Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

IT Product (TOE)

Reception Date of Application (Reception Number)	2017-02-14 (ITC-7629)
Certification Identification	JISEC-C0600
Product Name	Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer Diskless models
Version and Release Numbers	Controller ROM Ver. 1.11.33, FAX ROM Ver. 2.0.8
Product Manufacturer	Fuji Xerox Co., Ltd.
Evaluation Sponsor	Xerox Corporation
Conformance of Functionality	Product specific Security Target, CC Part 2 conformant
Assurance Package	EAL2 Augmented by ALC_FLR.2
Name of IT Security Evaluation Facility	Information Technology Security Center, Evaluation Department

This is to report that the evaluation result for the above TOE has been certified as follows.
2018-05-22

Fumiaki Manabe, 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

"Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer Diskless models" 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

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer Diskless models, Version Controller ROM Ver. 1.11.33, FAX ROM Ver. 2.0.8" (hereinafter referred to as the "TOE") developed by Fuji Xerox Co., Ltd., and the evaluation of the TOE was finished on 2018-05-10 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Xerox Corporation, and provide security information to procurement personnel 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") described in Chapter 10. 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 personnel who purchase the TOE 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 EAL2 augmented by ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is the multi-function device (hereinafter referred to as "MFD"), which has such basic functions as copy, print, network scan, and fax.

In addition to the basic MFD functions, the TOE provides security functions to protect the document data used in basic functions and the setting data affecting security, etc., from disclosure and alteration.

In regard to 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 clause.

1.1.2.1 Threats and Security Objectives

The TOE assumes the following threats and provides security functions against them.

The document data of users and the setting data affecting security, which are assets to be protected, may be disclosed or altered by unauthorized operation of the TOE or by unauthorized access to the communication data on the network to which the TOE is connected.

Therefore, the TOE provides security functions such as identification and authentication, access control, and encryption, to prevent the assets from unauthorized disclosure or alteration.

1.1.2.2 Configuration and Assumptions

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

The TOE is the targeted MFD model with which a hard disk is not equipped and the 3 Line Fax Kit is equipped.

The TOE is assumed to be located in an environment where physical components and interfaces of the TOE are protected from the unauthorized access. For the operation of the TOE, the TOE shall be properly configured, managed and maintained according to the guidance documents.

1.1.3 Disclaimers

The following restrictions are applied to the functions of the TOE and the scope guaranteed in this evaluation.

1) The TOE does not provide the following functions:
- The functions to delete or change a cryptographic key which is used to encrypt a SD memory.

2) The security functions that are certified under this evaluation will no longer be guaranteed when and after the following is conducted:
- The customer service engineers conduct maintenance.

3) The product with the following configuration is not the TOE that is guaranteed in this evaluation:
- The configuration with which a fax kit other than the 3 Line Fax Kit (product code: EC103351) is equipped.

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 2018-05, 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] prepared by the Evaluation Facility and evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. 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:	Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer Diskless models	
TOE Version:	Controller ROM	Ver. 1.11.33
	FAX ROM	Ver. 2.0.8
Developer:	Fuji Xerox Co., Ltd.	

Users can verify that a product is the evaluated and certified TOE by the following means.

Users operate on the control panel according to the procedure written in the guidance document, and confirm the name of the model, the version and optional information written in the print output of the Configuration Report.

- Model name: Either of the following

  Xerox VersaLink C7020, Xerox VersaLink C7025, Xerox VersaLink C7030

- Each version of Controller ROM, and FAX ROM

- Option

  Users confirm that the hard disk capacity is not written in the Configuration Report. Users also confirm that the 3 Line Fax Kit is shown as a fax kit type in the Configuration Report.

3. Security Policy

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

The TOE provides the basic MFD functions such as copy, print, network scan, and fax, and has functions to store the user document data in the TOE's internal SD memory and to communicate with user clients and various servers via network.

When those MFD functions are used, the TOE provides security functions including identification/authentication and access control of users, encryption of the document data stored in the SD memory, and encryption communication. By providing these security functions, the TOE prevents the user's document data and the setting data affecting security that are assets to be protected from being disclosed or altered by unauthorized persons.

The TOE assumes the following user roles:

- General User
  Any person who uses the basic MFD functions, such as copy, print, network scan, and fax, provided by the TOE.

- System Administrator
  A user who has been specifically granted the authority to configure settings of the TOE security functions. System administrator includes "key operator" who can use all the management functions, and "SA (system administrator privilege)" who can use a part of the management functions.

- Customer Engineer
  Customer service engineer who maintains and repairs the MFD.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1, and to satisfy the organizational security policies shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 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.CONSUME	An attacker who is not allowed to use TOE may use TOE functions without authorization.

