Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2014-05-21 (ITC-4506)
Certification No.	C0478
Sponsor	KONICA MINOLTA, INC.
TOE Name	bizhub C3850 / bizhub C3350 PKI Card System Control Software
TOE Version	A3GN30G0213999P
PP Conformance	None
Assurance Package	EAL3
Developer	KONICA MINOLTA, INC.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Information Security Evaluation Office

This is to report that the evaluation result for the above TOE is certified as follows.
2015-08-26

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass

"bizhub C3850 / bizhub C3350 PKI Card System Control Software" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

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

Table of Contents

1. Executive Summary 1
1.1 Product Overview 1
1.1.1 Assurance Package 1
1.1.2 TOE and Security Functionality 1
1.1.2.1 Threats and Security Objectives 2
1.1.2.2 Configuration and Assumptions 2
1.1.3 Disclaimers 2
1.2 Conduct of Evaluation 3
1.3 Certification 3
2. Identification 4
3. Security Policy 5
3.1 The Roles related to the TOE 5
3.2 Security Function Policies 5
3.2.1 Threats and Security Function Policies 5
3.2.1.1 Threats 6
3.2.1.2 Security Function Policies against Threats 6
3.2.2 Organizational Security Policies and Security Function Policies 7
3.2.2.1 Organizational Security Policies 7
3.2.2.2 Security Function Policies to Organizational Security Policies 7
4. Assumptions and Clarification of Scope 9
4.1 Usage Assumptions 9
4.2 Environmental Assumptions 9
4.3 Clarification of Scope 10
5. Architectural Information 11
5.1 TOE Boundary and Components 11
5.2 TOE Operating Environment 11
6. Documentation 14
7. Evaluation conducted by Evaluation Facility and Results 15
7.1 Evaluation Facility 15
7.2 Evaluation Approach 15
7.3 Overview of Evaluation Activity 15
7.4 IT Product Testing 16
7.4.1 Developer Testing 16
7.4.2 Evaluator Independent Testing 21
7.4.3 Evaluator Penetration Testing 22
7.5 Evaluated Configuration 25
7.6 Evaluation Results 25
7.7 Evaluator Comments/Recommendations 25

8. Certification 26
8.1 Certification Result 26
8.2 Recommendations 26
9. Annexes 27
10. Security Target 27
11. Glossary 28
12. Bibliography 30

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "bizhub C3850 / bizhub C3350 PKI Card System Control Software, Version A3GN30G0213999P" (hereinafter referred to as the "TOE") developed by KONICA MINOLTA, INC., and the evaluation of the TOE was finished on 2015-07 by Mizuho Information & Research Institute, Inc., Information Security Evaluation Office (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, KONICA MINOLTA, INC., and provide security information to procurement entities and consumers who are interested in this TOE.

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

This Certification Report assumes "procurement entities who purchase the TOE that is commercially available" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

bizhub C3850 / bizhub C3350, which the TOE is installed, are digital Multi Functional Peripherals (hereinafter referred to as the "MFP"), provided by KONICA MINOLTA, INC., composed by selecting and combining functions of copy, print, scan and FAX.

The TOE is "bizhub C3850 / bizhub C3350 PKI Card System Control Software" that controls the entire operation of the MFP, including the operation control processing and the image data management triggered by the panel of the MFP main body or through the network. The TOE provides the protection function against the disclosure of the highly confidential documents stored in the MFP. Note that the TOE does not possess the audit log function.

Moreover, against the risk of illegally taking out the HDD that is the medium to store image data in the MFP, the TOE can prevent unauthorized access by encrypting image data to be written in the HDD. Besides, the TOE provides the function to completely delete data area including image data stored in the HDD by a deletion method compliant with various overwrite deletion standards.

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

1.1.2.1 Threats and Security Objectives

The TOE counters each threat with the following security functions.

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

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

1.1.2.2 Configuration and Assumptions

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

It is assumed that the MFP including the TOE is installed in an office which is managed by an organization such as a company or its section, and is connected to the intra-office LAN.

It is assumed that IC card reader is usable with the MFP and a client PC, while Active Directly and the SMTP server are usable at the LAN.

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

Administrators and service engineers are assumed to be reliable. For example, it is assumed that they can keep the secret about their passwords and encryption passphrases.

It is assumed that an IC card used in the use of the TOE is limited to its authorized user only.

It is assumed that the TOE is used in a state where the setting of the enhanced security function is enabled.

1.1.3 Disclaimers

- The encryption of the communications of image files, a digital signature, the IC card used for authentication, IC card reader, exclusive driver, and the function of Active Directory are not assured in this evaluation.

