Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2011-04-25 (ITC-1348)
Certification No.	C0331
Sponsor	Fuji Xerox Co., Ltd.
Name of the TOE	Xerox WorkCentre 5325/5330/5335
Version of the TOE	Controller ROM Ver. 1.202.3, IOT ROM Ver. 30.19.0, ADF ROM Ver. 7.8.50
PP Conformance	None
Assurance Package	EAL3
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.
2011-12-09

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

Evaluation Result: Pass

"Xerox WorkCentre 5325/5330/5335" has been evaluated based on the standards required, in accordance with the provisions of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

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

Table of Contents

1. Executive Summary 5
1.1 Product Overview 5
1.1.1 Assurance Package 5
1.1.2 TOE and Security Functionality 5
1.1.2.1 Threats and Security Objectives 5
1.1.2.2 Configuration and Assumptions 6
1.1.3 Disclaimers 6
1.2 Conduct of Evaluation 6
1.3 Certification 6
2. Identification 7
3. Security Policy 8
3.1 Security Function Policies 8
3.1.1 Threats and Security Function Policies 8
3.1.1.1 Threats 8
3.1.1.2 Security Function Policies against Threats 9
3.1.2 Organisational Security Policies and Security Function Policies 10
3.1.2.1 Organisational Security Policies 10
3.1.2.2 Security Function Policies to Organisational Security Policies 11
4. Assumptions and Clarification of Scope 12
4.1 Usage Assumptions 12
4.2 Environment Assumptions 12
4.3 Clarification of Scope 15
5. Architectural Information 16
5.1 TOE Boundary and Component 16
5.2 IT Environment 17
6. Documentation 18
7. Evaluation conducted by Evaluation Facility and Results 19
7.1 Evaluation Approach 19
7.2 Overview of Evaluation Activity 19
7.3 IT Product Testing 19
7.3.1 Developer Testing 19
7.3.2 Evaluator Independent Testing 24
7.3.3 Evaluator Penetration Testing 26
7.4 Evaluated Configuration 28
7.5 Evaluation Results 29
7.6 Evaluator Comments/Recommendations 29
8. Certification 30
8.1 Certification Result 30

8.2 Recommendations 30
9. Annexes 31
10. Security Target 31
11. Glossary 32
12. Bibliography 35

1. Executive Summary

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Xerox WorkCentre 5325/5330/5335, Controller ROM Ver. 1.202.3, IOT ROM Ver. 30.19.0, ADF ROM Ver. 7.8.50" (hereinafter referred to as the "TOE") developed by Fuji Xerox Co., Ltd., and the evaluation of the TOE was finished on 2011-11-22 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It reports to the sponsor, Fuji Xerox Co., Ltd., and provides information to users and system operators who are interested in this TOE.

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

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

1.1 Product Overview

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

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

This TOE is Xerox WorkCentre 5325/5330/5335 and is the Multi Function Device (hereinafter referred to as "MFD"), which has such functions as copy, print, scan and fax.

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 which are assets to be protected and the setting data affecting security may be disclosed or altered by an unauthorized person due to unauthorized operation of the TOE, direct data read-out from the internal HDD in the TOE, and access to the communication data on the network where the TOE is installed.

Therefore, the TOE prevents unauthorized operations of the TOE by identifying and authenticating TOE users and permitting the available operations only to the corresponding users. The TOE also prevents direct data read-out from the internal HDD by encrypting the protected assets upon storing them to the internal HDD, and by overwriting the data upon deleting the protected assets. Furthermore, the TOE prevents unauthorized read-out and alteration of the communication data by applying encryption protocol at network communication.

1.1.2.2 Configuration and Assumptions

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

This TOE is assumed to be used at general office, connected to the internal network protected from threats on the external network by firewall, etc.

To operate the TOE, a reliable administrator shall be assigned. In addition, the TOE and other IT devices that communicate data with the TOE shall be properly configured, installed, and then maintained according to the guidance document.

1.1.3 Disclaimers

For this TOE, as described below, there are operational conditions, and there are also cases in which security functions are not provided.

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 "Table 7-6 TOE Configuration Condition" are changed, the configuration will not be assured by this evaluation.

The TOE provides the Direct Fax function; however, the function is limited to Local Authentication and is not subject to evaluation when Remote Authentication is used.

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 2011-11 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme" [1], "IT Security Certification Procedure" [2], and "Evaluation Facility Approval Procedure" [3] provided by the Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report [13] and evaluation evidential materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification oversight reviews are also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body are fully resolved, and the Certification Body confirmed that the TOE evaluation is 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 and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

Name of the TOE:	Xerox WorkCentre 5325/5330/5335	
Version:	Controller ROM	Ver. 1.202.3
	IOT ROM	Ver. 30.19.0
	ADF ROM	Ver. 7.8.50
Developer:	Fuji Xerox Co., Ltd.	

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 version information written in the guidance document with the version information displayed on the screen or that written in the print output of the configuration setting list.

