Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-10-04 (ITC-0310)
Certification No.	C0291
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 PKI Card System Control Software
Version of TOE	A2WU0Y0-0100-G00-F2pki
PP Conformance	None
Assurance Package	EAL3
Developer	Konica Minolta Business Technologies, Inc.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
2011-05-30

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

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

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

Evaluation Result: Pass

"bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 PKI Card System Control Software Version A2WU0Y0-0100-G00-F2pki" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 PKI Card System Control Software Version A2WU0Y0-0100-G00-F2pki" (hereinafter referred to as "the TOE") developed by Konica Minolta Business Technologies, Inc., and evaluation of the TOE was finished on 2011-04 by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Konica Minolta Business Technologies, Inc. and provides information to the users and system operators who are interested in this TOE.

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

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

1.1 Product Overview

Overview of the TOE functions and operational conditions is as follows. Refer to from Chapter 2 onwards for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

The bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502, which this TOE is installed, are digital Multi Functional Peripheral (hereinafter all the products are referred to as "MFP".), provided by Konica Minolta Business Technologies, Inc., composed by selecting and combining each functions of copy, print, scan and FAX.

The TOE is the "bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 PKI Card System Control Software" that controls the entire operation of MFP, including the operation control processing and the image data management triggered by the panel of the main body of MFP or through the network. For printer data transmitted to MFP from client PC among the highly confidential documents exchanged between MFP and client PC, the TOE supports the encryption print function, realized by using a special printer driver and IC card, and function to print with the use of exclusive driver (loadable driver) and the IC card that is used for generating the encryption print. It also provides the protection function for the scanned image data transmitted by e-mail from MFP by S/MIME using a loadable driver and an IC card. These security functions are realized by the coordination with the IC card and the TOE.

Moreover, against the danger of illegally bringing out HDD that is the medium to temporarily store image data processed in MFP, the TOE can prevent from unauthorized access by encrypting all the data including image data written in HDD by using ASIC. Besides, the TOE provides the function that deletes all the data of HDD completely by deletion method compliant with various overwrite deletion standards and the function that controls the access from the FAX public line against the danger of using Fax function as a steppingstone to

access internal network, so it contributes to the prevention of information leakage of the organization that uses MFP.

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

1.1.2.1 Threats and Security Objectives

This TOE counters each threat with the following security functions.

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

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

1.1.2.2 Configuration and Assumptions

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

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

It assumes that IC card is usable with MFP and a client PC and SMTP server is usable at LAN.

In this environment, MFP is managed not to be accessed from an external network when LAN is connected to an external network (outside of the organization such as internet).

It assumes that an administrator and a service engineer are reliable. For example, it assumes that they can keep the secret about their password and an encryption passphrase.

It assumes that IC card, used in the use of the TOE, is limited to rightful user only.

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

1.1.3 Disclaimers

- Encryption of the communication of image files, a digital signature, the IC card using for authentication, IC card reader, exclusive driver, and the function of Active Directory are not assured in this evaluation.

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

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

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation and completed on 2011-04 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report [13] and Observation Reports prepared by Evaluation Facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. The Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

Name of the TOE:	bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 PKI Card System Control Software
Version of the TOE:	A2WU0Y0-0100-G00-F2pki
Developer:	Konica Minolta Business Technologies, Inc.

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

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

3. Security Policy

This chapter describes the security function policies and the organisational security policies adopted to counter the TOE against the threats.

The TOE provides an encryption function with ASIC and a data deletion function to prevent leaking information when MFP is returned or discarded or HDD is taken illegally.

This TOE realizes the following functions for customer's demand.

- For highly confidential image files, a mechanism to encrypt when sending and receiving, to give a digital signature when sending from the TOE, and to print by only a user who sent when the TOE received.

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

3.1 Roles related to the TOE

The roles related to this TOE are defined as follows.

(1) User
An MFP user who owns IC card (In general, the employee in the office is assumed.)

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

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

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

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

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

3.2 Security Function Policies

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

3.2.1 Threats and Security Function Policies

3.2.1.1 Threats

This TOE assumes the threats shown in Table 3-1 and provides the functions against them.

