Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-01-29 (ITC-0284)
Certification No.	C0273
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	bizhub C652 / bizhub C552 / bizhub C452 PKI Card System Control Software
Version of TOE	A0P00Y0-0100-GM0-31
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.
2010-09-28

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 C652 / bizhub C552 / bizhub C452 PKI Card System Control Software Version A0P00Y0-0100-GM0-31" 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 C652 / bizhub C552 / bizhub C452 PKI Card System Control Software Version A0P00Y0-0100-GM0-31" (hereinafter referred to as "the TOE") developed by Konica Minolta Business Technologies, Inc., and evaluation of the TOE was finished on 2010-09 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 consumer" 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 are as follows. Refer on and after Chapter 2 for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

bizhub C652 / bizhub C552 / bizhub C452, which this TOE is installed, are digital multi-function products provided by Konica Minolta Business Technologies, Inc., composed by selecting and combining copy, print, scan and FAX functions. (Hereinafter all the products are referred to as "MFP".)

TOE is the "control software for bizhub C652 / bizhub C552 / bizhub C452" 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. TOE supports the function to print the encryption print realized by using a special printer driver and IC card by using exclusive driver (loadable driver) and the IC card that is used generating that encryption print for a printer data transmitted to MFP from client PC among the highly confidential document exchanged between MFP and client PC. Also, it provides the protection function for scan image data transmitted by mail from MFP by S/MIME using loadable driver and IC card. All are coordinated with IC card and TOE and realizes these security functions.

Moreover, for the danger of illegally bringing out HDD, which stores image data in MFP, TOE can encrypt all the data written in HDD including image data using ASIC (Application Specific Integrated Circuit). Besides, 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 public line against

the danger 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.

About 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 operational environment that this TOE assumes is described in the next clause.

1.1.2.1 Threats and Security Objectives

This TOE counters each threat by 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, 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, TOE encrypts and writes information in HDD by using the encryption function of ASIC outside of TOE.

1.1.2.2 Configuration and Assumptions

It assumes that the product of target of evaluation is operated in the following configuration and assumptions.

It assumes that the 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, the MFP is managed so that is not accessed from an external network when LAN is connected to an external network which is 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 en encryption passphrase.

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

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

1.1.3 Disclaimers

- The functions of IC card used in communication encryption of an image file, a digital signature and authentication, IC card reader, an exclusive driver and 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 which is an option part is installed.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2010-09 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 and Observation Report 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 concluded fully certification activities.

2. Identification

The TOE is identified as follows;

Name of TOE:	bizhub C652 / bizhub C552 / bizhub C452 PKI Card System Control Software
Version of TOE:	A0P00Y0-0100-GM0-31
Developer:	Konica Minolta Business Technologies, Inc.

At the time of TOE installation or others, a user can ask a service engineer to confirm that the product is this TOE evaluated and certified.

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

3. Security Policies

This chapter describes whether this TOE realizes functions as security service under what kind of policy or rule.

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 following functions for customer's demand.

- An encryption of highly confidential image files in transmission and reception. A digital signature in transmission from TOE. And a mechanism that only the user who sent a print file can print it when TOE received it.
- A mechanism not to permit access from an FAX public line port of MFP to an internal network

3.1 Roles related 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 from 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 that performs the maintenance service of MFP in cooperation with Konica Minolta Business Technologies, Inc. is assumed.)

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

(5) Responsible person of the organization that manages the maintenance of the MFP
A responsible person of the organization that manages the maintenance of MFP. Assigns service engineers who manage the maintenance of MFP.

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

3.2 Security Function Policies

TOE prepares security functions to counter threats shown in 3.2.1 and to fulfill the organizational security policies shown in 3.2.2.

3.2.1 Threats and Security Function Policies

3.2.1.1 Threats

This TOE assumes such threats presented in Table 3-1 and provides functions for countermeasure to 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 such as the setup various passwords can leak by the person with malicious intent when he/she analyzes the HDD or NVRAM in the MFP.
T.BRING-OUT-STORAGE (Unauthorized bringing out HDD)	- 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 leak by a malicious person or a user illegally when he/she brings out the files to analyze the HDD in a MFP. - A person or a user with malicious intent illegally replaces the 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 that such image files will leak.