T.DATA_SEC	A user who is allowed to use TOE may read or alter document data and security audit log data without authorization.
T.CONFDATA	A general user who is allowed to use TOE may read or alter the TOE setting data which only a system administrator is allowed to access.
T.COMM_TAP	An attacker may intercept or alter document data, security audit log data, and TOE setting data on the internal network.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies. Details of each security function are shown in Chapter 5.

1) Countermeasures against threat "T.CONSUME," "T.DATA_SEC" and "T.CONFDATA"

The TOE counters the threats by the following functions: User Authentication, System Administrator's Security Management, Customer Engineer Operation Restriction, and Security Audit Log.

The User Authentication function of the TOE is to allow only identified and authenticated users to use the TOE. When successfully identified and authenticated users attempt to manipulate the document data stored in the TOE, the TOE allows only users with access rights to access the document data.

The System Administrator's Security Management function of the TOE is to allow only identified and authenticated system administrators to refer to and change the data used for security functions. For general users, changing their own passwords is permitted.

The Customer Engineer Operation Restriction function of the TOE is to allow only identified and authenticated system administrators to refer to and change the setting data that control enabling and disabling of customer engineer operation restriction.

The Security Audit Log function of the TOE is to record security relevant events as audit logs. Only identified and authenticated system administrators can read out the stored audit logs. It is not possible to delete and modify the audit logs.

With the above functions, the TOE prevents the data to be protected from being disclosed or altered by unauthorized access to the TOE.

2) Countermeasures against threat "T.COMM_TAP"

The TOE counters the threats by the Internal Network Data Protection.

The Internal Network Data Protection function of the TOE is to use encryption communication protocol and to encrypt the communication data when the TOE communicates with client PCs and various servers.

With the above functions, the TOE prevents the data to be protected from being disclosed or altered by unauthorized access to the communication data.

3.1.2 Organizational Security Policies and Security Function Policies

3.1.2.1 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.VERIFY	The TOE shall execute self-test to verify the integrity of TSF executable code and TSF data.
P.FAX_OPT	The TOE shall ensure that the internal network cannot be accessed via public telephone line.
P.CIPHER	The TOE shall encrypt the document data and the security audit log data in the SD memory. (A cryptographic key does not need to be destructed.)

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the security functions to satisfy the organizational security policies shown in Table 3-2. Details of each security function are shown in Chapter 5.

1) Means of organizational security policy "P.VERIFY"

The TOE realizes this policy by the Self Test function.

The Self Test function of the TOE is to verify check sum of Controller ROM and FAX ROM upon booting. The TOE also checks the TSF data stored in NVRAM and SEEPROM to detect errors. Thus, this function verifies the integrity of TSF executable code and TSF data.

2) Means of organizational security policy "P.FAX_OPT"

The TOE realizes this policy by the FAX Flow Security functions.

The Fax Flow Security function of the TOE never transfer the data received from public telephone lines to the internal network. Thus, this function ensures that the internal network cannot be accessed via public telephone line.

3) Means of organizational security policy "P.CIPHER"

The TOE realizes this policy by the Flash Memory Data Encryption function.

The Flash Memory Data Encryption function of the TOE is to encrypt data to be written to the internal SD memory. The cryptographic algorithm is 256-bit AES.

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	A system administrator shall have the necessary knowledge of TOE security functions to perform the given role of managing the TOE and shall not operate the TOE with malicious intent.
A.USER	TOE users shall be trained and have competence about the TOE operation and precautions according to the policies of their organization and the product guidance.
A.SECMODE	A system administrator shall configure and set the TOE properly according to the security policy of organization and the product guidance document to manage the TOE and its external environment.
A.ACCESS	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

4.2 Environmental Assumptions

The TOE is assumed to be used at general office, connected to the internal network, and used from client PCs connected to the internal network. Figure 4-1 shows the general operational environment of the TOE.

It is possible to use the print function of the TOE by connecting client PCs to the TOE via USB ports