Table 3-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP (Lease-return and discard of MFP)	When leased MFPs are returned or discarded MFPs are collected, encrypted print files, scanned image files, on-memory image files, stored image files, HDD-remaining image files, image-related files, and highly confidential information like various passwords which were set up can be leaked by the person with malicious intent when he/she analyzes the HDD or NVRAM in MFP.
T.BRING-OUT-STORAGE (Unauthorized bringing out HDD)	- Encrypted print files, scanned image files, on-memory image files, stored image files, HDD-remaining image files, image-related files, and various passwords which were set up can be leaked by a malicious person or a user illegally when he/she brings out the files to analyze the HDD in MFP. - A person or a user with malicious intent illegally replaces HDD in MFP. In the replaced HDD, newly created files such as encrypted print files, scanned image files, on-memory image files, stored image files, HDD-remaining image files, image-related files, and various passwords which were set up are accumulated. A person or a user with malicious intent takes out to analyze the replaced HDD, so such image files will be leaked.

3.2.1.2 Security Function Policies against Threats

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

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

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

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

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

This threat assumes the possibility that the data in HDD to be leaked by being stolen from the operational environment under MFP used or by installing the unauthorized

HDD and bringing out with the data accumulated in it.

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

3.2.2 Organisational Security Policies and Security Function Policies

3.2.2.1 Organisational Security Policies

Organisational security policies required in use of the TOE is presented in Table 3-2.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.COMMUNICATION-CRYPTO (Encryption communication of image file)	Highly confidential image file (encrypted print files, scanned image files) which transmitted or received between IT equipments must be encrypted.
P.COMMUNICATION-SIGN (Signature of image file)	Digital signature must be added to a mail including highly confidential image files (scanned image files).
P.DECRYPT-PRINT (Decryption of image file)	Highly confidential image files (encrypted print file) received by MFP are permitted to print only to a user who generated that files.
P.REJECT-LINE (Access prohibition from public line)	An access to internal network from public line via the Fax public line portal must be prohibited.

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

3.2.2.2 Security Function Policies to Organisational Security Policies

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

(1) Security function to satisfy the organisational security policy [P.COMMUNICATION-CRYPTO (Encryption communication of image file)]

This organisational security policy regulates that image files which flows on network are encrypted to ensure the confidentiality. As this corresponds according to one's request, it does not need to encrypt all image data. It needs to encrypt data between MFP and user's client PC in handling encrypted print file or scan image file.

In this TOE, by supporting the function to encrypt scanned image files sent by e-mail from MFP to user's client PC (referred to as "S/MIME encryption function") and by

encrypting the encrypted print files sent from the client PC to MFP using the exclusive driver and an IC card, which is outside the scope of this TOE, it is possible to securely send and receive image files over the network.

(2) Security function to satisfy the organisational security policy [P.COMMUNICATION-SIGN (Signature of image file)]

This organisational security policy regulates that a signature is added to image files to be sent or received by e-mail in order to secure the integrity of the files. Because this function only needs to be available upon request, a signature does not need to be appended to all image files, except that any scanned image files to be handled need to have a signature.

The TOE has a function of interlocking with an IC card which is outside the scope of the TOE, for scanned image files to be sent by e-mail from MFP to a client PC of a user's own ("IC card operation support function") and a function of appending a signature to those scanned image files on its own ("S/MIME signature function"). With these functions, the TOE allows image files to be sent by e-mail while maintaining the integrity of the files.

(3) Security function to satisfy the organisational security policy [P.DECRYPT-PRINT (Decryption of image file)]

This organisational security policy regulates that only the user who generated an encrypted print file can decrypt and print that encrypted print file.

The TOE has a function of interlocking with an IC card which is outside the scope of the TOE, for encrypted print file (referred to as "IC card operation support function") and a function of that encrypted print files can be accepted to decrypt and print when IC card which generated the encrypted print files is used (referred to as "encrypted print file decryption function"), only the user who generated the encrypted print files can decrypt and print the encrypted print files.

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

This organisational security policy prohibits being accessed to internal network via the port of Fax public line on Fax unit installed to MFP. This function is provided when Fax unit is installed to MFP.

This TOE provides the function which prohibits the access to the data existing in internal network from public line via the port of Fax public line (referred as "Fax unit control function"), so that it enables to prohibit the access to the internal network via the port of Fax public line.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate this TOE, as useful information for assumed readers to judge the use of this TOE.

4.1 Usage Assumptions

Assumptions to operate the TOE are shown in Table 4-1.

The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN (Personnel conditions to be an administrator)	Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations 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 series of permitted operations given to them.
A.NETWORK (Network connection conditions for MFP)	When the intra-office LAN where MFP with the TOE will be installed is connected to an external network, access from the external network to MFP is not allowed.
A.SECRET (Operational condition on secret information)	Each password and encryption passphrase shall not be leaked from each user in the use of the TOE.
A.IC-CARD (Operational condition on IC card)	IC card is owned by rightful user in the use of TOE.
A.SETTING (Operational setting condition on security)	The following operation setting related to security is set to the TOE when a user uses the TOE. - Prohibit authentication operation when failing the input of password consecutively at a constant frequency. - Disable the use of the TOE update function via an internet. - Disable the use of the maintenance function. - Activate login authentication of service engineer. - Activate the HDD encryption function. - Disable the setting of administrator function excluding panel.