3. Security Policy

This chapter describes under what kind of policies or rules this TOE realizes functions as security service.

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 user, encryption of the data stored in HDD, data overwrite upon deleting the data 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). A key operator can use all management functions, and SA can use a part of management functions. The role of SA is set by key operator as required by the corresponding organisation.

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

The TOE also provides a security mechanism to protect against unauthorized access from the public telephone line used for fax to the internal network, according to the organisational security policy.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1. and to meet the organisational 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 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 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 threat "T.CONSUME" "T.DATA_SEC" "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 following functions: Hard Disk Data Overwrite and Hard Disk Data Encryption.

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, fax, and Direct 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 Hard Disk Data Overwrite function is to completely overwrite and delete the used document data in the document data area of the internal HDD after the job of each basic MFD function is completed.

With the above functions, the document data stored in the HDD are encrypted and prevented from unauthorized data read-out, and the used document data are overwritten and cannot be reproduced or restored.

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 SSL/TLS, IPSec, SNMPv3, 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 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

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

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.FAX_OPT	At the behest of the U.S. Government agency, it must be ensured that the internal network cannot be accessed via public telephone line.

3.1.2.2 Security Function Policies to Organisational Security Policies

The TOE provides the security functions to fulfill the Organisational Security Policies shown in Table 3-2.

1) Means for organisational 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 modem 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 organisational security policy, which requires inhibiting unauthorized access to the internal network from the public telephone line.

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 judge the use of the TOE.

4.1 Usage Assumptions

Assumptions required in use of the TOE are shown in Table 4-1.

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

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	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.SECMODE	In operating the TOE, a system administrator shall configure and set the TOE properly, according to the security policy of organisation and the product guidance document, to manage the TOE and its external environment.

4.2 Environment Assumptions

The MFD, which is this TOE, 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 board. 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.

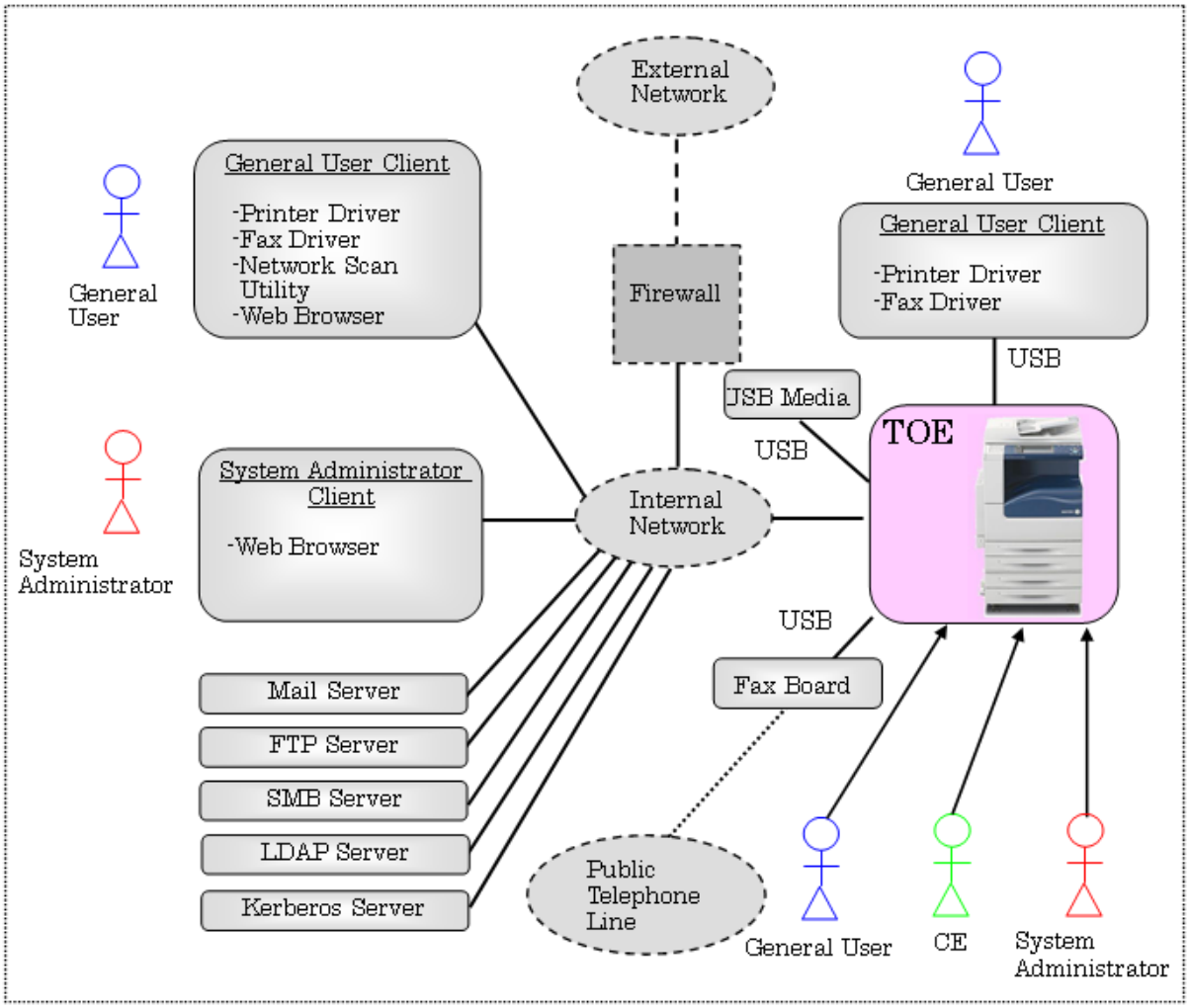

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following:

