Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2014-06-16 (ITC-4511)
Certification No.	C0482
Sponsor	Fuji Xerox Co., Ltd.
TOE Name	Japanese: Fuji Xerox ApeosPort-V 4020 Series Controller Software English: Fuji Xerox ApeosPort-V 4020 Series Controller Software
TOE Version	Controller ROM Ver. 1.2.0
PP Conformance	None
Assurance Package	EAL3 augmented with ALC_FLR.2
Developer	Fuji Xerox Co., Ltd.
Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE is certified as follows.

2015-09-17

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."

- 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
"Japanese: Fuji Xerox ApeosPort-V 4020 Series Controller Software, English: Fuji Xerox ApeosPort-V 4020 Series Controller 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

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "Japanese: Fuji Xerox ApeosPort-V 4020 Series Controller Software, English: Fuji Xerox ApeosPort-V 4020 Series Controller Software, Version Controller ROM Ver. 1.2.0" (hereinafter referred to as the "TOE") developed by Fuji Xerox Co., Ltd., and the evaluation of the TOE was finished on 2015-09-11 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Fuji Xerox Co., Ltd., 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") that is the appendix of this report together. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes procurement personnel who purchase Multi Function Device with this TOE installed to be a reader. Note that the Certification Report presents the certification result, based on assurance requirements to which the TOE conforms, and does not guarantee 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 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

This TOE is the controller software residing within the Multi Function Device (hereinafter referred to as "MFD"), which controls the entire MFD that has copy, print, scan, and fax functions.

In addition to the basic MFD functions such as copy, print, scan, and fax, this TOE provides security functions to protect the document data used in basic functions and the setting data affecting security, etc., from data 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 this TOE assumes are described in the next clause.

1.1.2.1 Threats and Security Objectives

This 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, direct data read-out from the internal HDD in the MFD, or 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 of the internal HDD data and the communication data, 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 MFD in which this TOE is installed is assumed to be located in an environment where physical components and interfaces of the MFD 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 operation and functions will not be assured by this evaluation.

In this evaluation, only the configuration, to which the setting condition such as restriction for customer engineer operation is applied, is evaluated as the TOE. If the TOE settings shown in "7.5 Evaluated Configuration" are changed, the configuration will not be assured by this evaluation.

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 2015-09, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[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 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:	Japanese: Fuji Xerox ApeosPort-V 4020 Series Controller Software English: Fuji Xerox ApeosPort-V 4020 Series Controller Software
Version:	Controller ROM Ver. 1.2.0
Developer:	Fuji Xerox Co., Ltd.

This TOE is the controller software of the following Fuji Xerox MFDs. In the case of MFDs for Japan, however, the optional Data Security Kit needs to be installed.

For Japan:
- ApeosPort-V 4020 Series

For overseas:
- ApeosPort-V 4020 Series

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

Users operate on the control panel according to the procedure written in the guidance document, and confirm that the installed product is the evaluated TOE by comparing the name and version information written in the guidance document with the name and version information displayed on the screen or that written in the print output of the configuration setting list.

3. Security Policy

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

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

When using those MFD functions, the TOE can prevent the user's document data that are assets to be protected and the setting data affecting security from being disclosed or altered by an unauthorized person, by applying the following security functions: identification/ authentication and access control of users, encryption of the data stored in HDD, and encryption communication protocol. Furthermore, the TOE has the function to record logs related to security functions.

The TOE provides access control function according to each role assuming the following roles:

- General User
  A general user is any person who uses copy, print, scan, and fax functions provided by the TOE.

- System Administrator (Key Operator + System Administrator Privilege [SA])
  A system administrator is an authorized administrator who configures TOE security function settings and other device settings; this term covers both key operator and SA (System Administrator Privilege).

- Customer Engineer
  A customer engineer is a customer service engineer who maintains and repairs MFD.

According to the organizational security policy, the TOE also provides a security mechanism to protect against unauthorized access to the internal network from the public telephone line used for fax, and the data overwrite function upon deleting the data stored in HDD, and the self-test function.

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 as countermeasures against them.

Table 3-1 Assumed Threats

Identifier	Threats
T.CONSUME	A user may access the TOE and use TOE functions without authorization.
T.DATA_SEC	A user who is authorized to use TOE functions may read document data and security audit log data exceeding the permitted authority range.
T.CONFDATA	A general user who is authorized to use TOE functions may read or alter the TOE setting data without authorization while only a system administrator is allowed to access the TOE setting data.
T.RECOVER	An attacker may remove the internal HDD to read out and leak the document data, used document data, and security audit log data from the HDD without authorization.
T.COMM_TAP	An attacker may wiretap 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.

1) Countermeasures against threats "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 allows only the authorized user who succeeds in identification/authentication to use the TOE functions. In addition, the authorized user can conduct only the permitted operations when handling Mailbox and document data.

