for the encryption or decryption is as follows.

- Various setting values treated by F.ADMIN
- Various setting values treated by F.SERVICE
- Various setting values forced by Security Enhanced function

* The following operational setting values are excluded because they are not in CF.

Image data encryption key password, Management data encryption key password, HDD lock password, User information(User ID, User password, etc.), Box information(Box ID, Box password, etc.), Maintenance function(through LAN, through serial port)

a. Management data encryption key generation Function

This generates the encryption key to encrypt setting files(Administrator password, CE password, etc.) stored in CF by using KonicaMinolta HDD encryption key generation algorithm (SHA-1) that is regulated by the KonicaMinolta encryption specification standard. KonicaMinolta HDD encryption key generation algorithm (SHA-1) is the algorithm to generate the encryption key by using the SHA-1 regulated by FIPS 180-1.

b. Management data encryption decryption Function

By using 128 bit encryption key generated by Management data encryption key passphrase, the setting files in CF are encrypted and stored with using AES encryption algorithm regulated by FIPS_PUB_197.

When setting files are read, they are decrypted and used on Volatile Memory. At the timing that the change of other values occur in setting files, the data is encrypted and stored each time.

11) HDD verification function (F.HDD)

This is a check function to permit reading from and writing in the HDD only when it is verified that the illegal HDD is not installed and is confirmed validity when the HDD lock password is set to HDD.

When the HDD lock password is set to HDD, the status of HDD is confirmed in the HDD operation verifying at the time of TOE starting. As a result of status check, when the HDD lock password certainly being set is returned as the result of status confirmation, the access to HDD is permitted. If the HDD lock password not being set is returned, the access to HDD is refused because of an illegitimate possibility.

12) Authentication Failure Frequency Reset Function (F.RESET)

This is a function to reset the number of authentication failure counted in each

authentication function including the administrator authentication. (Do not relate to the lock is valid or not.)

This function operates by activating TOE such that the main power supply is turned on, or it returns from the power failure. When it starts, the following numbers of authentication failure are reset. The object account locked is released.)

- The number of failure to authentication of administrator
- The number of failure to authentication using SNMP password
- The number of failure to authentication of service engineer
- The number of failure to authentication of each user
- The number of failure to authentication of each public user box

13) ROM Verification Function (F.CHECK)

This is a function to detect the falsification against binary file(TOE) which violates the security function.

At installation of TOE, a value is calculated and stored in NVRAM to detect the falsification against TOE on system controller. Afterwards each time when main power switch is ON, this value is recalculated to detect the falsification against TOE on system controller and compare the value with stored one. This enables to detect the falsification.

When it detects the falsification, the panel shows a message to call service engineer.

1.5.5 Threat

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

Table 1-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP	<ul style="list-style-type: none"> ·When the leaser returned or the discarded MFP were collected, secure print file, a user box file, on memory image file, the stored image file, the remaining image file, the image-related file, the transmission address data file and the set various passwords can leak by the person with malicious intent taking out and analyzing an HDD in MFP.
T.BRING-OUT -STORAGE	<ul style="list-style-type: none"> ·A secure print file, a user box file, a on memory image file, a stored image file, a remaining image file in HDD, an image-related file, a transmission address data file 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. ·A person or a user with malicious intent illegally replaces as HDD in MFP. In the replaced HDD, new files of the secure print file, a user box file, on memory image file, a stored image file, a remaining image file in HDD, an image related file, a transmission address data file 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	·Exposure of the user box file when a person or a user with malicious intent accesses the user box where other user owns, and downloads, prints and transmits the user box file (E-mail transmission, FTP transmission, fax transmission, and SMB transmission)
T.ACCESS-PUBLIC-BOX	·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 and SMB transmission) and removes and copies to the other user box the user box file.
T.ACCESS-SECURE-PRINT	·Exposure of the secure print file when a person or the user with malicious intent prints the secure print file which is not permitted to use.
T.ACCESS-NET-SETTING	·Malicious person or user changes the network settings that is 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. < The network setting which is related to user box file transmission > Setting related to the SMTP server ·Setting related to the NDS server ·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 file is exposed.
T.ACCESS-SETTING	·The possibility of leaking user box file and secure print file rises because malicious person or user changes the settings related to the enhanced security function.
T.BACKUP-RESTORE	·The user box file and the secure print file can leak by malicious person or user using the backup function and the restoration function illegally. Also, highly confidential data such as password can be exposed and each setting values are falsified.
T.BRING-OUT-CE	The following possibilities can be occurred by a person or a user with malicious intent illegally taking out and analyzing an Compact Flash Memory in MFP. · Setting values(Administrator password, CE password, SNMP password) will leak.