4.2 Environment Assumptions

This TOE is installed in any one of bizhub 652, bizhub 602, bizhub 552, bizhub 502, which is MFP provided by Konica Minolta Business Technologies, Inc.
It assumes that IC card reader is connected to MFP. It is optional whether Fax unit is installed.

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

It assumes that Active Directory, the directory service provided by Windows Server 2000 (or later), is connected to the intra-office LAN to authenticate user's IC card.

It assumes that a client PC which installed an exclusive printer driver and connected to IC card reader is connected to the intra-office LAN.

It assumes that SMTP server is connected to the intra-office LAN. It is optional whether DNS server is used in the intra-office LAN.

The reliability of hardware and software to be cooperated is outside the scope of this evaluation. (It shall be regarded as reliable enough.)

4.3 Clarification of scope

The reliability of ASIC, IC card, IC card reader, exclusive driver and Active Directory in the below is not the scope of this evaluation.

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

- To realize the organisational security policies, an encryption of communicating image files, a digital signature and authentication are necessary. Though this TOE cooperates with IC card, IC card reader, exclusive driver and Active Directory, these are outside of the TOE and are not the scope of this evaluation.

5. Architectural Information

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

5.1 TOE boundary and component

The TOE is the software that controls the entire operation of MFP. It is installed in the SSD on MFP controller in the main body of MFP. It is loaded and run on the RAM when main power is switched ON. The relation between the TOE and MFP is shown in Figure 5-1.

In Figure 5-1, FAX unit marked as * are optional parts of MFP. It assumes that FAX unit is installed when a user uses FAX function.

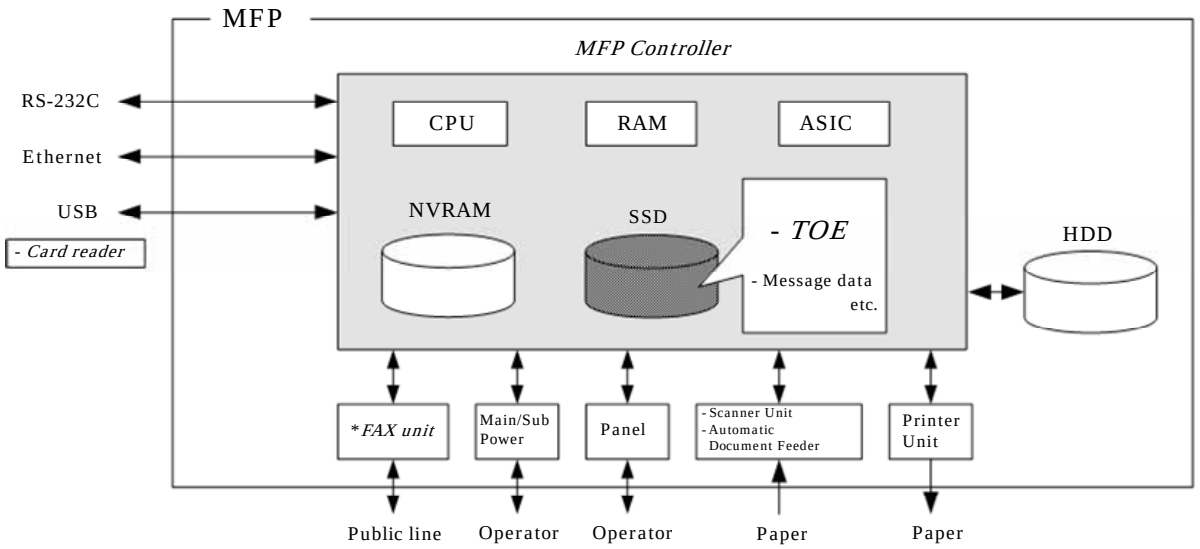

Figure 5.1 TOE boundary

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

- The part which provides interface through the network
  It controls Ethernet and provides communication function of TCP/IP base.

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

- The part which performs job management
  Job means the unit managing an execution control and operation order, of copy, print, scan, Fax, user box file operation and so on.
  The job is made and registered, when "the part which controls each device" receives the operation from "the part which provides interface through the network" or "the part which provides interface via the panel" and the reception from the Fax unit. The execution of the actual job is realized using the following "the part which executes common management", "the part which handles HDD" and "the part which controls each device".