3.2.1.2 Security Function Policies against Threats

This TOE counters against 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.

TOE provides the function to overwrite data for the deletion of all area of HDD and initializes the settings like passwords that is set in NVRAM (referred as "All area overwrite deletion function"), so it prevents the leakage of the protected assets and the security settings in HDD and NVRAM connected to 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 leaks 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 as "encryption key generation function") and supporting function with the ASIC (referred as "ASIC operation support function") by using the encryption function of ASIC outside of 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 Organizational Security Policies and Security Function Policies

3.2.2.1 Organizational Security Policies

Organizational security policy required in use of the TOE is presented in Table 3-2.

Table 3-2 Organizational Security Policies

Identifier	Organizational 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 equipment 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) 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 port of Fax public line must be prohibited.

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

3.2.2.2 Security Function Policies to Organizational Security Policies

TOE prepares the functions to fulfill the organizational security policies shown in Table 3-2.

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

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

In this TOE, by supporting the function encrypting scan image file which is transmitted to user's client PC from MFP by e-mail (referred as "S/MIME encryption processing function") and encrypting Encrypted print file which is transmitted to MFP from client PC with IC card and exclusive driver outside of TOE, image data which flows on network can be transmitted and received confidentially.

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

This organizational security policy prescribes that signature is added to ensure the integrity of image file which flows using e-mail. As this corresponds as one's request, it does not need to add signature all image data. It needs to add signature on handling scan image file.

In this TOE, by supporting the function transmitting scan image file to client PC from MFP by e-mail with IC card outside of TOE (referred as "IC card operation support function") and the function that TOE add signature using IC card (referred as "S/MIME signature function"), image data which flows using e-mail can be ensured the integrity and transmitted.

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

This organizational security policy prescribes that only the user who generated encrypted print files can decrypt and print encrypted print files concerned.

In this TOE, by supporting the function that the encrypted print files are with IC card outside of TOE (referred as "IC card operation support function") and the function that encrypted print files can be accepted to decrypt and print when IC card which generated the encrypted print files is used (referred as "encrypted print file decryption function"), only the user who generated the encrypted print files can decrypt and print the encrypted print files concerned.

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

This organizational 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 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 realizes to prohibit the access to the internal network via the port of Fax public line.

4. Assumptions and Clarification of Scope

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

4.1 Usage Assumptions

Assumptions when this TOE is operated present in the 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 the series of permitted operations given to them.
A.NETWORK (Network connection conditions for MFP)	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 (Operational condition about secret information)	Each password and encryption passphrase does not leak from each user in the use of TOE.
A.IC-CARD (Operational condition about IC card)	IC card is owned by rightful user in the use of TOE.
A.SETTING (Operational setting condition about security)	The following operation setting related to security is set when a user uses the TOE. - 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 panel.

4.2 Environment Assumptions

This TOE is installed in any one of bizhub C652, bizhub C552, bizhub C452, 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 the 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 IC card of user.

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 cooperate is outside the scope of this evaluation. (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.

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

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

5. Architectural Information

This chapter explains a purpose and a relation about the scope of TOE and the main configuration (sub systems).