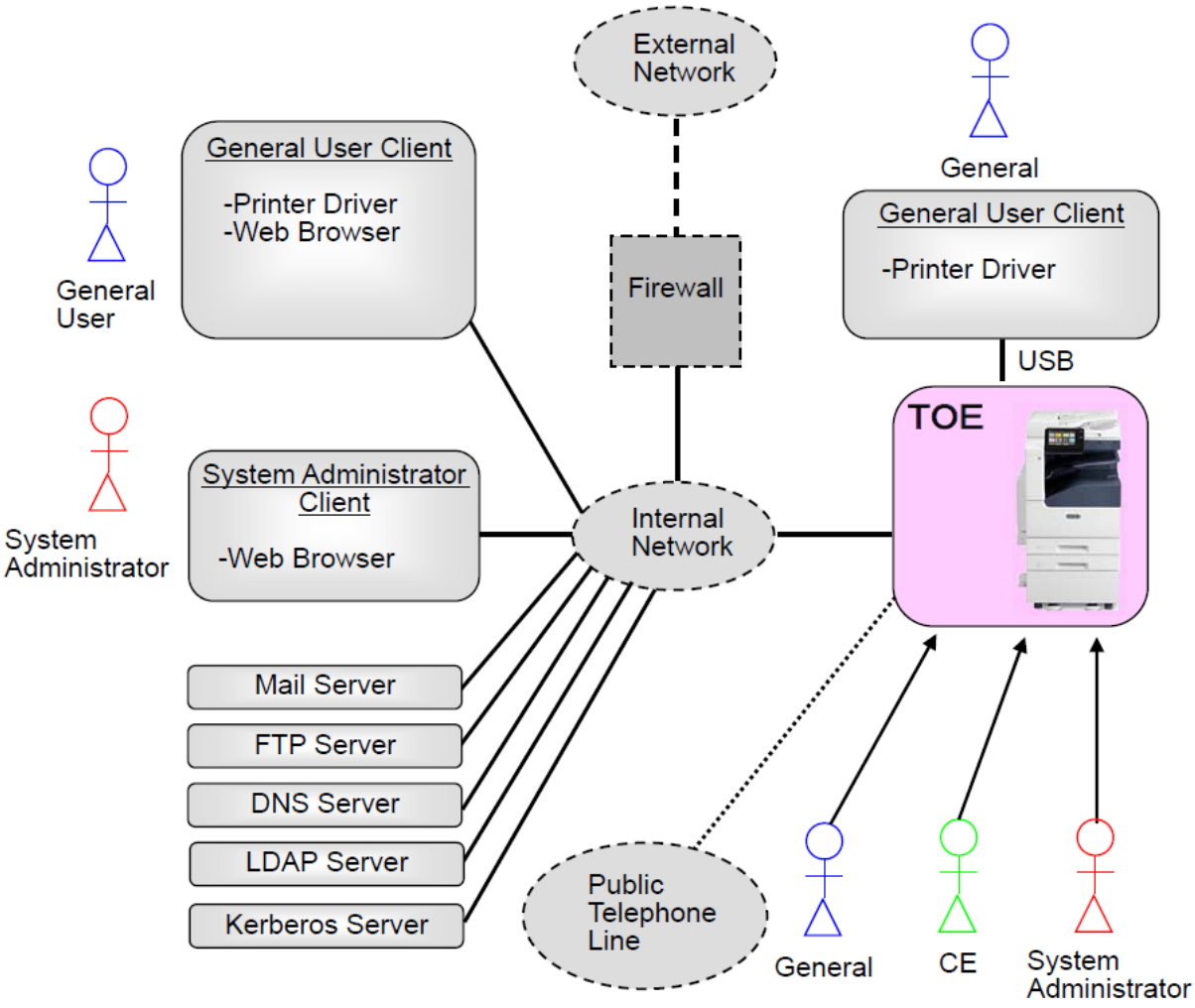

Figure 4-1 Operational Environment of the TOE

The following are components excluding the TOE in the operational environment of the TOE:

1) General User Client

General User Client is a general-purpose PC for general users and connected to the TOE via USB or the internal network. The following software is required:

- OS: Windows 7 or Windows 8.1
- Printer driver

When the client is connected to the internal network, the following software is required in addition to those listed above:

- Web browser (included with OS)

2) System Administrator Client

System Administrator Client is a general-purpose PC for system administrators and connected to the TOE via the internal network. The following software is required:

- OS: Windows 7 or Windows 8.1
- Web browser (included with OS)

3) LDAP Server, Kerberos Server

When Remote Authentication is set for the user authentication function on the TOE, authentication server of either LDAP server or Kerberos server is necessary. When Local Authentication is set, neither authentication server is necessary.

LDAP server is also used to acquire user attributes to identify SA role when Remote Authentication is used. Thus, even for the authentication with Kerberos server, LDAP server is necessary to use the SA role.

In this evaluation, the following software is used as LDAP server and Kerberos server.

- Windows Active Directory

4) Mail Server, FTP Server

The TOE has basic functions to transfer document data with Mail server and FTP server. These servers are necessary upon using the basic MFD functions.

5) DNS Server

The TOE uses the DNS server to retrieve IP addresses of various servers, etc.

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

4.3 Clarification of Scope

As described below, there are restrictions on the security functions of the TOE.

1) Restrictions for Remote Authentication

The TOE function that restricts the number of characters of password to be nine or more is not applied to user password stored in the Remote Authentication server (LDAP server or Kerberos server). A system administrator is responsible for ensuring that user password stored in the remote authentication server is long enough not to be predicted.

2) IPsec for IPv6

The TOE was evaluated with only IPsec protocol for IPv4. The TOE was not evaluated with IPsec for IPv6, so the operation with IPsec for IPv6 is not assured by this evaluation.

5. Architectural Information

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

5.1 TOE Boundary and Components

Figure 5-1 shows the components of the TOE. The scope of the TOE is the MFD including the Fax board.