- The part which executes common management
  This part manages various setting values and provides a measure which another part of

the TOE accesses to the setting value. Various setting values include information used to execute security function, like the authentication information.
This part provides the function executing identification and authentication and the function of access control.
This part realizes the following functions by using a function of IC card through IC card reader.
> Encryption, decryption and signature of S/MIME
> Decryption of an encryption print file

- The part which handles HDD
This part provides the handling of image data and input/output function to HDD.
In the input/output function to HDD, an encryption at the time of writing and a decryption at the time of reading are done by ASIC.
It overwrites all data of HDD with the directed method when the administrator indicates.

- The part which controls each device
This part controls scanner unit, printer unit and Fax unit and realizes the actual work of Copy, Print, Scan and Fax.
Moreover, it is the mechanism that does not allow to access an internal network from Fax unit.

- The part which provides support function
This part provides functions used for support of MFP (function for diagnostics of MSFP and function of updating the TOE).

5.2 IT Environment

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

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

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

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

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

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

(6) Panel
An exclusive control device for the operation of MFP, equipped with a touch panel of a

liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc. It is controlled by "the part which provides interface via the panel."

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

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

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

(10) USB
It can be connected with a card reader corresponded to IC card. A card reader is not pre-installed in MFP as a standard for selling circumstances, but sold as an optional part. It is an essential component under this ST assumption.

(11) IC card
An IC card that supports the standard specification of Common Access Card (CAC) and Personal ID Verification (PIV).
It supports "the part which executes common management" by the function which decrypts a common key, operates a signature to message digest and prepares a public key.

(12) RS-232C
Serial connection using D-sub 9 pins connectors is usable. The maintenance function is usable through this interface in case of failure.

(13) FAX Unit (*Optional part)
A device that has a port of Fax public line, which is used for transmitting and receiving FAX via the public line.
It is not pre-installed in the MFP as a standard for selling circumstances, but sold as an optional part. Fax unit is purchased when the organization needs it, and the installation is not indispensable.

6. Documentation

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

< For administrators and users >

- bizhub 652 / 602 / 552 / 502 for PKI Card System User's Guide [Security Operations] Ver.1.01

< For service engineers >

- bizhub 652 / 602 / 552 / 502 for PKI Card System SERVICE MANUAL SECURITY FUNCTION Ver.1.01

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Approach

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

7.2 Overview of Evaluation Activity

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

Evaluation has started on 2010-10 and concluded by completion of the Evaluation Technical Report dated 2011-04. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2011-01 and 2011-02 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff interview. Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2011-01.