The System Administrator's Security Management function allows only the authorized system administrator to refer to and change the setting data of security functions, and to change the Enable/Disable setting of security functions.

The Customer Engineer Operation Restriction function allows only the authorized system administrator to refer to and change the setting data that control Enable/Disable status of operation restriction for customer engineers.

The Security Audit Log function allows only the authorized system administrator to acquire and read the audit log, such as user log-in/out, job end, and setting changes. This function contributes to detection of unauthorized operations such as impersonation of

user. When the area to store the audit log becomes full, the oldest stored audit log is overwritten and a new audit log is stored.

With the above functions, only the operations permitted per valid TOE user can be conducted, thus unauthorized TOE use and access to protected assets can be prevented.

2) Countermeasures against threat "T.RECOVER"

The TOE counters the threat by the Hard Disk Data Encryption function.

The Hard Disk Data Encryption function is to encrypt the document data upon storing the data into the internal HDD when any of basic MFD functions such as copy, print, scan, network scan, and fax is used. It also encrypts the audit log data upon storing the audit log data, created by the Security Audit Log function, into the internal HDD.

The cryptographic algorithm is 256-bit AES. A cryptographic key is generated upon booting the TOE using the proprietary method of Fuji Xerox Co., Ltd., based on the 12 alphanumeric cryptographic seed key. The cryptographic seed key is set by system administrators when the TOE was installed. The generated cryptographic key is deleted when the power is turned off.

With this function, the document data stored in the internal HDD are encrypted and prevented from unauthorized data read-out.

3) Countermeasures against threat "T.COMM_TAP"

The TOE counters the threat by the Internal Network Data Protection function.

The Internal Network Data Protection function is to use the encryption communication protocol when the TOE communicates with client terminals (hereinafter referred to as "client") and various servers. The supported encryption protocols are TLS (TLS 1.0, TLS 1.1, TLS 1.2), IPSec, and S/MIME.

With this function, the encryption communication protocol is used for transmitting the document data in the internal network, security audit log data, and TOE setting data to prevent wiretapping and alternation of the 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.FAX_OPT	The TOE shall ensure that the internal network cannot be accessed via public telephone line.
P.VERIFY	The TOE shall execute self-test to verify the integrity of TSF executable code and TSF data.

P.OVERWRITE	The TOE shall execute HDD overwrite to delete the used document data stored in the internal HDD.

3.1.2.2 Security Function Policies to Organizational Security Policies

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

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

The Fax Flow Security function of the TOE is structured so that the TOE only receives fax data from the designated fax card and does not pass the data except for the fax function; thus, it has a mechanism that the data received from public telephone line will not be transferred to the internal network in any circumstances. This is to meet a requirement in the organizational security policy, which requires inhibiting unauthorized access to the internal network from the public telephone line.

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

The Self-test function of the TOE is to verify check sum of Controller 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 data.

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

The Hard Disk Data Overwrite function of the TOE is to overwrite and delete the internal HDD area where the document data are stored when the data are deleted after the job of basic MFD functions is completed. Thus, this function overwrites and deletes the used document data stored in the internal HDD.

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

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	A system administrator shall have the necessary knowledge of the 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 document.
A.SECMODE	In operating the TOE, a system administrator shall configure and set the TOE properly, according to the security policies of the organization and the product guidance document, to manage the TOE and its external environment.
A.ACCESS	The MFD in which the TOE resides shall be located in a monitored or restricted environment that provides protection from unauthorized access to the physical components and data interfaces of the MFD.

4.2 Environmental Assumptions

The MFD with this TOE installed is assumed to be used at general office, connected to the internal network protected from threats on the external network by firewall etc., and to public telephone line via fax card. Figure 4-1 shows the general operating environment for the TOE.

Internal network is connected to general user client, system administrator client, and server computer on which Mail server, FTP server, SMB server, LDAP server, and Kerberos server are installed, and the devices communicate document data etc., with the TOE.

The TOE users use the TOE by operating MFD control panel, general user client, or system administrator client that is connected to the internal network. General user client can operate the TOE via USB.