	<ul style="list-style-type: none"> · MFP will be operated with falsified setting values(Administrator password, CE password, other various setting operation values). · MFP will be operated with falsified TOE. · Image data in Compact Flash Memory from remaining image file in CF will leak.
--	---

1.5.6 Organisational Security Policy

There is no organizational security policy assumed to be applied to this TOE.

1.5.7 Configuration Requirements

The TOE operates on the bizhub 750, bizhub 600, ineo 750, ineo 600 which is the digital MFP provided by the Konica Minolta Business Technologies, Inc. The Encryption board is an option parts and is not equipped as a standard. When the encryption board is not installed, the function that relates to the encryption of image data cannot be used.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-2. The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-2 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	· 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	· 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	<ul style="list-style-type: none"> · The intra-office LAN where the MFP with the TOE will be installed is not intercepted. · 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	· Each password and encryption passphrase does not leak from each user in the use of TOE.
A.SETTING	<ul style="list-style-type: none"> · MFP with the TOE is used after enabling the enhanced security function. · MFP with the TOE is used after setting to prohibit the maintenance function(through LAN).
A.SERVER	· When the external server authentication is used for the user authentication method, the user information management server that is

	connected with the intra-official LAN installing MFP with TOE are performed appropriately the management of the account, access control and patch application, etc.
--	---

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

Documents attached to the TOE are listed below.

< Document for administrator / general user >

- 1)bizhub 750/600 User's Guide Security Operations (Ver. : 1.02)
(Japanese)
- 2)bizhub 750/600 User's Guide Security Operations (Ver. : 1.02)
(English)
- 3)ineo 750/600 User's Guide [Security Operations] (Ver.1.02) (English)

< Document for service engineer >

- 1)bizhub 750/600 Service Manual Security Function (Ver. 1.05) (Japanese)
- 2)bizhub 750/600 Service Manual Security Function (Ver. 1.05) (English)

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 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 report 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.

2.2 Overview of Evaluation Conducted

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

Evaluation has started on October, 2006 and concluded by completion the Evaluation Technical Report issued on March,2007 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 June, September and October in 2006 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 March 2007 and development environment checking at a development corporation companion May 2007

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.

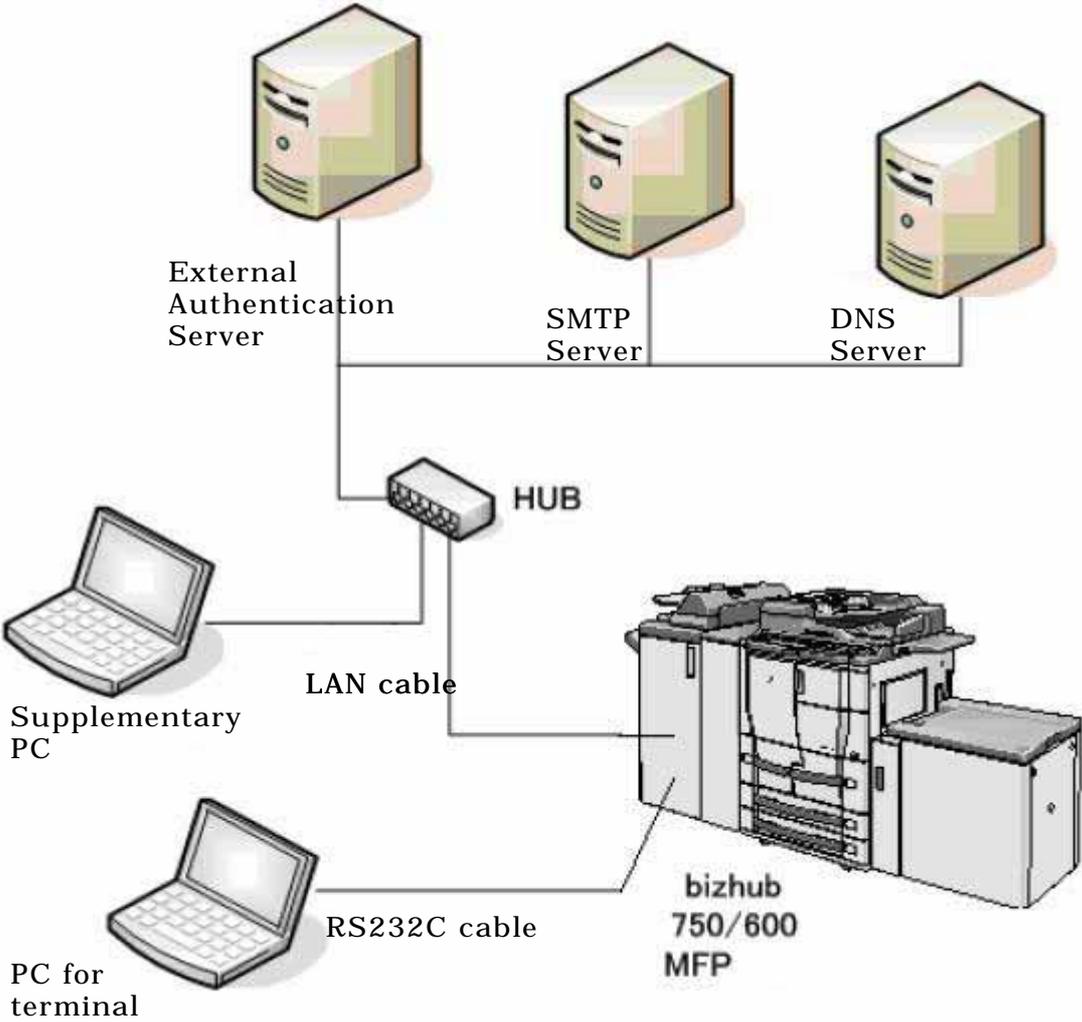
2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 2-1.



