Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-07-21 (ITC-0305)
Certification No.	C0294
Sponsor	Fuji Xerox Co., Ltd.
Name of TOE	Xerox Color 550/560 Printer
Version of TOE	Controller ROM Ver. 1.203.1, IOT ROM Ver. 62.23.0, IIT ROM Ver. 6.13.0, ADF ROM Ver. 12.4.0
PP Conformance	IEEE Std 2600.1-2009
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.
2011-06-23

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

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

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

Evaluation Result: Pass

"Xerox Color 550/560 Printer" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

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

Table of Contents

1. Executive Summary

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Xerox Color 550/560 Printer, Version Controller ROM Ver. 1.203.1, IOT ROM Ver. 62.23.0, IIT ROM Ver. 6.13.0, ADF ROM Ver. 12.4.0" (hereinafter referred to as "the TOE") developed by Fuji Xerox Co., Ltd., and evaluation of the TOE was finished on 2011-06-08 by Information Technology Security Center Evaluation Department (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Fuji Xerox Co., Ltd. and provides information to consumers and system operators who are interested in this TOE.

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

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

1.1 Product Overview

Overview of the TOE functions and operational conditions are as follows. Refer to from Chapter 2 onward 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 Xerox Color 550/560 Printer 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 from disclosure and alteration.

In regard to these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package. The TOE assumes threats and assumptions as described in the following sections.

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 unauthorized person by operation of the TOE and access to the communication data on the network to which the TOE is connected.

Thus, the TOE provides security functions such as identification and authorization, access control, and encryption to prevent unauthorized read-out or alteration of the assets to be

protected.

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 installed at an environment where the physical components of the TOE or its interface are protected from unauthorized access. To operate the TOE, the TOE shall be properly configured and maintained according to the guidance document.

1.1.3 Disclaimers

The user authentication that is subject to this evaluation is not performed when sending print data from the printer driver of the user client. Though the TOE performs user authentication upon sending print data when Local Authentication is used, this user authentication is not subject to 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 setting of those configuration conditions is changed, the configuration will not be assured by this evaluation.

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

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2011-06 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Reports prepared by Evaluation Facility and evaluation evidence 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 CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and concluded fully certification activities.

2. Identification

The TOE is identified as follows;

Name of TOE:	Xerox Color 550/560 Printer	
Version of TOE:	Controller ROM	Ver. 1.203.1
	IOT ROM	Ver. 62.23.0
	IIT ROM	Ver. 6.13.0
	ADF ROM	Ver. 12.4.0
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 the name of the TOE and the version information displayed on the screen or those 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 MFD functions are used, the TOE provides security functions that fulfill the security functional requirements required by the Protection Profile for digital MFDs, IEEE Std 2600.1-2009 [14] (hereinafter referred to as "the PP"). The security functions that the TOE provides include identification/authentication and access control of users, encryption of the data stored in HDD, data overwrite at deleting the data in HDD, and encryption communication protocol. The TOE prevents the user's document data that are assets to be protected and the setting data affecting security from being disclosed or altered by unauthorized person.

The TOE assumes the following roles when it is used:

- U.NORMAL
  Any person who uses copy, print, scan, and fax functions provided by the TOE. It is equivalent to general users.

- U.ADMINISTRATOR
  A user who has been specifically granted the authority to configure settings of TOE security functions. It is equivalent to system administrators (key operator and system administrator privilege [SA]).

- TOE Owner
  Any person or organizational entity responsible for protecting TOE assets and establishing the security objectives for the TOE operating environment.

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

The TOE's assets to be protected are as follows:

- User Document Data
  User Document Data consist of the information contained in a user's document.

- User Function Data
  User Function data are the information about a user's document or job to be processed by the TOE. Job Flow sheet and Mailbox are included.

- TSF Confidential Data
  TSF Confidential Data are the data used for security functions, and whose integrity and confidentiality are required. All the data used for security functions are defined as TSF Confidential Data in this TOE. For instance, it includes user ID along with user password, cryptographic seed key used to generate cryptographic key, setting values of security functions, and audit logs.

- TSF Protected Data
  TSF Protected Data are the data used for security functions, and whose integrity only is required. In the definition of this TOE, these data do not exist.

3.1 Security Function Policies

The TOE provides 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 functions to counter them. These threats are the same as those described in the PP.

Table 3-1 Assumed Threats

Identifier	Threat
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	User Function Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons

In the PP, in addition to the above threats, the threat of T.PROT.ALT (TSF Protected Data may be altered by unauthorized persons) exists. In this TOE, all TSF data are defined as TSF Confidential Data, and TSF Protected Data do not exist. Thus, T.PROT.ALT is not considered assumed threat.

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.DOC.DIS", "T.DOC.ALT" and "T.FUNC.ALT"

These are threats to user data. The TOE counters the threats by the following functions: User Authentication, Hard Disk Data Overwrite, Hard Disk Data Encryption, and Internal Network Data Protection.