1) Fax Board

Even when the MFD has a fax function, Fax Board connected to the MFD by USB is sold separately. A user who wants to use fax function needs to purchase the designated Fax Board.

2) General User Client

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

- OS: Windows XP, Windows Vista, or Windows 7
- Printer and fax 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)
- Network Scan Utility

3) System Administrator Client

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

- OS: Windows XP, Windows Vista, or Windows 7
- Web browser (included with OS)

4) 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.

5) Mail Server, FTP Server, SMB Server

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

6) USB Media

The USB Media is a commercial USB flash drive (USB memory). The TOE has basic functions to print document data stored in the USB Media and to store scanned document data into the USB Media. The USB Media is prepared if necessary upon using these basic MFD functions.

Note that the reliability of software and hardware other than the TOE shown in this configuration is not subject to the evaluation.

4.3 Clarification of Scope

As described below, there are restrictions on the security functions of the TOE. When these prohibited functions are used, problems such as disclosure of document data may occur. To counter these problems, the TOE settings and the IT environment need to be configured correctly according to the guidance, and an administrator is responsible for this.

1) 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.

2) In the user authentication function of the TOE, Local Authentication in which identification/authentication is performed using the information registered in the TOE, and Remote Authentication in which identification/authentication is performed using the external authentication server (LDAP or Kerberos protocol) are supported. When Remote Authentication is used at the TOE, the following restrictions are applied. Note that these restrictions are not applied to Local Authentication.

- The Direct Fax function of basic MFD functions is not subject to evaluation when Remote Authentication is used.
- Use of Network Scan Utility of general user client is not subject to evaluation when Remote Authentication is used.
- Identification/Authentication is not performed at the time the TOE receives the print data when Remote Authentication is used. (With "Store Print" function in this evaluation, however, print instruction is necessary after identification/authentication is performed from control panel in order to print data received by the TOE.)

5. Architectural Information

This chapter describes the objective and relevance regarding the scope of the TOE and the main components of the TOE.

5.1 TOE Boundary and Component

Figure 5-1 shows the MFD configuration, which is 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.