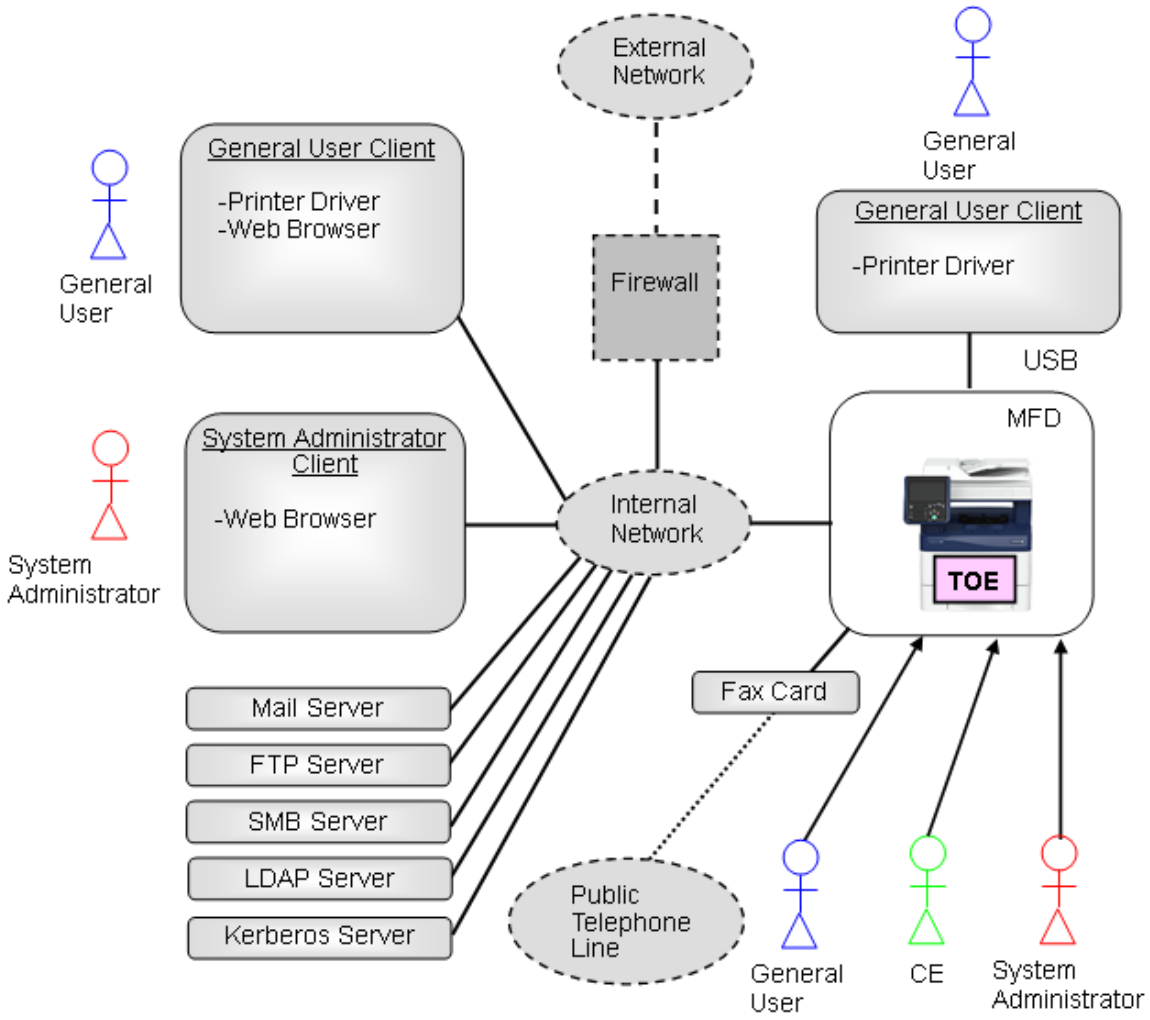

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following:

1) MFD

Multi Function Device in which the TOE is to be installed. This TOE can be installed in the following Fuji Xerox MFD series.

For Japan:
- ApeosPort-V 4020 series

For overseas:
- ApeosPort-V 4020 series

2) Fax Card

Some MFD models do not have the Fax Card as the standard. To use the fax function, a user needs to purchase the designated optional Fax Card if an MFD model does not have the Fax Card.

3) General User Client

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

- OS: Windows Vista or Windows 7
- 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)

4) 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 Vista or Windows 7
- Web browser (included with OS)

5) LDAP Server, Kerberos Server

When Remote Authentication is set for the user authentication function, 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

6) Mail Server, FTP Server, SMB Server

Since the TOE has basic functions to transfer document data with Mail server, FTP server, and SMB server, these servers are installed if necessary upon using basic MFD functions.

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 the 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) Print function

The print function of the TOE is of two types: "Store Print" in which the print data received from the general user client are temporarily stored in the internal HDD and then printed out according to the general user's instruction from the control panel, and "Normal Print" in which the data are printed out immediately when the MFD receives the data. In this evaluation, only the "Store Print" is subject to the evaluation, and the "Normal Print" is not. When the TOE to be evaluated is configured in accordance with the TOE configuration condition, "Store Print" is automatically performed even if "Normal Print" is executed from the general user client.

5. Architectural Information

This chapter explains the scope and the main components of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the MFD configuration with the TOE and the IT environment other than the MFD. In Figure 5-1, the MFD corresponds to controller board, control panel, internal HDD, ADF, IIT, and IOT. The TOE corresponds to a software part that realizes various functions and is stored in Controller ROM of the controller board. The MFD's hardware and fax card etc., are not within the boundary of the TOE.