- It is necessary to activate the setting of the enhanced security function. When it is activated, a part of MFP functions cannot be used. Refer to the description of each setting described in "1.4.3.5 Enhanced Security Function" of the ST.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2015-07, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and the Observation Report prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	bizhub C3850 / bizhub C3350 PKI Card System Control Software
TOE Version:	A3GN30G0213999P
Developer:	KONICA MINOLTA, INC.

Administrators and users can ask service engineers as below to confirm that the product is the evaluated and certified TOE.

TOE version, including TOE identification information, is displayed by the panel operation of service engineers. Administrators and users can confirm that the installed MFP is equipped with the evaluated and certified TOE, by confirming that TOE version is the same as the one described in a service manual.

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organizational security policies.

The TOE provides the encryption function and the overwrite deletion function to prevent the leakage of information when the MFP is returned or discarded, or the HDD is illegally taken out.

The TOE also realizes the following for customer's demand.

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

3.1 The Roles related to the TOE

The roles related to the TOE are defined as follows.

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

(2) Administrator
An MFP user who manages the MFP operation. An administrator manages MFP's mechanical operations and users. (In general, a person who is elected among the employees in the office is assumed to play this role.)

(3) Service engineer
A user, who manages the maintenance of the MFP, performs the repair and adjustment of the MFP. (In general, a person in charge of the maintenance service of the MFP at a sales company in cooperation with KONICA MINOLTA, 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. An administrator who manages the MFP operation is assigned.

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

Besides these, though not a TOE user, those who go in and out the office are assumed to be accessible persons to the TOE.

3.2 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Section 3.2.1, and to satisfy the organizational security policies shown in Section 3.2.2.

3.2.1 Threats and Security Function Policies

3.2.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the security functions to counter them.

Table 3-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP (Lease-return and discard of the MFP)	When leased MFPs are returned or when discarded MFPs are collected, encrypted print files, scanned image files, and stored image files can be leaked by a person with malicious intent when he/she analyzes the HDD in the MFP. In addition, administrator passwords and encryption passphrases can be leaked by a person with malicious intent when he/she analyzes the NVRAM in the MFP.
T.ACCESS-HDD (Unauthorized access to the HDD)	Data stored on the HDD such as all image files and passwords can be leaked by a person or a user with malicious intent when he/she illegally accesses to the HDD installed on the MFP (such as removing the HDD and connecting it to PC to analyze) without using the MFP.

3.2.1.2 Security Function Policies against Threats

The 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 the MFP)]

This threat assumes the possibility of leaking information from the NVRAM and the HDD of the MFP collected from users.

The TOE provides the function to overwrite data for the deletion of data area including image data in the HDD and the function to initialize information stored in the NVRAM, so they prevent the leakage of the protected assets stored in the NVRAM and the HDD of the MFP collected from users.

The following methods can be chosen as the HDD overwrite deletion methods. (For example, it indicates that the first one overwrites once by 0x00 and that the second one overwrites in the order of Random numbers, Random numbers, and 0x00. "Verification" means to check that the last overwriting was correctly performed by actually reading the HDD.)

- 0x00
- Random numbers => Random numbers => 0x00
- 0x00 => 0xFF => Random numbers => Verification
- Random numbers => 0x00 => 0xFF
- 0x00 => 0xFF => 0x00 => 0xFF
- 0x00 => 0xFF => 0x00 => 0xFF => 0x00 => 0xFF => Random numbers
- 0x00 => 0xFF => 0x00 => 0xFF => 0x00 => 0xFF => 0xAA
- 0x00 => 0xFF => 0x00 => 0xFF => 0x00 => 0xFF => 0xAA => Verification

(2) Security function to counter the threat [T.ACCESS-HDD (Unauthorized access to the HDD)]

This threat assumes the possibility of disclosure of the protected assets stored in the HDD by unauthorized access without using the MFP.

The TOE counters the threat by encrypting TSF data and image data stored in the HDD.

3.2.2 Organizational Security Policies and Security Function Policies

3.2.2.1 Organizational Security Policies

Organizational security policies required in use of the TOE are shown in Table 3-2.

Table 3-2 Organizational Security Policies

Identifier	Organizational Security Policy
P.COMMUNICATION-CRYPTO (Encrypted communication of image files)	Highly confidential image files (encrypted print files, scanned image files) which are transmitted or received between IT devices must be encrypted.
P.COMMUNICATION-SIGN (Signature of image files)	A digital signature must be added to a mail that contains highly confidential image files (scanned image files).
P.DECRYPT-PRINT (Decryption of image files)	Highly confidential image files (encrypted print files) received by the MFP are permitted to print only to a user who generated those files.