5.1 TOE boundary and component

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

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

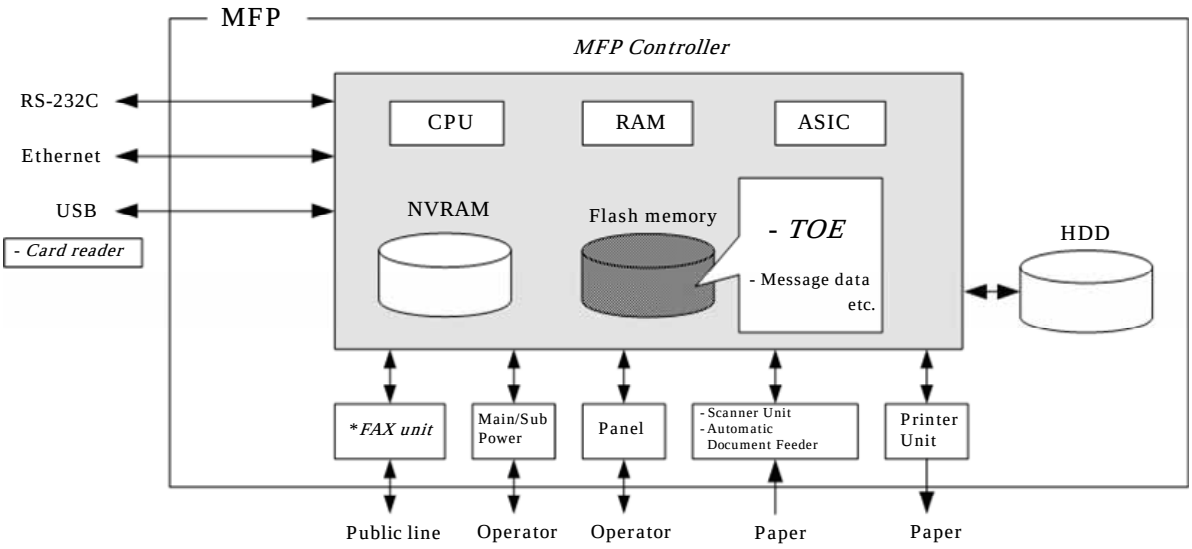

Figure 5-1 TOE boundary

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

- The part which executes common management
  This part manages every kind of setting value and provides a measure which another part of TOE accesses to the setting value. Every kind of setting value includes 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 the HDD.
  In input/output function to the HDD, an encryption at the time of writing and a decryption at the time of reading are done by ASIC.
  It overwrites all data of HDD with the directed method when the administrator directs.

- 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, the mechanism does not let to access an internal network from Fax unit.

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

5.2 IT Environment

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

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

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

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

(4) HDD
A hard disk drive of 250GB in capacity. This is used not only for storing image data as files but also as an area to save image data and destination data temporarily during extension conversion and so on. And the exclusive 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 the MFP, equipped with a touch panel of a liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc. It is controlled by "the part which provides interface via the panel."

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

(8) Printer unit
A device that actually prints the image data which were converted for printing when receives a print request by the 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 according to the circumstances in sales, 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 the case of failure.

(13) FAX Unit (optional part)
A device that has a port of Fax public line and is used for communications for FAX-data transmission via the public line.
Is not pre-installed in MFP as a standard function according to the circumstances in sales, 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 fully understanding and complying with the following documents in order to satisfy the assumptions.

< For administrators and users >

- bizhub C652 / C552 / C452 for PKI Card System User's Guide [Security Operations] Ver.1.00

< For service engineers >

- bizhub C652 / C552 / C452 for PKI Card System SERVICE MANUAL SECURITY FUNCTION Ver.1.03

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

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

7.2 Overview of Evaluation Activity

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

Evaluation has started on 2010-01 and concluded by completion the Evaluation Technical Report dated 2010-09. 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 2010-06 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 2010-06.

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

7.3.1 Developer Testing

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

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 7-1.