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

7.3 IT Product Testing

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

7.3.1 Developer Testing

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

1) Developer Testing Environment

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

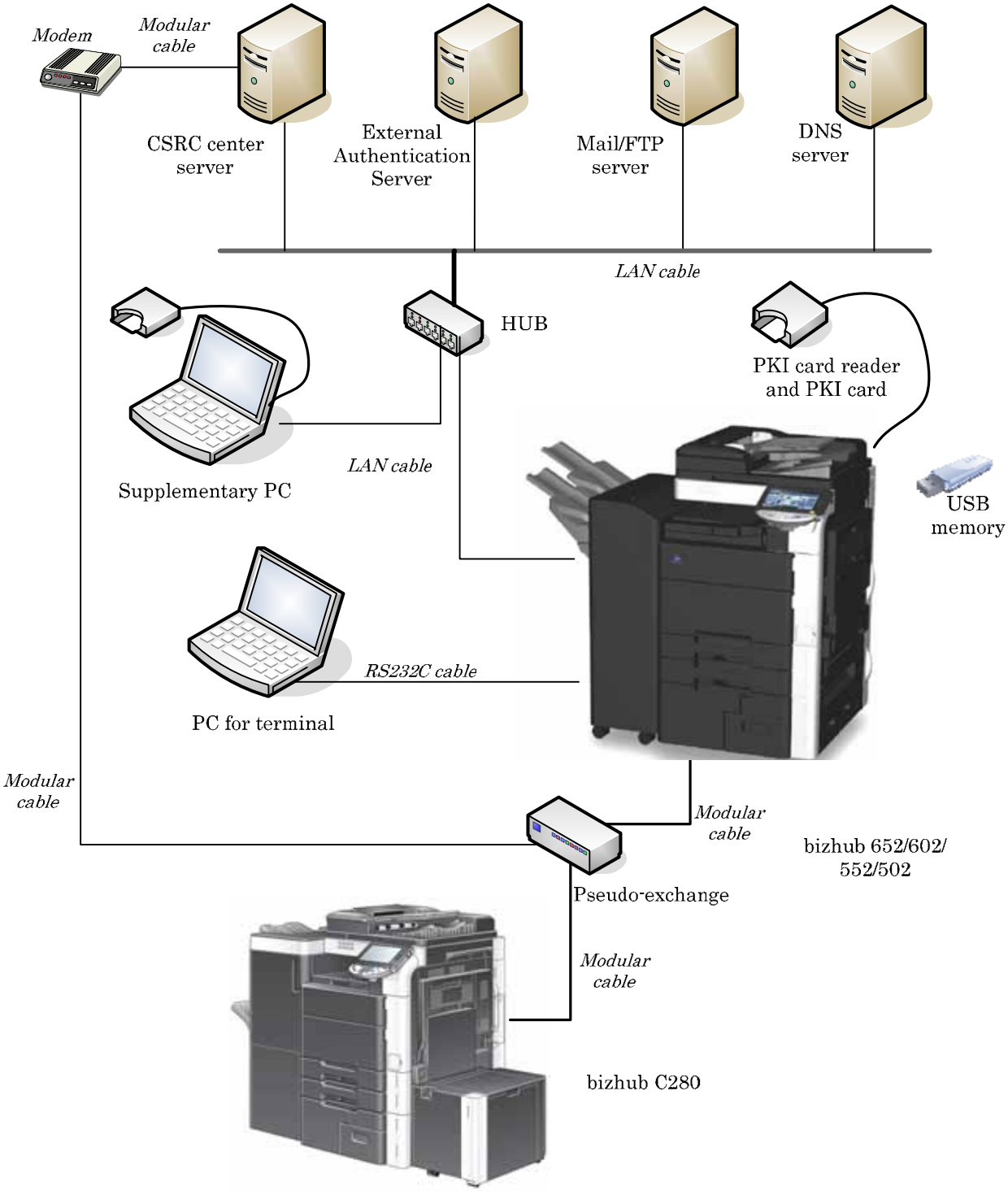

Figure 7-1 Configuration of the Developer Testing

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

2) Summary of Developer Testing

Summary of the developer testing is as follows.

a. Developer Testing Outline

Outline of the developer testing is as follows;

<Developer Testing Approach>
The testing was conducted to execute security functions through the external interface when the functions which have the external interfaces that the developer can use. It was conducted to obtain and analyze the executed results of security functions through dump tool or capturing tool of communication data when functions do not have the external interfaces that the developer can use.

<Tools for the Developer Testing>
Tools used for the tests are shown in the Table 7-1.

Table 7-1 Tools for the Developer Testing

Name of device and software	Outline and Purpose of use
KONICA MINOLTA 652 / 602 Series PCL Driver Ver.1.0.6.OSW1_01	Exclusive printer driver software for bizhub 652 /602 Series PKI Card System. Use for encrypted print.
ActiveClient 6.1	Driver software for smart card. Used as driver for PKI card in the supplementary PC.
SCR3310 USB Smart Card Reader Driver V4.41	Driver software for PKI card reader. Installed to the supplementary PC and used.
WireShark Ver. 1.2.2	Software tool for monitoring and analyzing the communication on the LAN. Used for getting communication log and confirming data.
Mozilla Thunderbird Ver. 2.0.0.21	General purpose mailer software. Used as the confirmation tool of S/MIME mail on the supplementary PC.
Open SSL Ver.0.9.8k (25-May-2009)	Software tool for hash function and encryption/decryption function. Used for confirming S/MIME signature.
Tera Term Pro Ver. 4.29	Terminal software executed in the terminal PC. Used to connect with MFP and to operate the terminal software installed in MFP to monitor the state of the TOE.
Disk dump editor Ver. 1.4.3	Software tool to display the contents in HDD. Used for confirming the contents of HDD.
Stirling Ver. 1.31	Binary editor software tool. Used for confirming the contents of decode S/MIME messages.
MIME Base64 Encode/Decode Ver. 1.0	Software tool to encode/decode of MIME Base64. Used for decoding of S/MIME messages.
Blank Jumbo Dog Ver. 4.2.2	Simple server software for intranet. Used as mailer server and FTP server function.
CSRC center software Ver. 2.6.1	Server software for CSRC center. CSRC is a maintenance service to manage the state of MFP which Konica Minolta business technologies, Inc. offers by remote.

b. Scope of Execution of the Developer Testing

The developer testing is executed on 38 items by the developer.
By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested. By the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been tested enough.

c. Result

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

7.3.2 Evaluator Independent Testing

The evaluator executed the sample testing to reconfirm the execution of the security function by the test items extracted from the developer testing. And the evaluator executed the evaluator independent testing (hereinafter referred to as "The Independent Testing") to reconfirm that security functions are certainly implemented from the evidence shown by the process of the evaluation.
It explains the independent testing executed by the evaluator as follows.