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

3.2.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the security functions to satisfy the organizational security policies shown in Table 3-2.

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

This organizational security policy regulates that image files which flow on the network are encrypted to ensure confidentiality. Because it only needs to be available upon request, it does not need to encrypt all image files, except that encrypted print files and scanned image files need to be encrypted between the MFP and user's client PC in handling.

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

and by encrypting the encrypted print files sent from the client PC to the MFP using the IC card and the exclusive driver, which are outside the TOE scope, it is possible to send and receive image files over the network in a confidential manner.

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

This organizational security policy regulates that a signature is appended to image files to be transmitted or received by e-mail in order to ensure 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 need to have a signature in handling.

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

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

This organizational security policy regulates that only a user who generated encrypted print files can decrypt and print those encrypted print files.

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

4. Assumptions and Clarification of Scope

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

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. The effective performances 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 administrators)	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 service engineers)	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 the MFP)	When the intra-office LAN, where the MFP with the TOE equipped will be installed, is connected to an external network, access from the external network to the MFP is not allowed.
A.SECRET (Operational conditions on secret information)	Each password and encryption passphrase used shall not be leaked from each user in the use of the TOE.
A.IC-CARD (Operational condition on IC card)	The IC card used is owned by the authorized user in the use of the TOE.

4.2 Environmental Assumptions

The TOE is installed in either bizhub C3850 or bizhub C3350, which is the MFP provided by KONICA MINOLTA, INC. It is assumed that the IC card reader is connected to the MFP.

It is assumed that the MFP including the TOE is installed in an office which is managed by an organization such as a company or its section, and is connected to the intra-office LAN.

It is assumed that Active Directory is connected to the intra-office LAN to authenticate user's IC card.

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

The SMTP server is assumed to be connected to the intra-office LAN. It is optional whether DNS server is used in the intra-office LAN.

It should be noted that the reliability of the hardware and the cooperating software shown in this configuration is out of the scope in the evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

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

- The encryption of communication of image files, digital signature, and authentication are necessary in order to realize the organizational security policies. Though the TOE cooperates with the IC card, IC card reader, exclusive driver, and Active Directory, these are outside the TOE scope and are not within the scope of this evaluation.

5. Architectural Information

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

5.1 TOE Boundary and Components

The physical scope of the TOE is the following software:

- Controller firmware (existing in the SSD)

The controller firmware is the software that controls the entire operation of the MFP, including the OS. The software provides a series of functions (basic functions) for office work such as copy, print, scan and FAX, as well as security functions.

5.2 TOE Operating Environment

Figure 5-1 shows the composition of the hardware environment in the MFP that the TOE needs for the operation. The MFP controller is installed in the MFP main body, and a controller firmware exists in the SSD on the MFP controller, and it is loaded onto the volatile RAM (referred to as the "RAM" in Figure 5-1) and operates when the MFP is turned on. The following Figure 5-1 shows characteristic hardware on the MFP controller and the hardware having MFP controller and interfaces.