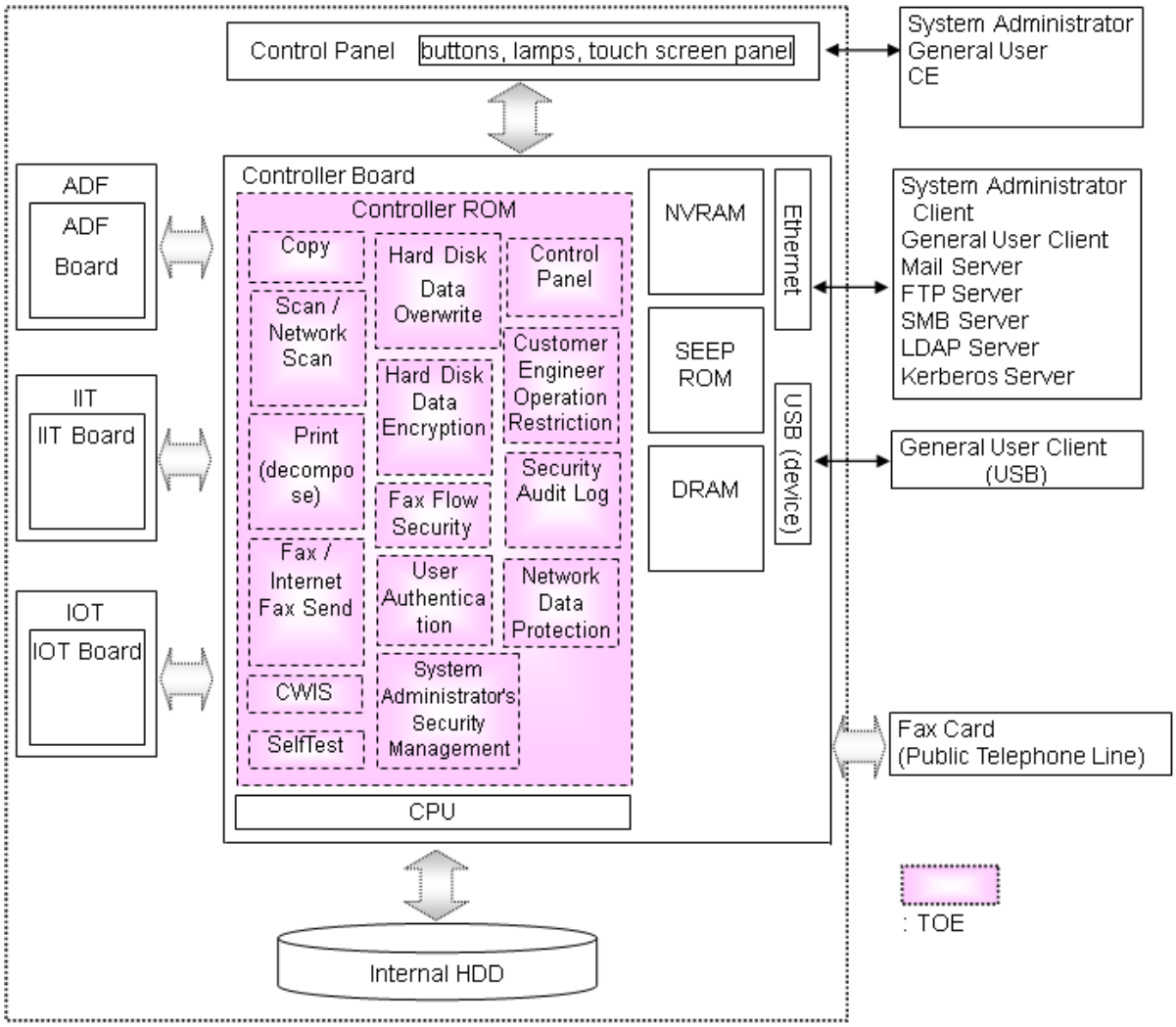

Figure 5-1 TOE boundary

The TOE functions consist of the security functions described in Chapter 3 and other basic MFD functions. Regarding the basic MFD functions, refer to Glossary in Chapter 11.

The security functions of the TOE are used when a user uses basic MFD functions. The following describes the relation between security functions and basic MFD functions.

1) When a user uses basic MFD functions, the System Administrator's Security Management function, and functions that refer to the audit log in the Security Audit Log function, the User Authentication function is applied and allows the authorized user to perform operations according to his/her role. A menu is displayed for the identified and authenticated user according to the user's role, and the user is allowed to use basic MFD functions, the System Administrator's Security Management function, and the Security Audit Log function. The operation by a user is executed after the user authority is checked to determine whether the operation is permitted for the user or not. In addition, when these functions are used, audit log is created by the Security Audit Log function.