The identification and authentication function and the access control function for MFD basic functions, which are both included in the User Authentication function of the TOE, allow only authorized users to use the TOE. For details of these functions, see 3.1.2.2 P.USER_AUTHORIZATION.

Furthermore, the access control function of user data, which is included in the User Authentication function of the TOE, controls access when the following operations are performed on document data, Mailbox, and Job Flow sheet, and allows only owners of the

data and system administrators to handle the data. The document data are stored either in Mailbox by the scan function or the fax-receive function or in the Private Print area by being sent from the printer driver of user client. The operations permitted are different depending on which area the document data are stored.

- Operation on the document data stored in Mailbox:
  Print, fax-send, transmission over network, and deletion
- Operation on the document data stored in the Private Print area:
  Print and deletion
- Operation on Mailbox:
  Registration of document data, registration of Job Flow sheet, changing of the name of Mailbox etc., and deletion of Mailbox
- Operation on Job Flow sheet:
  Execution, change, and deletion

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 MFD basic functions is completed. This function prevents the contents of the deleted document data from being read out from the internal HDD.

The Hard Disk Data Encryption function of the TOE is to encrypt the document data upon storing the data into the internal HDD. This function prevents the remaining document data within the internal HDD from being leaked when the internal HDD is taken off from the TOE upon maintenance or disposal. The cryptographic algorithm is 128-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.

The Internal Network Data Protection function of the TOE is to use encryption communication protocol when the TOE communicates with client terminals and servers. The supported encryption communication protocols are SSL/TLS, IPSec, SNMPv3, and S/MIME. This function prevents communication data from being leaked or altered.

With the above functions, the TOE prevents the data to be protected from being disclosed or altered by unauthorized usage of the TOE or by unauthorized access to the data stored in the internal HDD and to the communication data.

2) Countermeasures against threat "T.CONF.DIS" and "T.CONF.ALT"

These are the threats to the TSF data that affect security functions. The TOE counters the threats by the following functions: User Authentication, System Administrator's Security Management, Customer Engineer Operation Restriction, and Internal Network Data Protection.

The System Administrator's Security Management function of the TOE is to allow only identified and authenticated system administrators to refer to and change the security function setting data and to enable and disable security functions.

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

The User Authentication function and the Internal Network Data Protection function are the same functions as those described in 1).

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

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

Organisational security policies imposed on the use of the TOE are shown in Table 3-2. These organisational security policies are the same as those described in the PP.

Table 3-2 Organisational Security Policies

Identifier	Organisational Security Policy
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

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.USER.AUTHORIZATION"

The TOE realizes this policy by the User Authentication function.

The User Authentication function of the TOE allows only identified and authenticated users to use the TOE. Furthermore, the TOE restricts the number of characters of authentication password to be nine or more upon the password registration to strengthen the identification and authentication function.

Note that receiving fax and receiving print data that are sent from the printer driver of user client are permitted without identification and authentication that are performed to realize the above P.USER.AUTHORIZATION, and the received document data are stored in the TOE. To perform printing etc. of the document data stored in the TOE, operation from the TOE control panel etc. is required, and identification and authentication are also required.

The access control function included in the User Authentication function of the TOE is to control access when a user uses such MFD basic functions as copy, print, scan, network scan, or fax and to allow only authorized users to use those functions. With this function, the TOE refers to the identifiers of permitted users that are set for each MFD basic function to check whether the user is permitted to use the function.

With the above functions, the TOE allows only authorized users to use the TOE.

2) Means for organisational security policy "P.SOFTWARE.VERIFICATION"

The TOE realizes this policy by the Self Test function.

The Self Test function of the TOE is to verify check sum of Controller ROM 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.

3) Means for organisational security policy "P.AUDIT.LOGGING"

The TOE realizes this policy by the Security Audit Log function.

The Security Audit Log function of the TOE is to generate audit logs and store them in NVRAM and the HDD of the TOE when security events occur upon the use of security functions. Only identified and authenticated system administrators can read out the stored audit logs via web browser.

4) Means for organisational security policy "P.INTERFACE.MANAGEMENT"

The TOE realizes this policy by the User Authentication and the Information Flow Security functions.

The User Authentication function of the TOE allows only identified and authenticated users to use the TOE. Furthermore, the TOE terminates a session when the state that a user does not perform any operations continues for the specified amount of time.

With the Information Flow Security function of the TOE, the data received from various TOE interfaces cannot be transferred to LAN unless the data are processed by the TOE.

The above functions prevent unauthorized use of the TOE interfaces.