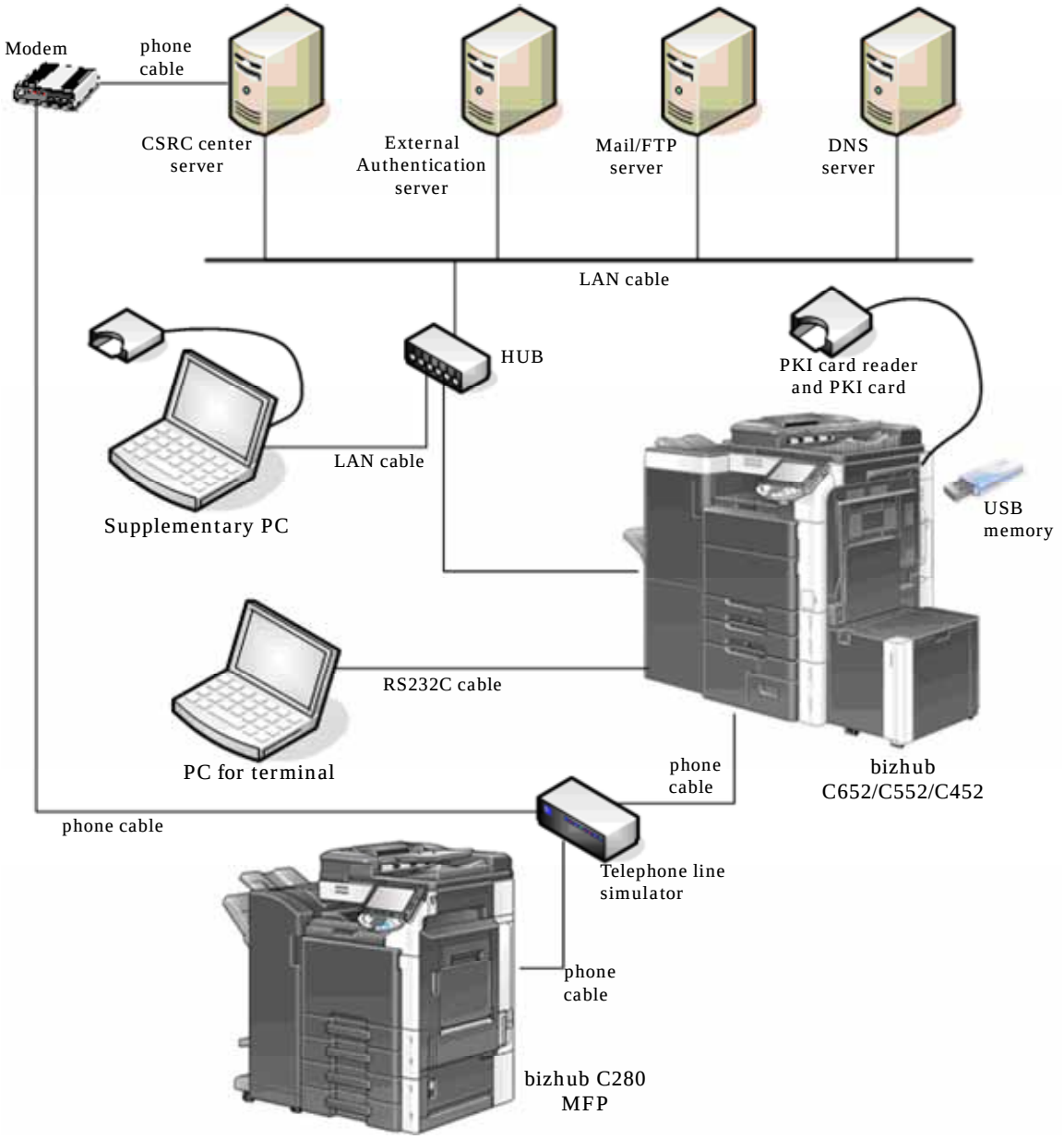

Figure 7-1 Configuration of Developer Testing

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

2) Outlining of Developer Testing

The tests performed by the developer are as follows;

a. Test outline

Outline of the tests performed by the developers are as follows;

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

use.