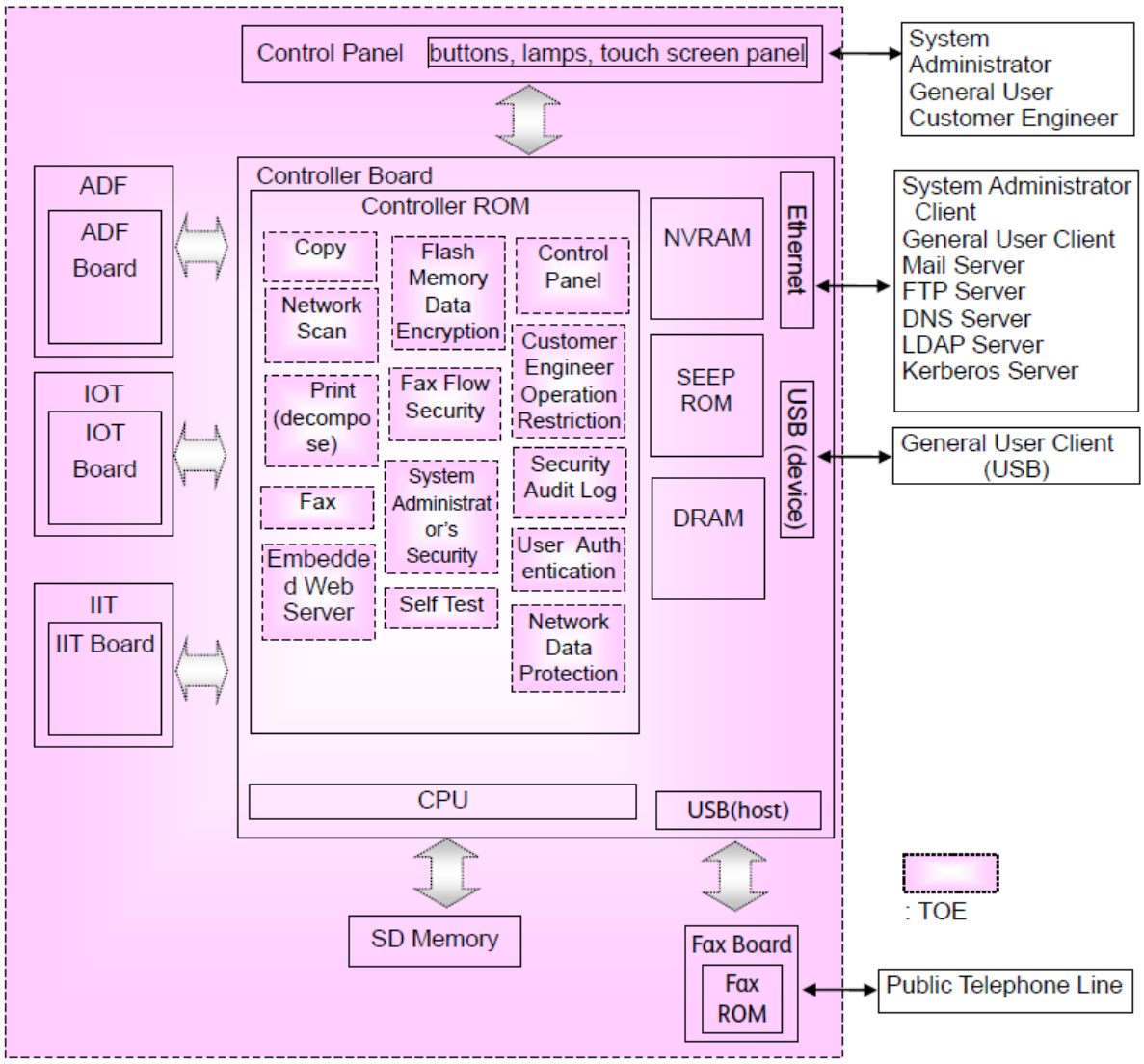

Figure 5.1 Components of the TOE

The TOE has security functions and other basic MFD functions. The following describe the security functions of the TOE. Regarding the basic MFD functions, please refer to Glossary in Chapter 11.

1) User Authentication

This function includes the following two functions: identification and authentication of users, and access control for user data.

a) Identification and authentication of users

This is the function to identify and authenticate TOE users with their IDs and passwords. Identification and authentication are applied to the following user interfaces.

- Control panel
- Client PCs (Web browsers)

For the print data sent from Client PCs (printer drivers), only the identification of a user ID is performed, and the authentication using a password is not performed.

The following types of authentication are available: "Local Authentication" that uses user IDs and passwords stored in the TOE, and "Remote Authentication" that uses LDAP servers and Kerberos servers outside the TOE.

For enhanced security, the following are provided for the user identification and authentication.

- For Local Authentication, users are required to use passwords of nine or more characters.
- For Local Authentication, if a system administrator fails to be authenticated for five times in a row, the authentication process is suspended. This restriction is not applied to general users.

b) Access control for user data

This is the function to restrict the access to document data stored in the TOE to only authorized users.