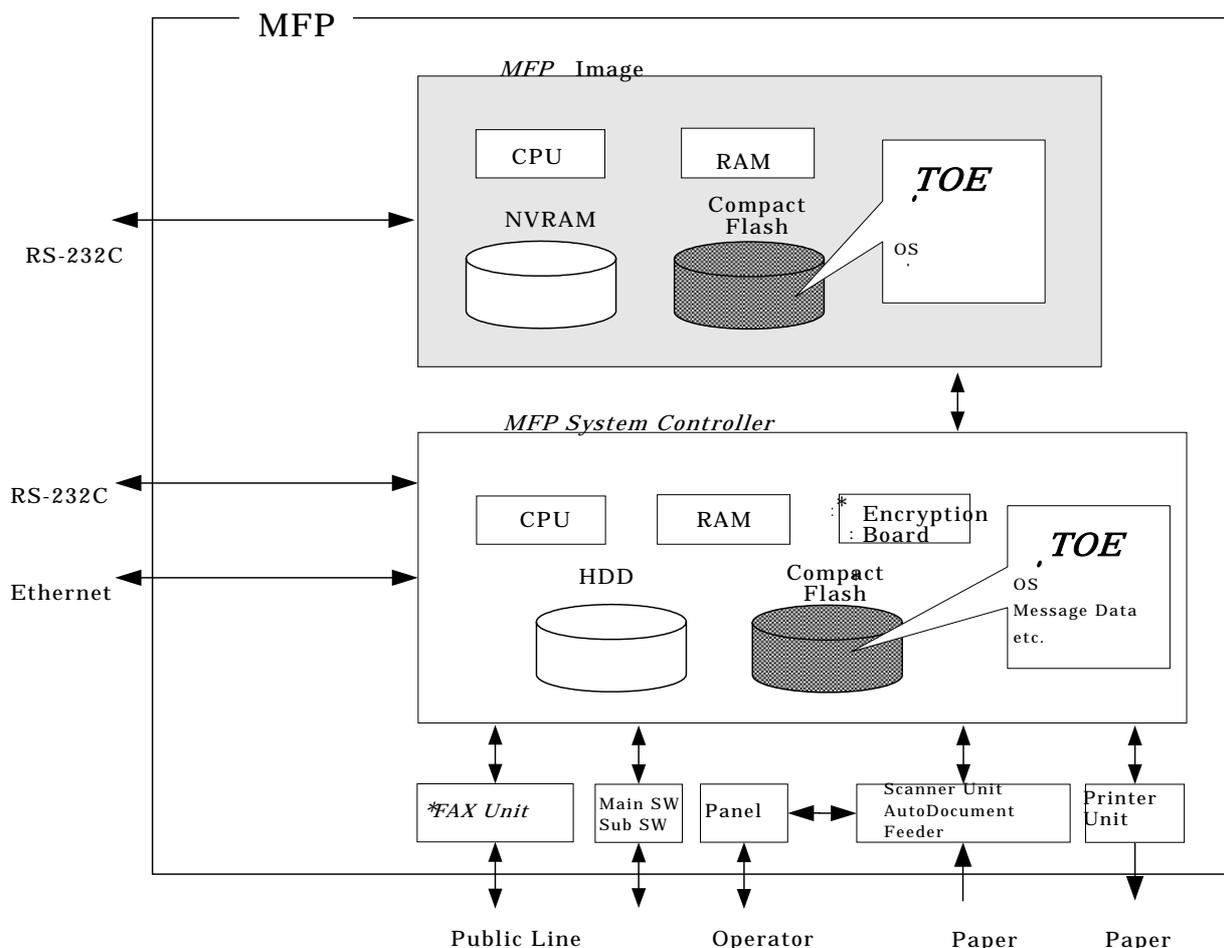


Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

a. Test Configuration

The configurations of the tests performed by the developer are shown in Figure 2-1. Developer testing is performed at the same TOE testing environment with the TOE configuration identified in ST. However, local connection unit (option parts) is eliminated from the configuration of MFP.

b. Testing Approach

For the testing, following approach was used.

Check the change of setting values, the authentication method and the check of access control, by using the external interface (panel, network, and power supply OFF/ON) and check the change of output message and its operation, and the behavior of them. In network, it can access using HTTPS protocol, TCP Socket (API of TCP base using for the access from application), Open API (API of XML base using for the access from application) and SNMP (operate MIB) used by PageScope Web Connection (PSWC). Each protocol can observe the behavior of security function by sending and receiving the test data of each protocol using test tool. Also, it can check by using the test tool that the session information of when using HTTPS protocol or when using OpenAPI, is generated correctly. For the security function that cannot verify by using the interface of , it

performs the test procedure for each and checks the adequacy of the behavior. Outlining of the concerned test is as follows.

- To check that all area overwrite deletion function operates correctly (HDD is deleted by “0x00 0xFF 0x00 0xFF 0x00 0xFF 0xAA verify,” area of use for administrator is initialized,) it accepts the method to check by using the tool to dump display of the HDD contents and to edit.
- To check that the encryption key is appropriately generated, it accepts the method to refer directly the data on the memory on the terminal screen connected directly to the machine.
- To check that the management data encryption function and the deletion function of remaining information in CF are correctly operated(whether management data such as administrator password is the same before encryption and after decryption), it accepts the method to confirm the content of CF by using editable and dump showing tool.
- To check that HDD lock password functions effectively, it accepts the method to check the error occurrence status by exchanging with other HDD that is not set the HDD lock password.
- As the behavior of the service mode(separation setting function of telnet) and service mode(operation setting of serial port) are restricted by service engineer, the method to observe the display of operational panel is adopted to confirm the behavior of security function.
- 23 In the case that the data in CF is falsified, the method to observe the error occurrence by attaching the CF(once taken out and data falsified) again to MFP is adopted to confirm whether the ROM verification function is effective or not.

c. Scope of Testing Performed

Testing is performed about 129 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 high-level design and the subsystem interfaces.

d. 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.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

The evaluator used test configuration that are identical to those used by the developer.

But the connection method of inspection PC is changed because of the difference of test method.

For the intrusion tests, it was performed with the same configuration. Figure 2-2 shows its schematic.