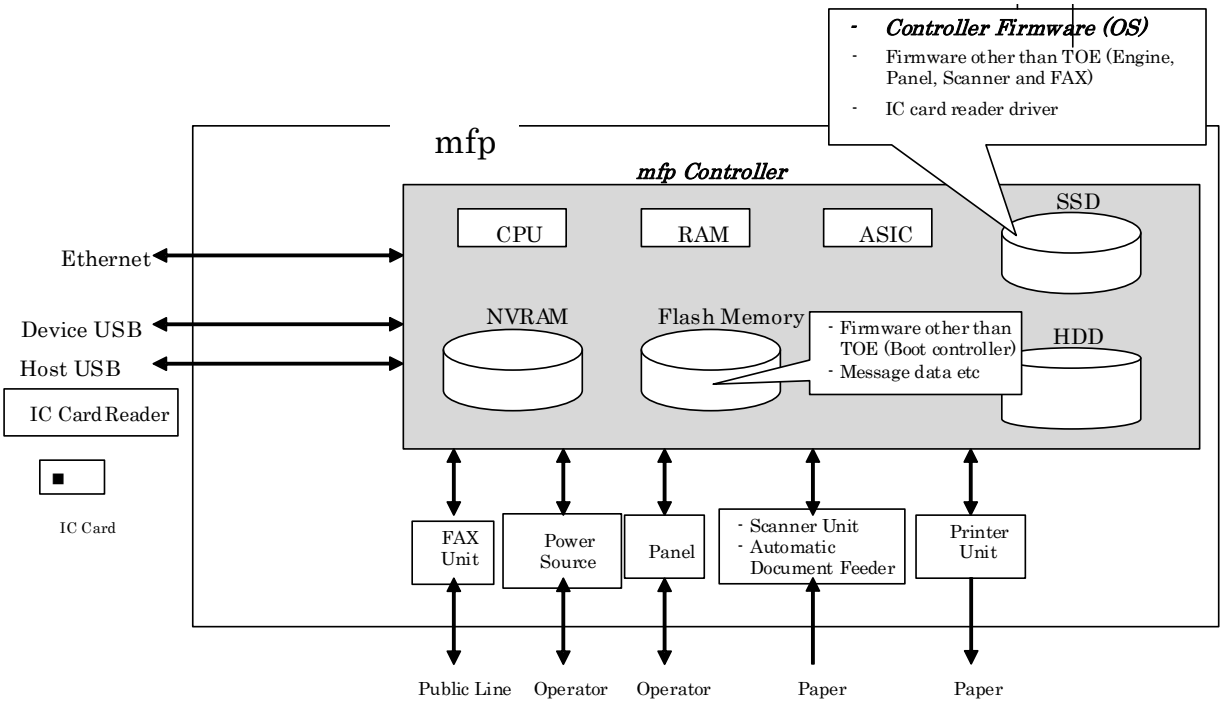

Figure 5-1 Hardware composition relevant to the TOE

- Flash Memory
  A memory medium that stores object code of Boot controller which controls just after power-on. It also stores message data in supported languages to display responses for access from the panel or network, and stores various setting values used in the TOE processing, which are required for the MFP operation.

- HDD (Hard Disk Drive)
  Image data as well as IC card ID are stored.

- NVRAM
  A non-volatile memory. This memory medium stores various setting values used in the TOE processing, which are required for the MFP operation. The NVRAM stores administrator passwords, CE passwords and encryption passphrases.

- Panel
  An exclusive control device for the MFP operation, equipped with a touch panel of a liquid crystal monitor, numeric keypad, start key, stop key, screen switch key, etc.

- Power Source
  Power switches for activating the MFP.

- Ethernet
  Ethernet connection interface device, supporting 10BASE-T, 100BASE-TX, and Gigabit Ethernet.

- Device USB
  A port on the back of the MFP main body for local printing.

- Host USB
  A USB port on the panel side of the MFP for connecting the IC card reader. A user can access to the MFP using the IC card. It can be used for TOE update, printing from the USB flash drive connected to the USB interface, or storing scanned data. Note that the encryption print and S/MIME encryption processing functions are not included in this printing and scanning.

- FAX Unit
  A device that is used for FAX communications via the public line.

- Scan Unit / Automatic Document Feeder
  A device that scans images and photos from paper and converts them into digital data.

- Printer Unit
  A device to actually print image data which were converted for printing when receiving a print request from the MFP controller.

- SSD (Solid State Drive)
  A flash memory drive. A storage medium that stores object code of controller firmware for overall control software, which is the TOE, object code of firmware other than the TOE, such as Engine, Panel, Scanner and FAX, and IC card reader driver.

- ASIC (Application Specific Integrated Circuit)
  An integrated circuit designed for overall image processing. It also processes image development and color adjustment when the image is printed.

- IC Card
  An IC card that supports the standard specification of Common Access Card (CAC) and Personal ID Verification (PIV).

- IC Card Reader
  A device to read IC cards.

- IC Card Reader Driver
  A driver to access to an IC card reader.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

<For administrators and users (for overseas)>

- bizhub C3850/C3350 for PKI Card System User's Guide [Security Operations] Ver.1.04

<For administrators and users (for Japan)>

- bizhub C3850/C3350 for PKI Card System User's Guide [Security Operations] Ver.1.04

<For service engineers (for overseas)>

- bizhub C3850/C3350 for PKI Card System SERVICE MANUAL [SECURITY FUNCTION] Ver.1.03

<For service engineers (for Japan)>

- bizhub C3850/C3350 for PKI Card System SERVICE MANUAL [SECURITY FUNCTION] Ver.1.03

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Mizuho Information & Research Institute, Inc., Information Security Evaluation Office that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which is agreed on mutual recognition with ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

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

7.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report as follows.

The evaluation has started on 2014-05 and concluded upon completion of the Evaluation Technical Report dated 2015-07. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Additionally, for site inspections, considering the previous inspections for the same series of the TOE, the evaluator directly visited the development and manufacturing sites on 2014-10, 2015-01 and 2015-04 and examined procedural status of configuration management, delivery, and security measures, focusing on the different parts of those from the same series of the TOE, by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2015-04.