<Tools and others used at Testing>

Table 7-1 Tools and others used in developer testing

Name of hardware and software	Outline and Purpose of use
KONICA MINOLTA C652 Series PCL Driver Ver.3.0.16.BT12_01	Exclusive printer driver software for bizhub C652 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	Tool for monitoring and analyzing of the communication on the LAN. Used to get communication log and confirm 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)	Tool software for hash and encryption/decryption function. Used to confirm 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 the MFP to monitor the state of TOE.
Disk dump editor Ver. 1.4.3	Tool software to display the contents in the HDD. Used to confirm the contents in the HDD.
Stirling Ver. 1.31	Binary editor software. Used to confirm the contents of decode S/MIME message.
MIME Base64 Encode/Decode Ver. 1.0	Tool software to encode/decode of MIME Base64. Used to decode of S/MIME message.
Blank Jumbo Dog Ver. 4.2.2	Simple server software for intranet. Used as mailer server and FTP server function.
CSRC center software Ver. 2.4.0	Server software for CSRC center. CSRC is maintenance service to manage the state of MFP which Konica Minolta business technologies, Inc. offers by remote.

b. Scope of Testing Performed

Testing is performed 38 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the TOE design and the subsystem interfaces.

c. Result

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

7.3.2 Evaluator Independent Testing

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

1) Evaluator Independent Test Environment

Configuration of test performed by the evaluator shall be the same configuration with developer testing.
Configuration of test performed by the evaluator is showed in the Figure 7-1. Test configuration performed by the evaluator shall be the same configuration with TOE configuration identified in ST.
Only bizhub C652 / bizhub C552 are chosen as MFP which TOE is loaded, however it is judged not to have any problem as a result that the following confirmation was done by evaluator.

- It was confirmed by a document offered from developer that a difference of bizhub C652 / bizhub C552 / bizhub C452 is only copy / print speed.

2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. In terms of Evaluator Independent Testing

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

<Viewpoints of Test>
(1) Based on the situation of developer test, test as many security functions as possible.
(2) Test targets are all probabilistic and permutable mechanism.
(3) Test the behavior depending on the differences of password input methods to TSI for the test 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 character, test the necessary variations.

b. Outlining of Evaluator Independent Testing

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

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

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

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

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

Viewpoints of Independent Test	Overview of Testing
(1) Viewpoint	Tests were performed that were judged to be necessary in addition to developer tests.
(2) Viewpoint	Tests were performed with changing the number of letters and the types of letters by paying attention to the probabilistic and permutable mechanism at identification and authentication or etc. by the administrator.
(3) Viewpoint	Tests were performed with considering the operated interfaces to confirm the behavior depending on the difference of password input method.
(4) Viewpoint	Tests were performed with considering the complexity of S/MIME encryption function to confirm the action at encrypting scan image data and transmitting by e-mail.
(5) Viewpoint	Tests were performed with judging the functions being innovative and unusual character to confirm the action of Fax unit control function, encryption key generation function of HDD encryption and encryption print function.

c. Result

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

7.3.3 Evaluator Penetration Testing

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

1) Outlining of Evaluator Penetration Testing

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

a. Vulnerability of concern

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

<Vulnerability requiring the penetration tests>
(1) Possibility to be activated the unexpected service.
(2) Possibility to be detected the public vulnerability by the vulnerability checking tool.
(3) Possibility to affect the security functions by the power ON/OFF.
(4) Possibility to be wiretapped data transferred between card reader, MFP and external authentication server.
(5) Possibility to be operated by an operator with different authority by competition of the certification from different interface.
(6) Lack of the conviction for the operation of mechanism reducing a threat in a specific condition when HDD is brought out.