2) In the above case 1), the Hard Disk Data Encryption function encrypts the document data and audit log to be stored in the internal HDD, and the Hard Disk Data Overwrite function is used upon deleting the document data. These processing are applied not only to the document data stored or deleted intentionally by users, but also to the document data stored temporarily and unintentionally in the internal HDD during the processing of copy function, etc.

3) When the MFD with the TOE installed and other IT devices communicate via the internal network in the above case 1), the Internal Network Data Protection function is used. Furthermore, the Fax Flow Security function is applied for fax.

5.2 IT Environment

When user authentication by Remote Authentication is enabled, the TOE obtains the result of identification and authentication of a user from the Remote Authentication server (LDAP server or Kerberos server). However, a key operator is not identified and authenticated by using the Remote Authentication server, but identified and authenticated by using the key operator information registered to the TOE. Furthermore, when Remote Authentication is selected in the TOE settings, even with LDAP server or Kerberos server, the TOE uses the user attribute acquired from LDAP server to determine if the user has SA role.

For various servers and clients that are connected to the MFD via the internal network, the TOE communicates using various encryption communication protocols. First of all, the TOE uses IPSec for these servers and clients. Furthermore, TLS is used for web browser of clients, and S/MIME is used for mails transmitted with Mail server. When the TOE communicates with the authentication server, LDAP (TLS) protocol and Kerberos protocol are used to encrypt the data related to identification and authentication.

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.

1) For Japan

- ApeosPort-V 4020 Administrator Guide (ME7080J1-1)
  (SHA1 hash value: cec1802aa23f987e630645b2bef127367a6820e6)

- ApeosPort-V 4020 User Guide (ME7079J1-1)
  (SHA1 hash value: 17d5753592f65779de2f544f6b96f62cb7b26268)

- ApeosPort-V 4020 Security Function Supplementary Guide (ME7082J1-2)
  (SHA1 hash value: 8e8af4eb6e41a31dbf5acadcf7747af255d8820c)

2) For overseas

- ApeosPort-V 4020 Administrator Guide (ME7089E2-1)
  (SHA1 hash value: 7a1739bbfc1f84e497046ca91359a2f03df86493)

- ApeosPort-V 4020 User Guide (ME7088E2-1)
  (SHA1 hash value: 7bcadac2df7e9b5ec788b9717c536765977228db)

- ApeosPort-V 4020 Security Function Supplementary Guide (ME7090E2-2)
  (SHA1 hash value: e8ccd4612db6cc1e26463fc50b674f2778fb8129)

* Note: SHA1 hash value
  The guidance documents are stored on the CD that is included with the MFD product. TOE Users can confirm the integrity of the guidance documents by comparing their calculated SHA1 hash values.

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 2014-06 and concluded upon completion of the Evaluation Technical Report dated 2015-09. 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 and manufacturing sites on 2014-10 and 2014-12, and examined procedural status conducted in relation to each work unit for configuration management, delivery and development security, 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 2015-05.

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.

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.