1) Independent Testing Environment

Configuration of testing performed by the evaluator shall be the same configuration with developer testing.
Configuration of testing performed by the evaluator is showed in the Figure 7-1. Testing configuration performed by the evaluator shall be the same configuration with TOE configuration identified in ST.

Only bizhub 602 / bizhub 552 are chosen as MFP which the TOE is loaded, however it is judged not to have any problem as a result of the following confirmation by evaluator.

- It was confirmed by a document offered from the developer that a difference of bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 is only copy / print speed.

2) Summary of Independent Testing

Independent testing performed by the evaluator is as follows;

a. Viewpoints of Independent Testing

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

<Viewpoints of Testing>
(1) Based on the situation of the developer testing, test as many security functions as possible.
(2) Test all probabilistic and permutable mechanism.
(3) Test behaviors depending on the differences of password input methods to TSI for the testing of the probabilistic and permutable mechanism.
(4) Based on the complexity of interfaces, test the necessary variations.
(5) For the interfaces with innovative and unusual characters, test the necessary variations.

b. Outline of Independent Testing

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

<Independent Testing Approach>
The testing was conducted to execute security functions through the external interface when the functions have the interfaces that evaluator can use. It was conducted to obtain and analyze the executed results of security functions through dump tool or capturing tool of the transmitted data when functions do not have the external interfaces that the evaluator can use.

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

<Outline of each independent testing viewpoint>
Outline of each independent testing viewpoint is shown in Table 7-2.

Table 7-2 Viewpoints of Independent Testing and Overview of Testing

Viewpoints of Independent Testing	Overview of Testing
(1) Viewpoint	Testing was performed, which were judged to be necessary in addition to developer testing.
(2) Viewpoint	Testing was performed with changing the digit number of characters and the types of characters by paying attention to the probabilistic and permutable mechanism at the identification and authentication, etc., by the administrator.
(3) Viewpoint	Testing was performed with considering the operated interfaces to confirm the behavior depending on the difference of password input method.
(4) Viewpoint	Testing was performed with considering the complexity of S/MIME encryption function to confirm the action at encrypting scanned image data and transmitting by e-mail.
(5) Viewpoint	Testing was performed to confirm the action by judging the functions, such as Fax unit control function, encryption key generation function of HDD encryption and encryption print function, to be innovative or not general.

c. Result

All the executed independent testing was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.3.3 Evaluator Penetration Testing

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

1) Summary of the Penetration Testing

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

a. Vulnerability of concern

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

<Vulnerability requiring the penetration testing>
(1) Possibility to be activated the unexpected service that relates to the component used for the TOE.
(2) Concerns of the existence of the vulnerabilities within the public domain that relates to the components used for the TOE.
(3) Detected the concern to be bypassed or falsified the security functions depends on the timing of the power ON/OFF, when it is retrieved it to the documentations.
(4) It makes it difficult to confirm that there is no concern of attack to the communication between card reader and MFP or between the related MFP and the external authentication server, when it is retrieved if there is a concern of attacking by wiretapping communications, to the development evidence.
(5) Several types of interface supporting the authentication function exist, as it is known from the ST. It is concerned that the possibility to be operated by an operator with different authority by considering when it competes with the authentication from different types of interface from the development evidence.
(6) Several mechanisms protects the data in HDD not to be read, even when HDD is brought out and connected to the same types of MFP, as it is known from the development evidence. However, it is uncertain about a part of operation of mechanism.