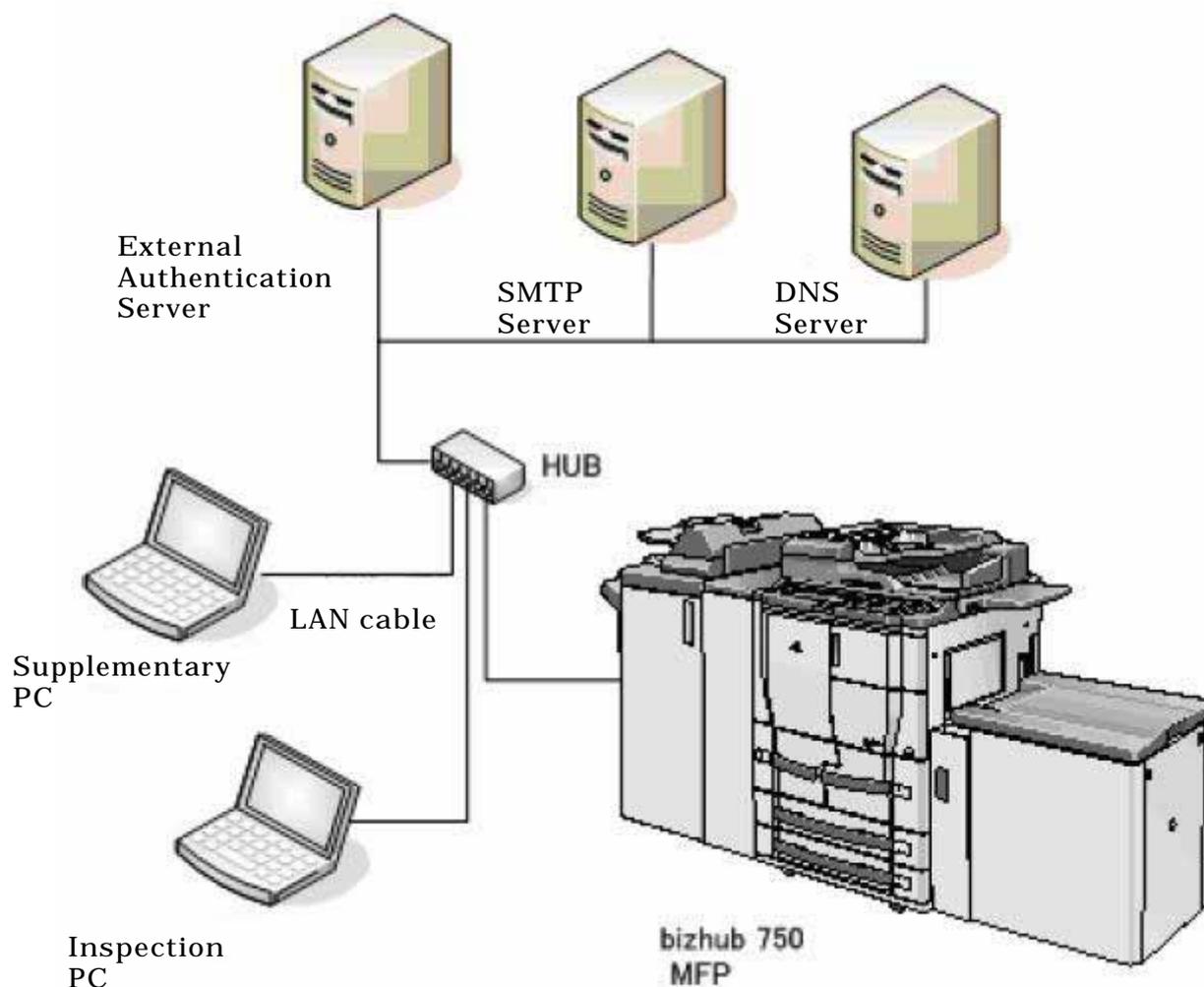


Figure2-2 Developer test (Intrusion test) configuration

2) Outlining of Evaluator Testing

a. Test configuration

The configurations of the tests performed by the evaluator are shown in figures 2-1 and 2-2. The evaluator tests were performed in TOE test environment identical to the TOE configuration identified by ST.

b. Testing Approach

For the evaluator testing, the approach that is same as the developer test was used.

c. Scope of Testing Performed

The evaluator performed 66 tests in total: 30 independent test and 36 sampled developer tests. As the selection criteria of the test, followings take into account.

Security function that is suspected to operate along the specifications by the developer test.

More important security function than other security function

Security function set as the object of strength of function

Function that is used from different interface

Also, intrusion tests performed by evaluator are conducted as follows.

TOE can perform three kinds of operations such as the operation by the panel, the operation through the network by HTTPS protocol, TCP Socket, OpenAPI and SNMP, and the operation by power supply OFF/ON of Printer. The operation by the panel and the power supply OFF/ON of Printer can be considered impossible to perform the unauthorized operations such as operation other than assumed usage because of the physical restriction of Printer and the operation panel. On the other hand, the operation via the network has broad option and is easy to perform the operation other than expected input.

With a focus on the items related to the network, 9 intrusion tests were invented in consideration of the following 3 points.

Verify the truth of insistence based on the vulnerability analysis of developer.

Verify the response to the clear vulnerability, that evaluator thinks.

Verify the truth of insistence of the strength of function of developer.