As to the document data stored in the Store Print, only the user who is verified to be the owner of the data can perform operations on the document data. As to the document data stored in the Faxbox, only system administrators are allowed to perform operations on the data.

2) System Administrator's Security Management

This is the function that permits only identified and authenticated system administrators to configure, refer to, and change the setting of the data used for security functions. For general users, changing their own passwords is permitted.

3) Customer Engineer Operation Restriction

This is the function with which system administrators restrict the operation by customer engineers. Only identified and authenticated system administrators are permitted to refer to and change the setting data that control enabling and disabling of customer engineer operation restriction. If customer engineer operation is restricted, customer engineers are required to enter the password set by a system administrator in order to operate the MFD.

4) Security Audit Log

This is the function that records security relevant audit events as audit logs. Only identified and authenticated system administrators can read out the audit logs stored in the TOE via Web browsers. It is not possible to delete or modify the audit logs.

Up to 15,000 events can be stored as audit logs. When the number of events exceeds the limit, the oldest event is deleted to record a new event.

5) Flash Memory Data Encryption

This is the function that encrypts data to be stored in the internal SD memory. The cryptographic algorithm is 256-bit AES. A cryptographic key is created using the SHA-256 algorithm based on values generated randomly by the TOE. A cryptographic key is automatically created when power of the TOE is turned on for the first time in the factory. The cryptographic key cannot be deleted or changed.

6) Internal Network Data Protection

This is the function that encrypts communication with IT devices using the following protocols and methods.

- IPsec, TLS (v1.0, v1.1, v1.2), S/MIME

7) Fax Flow Security

This is the function that prevents data transfer from public telephone lines to the internal network. The TOE is structured so that it receives fax data only from the specified fax board and transfers the received data to no destination other than the fax function.

8) Self Test

This is the function that conducts the following self tests when the TOE is turned on.

- Verification of the check sum of Controller ROM and FAX ROM
- Verification of TSF data stored in NVRAM and SEEPROM

5.2 IT Environment

When user authentication by Remote Authentication is enabled, the TOE uses an external authentication server (LDAP server or Kerberos server) to identify and authenticate users. The TOE also checks whether a user has the SA role or not by using LDAP server, in case of Remote Authentication.

6. Documentation

The identification of the 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.

- Xerox VersaLink Series Multifunction and Single Function Printers
  System Administrator Guide; Version 2.0 October 2017
  (SHA256 hash value:
  55ec10501077ecf5434d2663b080caa91d3ad8b30b612d008afb7e3f79545b50)

- Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer
  User Guide; Version 2.0 October 2017
  (SHA256 hash value:
  b6922d2ef69d713559d8f9918b6045ca6eea37b9bfd3bf03979131002454b504)

- Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer
  Security Function Supplementary Guide; Version 1.0 March 2018
  (SHA256 hash value:
  08327e27d2d03773d85ab0091b32df65b533ea384fd11b956179e0fa75f1def7)

Note that these documents are not delivered together with the TOE. Users must download them from the Xerox Corporation website. TOE Users can confirm the integrity of the downloaded documents by comparing their calculated SHA256 hash values with the values described above.

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Information Technology Security Center, Evaluation Department 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 2017-02 and concluded upon completion of the Evaluation Technical Report dated 2018-05. 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, the evaluator directly visited the development site on 2017-04, 2017-07 and 2017-08, and examined procedural status conducted in relation to each work unit for configuration management and delivery, 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 2017-08.

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.