4. Assumptions and Clarification of Scope

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

4.1 Usage Assumptions

Assumptions required in the use of the TOE are shown in Table 4-1. These assumptions are the same as those described in the PP.
The effective performance of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

Identifier	Assumption
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 Environment Assumptions

The MFD, which is the TOE, is assumed to be used at general office, linked to internal network protected from threats on the external network by firewall, etc. Figure 4-1 below shows general environment for TOE operation.

The TOE users use TOE by operating TOE control panel, general user client, or system administrator client.

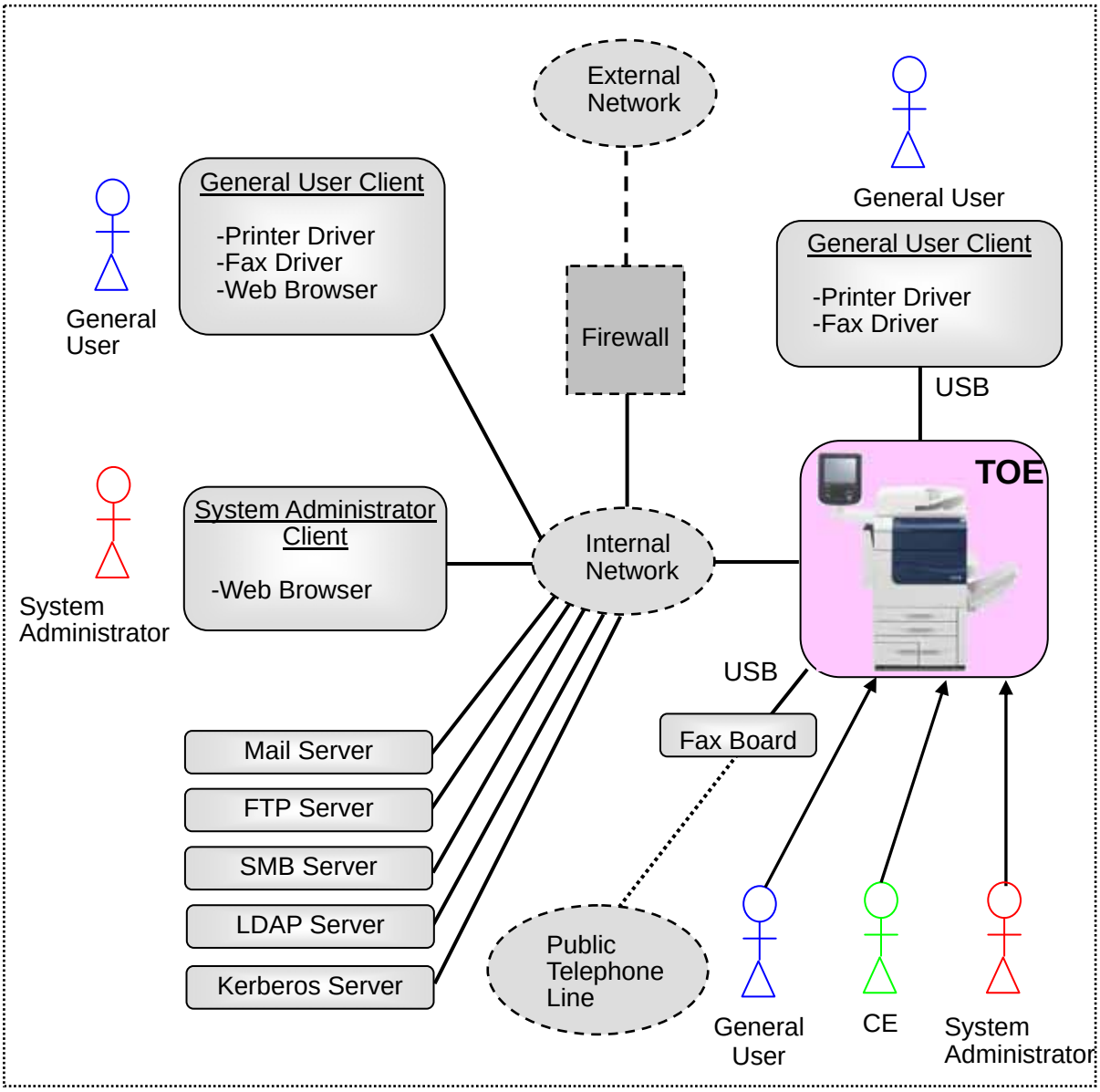

Figure 4-1 Operational Environment of TOE

The operational environment of TOE consists of the following:

1) Fax Board
The TOE has a fax function, but Fax Board connected to TOE via USB is sold separately. A user who wants to use the fax function needs to purchase the designated Fax Board.

2) General User Client
General User Client is a general-purpose PC for general user and linked to the TOE via USB or internal network. The following software is required:
- OS: Windows XP, Windows Vista, or Windows 7
- Printer driver and fax driver

When the client is linked to internal network, the following software is required in addition to those listed above:
- Web browser (included with OS)

3) System Administrator Client
System Administrator Client is a general-purpose PC for system administrators and

connected to TOE via 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 user authentication function, authentication server of either LDAP server or Kerberos server, will be necessary. When Local Authentication is set, neither authentication server is necessary.