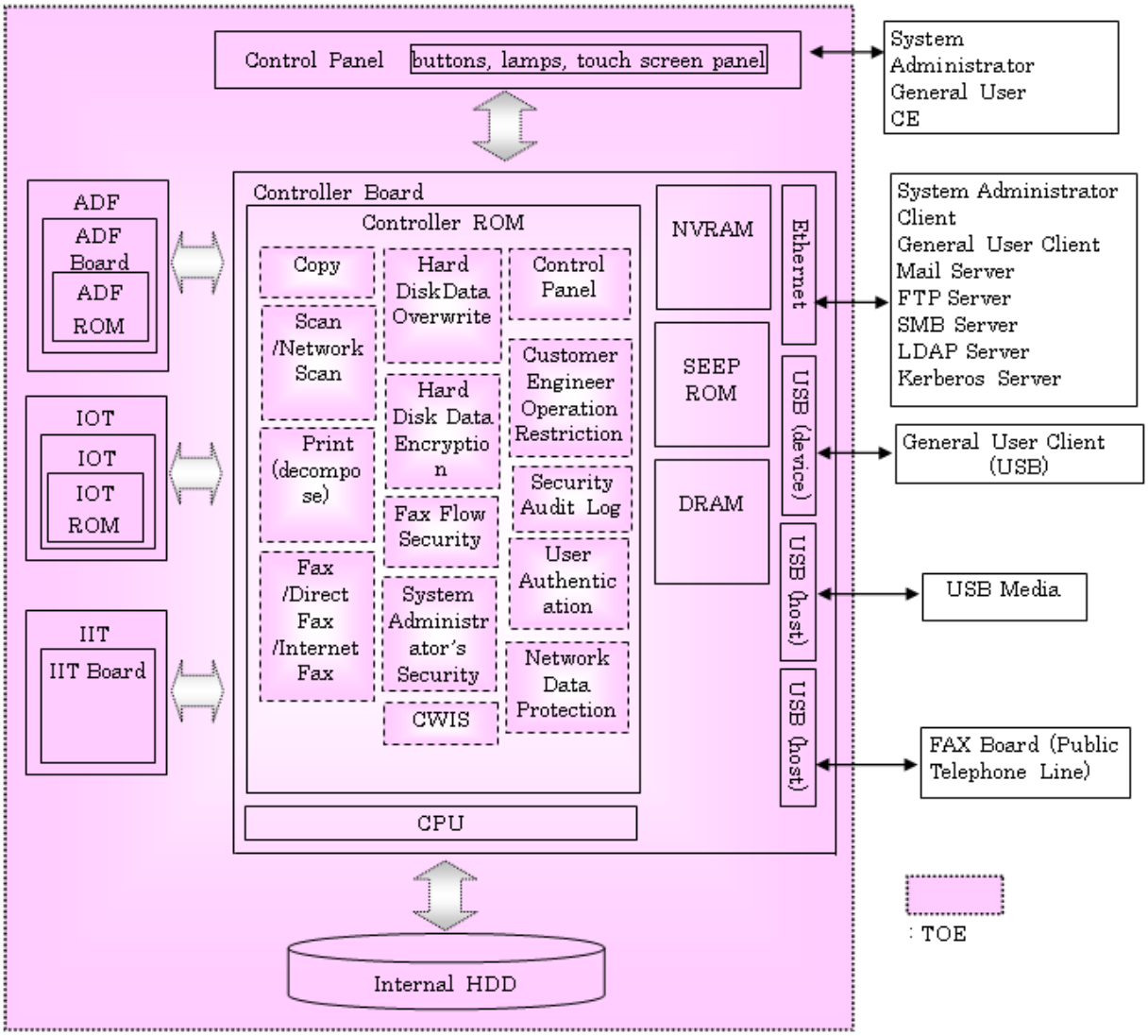

Figure 5-1 TOE boundary

The TOE consists 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 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 user, but also to the document data stored temporarily and unintentionally in 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 either LDAP server or Kerberos server, the TOE uses the user attribute acquired from LDAP server to determine if the user has SA role.

Various servers, system administrator client, and general user client that are connected to the MFD via internal network perform communication using the encryption communication protocol IPSec. Furthermore, SSL/TLS is used for web browser to be installed to client, S/MIME is used for mails transmitted with Mail server, and SNMPv3 is used for network management. The data related to identification and authentication on the internal network between the TOE and the communication destination are encrypted by using LDAP (SSL/TLS) protocol and Kerberos protocol.

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.

- Xerox WorkCentre 5325/5330/5335 System Administrator Guide
  (version 1.0, September 2011)

- Xerox WorkCentre 5325/5330/5335 User Guide
  (version 1.0, September 2011)

- Xerox WorkCentre 5325/5330/5335 Security Function Supplementary Guide
  (version 1.0, September 2011)

Note that these documents are not shipped with the TOE. Users must download them from the Xerox Corporation website: http://www.support.xerox.com/support/.

7. Evaluation conducted by Evaluation Facility and Results

7.1 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 are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.2 Overview of Evaluation Activity

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

Evaluation has started on 2011-04 and concluded by completion of the Evaluation Technical Report dated 2011-11. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2011-09, and examined procedural status conducted in relation to each work unit for configuration management, delivery and development security in life-cycle support by investigating records and interviewing staff. For some development and manufacturing sites, site visits were omitted as the Evaluation Facility determined that the examination details of the past CC-certified products could be reused. Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2011-09 and 2011-10.

Concerns found during the evaluation process were reviewed by the developer, and all the concerns were solved eventually.