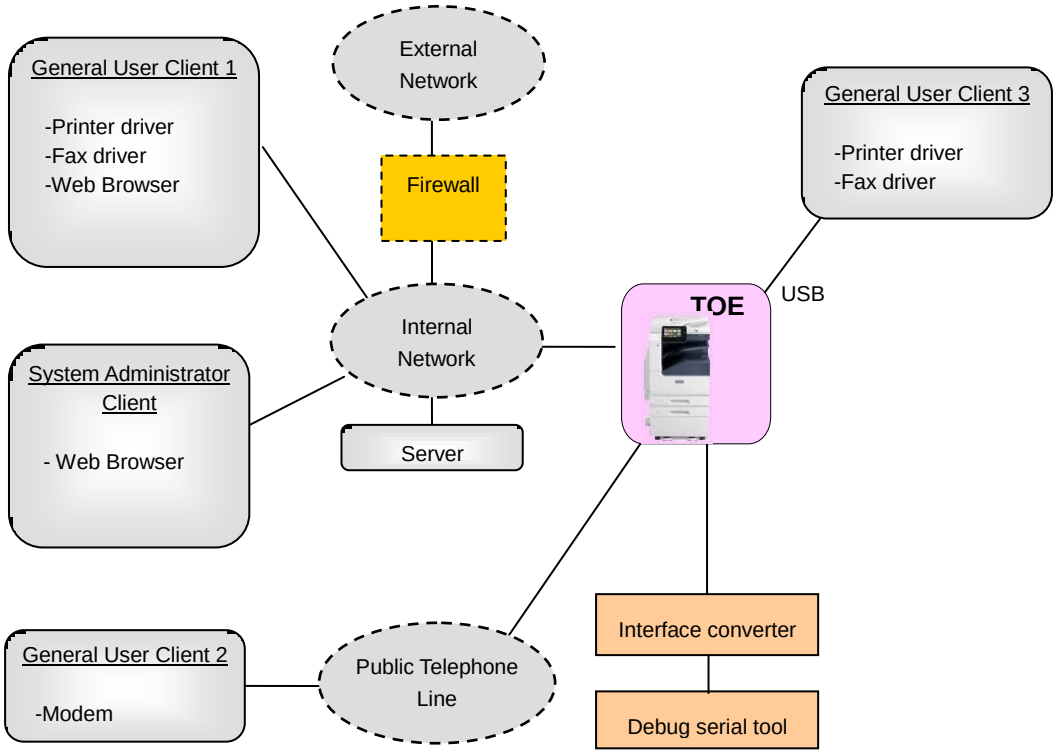

Figure 7-1 Configuration of the Developer Testing

Configuration items for the developer testing are shown in Table 7-1 below.

Table 7-1 Configuration Items for the Developer Testing

Items	Description
TOE	Xerox VersaLink C7020, C7025, C7030 Diskless models (Controller ROM Ver. 1.11.33, FAX ROM Ver. 2.0.8)
Server	Used as various servers. - PC with Microsoft Windows Server 2008 R2 SP1 - Mail server: Xmail Version 1.27 - FTP server: Standard software in OS - DNS server: Standard software in OS - LDAP server: Standard software in OS - Kerberos server: Standard software in OS
System Administrator Client	Used as system administrator client. The testing is performed with the following two models: a) PC with Microsoft Windows 7 Professional SP1 (Web browser: Microsoft Internet Explorer 11) b) PC with Microsoft Windows 8.1 (Web browser: Microsoft Internet Explorer 11)
General User Client 1	Used as general user client (connected via internal network). The testing is performed with the following two models: a) PC with Microsoft Windows 7 Professional SP1 (Web browser: Microsoft Internet Explorer 11) b) PC with Microsoft Windows 8.1 (Web browser: Microsoft Internet Explorer 11) Additionally, the following software is used. - Printer driver and fax driver: PCL6 Print Driver Version 5.511.8 * Fax drivers are used for confirming that they cannot be used.
General User Client 2	Used for confirming send/receive fax. - PC with Microsoft Windows 8.1 * PC modem port is connected to public telephone line.
General User Client 3	Used as general user client (connected via USB port for printer). - PC with Microsoft Windows 8.1 - Printer driver and fax driver: PCL6 Print Driver Version 5.511.8 * Fax drivers are used for confirming that they cannot be used.
Debug Serial	Debugging terminal of the MFD; i.e., PC whose serial port is connected to the terminal port of the MFD for debugging via interface converter. - PC with Microsoft Windows 7 Professional SP1 - Terminal Software: Tera Term Pro Version 2.3
Interface converter	Fuji Xerox-unique conversion board to connect the MFD and debug serial.

Public Telephone Line	Use a pseudo exchange system (N4T-EXCH by How Inc.) as an alternative of public telephone line.

The TOEs tested by the developer are the all models of the TOE, which have the same TOE identification of Chapter 2. However, the test items differ depending on the model.

The developer tested one model of the TOE, Xerox VersaLink C7030, on all test items. Other models were tested on only some of the test items. The evaluator evaluated the developer testing as sufficient, since the models of different model numbers differ only in the printing speed, and they have the same implementation of the security functionalities.

The developer testing was performed in the same TOE testing environment as the TOE configuration identified in the ST.

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>

(1) The behavior that can be observed at the external interface of the TOE

Operate basic MFD functions and security management functions from the MFD control panel, system administrator client, and general user client, and confirm the response, MFD behavior, communication data, and audit log.

(2) The behavior that cannot be observed at the external interface of the TOE

The following approaches were employed to confirm the behavior that cannot be observed at the external interface of the TOE:

- Check the internal behaviors of the TOE using the developer interfaces.

- Check the behavior of modules such as an encryption function using the firmware modified for the developer testing.

- Confirm that the encryption algorithm is implemented as specified by comparing the data that were obtained by the above approach and the known data calculated by a different approach.