In addition, LDAP server is used to acquire the user attribute to identify SA role upon Remote Authentication. Thus, even for the authentication with Kerberos server, LDAP server is necessary to use the SA role.

5) Mail Server, FTP Server, SMB Server
A server is installed if necessary upon using MFD basic functions.

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

4.3 Clarification of Scope

1) In the user authentication 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 for Local Authentication.

- Direct Fax function of MFD basic functions is not subject to evaluation when Remote Authentication is used.
- The TOE function that restricts the number of characters of password to be nine or more is not applied to user password stored in the Remote Authentication server.

2) In this evaluation, the following is not the security function to be evaluated because it is considered that SFR required by the PP does not require the identification and authentication by the TOE upon sending print data from the printer driver of user client to MFD.

- Printer driver requires users to enter user ID and password. This authentication which uses user password is not the target of this evaluation.
(In fact, when Local Authentication is used, the authentication processing is performed in the TOE. When Remote Authentication is used, password is not used in the TOE.)

The user ID preset in printer driver is identified in the TOE, and print data are classified and stored according to the user ID. The implementation of identification function is necessary for the TOE, and this function is included in the security functions to be evaluated.

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 configuration of MFD, which is the TOE, and the IT environment other than MFD. In Figure 5-1, the entire colored area indicates the TOE.