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

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

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

7.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

Figure 7-1 shows the testing configuration performed by the developer, and Table 7-1 shows a list of main components.

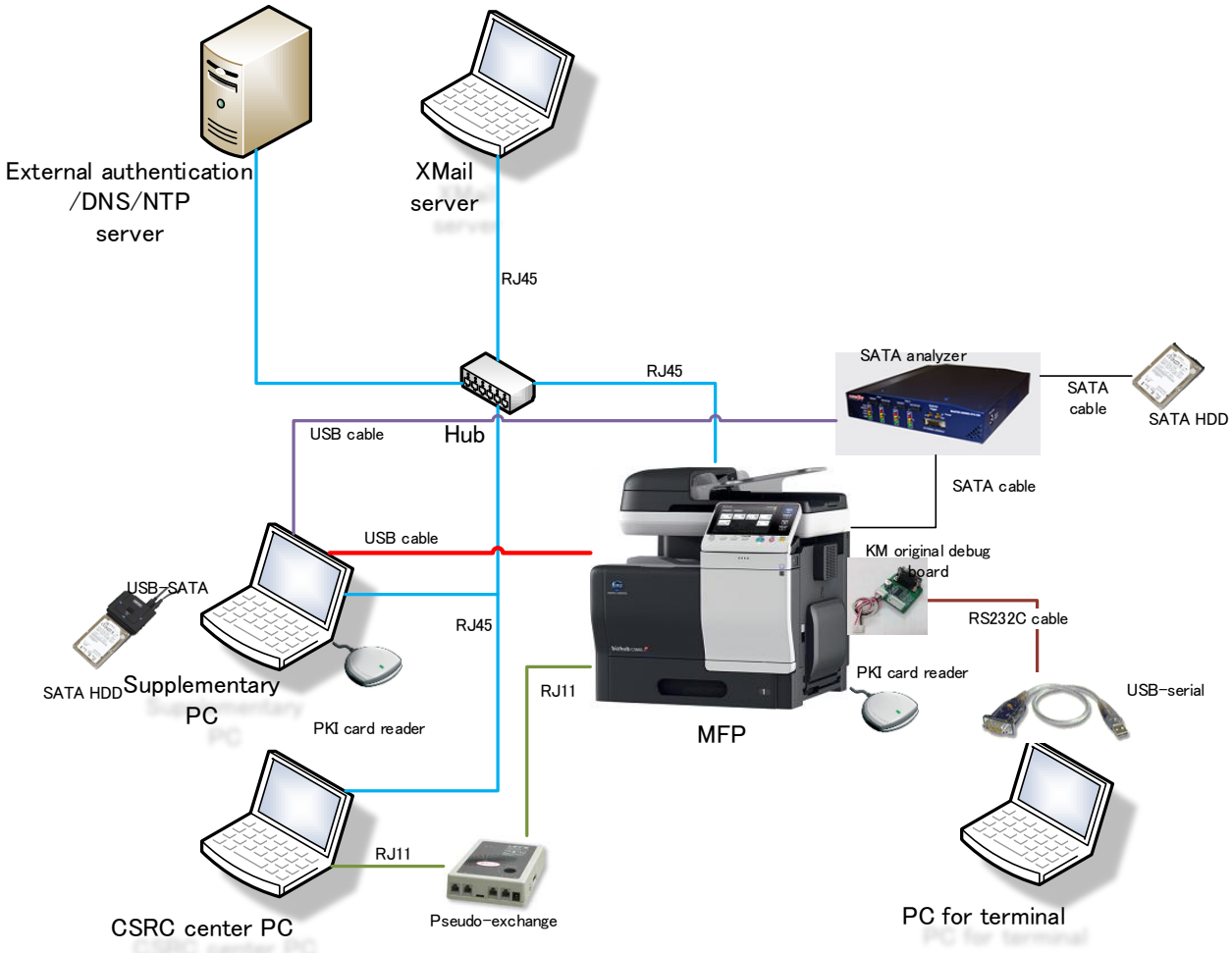

Figure 7-1 Configuration of the Developer Testing

It has been confirmed by the evaluator that the developer testing was performed in the same TOE testing environment as the TOE configuration identified in the ST.

The specific rationales are described as follows:

- The TOE is installed to the same MFP (bizhub C3850 / bizhub C3350) as identified in the ST.
- Although the CSRC center PC (CSRC is a maintenance service to remotely control MFP device status), a device for debug, and a device to capture data that the MFP writes onto the HDD are connected, they do not affect the operation of TOE security functions and testing results.