<Developer Testing Tools>

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

Table 7-2 Developer Testing Tools

Tool Name	Outline and Purpose of Use
Protocol Analyzer (Wireshark Version 1.10.6)	Monitor the communication data on the internal network, and confirm that the encryption communication protocol is IPsec or TLS as specified.
Mailer (Microsoft Windows Live Mail 2011)	Transmit E-mails with the TOE via Mail server, and confirm that the encryption and signature by S/MIME are as specified.
HTTP debugger (Fiddler 2.4.7.1)	A tool to mediate the communication between a Web browser (client PC) and a Web server (MFD) and to refer to and change the data communicated between them.
Debug Serial and Interface Converter * See Table 7-1 for configuration.	Read out the data written on the internal SD memory and check the contents.
Nmap Ver.7.31	A tool to detect available network service ports.

<Content of the Performed Developer Testing>

Basic MFD functions and security management functions are operated from every interface, and it was confirmed that the security functions to be applied to various input parameters are operated as specified. Regarding the user authentication function, it was confirmed that each case of local authentication, remote authentication (LDAP server), and remote authentication (Kerberos server), behaves as specified according to the user role.

The variations of the input parameters include the rewrite of communication data between web browsers and the TOE.

b. Scope of the Performed Developer Testing

The developer testing was performed on 67 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.

c. Result

The evaluator confirmed an 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 sampling 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 ensure that security functions are certainly implemented from 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 independent testing performed by the evaluator is the same as that of the developer testing shown in Figure 7-1, except for the following.

- As the TOE, only Xerox VersaLink C7020 and Xerox VersaLink C7030 were used.
- As a fax destination, Xerox VersaLink C505, which is an MFD, was used instead of general user client 2.

The evaluator judged that testing on 2 representative models is sufficient, since other models differ only in print speeds according to the model number.

The evaluator determined that changing the fax destination does not affect the security functions of the TOE.

The independent testing was performed in the same environment as the TOE configuration identified in the ST.

The testing tools and components in the independent testing environment were the same as those used in the developer testing and some of them include tools and components developed by the developer. The validity verification and operation tests for the testing tools and components were performed by the evaluator.

2) Summary of the Independent Testing

A summary of the Independent testing is 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 evidential materials are shown below.

<Viewpoints of the Independent Testing>

(1) For interfaces to which strict testing was not performed on the behavior of security functions in the developer testing, confirm the behavior of them with different parameters.

(2) As the sampling testing, select the test items of the developer testing from the following viewpoints:
- Check all the security functions and the external interfaces.
- Check the access control for the combinations of all user types and Faxbox as well as those of all user types and Store Print.
- Check all the authentication methods (local authentication, remote authentication by Kerberos server, remote authentication by LDAP server).

b. Independent Testing Outline

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

<Independent Testing Approach>
The independent testing was performed by the evaluator using the same testing approach as the developer testing.

<Independent Testing Tools>
The same testing tools as those of the developer testing were used.

<Content of the Performed Independent Testing>
The evaluator performed the sampling testing of 50 items and the additional testing of 4 items, based on the viewpoints of the independent testing.

Table 7-3 shows viewpoints of the independent testing and the content of the major testing corresponding to them.

Table 7-3 Major Independent Testing Performed

Viewpoint	Outline of the Independent Testing
Viewpoint (1)	Confirm that the user roles and account lock are as specified when the Remote Authentication is used.
Viewpoint (1)	Confirm that the behavior of the TOE is as specified when users who own document data are unregistered while their document data exist in the TOE.
Viewpoint (1)	Confirm that the TOE does not accept print jobs if an option other than the Store Print is specified for the print jobs from the printer driver.

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 concern that known vulnerabilities may exist in the network interfaces.

(2) There is a concern that known vulnerabilities may exist in the print processing.

(3) There is a concern that the TOE behaves unexpectedly for the unexpected entry on the control panel.

(4) There is a concern of unauthorized access by USB port.

(5) There is a concern that security functions do not behave properly, being affected by unauthorized access during initialization processing.

b. Penetration Testing Outline

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

<Penetration Testing Environment>
Penetration Testing was performed in the same environment as that of the evaluator independent testing, except for the additional PC with tools for penetration testing. Table 7-4 shows details of tools used in the penetration testing.

Table 7-4 Penetration Testing Tools

Tool Name	Outline and Purpose of Use
Nmap Version 7.60	A tool to detect available network service ports.
netcat Version 1.11	A tool to transfer data to network ports.
Fiddler Version 4.4.9.0	A tool to mediate the communication between Web browser and Web server (TOE), which refers to and changes the communication data between them.
OWASP ZAP Version 2.6.0	A tool to inspect vulnerabilities of the Web application.
SSLScan Version 1.8.2	A tool to check whether SSL/TLS cipher suites are supported or not.
Metasploit Version 4.6.2 and 4.13.0	The tool is used for the creation of the testing data to inspect the vulnerabilities caused by PDF files.
PRET Version 0.36	A tool to inspect various vulnerabilities in a printing processing.

<Content of the Performed Penetration Testing>
Table 7-5 shows vulnerabilities of concern and the content of the penetration testing corresponding to them.