b. Scope of Test Performed

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

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

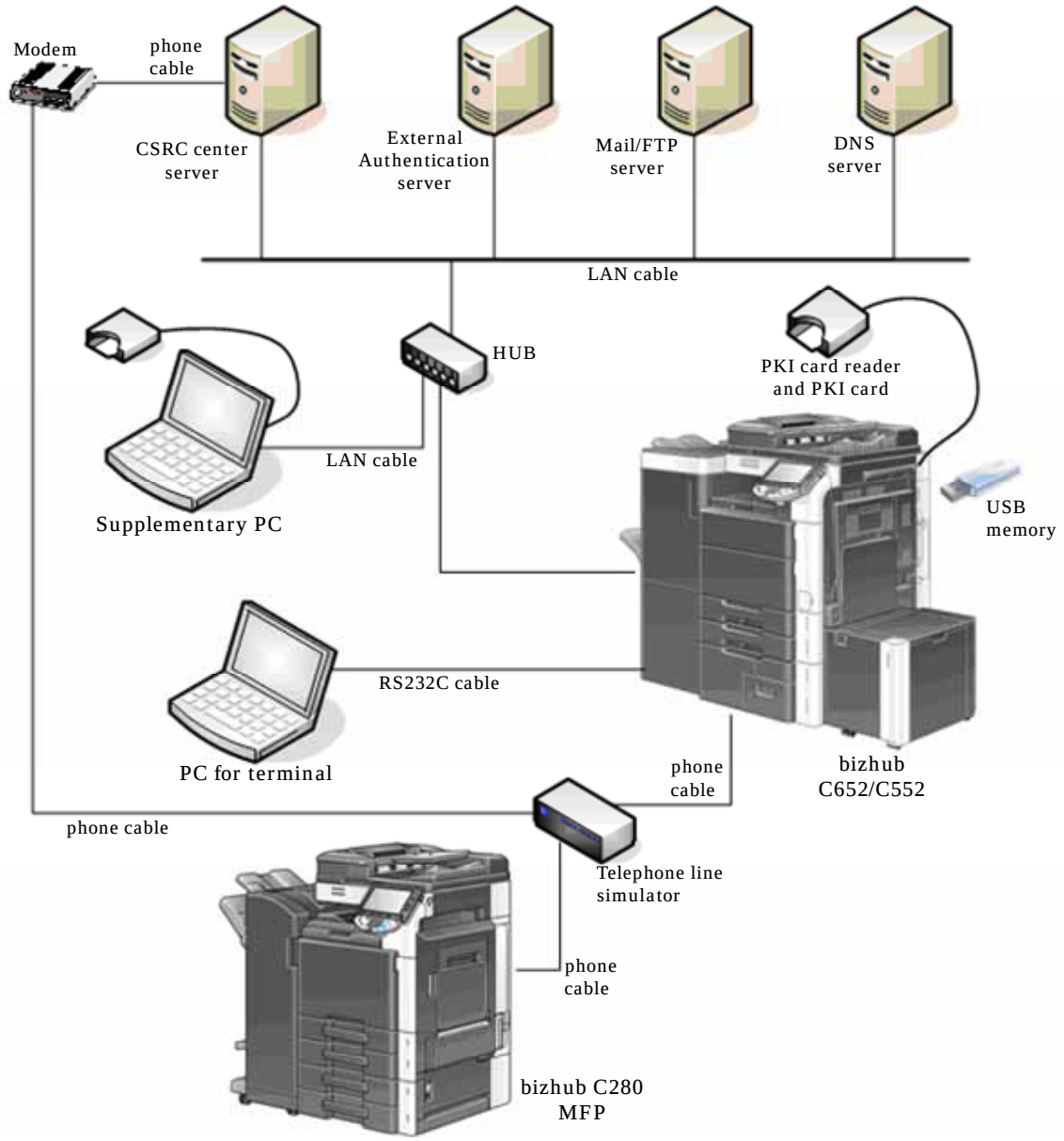

Figure 7-2 Environment of Penetration Testing

<Testing Approach>
Tests were done to use the following methods; method to check by the visual observation of the behavior after stimulating TOE with operating from the operational panel, method to check by the visual observation of the behavior after accessing 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 vulnerability by the vulnerability checking tool with

operating the inspection PC.