b. Outline of Penetration Testing

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

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

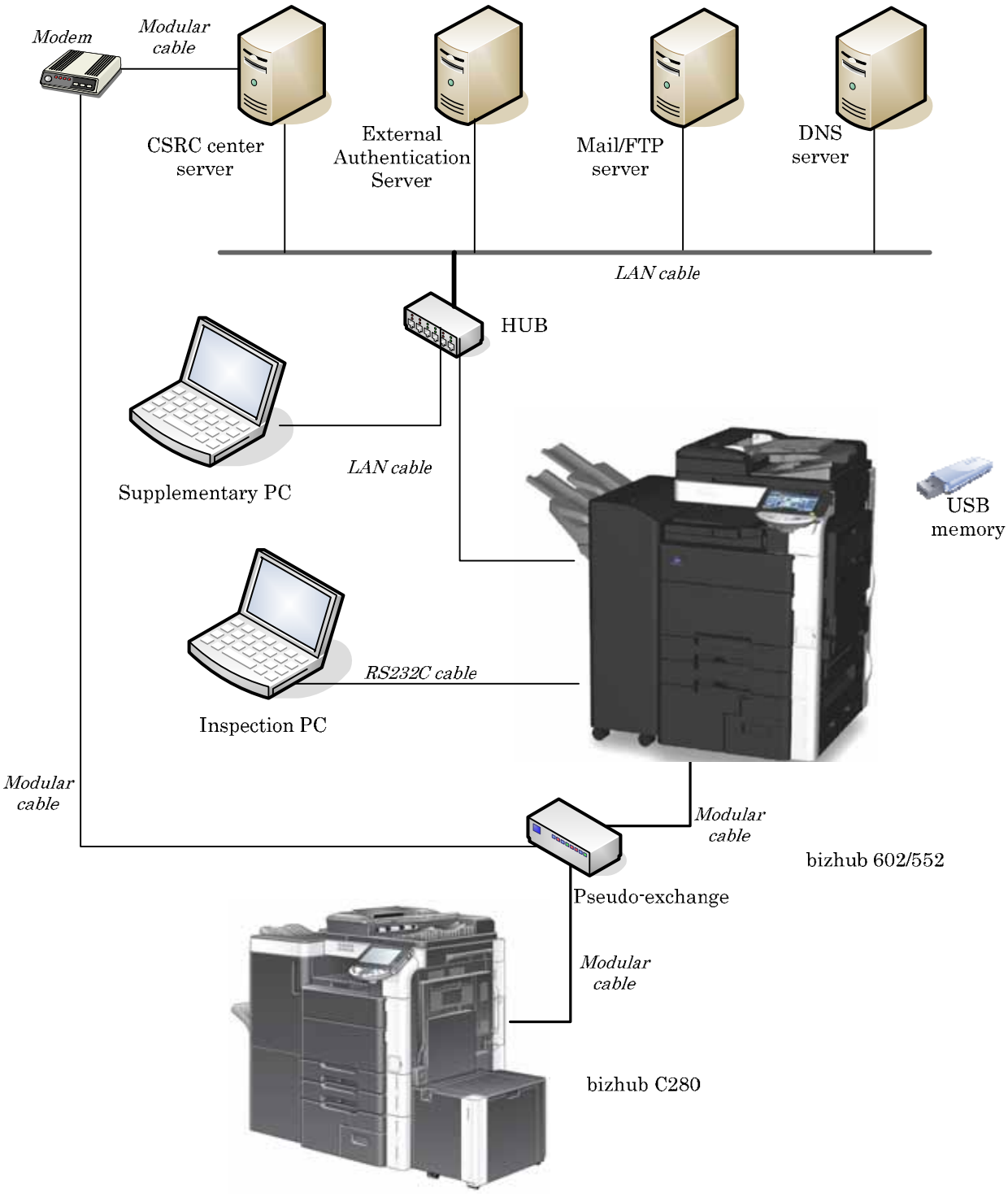

Figure 7-2 Environment of Penetration Testing

<Penetration Testing Approach>
The testing was conducted to use the following methods; method to check with the visual observation of the behavior after stimulating the TOE by operating from the operational panel, method to check with the visual observation of the behavior after accessing the TOE through network with operating the supplementary PC, method to check the behavior with test tool by using test tool, method to check authentication operation by using IC card, method to check data transferred between IC card and TOE in authentication process, method to scan the publicly known vulnerabilities with the vulnerability checking tool by

operating the inspection PC.

<Tools and others used at Penetration Testing>
The tools, etc., used at tests are shown in Table 7-3.

Table 7-3 Configuration of Penetration Testing

Testing Configuration Environment	Details
Inspection object (TOE)	- TOE installed in bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 (Version: A2WU0Y0-0100-G00-F2pki) - Network configuration Penetration Testing was done by connecting each MFP with hub or cross-cable.
Supplementary PC	- PC with network terminal operated on Windows XP SP2 or Windows 2000 SP4. - Using the tools shown in Table 7-1 (Thunderbird, Disk dump editor etc.) and software for USB analyzer (made by CATC) - Connect MFP by using printer driver, IC card etc. and it is possible to use the encryption print function.
Inspection PC	- Inspection PC is a PC with network terminal operated on Windows XP SP3, and is connected to MFP with cross-cable to perform vulnerability testing. - Explanation of testing tools. (The operational check of the following tool is finished in network environment in Mizuho Information & Research Institute, Inc. Plug-in and vulnerability database are applied the latest version on Jan. 12, 2011.) (1)snmpwalk Version 3.6.1 MIB information acquiring tool (2)openSSL Version 0.9.8q encryption tool of SSL and hash function (3)Nessus 4.4.0.(build 15045) Security scanner to inspect the vulnerabilities existing on the System (4)WireShark 1.4.2 Packet analyzer software that can analyze protocols more than 800

<Implementation items of Penetration Testing>
The concerned vulnerabilities and the corresponding penetration testing are shown in Table 7-4.