Table 7-5 Outline of the Penetration Testing

Vulnerability	Penetration Testing Outline
(1)	- Executed Nmap for the TOE and confirmed that the open port cannot be misused. - Conducted various entries to Web server (TOE) using OWASP ZAP, Web browser and Fiddler, and confirmed that there is no known vulnerability. - Executed SSLScan for the TOE, and confirmed that weak encryption methods are not supported.
(2)	- Confirmed that the unauthorized processing is not executed even if print job commands and print files including unauthorized processing are input to the TOE.
(3)	- Confirmed that the character of out-of-spec length, character code, and special key cannot be entered from the control panel.
(4)	- Confirmed that, other than the intended functions such as print, it cannot be used even when attempting to access the TOE by connecting the client for the penetration testing to each USB port of the TOE.
(5)	- Confirmed that operation is rejected during initialization processing of the MFD after the power-on.

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

TOE configuration conditions for this evaluation are as described in the guidance documents shown in Chapter 6. To enable security functions of the TOE and securely use them, system administrators of the TOE need to configure the TOE settings to satisfy the configuration conditions as described in the guidance. If these setting values are changed to the values different from those specified in the guidance, the configuration will not be assured by this evaluation.

TOE configuration conditions include settings that disable some functions which the TOE provides. For example, setting values for the TOE as described below are included.

- Customer Engineer Operation Restriction: [Enabled]
- Direct Fax (Fax driver): [Disabled]
- SNMP: [Disabled]
- Print from USB, Store to USB: [Disabled]

System administrators of the TOE need to be noted that TOE configuration conditions include the settings to disable some functions that the TOE provides. If these setting values are changed to the values different from those specified in the guidance, the configuration will not be assured by this evaluation.

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.

- Security functional requirements: Common Criteria Part 2 Conformant
- 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 EAL2 package
- Additional assurance component ALC_FLR.2

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

7.7 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

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

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

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

3. 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 the submitted Evaluation Technical Report and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL2 augmented by ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

Procurement personnel who are interested in this TOE need to consider whether the scope of this evaluation and the operational requirements of this TOE satisfy the operational conditions that they assume, by referring to the descriptions in "1.1.3 Disclaimers," "4.3 Clarification of Scope," and "7.5 Evaluated Configuration."

Especially, when maintenance function is enabled for use, any effects on security functions of this TOE are out of the scope of this evaluation. Therefore, it is a responsibility of the administrator to decide whether to accept maintenance.

9. Annexes

There is no annex.

10. Security Target

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

Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer Diskless models Security Target, Version 1.1.1, March 20, 2018, Fuji Xerox Co., Ltd.

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.

ADF	Auto Document Feeder
IIT	Image Input Terminal
IOT	Image Output Terminal
MFD	Multi-Function Device
NVRAM	Non Volatile Random Access Memory
SA	System Administrator privilege
SD	Secure Digital
SEEPROM	Serial Electronically Erasable and Programmable Read Only Memory

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

Copy Function:	Copy Function is to read the original data from IIT and print it out from IOT according to the general user's instruction from the control panel.
Customer Engineer (CE):	Customer service engineer who maintains and repairs the MFD.
Embedded Web Server Function:	Embedded Web Server is a service used by general users and system administrators via the Web browser in order for them to confirm the status of the TOE, change settings of the TOE, and job deletion of the TOE.
Faxbox:	An area to store the document data received by the fax function.
Fax Function:	Fax function is to send and receive fax data. Fax sending function is a function to read the original data from IIT and send them to the destination via public telephone line, according to the general user's instruction from the control panel. Fax receiving function is a function to receive the document data via a public telephone. The received data are stored in the Faxbox, and printed out according to the system administrator's instruction from the control panel.

Key Operator:	Key operator is a system administrator who can use all the management functions.
Network Scan Function:	Network Scan function is to read the original data from IIT according to the general user's instruction from the control panel, and automatically send to FTP server or Mail server according to the setting of the MFD.
Print Function:	Print function is to print out the data from IOT, which are sent to the MFD from printer driver of a general user client. The received print data are stored into the Store Print inside the MFD, and printed out according to the general user's instruction from the control panel.
SA:	SA is a system administrator who can use a part of management functions. The role of SA is set by key operator as required by the corresponding organization.
Store Print:	An area in the MFD to store print data sent from a general user client to the MFD.
System Administrator:	An authorized administrator who configures TOE security functions and other device settings. This term covers both key operator and SA (System Administrator privilege).

12. Bibliography

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

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

[3] Requirements for Approval of IT Security Evaluation Facility, October 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] Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer Diskless models Security Target, Version 1.1.1, March 20, 2018, Fuji Xerox Co., Ltd.

[13] Xerox VersaLink C7020/C7025/C7030 Color Multifunction Printer Diskless models Evaluation Technical Report, Version 1.6, May 10, 2018, Information Technology Security Center, Evaluation Department