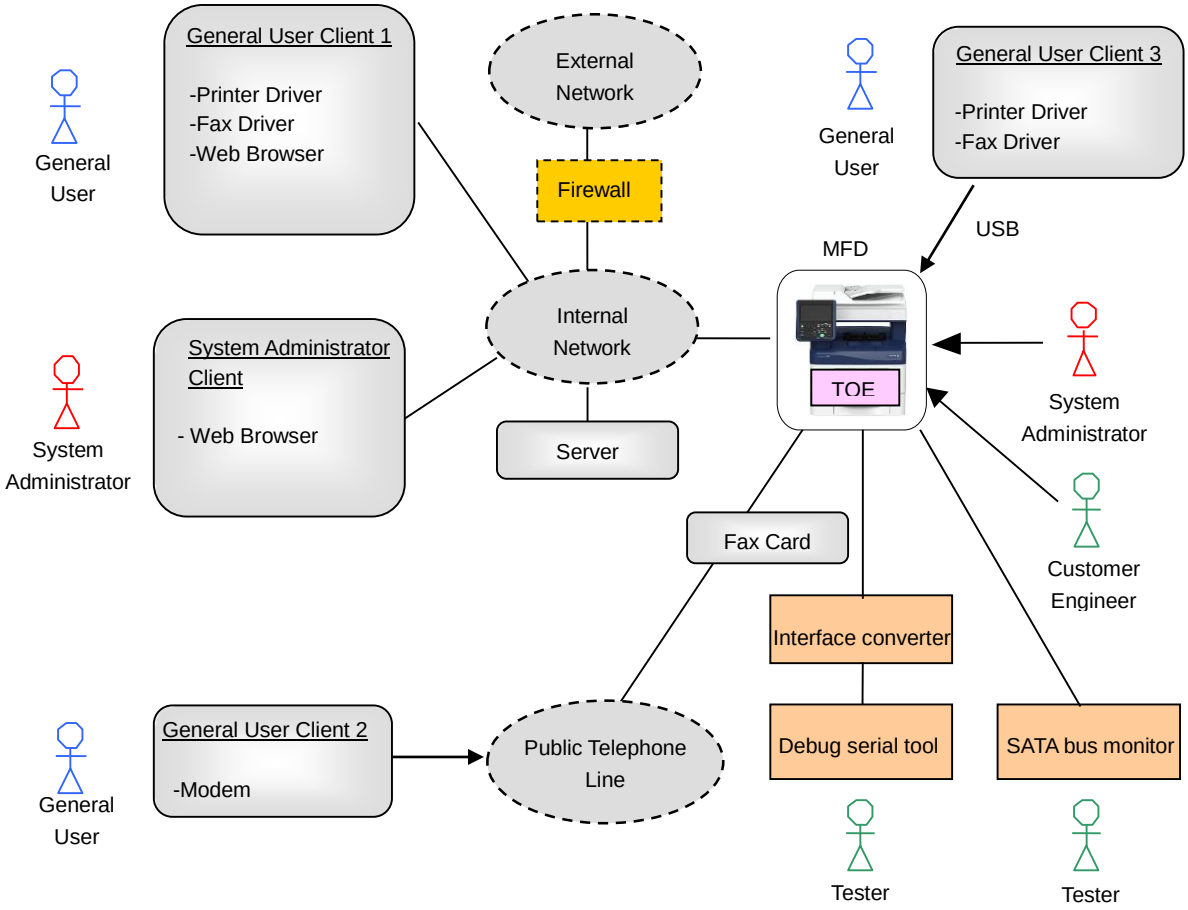

Figure 7-1 Configuration of the Developer Testing

The TOE tested by the developer is the same TOE as in TOE Identification of Chapter 2.

The MFDs used in the testing are all the MFD models described in TOE identification of Chapter 2.

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

Table 7-1 Configuration Items for the Developer Testing

Items	Description
MFD	For Japan: ApeosPort-V 4020 For overseas: ApeosPort-V 4020
Server	Used as various servers. - PC with Microsoft Windows Server 2008 R2 SP1 - Mail Server: Xmail Version 1.27 - FTP/SMB/LDAP servers: 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 8) b) PC with Microsoft Windows VISTA Business SP2 (Web browser: Microsoft Internet Explorer 7)
General User Client 1	Used as general user client (connected via internal network) and used as the destination of Internet Fax. The testing is performed with the following two models: a) PC with Microsoft Windows 7 Professional SP1 (Web browser: Microsoft Internet Explorer 8) b) PC with Microsoft Windows VISTA Business SP2 (Web browser: Microsoft Internet Explorer 7) Additionally, the following software is used for a) and b). For Japan: - Printer driver: ART EX Print Driver Version 6.9.0 - Fax driver: ART EX Direct Fax Driver Version 2.8.0 For overseas: - Printer driver and fax driver: PCL6 Print Driver Version 6.9.0 Fax drivers are used for confirming that they cannot be used.
General User Client 2	Used to send/receive fax. - PC with Microsoft Windows VISTA Business SP2 * 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 VISTA Business SP2 For Japan: - Printer driver: ART EX Print Driver Version 6.9.0 - Fax driver: ART EX Direct Fax Driver Version 2.8.0 For overseas: - Printer driver and fax driver: PCL6 Print Driver Version 6.9.0 Fax drivers are used for confirming that they cannot be used.

Items	Description
SATA Bus Monitor	A tool to monitor the SATA bus data transferred to and from the internal HDD. - PC with Windows 7 SP1 to which the dedicated device, ST2-31-2-A by Catalyst Enterprises, is connected - Dedicated software: stx_sata_protocolsuite V4.20
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 Windows 7 Professional SP1 - 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.
Fax Card	An option of MFD by Fuji Xerox - Fax ROM Ver. 102.4.0

The evaluator evaluated that external network and firewall do not affect the testing.

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) Operate basic MFD functions and security management functions from the MFD control panel, system administrator client, and general user client, and confirm the MFD behavior, panel display, and audit log contents as a result.

(2) To confirm the Hard Disk Data Overwrite function, use the SATA bus monitor as a testing tool and read out and check the data to be written to the internal HDD and the contents of the internal HDD after the data are written.

(3) To confirm the Hard Disk Data Encryption function, use the serial port for debugging to directly refer to the document data etc., stored in the internal HDD and check that document data etc., are encrypted. In addition, confirm that the encrypted internal HDD cannot be used and an error is displayed on the control panel when the internal HDD is replaced with that of another MFD with different cryptographic key.