7.3 IT Product Testing

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

7.3.1 Developer Testing

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

1) Developer Testing Environment

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

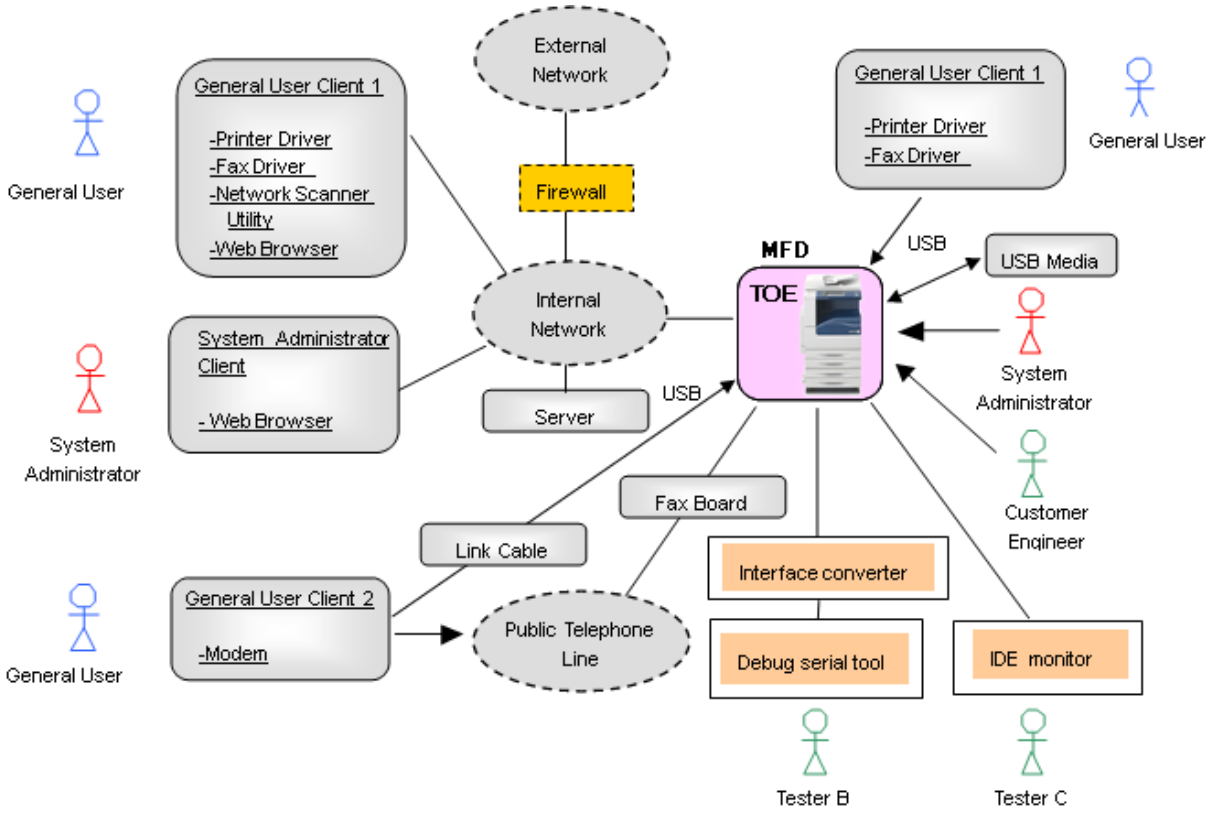

Figure 7-1 Configuration of the Developer Testing

The TOE subject to evaluation is WorkCentre 5325 and is the same TOE as in TOE identification of Chapter 2. The evaluator evaluated the testing by one representative model as sufficient since the other models have the same software and behavior of security functions as those of the TOE and are different only in the process speed of copy and print etc.

Configuration items other than the TOE are shown in Table 7-1 below.

Table 7-1 Configuration Items for Developer Testing

Items		Description
Server		Used as Mail server, LDAP server, and Kerberos server. • Microsoft Windows Server 2008 Service Pack 2 (LDAP server, Kerberos server) • Wireshark Version 1.4.6 • Xmail Version 1.27
System Administrator Client		Used as system administrator client.
	System Administrator Client (1)	• Microsoft Windows 7 Professional • Microsoft Internet Explorer 8 • Wireshark Version 1.4.6
	System Administrator Client (2)	• Microsoft Windows XP Professional Service Pack 3 • Microsoft Internet Explorer 6

	System Administrator Client (3)	• Microsoft Windows VISTA Business Service Pack 2 • Microsoft Internet Explorer 7 • Microsoft Windows Mail
General User Client 1		Used as general user client (connected via the internal network) and SMB server. • SMB server: Standard software in OS
	General User Client 1(1)	• Microsoft Windows 7 Professional • Microsoft Internet Explorer 8 • Network Scan Utility Ver.1.8.3 • Printer and fax driver Version 5.235.0 • Wireshark Version 1.4.6
	General User Client 1(2)	• Microsoft Windows XP Professional Service Pack 3 • Microsoft Internet Explorer 6
	General User Client 1(3)	• Microsoft Windows VISTA Business Service Pack 2 • Microsoft Internet Explorer 7 • Microsoft Windows Mail
General User Client 2		Used to send/receive fax and to confirm that USB port for connecting MFD fax cannot be used for other uses. PC modem port is connected to public telephone line. PC USB port is connected to the USB port for MFD fax board via link cable (USB cable). • Microsoft Windows XP Professional Service Pack 3 • Microsoft Internet Explorer 6 • Network Scan Utility Ver.1.8.3 • Printer and fax driver Version 5.235.0
General User Client 3		Used as general user client (connected via printer USB port). • Microsoft Windows XP Professional Service Pack 3 • Microsoft Internet Explorer 6 • Network Scan Utility Ver.1.8.3 • Printer and fax driver Version 5.235.0
USB Media		• Clip Drive by BUFFALO
IDE Monitor (PC and dedicated device)		A tool to monitor the data transmitted through the connected IDE bus of HDD. To PC with Windows XP, connect the dedicated device (by Catalyst Enterprises) that can directly monitor from IDE bus, and use the dedicated software (Serial ATA Analyzer). • Microsoft Windows XP • Serial ATA Analyzer Version 1.984.0401
Debug Serial		Debugging terminal of MFD. Device for use: Serial port of PC for system administrator client is connected to the terminal port for MFD debugging via Fuji Xerox-unique conversion board. • Microsoft Windows 7 Professional • TeraTerm Pro Version 2.3
Interface converter		A development tool to connect MFD and debug serial.
Internal network		Use a switching hub.
Public Telephone Line		Use a pseudo exchange system (by How inc.) as an alternative of public telephone line.
Fax Board		An option of MFD by Fuji Xerox. • Fax ROM Version 1.1.11
Link Cable		A cable that connects MFD and general user client 2 via USB.