Table 7-4 Overview of Penetration Testing

Concerned vulnerabilities	Overview of Testing
(1) Vulnerability	Testing was performed to confirm possibility of abusing by using the tool such as Nessus and behavior inspection.
(2) Vulnerability	Testing was performed to confirm possibility of abusing by using the tool such as Nessus and result analysis.
(3) Vulnerability	Testing was performed to confirm that the forced power ON/OFF does not affect the security function of initialization process, screen display and etc.

Concerned vulnerabilities	Overview of Testing
(4) Vulnerability	Testing was performed to confirm that information to affect security functions from data transferred between the card reader, MFP and the external authentication servers are not leaked out.
(5) Vulnerability	Testing was performed to confirm that there is not the situation to be operated with different authority from the operator, in the case which tried the authentication with IC card in the authenticated state from the operation panel and in the reverse case.
(6) Vulnerability	Testing was performed to confirm whether a mechanism reducing a threat operates under a specific condition.

c. Result

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

7.4 Evaluated Configuration

(1) Operating model

It is assumed that this TOE is installed in any one of bizhub 652, bizhub 602, bizhub 552, bizhub 502, which is MFP, provided by Konica Minolta Business Technologies, Inc.
Because of the reasons shown in 7.3.2, the evaluation is considered to be conducted in all models though the evaluation was not conducted in these all models.

(2) Setting of TOE

The evaluation was conducted in the following setting.

- Prohibit authentication operation when failing the input of password consecutively constant frequency.
- Disable the use of the TOE update function via an internet.
- Disable the use of the maintenance function.
- Activate login authentication of service engineer.
- Activate the HDD encryption function.
- Disable the setting of administrator function excluding from a panel.

These setting are as the setting shown in the ST.

7.5 Evaluation Results

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

In the evaluation, the followings were confirmed.

- PP Conformance: none

- Security functional requirements: Common Criteria Part 2 Extended

- Security assurance requirements: Common Criteria Part 3 Conformant

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

- All assurance components of EAL3 package

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

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

The certification body conducted the following certification based on 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.

8.1 Certification Result

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

8.2 Recommendations

- This TOE depends on the functions of ASIC (installed in MFP), IC card, IC card reader, exclusive driver and Active Directory to counter threats and to fulfill the organisational security policies. (Refer to 4.3) The reliability of these functions is not assured in this evaluation, and it depends on operator's judgment.

- The information to authenticate IC card with Active Directory server is registered to Active Directory at the time of issuing the IC card by a corporation which issues IC card.

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

9. Annexes

There is no annex.

10. Security Target

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

bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 PKI Card System Control Software Security Target Version 1.03 (March 18, 2011) Konica Minolta Business Technologies, Inc.

11. Glossary

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

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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

CAC	Common Access Card
DNS	Domain Name System
FTP	File Transfer Protocol
HDD	Hard Disk Drive
MFP	Multiple Function Peripheral
MIB	Management Information Base
NVRAM	Non-Volatile Random Access Memory
PIV	Personal ID Verification
RAM	Random Access Memory
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SSL	Secure Socket Layer
S/MIME	Secure Multipurpose Internet Mail Extensions
USB	Universal Serial Bus

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

CAC	IC card which is issued by the certification organization in the Department of Defense.

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

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

Intra-office LAN
: Network which the TOE is connected and is connected to the external network through firewall, etc.

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

PIV
: Personal ID verification method to carry out with a certificate published by a federal office or a related information.

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

SNMP
: Protocol to manage various devices through network

SSL
: Protocol to transmit by encrypting information through the Internet

12. Bibliography

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

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

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

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

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

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

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

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

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

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

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

[12] bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 PKI Card System Control Software Security Target Version 1.03 (March 18, 2011) Konica Minolta Business Technologies, Inc.

[13] bizhub 652 / bizhub 602 / bizhub 552 / bizhub 502 PKI Card System Control Software Evaluation Technical Report First Version (April 27, 2011) Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security