Table2-2 shows the intrusion test item list.

Table 2-2 Intrusion Test Item List

Test No.	Intrusion Testing name for vulnerability test based on [VLA]	Intrusion Test Perspective of idea
VLA-T1	Security objective situation assurance test of network I/F (1)	Perspective
VLA-T2	Security objective situation assurance test of network I/F (2)	Perspective
VLA-T3	Assurance test of official vulnerability	Perspective
VLA-T4	Assurance test of official vulnerability (OpenSSL)	Perspective
VLA-T5	Security function assurance test against HTTP request	Perspective
VLA-T6	Assurance test of Web server function	Perspective
VLA-T7	Assurance test related to the strength of function	Perspective
VLA-T8	Assurance test for random nature of cookie	Perspective
VLA-T9	Setting Assurance test of setup function	Perspective

d. Result

All evaluator testing conducted is completed correctly and could confirm the behavior of the TOE. The evaluator also confirmed that all the test results are consistent with the behavior.

2.4 Evaluation Result

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

3. Conduct of Certification

The following certification was conducted 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.

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

.

4. Conclusion

4.1 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 verified the TOE is satisfied the EAL3 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations 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
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
HDD	Hard Disk Drive
LAN	Local Area Network
IP	Internet Protocol
SNMP	Simple Network Management Protocol
NVRAM	Non-Volatile Random Access Memory

The glossaries used in this report are listed below.

Printer Controller	Controller that controls all the operation of Printer including the operation control process received from the network or the Printer panel and the management of image data. TOE is the software that operates on that controller.
Flash Memory	Memory device that performs the high speed and high integration of EEPROM and carried the batch deletion mechanism.
Secure Print	This is the printing method that restricts by the password authentication. Print data of file which is desired to print by using the printer driver from PC is sent and a printer driver exchanges that data into image file by the printer. To print that image data, specify the password by the printer driver and printing by printer is allowed only when that password is authenticated.

User Box	Directory that is created in the HDD area in order to store the image files in the Printer.
Service Engineer	A user who performs the management of maintenance for the Printer. Performs the repair and adjustment of Printer. In general, it is the person in charge at the sales companies or agencies that performs the maintenance service of Printer and that is in cooperation with Konica Minolta Business Technologies, Inc.
Service Mode	Operation panel screen area which can operate Printer function that is prepared for the service engineer.
CE password	Kind of password collating when entering the service mode
Remaining Image File	File that remains in the HDD data area. It is the image file that cannot be deleted by general deletion operation.
Transmission Address Data File	File including address transmitting an image, such as an E-mail address and a phone number etc.
Account Lock	Unable to perform continuous password authentication when the operation of password authentication is failed consecutively, or its situation.

6. Bibliography

- [1] bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Seigyo Software Security Target Version1.08 (February 20th, 2007) KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.
- [2] IT Security Evaluation and Certification Scheme, July 2005, Information-technology Promotion Agency, Japan EC-01
- [3] IT Security Certification Procedure, July 2005, Information-technology Promotion Agency, Japan EC-03
- [4] Evaluation Facility Approval Procedure, July 2005, Information-technology Promotion Agency, Japan EC-05
- [5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031
- [6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- [7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
- [8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031 (Translation Version 1.2 January 2001)
- [9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (Translation Version 1.2 January 2001)
- [10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (Translation Version 1.2 January 2001)
- [11] ISO/IEC 15408-1:1999 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
- [12] ISO/IEC 15408-2:1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- [13] ISO/IEC 15408-3:1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
- [14] JIS X 5070-1:2000 - Security techniques - Evaluation criteria for IT security - Part 1: General Rules and general model
- [15] JIS X 5070-2:2000 - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- [16] JIS X 5070-3:2000 - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

- [17] Common Methodology for Information Technology Security Evaluation
CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999
- [18] Common Methodology for Information Technology Security Evaluation
CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999
(Translation Version 1.0 February 2001)
- [19] JIS TR X 0049:2001 – Common Methodology for Information Technology Security
Evaluation
- [20] CCIMB Interpretations (as of 01 December 2003)
- [21] CCIMB Interpretations (as of 01 December 2003)
(Translation Version 1.0 August 2004)
- [22] bizhub 750 / bizhub 600 / ineo 750 / ineo 600 Zentai Seigyo Software Evaluation
Technical Report Version 3, March 8th, 2007, Mizuho Information & Research
Institute, Inc. Center for Evaluation of Information Security