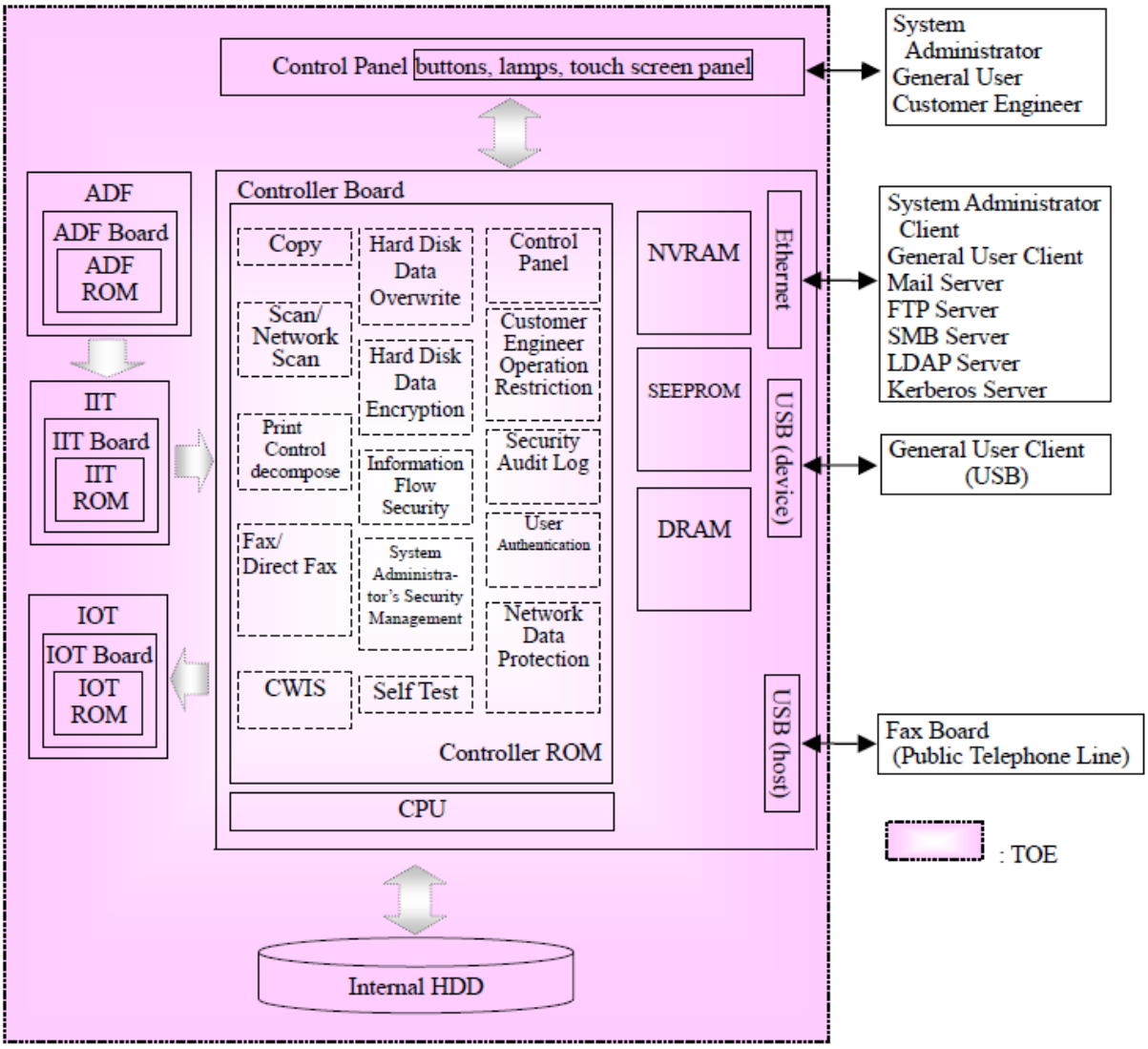

Figure 5-1 TOE Boundary

In Figure 5-1, the functions installed on the controller board are security functions described in Chapter 3 and MFD basic functions. Regarding the MFD basic functions, refer to Terminology in Chapter 11.

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

1) Operations from general user client (printer driver)

When a user sends a print request of document data from the printer driver of general user client that is connected to the TOE via Ethernet or USB, the document data as well as the user identifier are stored in the Private Print area within the internal HDD by using the User Authentication function. (Note that user authentication is performed when Local Authentication is used, but this is not the security function to be evaluated.) The document data stored in the Private Print area are printed out by operating the control panel.

2) Operations from general user client (fax driver)

When a user sends a fax-send request of document data from the fax driver of general user client that is connected to the TOE via Ethernet or USB, the User Authentication function identifies and authenticates the user, and the document data of the identified and authenticated user are not stored in the TOE and are immediately faxed. (Note that, in this evaluation configuration, this Direct Fax function can be used only when Local Authentication is used and cannot be used when Remote Authentication is used.)

3) Operations from control panel

When a user uses TOE basic functions such as copy, print, scan, network scan, and fax, the User Authentication function identifies and authenticates the user, and allows only authorized users to operate the TOE. The document data scanned into the TOE by the scan function and the fax-receive function are stored in Mailbox within the internal HDD.

When the identified and authenticated user handles document data etc. stored in Mailbox and the Private Print area within the internal HDD, the User Authentication function controls access and allows only owners of the data and system administrators to handle the data.

When a user uses the System Administrator's Security Management function by operating the control panel, the User Authentication allows only identified and authenticated users who have administrator privileges to use the System Administrator's Security Management function.

4) Operations from web browser

When a user handles document data etc. stored in Mailbox of the internal HDD by operating web browser, the User Authentication function identifies and authenticates the user and allows only authorized users to operate the TOE. Furthermore, the access control function allows only owners of the data and system administrators to handle the data. The document data stored in Mailbox can be printed out by operating web browser as well as the control panel.

When a user uses the System Administrator's Security Management function and the function of the Security Audit Log function that refers to audit logs by operating web browser, the User Authentication function allows only identified and authenticated users who have administrator privileges to operate the TOE.

5) Internal HDD data protection

In the above cases 1) to 4), the Hard Disk Data Encryption function is used to encrypt the document data stored in the internal HDD, and the Hard Disk Data Overwrite function

is used when the document data are deleted. These processes are applied not only to the document data intentionally stored and deleted by a user, but also to the document data temporarily and unintentionally stored in the internal HDD during the process of such functions as copy.

6) Network protection

In the above cases 1) to 4), the Internal Network Data Protection function uses encryption communication protocol when the TOE communicates with other IT devices via LAN. The Information Flow Security function prevents unauthorized forwarding of the data that are input from various interfaces.

7) Generation of audit logs

The Security Audit Log function generates audit logs when security functions are used in the above cases 1) to 4), and when the establishment of encryption communication protocol fails in the above case 6).

5.2 IT Environment

When the TOE communicates with external IT devices via network, IPSec protocol is used. Furthermore, SSL/TLS is used when communicating with web browser installed on client, S/MIME is used when sending e-mails to and receiving e-mails from Mail server, and SNMPv3 is used for network management.

When Remote Authentication via LDAP server is selected in the TOE settings, user ID and password are verified in LDAP server and its result is used by the TOE. When Remote Authentication via Kerberos server is selected, identification/authentication is performed by the coordinated operation of Kerberos server and the TOE.

In addition, 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.

6. Documentation

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

- Xerox Color 550/560 Printer User Guide
  (Version 1.0, August 2010)

- Xerox Color 550/560 Printer System Administrator Guide
  (Version 1.0, August 2010)

- Xerox Color 550/560 Printer Security Function Supplementary Guide
  (Version 1.0, April 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 CEM in accordance with the assurance components in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. In the Evaluation Technical Report, it explains the summary of the TOE, the content of evaluation and verdict of each work unit.

7.2 Overview of Evaluation Activity

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

Evaluation has started on 2010-07 and concluded by the completion of the Evaluation Technical Report dated 2011-06. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted.