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

Table 7-3 Configuration of Penetration Testing

Test Configuration Environment	Details
Inspection object (TOE)	- TOE installed in bizhub C652 / bizhub C552 / bizhub C452 (Version: A0P00Y0-0100-GM0-31) - Network configuration Penetration Tests were done by connecting each MFP with hub or cross-cable.
Supplementary PC	- PC with network terminal operated on Windows XP SP2 or Windows2000 SP4. - Using the tools shown in table 7-1 (Thunderbird, Disk dump editor etc.) and software for USB analyzer (made by CATC) - Connect the 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 SP2, and is connected to MFP with cross-cable to perform penetration tests. - Explanation of test tools. (The operation 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 Jun. 11, 2010.) (1)snmpwalk Version 3.6.1 MIB information acquiring tool (2)openSSL Version 0.9.8n encryption too of SSL and hash function (3)Nessus 4.2.2.(build 9129) Security scanner to inspect the vulnerability existing on the System (4) Wireshark 1.2.4 Packet analyzer software that can parse protocols more than 800.

<Concerned vulnerabilities and Test outline>
The concerned vulnerabilities and the corresponding tests outline are shown in Table 7-4.

Table 7-4 Concerned vulnerabilities and Overview of Testing

Concerned vulnerabilities	Overview of Testing
(1) Vulnerability	Tests were performed to confirm possibility of abusing by using the tool such as Nessus and behavior inspection.
(2) Vulnerability	Tests were performed to confirm possibility of abusing by using the tool such as Nessus and result analysis.

Concerned vulnerabilities	Overview of Testing
(3) Vulnerability	Tests were performed to confirm that the forced power ON/OFF does not affect the security function of initialization process, screen display and etc.
(4) Vulnerability	Tests were performed to confirm that information to affect security function from data transferred between the card reader and the external authentication servers does not leak out.
(5) Vulnerability	Tests were performed to confirm that there is not the situation to be operated with different authority from the operator, in the case which tried the certification with IC card in a state certified at the operation panel and the reverse case.
(6) Vulnerability	Tests were performed to confirm whether a mechanism reducing a threat operates in a specific condition.

c. Result

In the conducted evaluator penetration tests, the exploitable vulnerability that attackers who have the assumed attack potential could exploit was not found.

7.4 Evaluated Configuration

(1) Operating model

It is assumed that this TOE is installed in any one of bizhub C652, bizhub C552, bizhub C452 which is MFP provided by Konica Minolta Business Technologies, Inc.
Because of the reason shown in 7.3.2, the evaluation is considered to have been done in all models though the evaluation was not done in these all models.

(2) Setting of TOE

The evaluation was done 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 panel.

These setting are as the setting shown in 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.

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

- All assurance components of EAL3 package

In the evaluation, the following were confirmed.

- PP Conformance: none
- Security functional requirements: Common Criteria Part 2 Extended
- Security assurance requirements: Common Criteria Part 3 Conformant

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

There is no evaluator recommendation that attention should be called to consumer.

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 Report and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL3 in the CC part 3.

8.2 Recommendations

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

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

- If FAX unit which is option is not installed, FAX unit control function that is security function is unnecessary. (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 C652 / bizhub C552 / bizhub C452 PKI Card System Control Software Security Target Version 1.01, April 15, 2010, Konica Minolta Business Technologies, Inc.

11. Glossary

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

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

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

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
SSL	Secure Socket Layer
S/MIME	Secure Multipurpose Internet Mail Extensions
USB	Universal Serial Bus

The definition of terms used in this report is listed below.

CAC	IC card which is issued by the certification organization in the Department of Defense.
FTP	File Transfer Protocol used at TCP/IP network.
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.
SNMP	Protocol to manage various devices through network
SSL	Protocol to transmit encrypted data through the Internet
S/MIME	Standard of e-mail encryption method Transmitting the encrypted message using RSA public key cryptosystem and needs electric certificate published from certification organization
Intra-office LAN	Network connected TOE and being secured by using switching hub and eavesdropping detection device in the office environment, also being securely connected to the external network through firewall
External network	Access restricted Network from TOE connected intra-office LAN by firewall or other

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 C652 / bizhub C552 / bizhub C452 PKI Card System Control Software Security Target Version 1.01, April 15, 2010, Konica Minolta Business Technologies, Inc.

[13] bizhub C652 / bizhub C552 / bizhub C452 PKI Card System Control Software Evaluation Technical Report Version 2, September 15, 2010, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security