(4) To confirm the Hard Disk Data Encryption function, compare the generated cryptographic key and encrypted data by the TOE with the known data calculated by the specified algorithm, and confirm that the algorithm to generate a cryptographic key and the cryptographic algorithm are as specified.

(5) To confirm the encryption communication protocol function such as IPSec, use the testing tool to be described later and check that the encryption communication protocol is used as specified. Also confirm the protection function against various Web inputs and print job commands.

(6) Connect the general user client 2 via public telephone line and use it for transmitting fax with MFD. Besides, to confirm the Information Flow Security function, check that dial-up connection from general user client 2 to the TOE via public telephone line is disabled.

<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
SATA Bus Monitor (PC and dedicated device) * See Table 7-1 for configuration.	Monitor the data in SATA bus for connecting the internal HDD in the MFD, and check the data to be written to the internal HDD, and also read out the data written in the internal HDD.
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 refer and change the communication data between a Web browser (client) and a Web server (MFD).
Debug Serial and Interface Converter * See Table 7-1 for configuration.	Read out the data written on the internal HDD and check the contents.

<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.

In addition, it was confirmed that the following operate as specified: the behavior upon error occurrence such as the processing halt of the data overwrite by MFD power-off and its restart by MFD power-on.

b. Scope of the Performed Developer Testing

The developer testing was performed on 77 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 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 fax destination, Fuji Xerox ApeosPort-V C3320 MFD was used.

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, including the developer's proprietary debug environment (debug serial and interface converter), in the independent testing are the same as those used in the developer testing, and 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 documents are shown below.

<Viewpoints of the Independent Testing>

(1) For interfaces to which strict testing is 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 testing 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 Mailbox as well as those of all user types and Private Print.
- Check all the authentication methods (local authentication, remote authentication by Kerberos server, and remote authentication by LDAP server).

b. Independent Testing Outline

The evaluator devised the sampling testing and the additional testing to the developer testing from the above viewpoints of the independent testing. An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

The evaluator used the same method as the developer testing and performed the same testing and the testing with changed parameters.

<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 57 items and the additional testing of 7 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 behavior of the TOE is as specified when the entry for changing or entering passwords exceeds the limit values.
Viewpoint (1)	Confirm that access control to Mailbox for system administrators is as specified.
Viewpoint (1)	Test whether or not the account lock is performed as specified, and also test whether the account lock is performed as specified even when different user accounts exist.

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.

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 corresponding to this TOE regarding the publicly available vulnerability information, such as the possibility of unauthorized use of network service and various vulnerability of Web.

(2) There is a concern corresponding to this TOE regarding the unexpected execution of processing by PDF files and unauthorized access by print job commands, according to the publicly available vulnerability information.

(3) There is a concern that the TOE behaves unexpectedly for the entry exceeding the limit value or the entry of unexpected character code on the interface other than Web, such as control panel.

(4) There is a concern of unauthorized access by USB port according to the analysis of vulnerability on the documentation.

(5) There is a concern that the security function is invalidated when NVRAM and SEEPROM, to which the setting data are stored, are initialized, according to the analysis of vulnerability on the documentation.

(6) There is a concern that the documents as protected assets become inconsistent when multiple users access the documents in Mailbox, according to the analysis of vulnerability on the documentation.

(7) There is a concern that security functions do not behave properly, affected by unauthorized access during initialization processing or by run-down of battery for MFD's system clock.

As to a cryptographic key, based on the analysis of the mechanism to generate a cryptographic key from the cryptographic seed key set by system administrator, the evaluator evaluated that an attacker with the assumed level of attack capability cannot obtain or predict a cryptographic key.

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 personal computer with tools for the penetration testing. Table 7-4 shows details of tools used in the penetration testing.

Table 7-4 Penetration Testing Tools

Tool Name		Purpose of use
PC for Penetration Testing		Client with Windows 7 or Windows VISTA, which operates the following penetration testing tools.
	Nmap Ver.6.40	A tool to detect available network service ports.
	Fiddler V4.4.9.0	A tool to refer to and change the communication data between web browser (Client) and web server (TOE). The tool enables to send any data to web server without any restriction of web browser by using Fiddler.
	ContentsBridge Version 7.3.0	Printer software for PC by Fuji Xerox.
	Metasploit Ver.4.6.2	The tool is used for the creation of the testing data to inspect the vulnerabilities caused by PDF files.

<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 web browser and Fiddler, and confirmed that there is no known vulnerability such as bypass of identification/authentication, buffer overflow, and various injections.