Additionally, the evaluator directly visited the development and manufacturing sites on 2010-12 and 2011-02, and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff interview.

There are two MFD assembly plants, one is in China and the other is in Korea. The TOE is shipped from either of them. The evaluator visited the assembly plant in China, but the evaluator didn't visit the assembly plant in Korea. For Korea site, the evaluator evaluates that the security measures required for the site are same as those for China site, and gains the confidence that those measures are applied by investigating the evidences and interviewing Japanese staff who knows the status of Korea site.

Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-12.

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

Concerns that the Certification Body found about the evaluation process were described as a certification oversight review, and it was sent to Evaluation Facility. After Evaluation Facility and the developer examined it, these concerns were reflected in the evaluation report.

7.3 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. The evaluator performed the recurrence testing, additional testing and penetration testing based on vulnerability assessments, which are determined to be necessary from the evidence shown in the process of the evaluation, and results from the verification of the developer testing.

7.3.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the evidential 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.

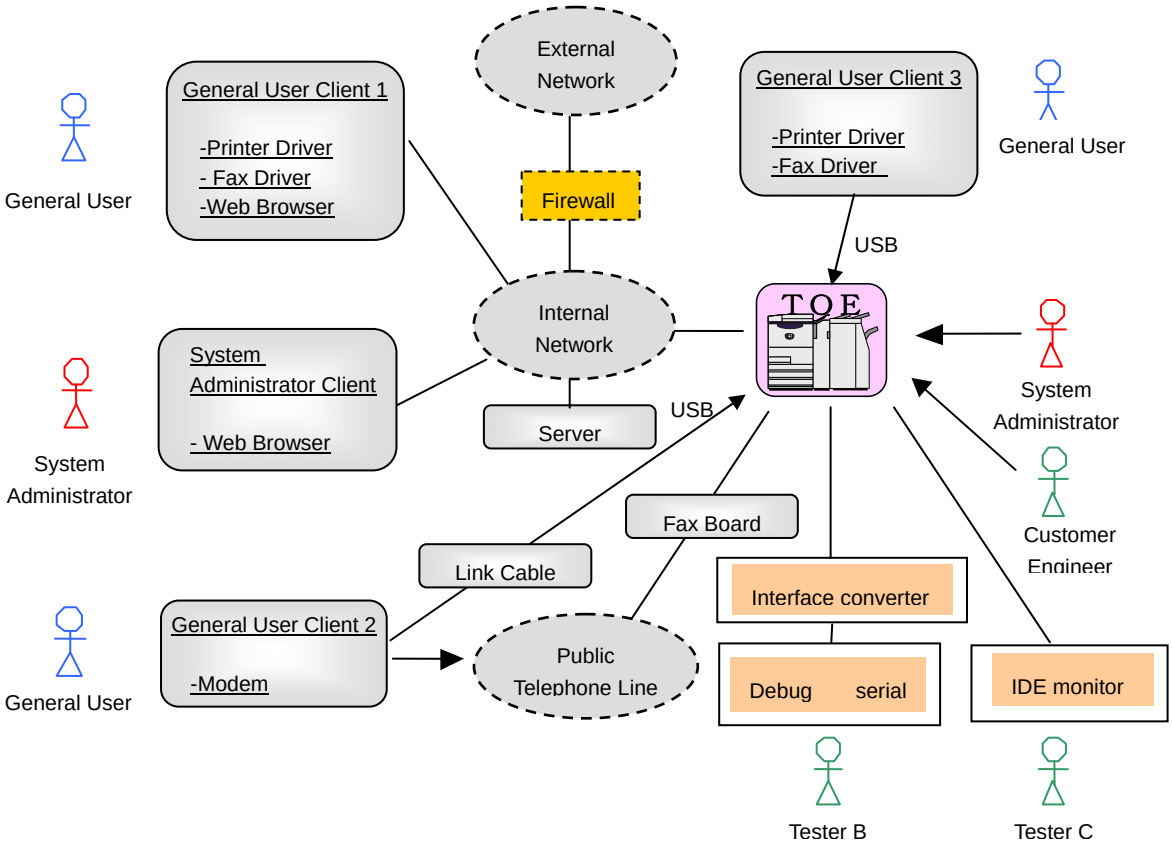

Figure 7-1 Configuration of Developer Testing

The TOE subject to evaluation is Xerox Color 560 Printer 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 model has the same software and behavior of security functions as those of the TOE and is different only in the process speed of copy and print etc.