External network and firewall are not used because they do not affect the testing. The FTP communication function was confirmed separately, and the evaluator evaluated that there are no problems in the operation.

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

2) Summary of Developer Testing

Summary of the developer testing is as follows.

a. Outline of Developer Testing

The testing performed by the developer is outlined as follows;

<Developer Testing Approach>

The developer performs the following testing for security functions.

(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 IDE monitor as a testing tool to read out and check the data to be overwritten to the internal HDD and the internal HDD contents after the data for overwriting are written in.

(3) To confirm the Hard Disk Data Encryption function, use the serial port for debugging to directly refer to the documents etc. stored in the internal HDD and check that documents 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 of the same model 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.

(6) Connect the general user client 2 via public telephone line and use it for transmitting fax with the MFD. To confirm the fax flow security function, check that dial-up connection from general user client 2 to the TOE via public telephone line is disabled. Furthermore, check that the TOE operation is disabled even after directly connecting from the general user client 2 to the USB port for connecting fax board.

<Developer Testing Tools>

The tools used for the developer testing are shown in Table 7-2 below.

Table 7-2 Tools for Developer Testing

Tool Name	Outline/Objective
IDE Monitor (PC and dedicated device) *See Table 7-1 for configuration.	Monitor the data in IDE bus for connecting HDD in MFD, and check the data to be written to HDD, and also read out the data written in HDD.
Protocol Analyzer (Wireshark Version 1.4.6)	Monitor the communication data on the internal network, and confirm that the encryption communication protocol is IPSec, SSL/TLS, or SNMPv3 as specified.
Mailer (Microsoft Windows Mail)	Transmit E-mails with the TOE via mail server, and confirm that the encryption and signature by S/MIME are as specified.
Debug Serial (PC for debugging MFD)	Read out the data written on the internal HDD and check the contents.
Interface Converter	Fuji Xerox-unique converter that connects output connector of controller board and debug serial (PC for debugging).

<Content of execution of the 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 are 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, and the prevention of access to the internal network from fax.

b. Scope of Execution of the Developer Testing

The developer testing was performed on 72 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 consistencies between the expected testing results and the actual results of testing performed by the developer. The evaluator confirmed the approach of the testing performed by the developer and legitimacy of tested items, and confirmed that the testing approach and results are consistent with those described in the testing plan.

7.3.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm that the security functions are certainly executed by testing the items extracted from the developer tests, and the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further assurance that security functions are certainly performed, based on the evidence shown during the process of the evaluation.
The independent testing performed by the evaluator is explained below.

1) Evaluator Independent Testing Environment

Configuration of the independent testing performed by the evaluator is shown in Figure 7-2 below. The configuration elements of the independent testing performed by the evaluator were the same as those of the developer testing.

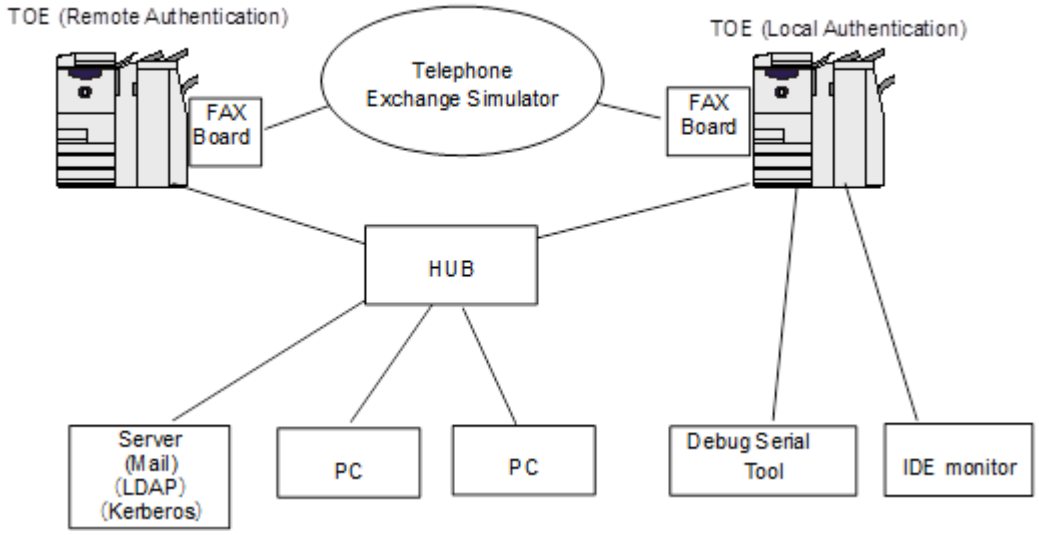

Figure 7-2 Evaluator Independent Testing Configurations

Among the models identified in TOE identification of Chapter 2, the evaluator tested on WorkCentre 5325 (Local Authentication is set) and WorkCentre 5330 (Remote Authentication is set). The evaluator evaluated that it can be confirmed that there are no differences in security functions between the models by testing on another model in addition to the same model used in the developer testing.