Table 7-1 Main Components of the Developer Testing

No.	Name of Component	Outline and Purpose of Use
1	bizhub C3850/ bizhub C3350 (MFP)	The MFPs for testing with the TOE installed for firmware. - TOE reference Name: bizhub C3850 / bizhub C3350 PKI Card System Control Software Version: A3GN30G0213999P
2	IC card reader (AU-211P / Identive SCR-3310 / SCR-3310v2)	It reads IC card information from an IC card. It is connected to the MFP and supplementary PC.
3	IC card (PIV/CAC)	IC card to achieve the PKI function. It is used for "Card authentication," "encryption print," and "S/MIME sending and receiving," etc.
4	Supplementary PC	It is a network-connected PC which runs on Windows 7 Professional SP1. It is used for tests that require the network access, such as the SNMP, encryption print, and S/MIME e-mail receiving.
5	External Authentication / DNS / NTP Server	A server which runs on WindowsServer2003R2 SP2 or WindowsServer2003 SP2. It provides the following server functions: - External Authentication (managing access authority (of owner) using Active Directory) - DNS server (translating domain names into IP addresses) - NTP server (adjusting the time of the supplementary PC)
6	XMail Server	A server used to send and receive e-mail on the Internet. It performs operation tests based on the network setting of the MFP.
7	HUB	A connection device for building the LAN. It uses a HUB that can achieve TCP/IP connection of 100BASE-T specification.

No.	Name of Component	Outline and Purpose of Use
8	RJ45 (LAN cable)	A communication cable, which is 10BASE / 100BASE-T compliant, for connecting the MFP to the HUB, or connecting the backbone network connected to the supplementary PC, external authentication server, and XMail server, to the HUB.
9	USB cable	A cable for connecting the MFP to the supplementary PC.
10	SATA Protocol Analyzer	A tool to capture the HDD write processing.
11	USB-SATA	Adaptor for connecting SATA HDD to the PC via the USB.
12	CSRC Center PC	It is used to verify that the use of the CSRC is restricted.
13	Terminal PC	It is used for debug operation via the KM original debug board.
14	USB-Serial cable	A USB to serial conversion cable. It adds a serial port to the supplementary PC.
15	RS232C cable	A communication cable for connecting a serial port to the KM original debug board.
16	KM original debug board	The KM original PCB for debugging. By connecting this board to the MFP with RS232C cable, it enables debug operation from the terminal PC.
17	Pseudo-exchange	By connecting the modem in the PC to the MFP with a modular cable, it realizes pseudo-public line.
18	RJ11 (Modular cable)	A telephone line cable of RJ11 type.

Note: "SATA HDD" in Figure 7-1 indicates the HDD that is built in the MFP.

2) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

As an interface to stimulate security functions, panel operation of the MFP and operation from the supplementary PC which is connected to the MFP via network or USB were used. To confirm the operation results of the security functions, a method to visually confirm the panel display, display on the supplementary PC with network connection, and display on the terminal PC for output from the debug board, and a method to confirm the results captured by an analysis tool connected to the MFP were adopted. Concerning the HDD encryption function, a test on mounting the HDD and decryption test for encrypted files

were conducted using the PC environment with equivalent functions. Concerning communication data on the network, the content is confirmed by capturing communication packets on the supplementary PC.

<Developer Testing Tools>

Table 7-2 shows software and tools used in the developer testing.

Table 7-2 Developer Testing Tools

No.	Name of device and software	Outline and Purpose of use
1	KONICA MINOLTA C3850 Series PCL v1.3.6.0	Exclusive printer driver software for PKI Card System.
2	ActiveClient v7.0.2.25	Driver software for IC card. It is used as a driver for IC card in the supplementary PC.
3	WireShark Ver. 1.12.0	Software tool for monitoring and analyzing the communications on the LAN. It is used for acquiring communication logs.
4	Mozilla Thunderbird Ver. 31.0	General purpose mailer software. It is used as a confirmation tool of S/MIME mails on the supplementary PC.
5	Open SSL Ver.1.0.1h	Software tool for the hash function and encryption / decryption function. It is used for verifying S/MIME signature.
6	Tera Term Pro Ver. 4.82	Terminal software executed in the terminal PC. It is used to connect with the MFP and to operate the terminal software installed in the MFP to monitor the state of the TOE.
7	Stirling Ver. 1.31	Binary editor software tool. It is used for confirming encryption keys, contents of decode S/MIME messages and editing print files.
8	Base64 encoder V4.41	Software tool to encode/decode Base64 encoder. It is used for decoding S/MIME messages.
9	XMail Ver.1.27 XMailCFG241b.zip	It is used for the mail server function.
10	Apache 2.2.25	Software for Web server. It is used for managing Xmail (mail server).
11	ActivePerl 5.16.3.1603	perl interpreter software. It is used for mail server operation.
12	Internet Explorer Ver. 11	General purpose browser software. It is used for configuring the MFP setting.
13	LeCroy STX SATA Protocol Suite Ver.4.20 Build10	It is used to capture the HDD write processing when the HDD overwrite deletion is performed.