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

Table 7-1 Devices for Developer Testing

Device Name	Description
Server	Used as Mail server, LDAP server, and Kerberos server. - PC with Windows Server 2008 sp2 - Various servers: Standard software in OS
System Administrator Client	Used as system administrator client. The testing is performed with one of the following three models. a) PC with Windows 7 professional (Web browser: Internet Explorer 8) b) PC with Windows XP professional sp3 (Web browser: Internet Explorer 6) c) PC with Windows VISTA business sp2 (Web browser: Internet Explorer 7)
General User Client 1	Used as general user client (connected via internal network) and SMB server. The testing is performed with one of the following three models. a) PC with Windows 7 professional (Web browser: Internet Explorer 8) b) PC with Windows XP professional sp3 (Web browser: Internet Explorer 6) c) PC with Windows VISTA business sp2 (Web browser: Internet Explorer 7) Additionally, the following software is used. - Printer driver and fax driver: Version 6.00 - SMB server: Standard software in OS
General User Client 2	Used to send/receive fax and to confirm that USB port for connecting MFD fax cannot be used for other use. - PC with Windows XP professional sp2 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).
General User Client 3	Used as general user client (connected via USB port for printer). - PC with Windows XP professional sp2 - Printer driver and fax driver: Version 6.00
IDE Monitor	A tool to monitor the data transmitted through the connected IDE bus of HDD. - IDE-POCKET (by TOYO Corporation) of dedicated device is connected to the PC with Windows XP - Software: IDE-WinU V1.9.3 (by TOYO Corporation)
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. - Software: Tera Term Pro version 2.3
Public Telephone Line	Use a pseudo exchange system as an alternative of public telephone line.
Fax Board	An option of MFD by Fuji Xerox - Fax ROM Ver 1.1.2

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>
(1) Operate MFD basic 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 and read out and check the data to be written to HDD and the contents of the HDD after the data are written.

(3) To confirm the Hard Disk Data Encryption function, use the serial port for debugging, directly refer to the document data stored in HDD, and check that document data are encrypted. In addition, confirm that the encrypted HDD cannot be used and an error is displayed on the control panel even after the HDD is replaced with that of other device.

(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 observe that the encryption communication protocol is applied as specified.

(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 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	Description
IDE Monitor (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. Also, read out the data written in HDD.
Protocol Analyzer Wireshark Version 1.2.3	Monitor the communication data on the network, and confirm that the encryption communication protocol is IPSec, SSL/TLS, or SNMPv3 as specified.

Mailer Windows Live Mail Version 2009	Transmit mails with TOE via mail server, and confirm that the encryption and signature by S/MIME are as specified.

<Developer Testing Effort>
MFD basic functions and security management functions are operated from every interface, and it is confirmed that the security functions to be applied to various input parameters behave as specified. Regarding user authentication function, it is confirmed that local authentication, remote authentication (LDAP server), and remote authentication (Kerberos server) behave as specified according to the user role.

In addition, it is confirmed that the processing halt by MFD power off and its restart by MFD power on and the prevention of access to internal network from fax behave as specified.

b. Scope of Developer Testing Performed

The developer testing is performed 72 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the TOE functional specification had been tested. By the depth analysis, it was verified that all subsystems and subsystem interfaces described in the TOE high-level design had been tested enough.

c. Result

The evaluator confirmed consistencies between the expected testing results and the actual testing results performed by the developer. The evaluator confirmed the testing approach 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 independent testing to reconfirm that security functions are certainly implemented based on the evidence shown in the process of the evaluation. The overview of the independent testing performed by the evaluator is described as follows;

1) Evaluator Independent Testing Environment
Configuration of the test performed by the evaluator is shown in Figure 7-2 below.

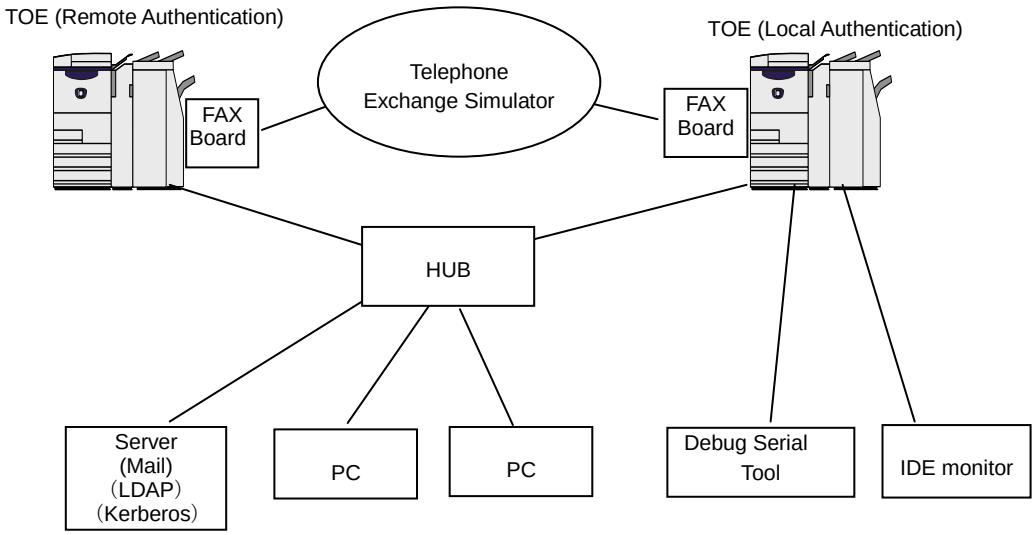

Figure 7-2 Configuration of Evaluator Testing

The configuration of the testing performed by the evaluator was the same as the configuration of the developer testing.