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

2) Summary of Independent Testing

Summary of the evaluator independent testing is as follows.

a. Viewpoint of Independent Testing

The evaluator projected the independent testing in terms of the following viewpoints, based on the developer testing and the provided evaluation evidential materials, in order to verify by the evaluator him/herself that the TOE security functions work as specified.

<Viewpoints of Independent Testing>

(1) The independent testing is to confirm the behavior of interfaces and parameters to which strict testing is not performed on the behavior of security functions in the developer testing.

b. Independent Testing Outline

The independent testing performed by the evaluator is outlined 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. Table 7-2 shows the tools used in the independent testing by the evaluator.

<Content of the Performed Independent Testing >

Table 7-3 shows outline of the independent testing performed by the evaluator with corresponding viewpoints of independent testing.

Table 7-3 Performed Independent Testing

Viewpoint of Independent Testing	Outline of the Independent Testing
(1)	Confirm that the behavior of the TOE is as specified when the entry for changing or entering passwords exceeds the limit values.
(1)	Confirm that access control to Mailbox for system administrators is as specified.
(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.
(1)	Test whether the behavior of the access control is as specified when LDAP server, in which user attributes are stored, is not used for Remote Authentication (when Kerberos server is used for the remote authentication server). (Note that a user is not identified as SA, but identified as a general user.)

c. Result

The evaluator completed all the independent testing correctly and confirmed the behavior of the TOE. The evaluator confirmed that all the testing results are consistent with the expected behavior.

7.3.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (herein after referred to as the "penetration testing") to test the items that possibly have exploitable vulnerabilities in the assumed environment of use and at the assumed attack level, based on the evidence shown during the process of the evaluation. The penetration testing performed by the evaluator is explained below.

1) Summary of the Penetration Testing

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

a. Vulnerability of concern

The evaluator searched into the provided evidence and information within the public domain for the potential vulnerabilities, and 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, various vulnerability of Web, and the selection of insecure encryption upon SSL communication.

(2) 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.

(3) There is a concern of unauthorized access by USB port from the analysis of vulnerability on the provided evidence.

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

(5) There is a concern that the documents as protected assets become inconsistent when multiple users access the documents in Mailbox, from the analysis of vulnerability on the provided evidence.

(6) 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.

b. Outline of Penetration Testing

The evaluators performed the following penetration testing to identify possibly exploitable vulnerabilities.

< Penetration Testing Environment>

Penetration testing was performed with the same configuration items as those of the evaluator independent testing shown in Figure 7-2, except additional personal computer with tools for penetration testing. Details of the used tools are shown in Table 7-4 below.

Table 7-4 Tools for Penetration Testing

Name		Outline/Objective
PC for Penetration Testing		Client with Windows XP, Windows Vista or Windows 7, which operates the following penetration testing tools
	Zenmap+Nmap Ver.5.51	A tool to detect the available network service port (Zenmap provides GUI of port scan tool Nmap.)
	Fiddler2 V2.3.4.3	A tool to refer to and change the communication data between web browser (Client) and web server (MFD). The tool enables to send any data to web server without any restriction of web browser by using Fiddler2.
	ContentsBridge Utility Version 7.2.0	Printer software for PC by Fuji Xerox

<Contents of Penetration Testing Performed>

Table 7-5 shows outline of the penetration testing for the vulnerabilities of concern.

Table 7-5 Outline of Penetration Testing

Corresponding Vulnerability	Outline of Testing
(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 Fiddler2, and confirmed that there is no vulnerability in the public domain such as bypass of identification/authentication, buffer overflow, and various injections. - Confirmed that the communication cannot be made except by the encryption communication protocol specified by the TOE even when the setting of the Personal Computer used as client is changed to the unrecommended value for the encryption communication protocol.
(2)	- 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 (network scan utility, printer driver).
(3)	- Confirmed that other than the intended functions, such as print and fax, it cannot be used even when attempting to access the TOE by connecting the Client for penetration testing to each USB port of the TOE.
(4)	- 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.
(5)	- Confirmed that the access is rejected during the operation by others when multiple users access documents in Mailbox.
(6)	- Confirmed that operation is rejected during initialization processing of the MFD right after the power-on. - Confirmed that security functions related to reliable time stamps behave properly when time cannot be displayed due to run-down of the battery of MFD system clock.

c. Result

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

7.4 Evaluated Configuration

TOE configuration conditions for this evaluation are shown in Table 7-6 below. To enable security functions of this TOE and use them safely, system administrators need to configure the TOE setting to satisfy them.