No.	Name of device and software	Outline and Purpose of use
14	Knoppix7.0.2 LiveCD	Software to temporarily change the OS of the supplementary PC to Linux to operate in order to prepare the encryption environment which is equivalent to that of the MFP.
15	CSRC Ver. 2.8.1 Rev.03	Application for the CSRC. It is used for confirming that the usage of the CSRC is restricted.
16	Fiddler.exe Ver.2.4.6.2	Software to monitor and analyze Web access such as http. It is used for performing IPP protocol tests between the MFP and supplementary PC.
17	IC card reader driver (for device/IC card reader) Ver.A3GN0Y0-A401-G00-00	It is used for reading IC card from IC card reader with the MFP.
18	MG-SOFT MIB Browser Professional SNMPv3 Edition Ver.12.20.0.5040	Exclusive browser software for the MIB. It is used for the SNMP related tests.

<Conduct of the Developer Testing>

The TOE security functions are performed by manual operation of the panel on the MFP or manual operation using a printer driver on the supplementary PC.

The HDD encryption function is performed using Linux OS environment with the equivalent functions.

The behavior and responses of the security functions are confirmed by visual check of the panel display, visual check of printing results, analyzing data on the input/output pathway of the HDD collected by analysis tools, visual check of results displayed on the supplementary PC, observing output from the debug board by a terminal PC and analyzing data of the captured communication packets, in order to ensure that the observed testing results and the expected results are consistent.

b. Scope of the Performed Developer Testing

The developer testing was performed on 55 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 sufficiently tested.

c. Result

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

7.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further assurance that security functions are certainly implemented, based on the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The configuration of the testing performed by the evaluator is the same configuration with the developer testing shown in Figure 7-1.

It is regarded that the evaluator testing was performed in a TOE testing environment which is the same as the TOE configuration identified by the ST, for the same rationale as described in “7.4.1 Developer Testing.”

2) Summary of the Independent Testing

A summary of the independent testing performed by the evaluator is described as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluator designed from the developer testing and the provided evaluation documentation are shown below.

<Viewpoints of Testing>

(1) The testing is performed by adding types and combinations of operation cases and input parameters in regard to the TSFs that are judged to be insufficient in the developer testing from the viewpoints of completeness of operation cases and input parameters.
(2) In regard to the types of interfaces to input parameters, the testing is performed by adding other combinations which are different from the developer testing in order to confirm the TSF behavior and its interaction more strictly.
(3) To cover all security functions which are provided by the TOE, it should be considered by conducting the independent testing and sampling tests.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

The same testing approach as that of the developer testing was used.

<Independent Testing Tools>

The same testing tools as those used in the developer testing shown in Table 7-2 were used. Checking these specifications, operation tests and calibration were performed by the evaluator.

<Content of the Performed Independent Testing>

Based on the viewpoints of the independent testing, the evaluator performed 7 items of the independent testing and 20 items of sampling tests. Table 7-3 shows the contents of the main testing performed and the viewpoints of the independent testing corresponding to them.

Table 7-3 Main Independent Testing Performed

Viewpoints of Independent Testing	Overview of Testing
(1)	Testing was performed for encryption passphrase settings and various password settings by adding irregular input values.
(1)	Against the developer testing performed with one encrypted print file registered, i.e., testing with normal operation and power-off operation, testing was added with multiple encrypted print files registered.
(1) (2)	Against the developer testing performed using the CAC card (S/MIME encryption), testing was added using the PIV card.
(1)	Testing was performed to input unacceptable values with the enhanced security function being enabled against parameters of password protocols.

c. Result

All the independent testing performed by the evaluator 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.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation. The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

(1) There is a risk that an unexpected network port interface exists and the TOE can be accessed from it, or there is a risk that protected assets are disclosed by the unauthorized data transmission to open ports.
(2) There is a risk of classified information being leaked and security functions being bypassed by analyzing or falsifying the TOE itself.
(3) There is a risk of security functions being bypassed by the unexpected user operation.
(4) There is a risk of security functions being bypassed by inputting unexpected values to the interface.
(5) There is a risk of security functions being bypassed by operating with the TOE resource depletion.
(6) There is a risk of TSF data and assets being leaked by the interception of communication paths at the time of IC card authentication.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The penetration testing was conducted with the same testing configuration as that of the evaluator independent testing. (Only a test PC, on which tools for the penetration testing were installed, was added.)