(2)	- Confirmed that the processing is not executed when a PDF file including unauthorized processing is input. - Confirmed that the assets could not be accessed when directories are searched using a print job command.
(3)	- Confirmed that it becomes an error when the character of out-of-spec length, character code, and special key are entered from control panel, or general user client (printer driver).
(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 PC for the penetration testing to each USB port of the TOE.
(5)	- Confirmed that an error occurs and the TOE cannot be used even after replacing NVRAM and SEEPROM with the new ones to which no setting is applied.
(6)	- Confirmed that the access is rejected during the operation by others when multiple users access document data in Mailbox.
(7)	- Confirmed that operation is rejected during initialization processing of the MFD right after the power-on. - Confirmed that an error is displayed and the MFD cannot be used when the power is turned on while the battery for the system clock of the MFD has run down.

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 described in the guidance "Security Function Supplementary Guide" shown in Chapter 6. To enable security functions of the TOE and use them safely, system administrators 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.

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

- Customer Engineer Operation Restriction: [Enabled]
- WebDAV setting (Network Scan utility): [Disabled]
- Direct Fax (Fax driver): [Disabled]
- Maintenance via public telephone lines or Ethernet: [Disabled]
- Print from USB / Store to USB: [Disabled]
- Receive Mail: [Disabled]
- SNMP: [Disabled]

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 followings 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 EAL3 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. 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.

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 augmented with 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 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 outside the scope of this evaluation. Therefore, it is the 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 within a separate document of this certification report.

Fuji Xerox ApeosPort-V 4020 Series Controller Software Security Target, Version 1.1.6, September 4, 2015, 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
CWIS	CentreWare Internet Service
IIT	Image Input Terminal
IOT	Image Output Terminal
MFD	Multi Function Device
NVRAM	Non Volatile Random Access Memory
SA	System Administrator privilege
SEEPROM	Serial Electronically Erasable and Programmable Read Only Memory

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

Control Panel:	A panel of the MFD on which buttons, lamps, and a touch screen panel are mounted to operate the MFD.
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 of the MFD.
Cryptographic Key:	12 alphanumeric cryptographic key set by a system administrator. When encrypting document data in the internal HDD, it is generated based on the data.
Customer Engineer (CE):	CE is a customer service engineer who maintains and repairs the MFD.
CWIS Function:	CWIS is a service via the Web browser of the user client, to confirm the status of the TOE, change settings of the TOE, retrieve the document data, and request prints.
Document Data:	Document data means a generic term for data, including characters and images, processed by copy, print, scan or fax functions of the MFD.

Fax Driver:	Software for Direct Fax function, which enables a general user to send fax data to the destination directly from a general user client through MFD. The TOE is configured so that this software cannot be used.
Fax Function:	Fax function is to send and receive fax data. According to the general user's instruction from the control panel to send a fax, the original data is read from IIT and sent to the destination via public telephone line. The document data sent from the sender's machine via public telephone line is received and printed out from the recipient's IOT.
General User:	A general user is any person who is allowed to use basic functions of the TOE, such as copy, print, scan, and fax.
Internet Fax Send Function:	Internet Fax Send function is to send fax data via the Internet, not via public telephone line.
Key Operator:	A key operator is a system administrator who can use all the management functions.
Mailbox:	A logical box created in the internal HDD inside the MFD. Mailbox can store the scanned document data or the document data received via fax, categorizing by users and senders.
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, SMB server, and Mail server according to the setting of the MFD.
Network Scan Utility:	Software for a general user client to retrieve the document data stored in Mailbox of the MFD. The TOE is configured so that this software cannot be used.
Normal Print:	In normal print, the data is printed out immediately when the MFD receives the data. See the description of "Print Function."
Printer Driver:	Software to convert the document data on a general user client into print data written in page description language (PDL), a readable format for MFD.
Print Function:	Print function is to print out the data from IOT, which are sent to the MFD according to the instruction from a general user client. The print function is of two types: "Normal Print" and "Store Print," but in this evaluation, only the "Store Print" is subject to the evaluation.

SA:	SA is a system administrator who can use a part of management functions. The role of SA is set by a key operator as required by the corresponding organization.
Scan Function:	Scan function is to read the original data from IIT and then store them into the Mailbox inside the MFD according to the general user's instruction from the control panel of the MFD. The stored document data can be retrieved from the control panel or Web browser.
Security Audit Log Data:	The chronologically recorded data of important events that occurred inside the device, such as device failure, configuration change, and user operation.
Store Print:	In store print, the print data is temporarily stored in the HDD inside the MFD and then printed out according to the general user's instruction from the control panel. See the description of "Print Function."
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).
TOE Setting Data:	The data which may affect the TOE security functions.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, 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] Fuji Xerox ApeosPort-V 4020 Series Controller Software Security Target, Version 1.1.6, September 4, 2015, Fuji Xerox Co., Ltd.

[13] Fuji Xerox ApeosPort-V 4020 Series Controller Software Evaluation Technical Report, Version 2.7, September 11, 2015, Information Technology Security Center, Evaluation Department