Table 7-6 TOE Configuration Condition

Item Number	Setting Item	Setting Value
1	Hard Disk Data Overwrite	Set to [1 Overwrite] or [3 Overwrites].
2	Hard Disk Data Encryption	Set to [Enabled].
3	Passcode Entry from Control Panel	Set to [Enabled].
4	Maximum Login Attempts	Set to [5] Times.
5	SSL/TLS Communication	Set to [Enabled].
6	IPSec Communication	Set to [Enabled].
7	S/MIME Communication	Set to [Enabled] .
8	User Authentication	Set to [Local Authentication] or [Remote Authentication]. (Note: Both setting are evaluated. For Remote Authentication, either LDAP or Kerberos setting is mandatory.)
9	Store Print	Set to [Save As Private Charge Print].
10	Audit Log	Set to [Enabled].
11	SNMPv3 Communication	Set to [Enabled].
12	Customer Engineer Operation Restriction	Set to [Enabled].
13	Direct Fax	Set to [Disabled] at Remote Authentication.
14	Network Scan utility (WebDAV setting)	Set to [Disabled] at Remote Authentication.
15	Minimum password length for general user and SA	Set to [9] characters. (Note: For Remote Authentication, at least 9-character password shall be set on LDAP and Kerberos server side.)
16	Number of characters of SNMPv3 password	Authentication password and privacy (encryption) password shall be set to be eight or more characters.

7.5 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

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

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

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

1. Submitted evidential materials were sampled, the contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
2. Rationale of 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.

The Certification Body confirmed there was no concern in the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

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

8.2 Recommendations

In operating this TOE, if the TOE setting is configured according to the attached document, configuration conditions with which this evaluation is conducted are to be satisfied. If the setting value of the TOE is changed from the configuration conditions, it shall be noted that it will not be assured by this evaluation.

Local Authentication and Remote Authentication are available as the user authentication function in this TOE, but there are restrictions on the function subject to evaluation when the operation with Remote Authentication is selected, compared with the case of Local Authentication. For more details, see "4.3 Clarification of Scope."

In this evaluation, the distribution of documents is evaluated up to the point where documents are uploaded to the website of Xerox Corporation. Note that users are responsible for downloading them, and they need to download them from the following legitimate website: http://www.support.xerox.com/support/.

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.

Xerox WorkCentre 5325/5330/5335 Security Target, Version 1.0.9, November 21, 2011, 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	Center Ware Internet Service
IIT	Image Input Terminal
IOT	Image Output Terminal
MFD	Multi Function Device
NVRAM	Non Volatile Random Access Memory
SA	System Administrator privilege; SA can use a part of management functions. The role of SA is set by key operator as required by the corresponding organisation. See the description of "System Administrator".
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.
Control Panel:	A panel of MFD on which buttons, lamps, and a touch screen panel are mounted to operate the MFD.
Customer Engineer (CE):	CE is a customer service engineer who maintains and repairs MFD.
Cryptographic Key:	Cryptographic key is used when encrypting/decrypting document data.
Direct Fax Function:	Direct Fax function is a function in which, according to the instruction from a general user client, the print data is sent to the MFD as a print job, and then sent to the destination via public telephone line without being printed out.

Document Data:	Document data means all the image data transmitted across the MFD when any of copy, print, scan or fax functions is operated by a general user.
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 user can send the fax data just as printing.
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:	General user is any person who are allowed to use basic functions of the TOE, such as copy, print, scan, and fax.
IDE Bus:	IDE Bus is a data transmission channel between controller board and internal HDD of MFD in order to send and receive data.
Internet Fax Function:	Internet Fax function is to send and receive fax data via the Internet, not via public telephone line.
Key Operator:	Key operator is a system administrator who can use all the management functions. See the description of "System Administrator".
Mailbox:	A logical box created in 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 MFD.
Network Scan Utility:	Software for a general user client to retrieve the document data stored in Mailbox of MFD.
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. The print function also includes the function to print document data stored in an external USB Media by designating the data from the control panel.
Scan Function:	Scan function is to read the original data from IIT and then store them into the Mailbox inside the MFD or the external USB Media according to the general user's instruction from the control panel. The stored document data can be retrieved via Network Scan Utility or CWIS using Web browser.
Security Audit Log Data:	The chronologically recorded data of important events of the TOE. The events such as device failure, configuration change, and user operation are recorded based on when and who caused what event and its result.
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 operations.
USB Media	A USB flash drive (USB memory) that is used for storing scanned document data and for printing stored document data.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, February 2011, Information-technology Promotion Agency, Japan, CCS-01

[2] IT Security Certification Procedure, February 2011, Information-technology Promotion Agency, Japan, CCM-02

[3] Evaluation Facility Approval Procedure, February 2011, Information-technology Promotion Agency, Japan, CCM-03

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

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

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

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

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

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

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

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

[12] Xerox WorkCentre 5325/5330/5335 Security Target, Version 1.0.9, November 21, 2011, Fuji Xerox Co., Ltd.

[13] Xerox WorkCentre 5325/5330/5335 Evaluation Technical Report, Version 1.3, November 22, 2011, Information Technology Security Center, Evaluation Department