In addition to the tools used for the developer testing shown in Table 7-2, the tools shown in Table 7-4 were used in the penetration testing.

Table 7-4 Penetration Testing Tools

No.	Name of tool and software	Outline and purpose of use
1	nmap Version 6.47	Port scan tool
2	snmpwalk Version 3.6.1	MIB information acquisition tool
3	Nessus Version 6.3.3	Security scanner
4	Nikto Version 2.1.5	Security scanner
5	Extrstr Version 0.2	Binary analysis tool
6	USB Explorer Model 200	USB analyzer
7	USB Analysis Software Version 3.3.4015.1	USB analyzer software

<Conduct of the Performed Penetration Testing>

Table 7-5 shows vulnerabilities of concern which are identified in searching potential vulnerabilities and the content of the penetration testing corresponding to them. The evaluator conducted the following penetration testing on 9 items in order to identify the risk of potential vulnerabilities being exploited.

Table 7-5 Overview of the Penetration Testing

Vulnerabilities of Concern	Overview of Testing
(1)	Testing was performed by using port scan tools to confirm that there is no unexpected network port. It is also confirmed that there is no vulnerability against unauthorized inputs in the ports in use by using security scanner, etc.
(2)	Testing was performed to confirm that the acquisition or falsification of classified information cannot be performed by analyzing the TOE binary.
(3)	Testing was performed to confirm that the TOE does not behave in an unexpected way by operating power source with irregular timings that are different from the normal operation.
(4)	Testing was performed to confirm that there is no unexpected behavior caused by unauthorized data received from the client PC or input data from USB devices.
(5)	Testing was performed to confirm that the TOE does not behave in an unexpected way when it is operated with the TOE resource depletion such as HDD capacity.
(6)	Testing was performed to observe communications via the USB cable between IC card and the TOE as well as communications via the LAN cable between the TOE and the external authentication server during the IC card authentication, and to confirm that there is no data which easily result in a leakage of TSF data and assets.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

(1) Operating model
It is assumed that the TOE is installed in either bizhub C3850 or bizhub C3350, which is the MFP provided by KONICA MINOLTA, INC.
The evaluation was performed using these two models.

(2) TOE Setting
The evaluation was performed with the setting of the "enhanced security function" activated.
This setting is as the setting shown in the ST.

7.6 Evaluation Results

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

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

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 only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to consumers.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.

2. Contents pointed out in the Observation Report shall properly be solved.

3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility.

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

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Report and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 in the CC Part 3.

8.2 Recommendations

- The TOE depends on the following functions to counter threats and to fulfill the organizational security policies. (Refer to Section 4.3.)

  > IC card, IC card reader, exclusive driver
  > Active Directory

  The reliability of these functions is not assured in this evaluation, and it depends on procurement entities' judgment.

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

9. Annexes

There is no annex.

10. Security Target

The Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

bizhub C3850 / bizhub C3350 PKI Card System Control Software Security Target
Version 1.09 (July 24, 2015) KONICA MINOLTA, INC.

11. Glossary

The abbreviations relating to the 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
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 authority in the US Department of Defense.
External network	Network where access is restricted with the intra-office LAN that is connected to the TOE, by firewall, etc.
Intra-office LAN	Network to which the TOE is connected, and which is connected to the external network through firewall, etc.
MIB	Various setting information, which the various devices that are managed using the SNMP release to the public.
NVRAM	Random access memory that has a non-volatile and memory keeping character even at the power OFF.
PIV	Personal identity verification method to carry out using a certificate issued by a federal office or using related information.
S/MIME	Standard of e-mail encryption method. Transmitting and receiving the encrypted messages using RSA public key encryption method. An electric certificate issued by the certification authority is necessary.
SNMP	Protocol to manage various devices via network.
SSL	Protocol to transmit information by encrypting via the Internet.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Documentation, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, June 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, June 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001 (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002 (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003 (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004 (Japanese Version 1.0, November 2012)

[12] bizhub C3850 / bizhub C3350 PKI Card System Control Software Security Target Version 1.09 (July 24, 2015) KONICA MINOLTA, INC.

[13] bizhub C3850 / bizhub C3350 PKI Card System Control Software Evaluation Technical Report, Version 5 (130785-01-R003-05), July 27, 2015, Mizuho Information & Research Institute, Inc. Information Security Evaluation Office