The target TOE was the same as that in the developer testing, and Xerox Color 560 Printer was used for both the TOE (remote authentication) and the TOE (local authentication). The MFD was used instead of the PC used in the developer testing for sending/receiving fax with MFD, and the evaluator evaluated that it does not affect the test of security functions.

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

2) Summary of Evaluator Independent Testing
Summary of the evaluator independent testing is as follows;

a. Viewpoints of Independent Testing

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

<Viewpoints of Independent Testing>
(1) Perform the same testing as the developer testing to be convinced that the TOE behaves as tested by the developer and confirm the validity.

(2) Confirm the behavior of untested parameters since there is an interface to which strict testing on the behavior of security functions is not performed in the developer testing.

b. Outline of Independent Testing
The independent testing performed by the evaluator is outlined as follows;

<Independent Testing Approach>
Using the same method as of the developer testing, the same testing and the testing with changed parameters are performed.

<Independent Testing Tools>
The same testing tool as that of the developer testing was used.

<Contents of Independent Testing Performed>
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 independent testing
(1)	Test all the items tested by the developer and confirm that the same result as that by the developer can be obtained. (Excludes the test to confirm that the algorithm to generate a cryptographic key and the cryptographic algorithm are as specified)
(2)	Confirm that the followings are as specified: - Behavior of limit value for password length upon password change and entry - Bahavior of account lock in case there are failed cases and successful cases of identification and authentication for user IDs of system administrators. (Note: The number of successive failure times of identification and authentication for a user ID is tracked correctly, even when a successful case of another user ID comes in between the failed cases.) - Access control to Mailbox for system administrator
(2)	Confirm that the behavior of access control without using LDAP server that stores user attributes is as specified in Remote Authentication (Kerberos server). (Note: Recognized as general user, not as SA)

c. Result

All the independent testing performed by the evaluator was completed correctly, and the evaluator confirmed the behavior of TOE. The evaluator confirmed that all the test results are consistent with the expected behavior.

7.3.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing regarding the possibility of exploitable concern at assumed environment of use and attack level. The overview of the penetration testing performed by the evaluator is described as follows;

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 the information publicly

available for the potential vulnerabilities, and identified the following vulnerabilities that 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 from USB port according to 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, according to the analysis of vulnerability on the provided evidence.

(5) There is a concern that the document data as a protected asset become inconsistent when multiple users access the document data in Mailbox, according to the analysis of vulnerability on the provided evidence.

b. Outline of Penetration Testing

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

< Penetration Testing Environment>

Penetration Testing was performed in the same environment as that of the evaluator independent testing shown in Figure 7-2, except adding the PC with a tool for penetration testing. Details of the used tool are shown in Table 7-4 below.

Table 7-4 Tools for Penetration Testing

Tool Name		Description
PC for Penetration Testing		PC with Windows XP, Windows 7 or Windows VISTA which operates the following penetration testing tools.
	(a) Nmap Ver.5.21	A tool to detect the available network service port
	(b) Fiddler2 V2.3.0.0	A tool to mediate the communication between web browser (PC) and web server (TOE), and to refer to and change the communication data between web browser (PC) and web server (TOE). It able to send any data to web server without any restriction of web brower by using Fiddler2.

<Contents of Penetration Testing Performed>

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

Table 7-5 Outline of Penetration Testing

Vulnerability of concern	Outline of penetration testing
(1)	- Executed Nmap for TOE and confirmed that the open port cannot be misused. - Performed various entries to Web server (TOE) using web browser and Fiddler2, and confirmed that there is no known vulnerability 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 PC 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 (printer driver).
(3)	- Confirmed that other than the intended functions such as print and fax cannot be used, even when attempting to access the TOE by connecting the PC 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 operations by others when multiple users access the document data in Mailbox.

c. Result

In the penetration testing performed by the evaluator, the exploitable vulnerability could not be found that attackers with the assumed attack potential could exploit.

7.4 Evaluated Configuration

TOE configuration conditions for this evaluation are shown in Table 7-6 below.

Table 7-6 TOE Configuration Condition

Item No.	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, setting either LDAP or Kerberos is mandatory.)
9	Store Print	Set to [Save As Private Charge Print]
10	Auto Clear	Set to [Enabled]
11	Audit Log	Set to [Enabled]
12	SNMPv3 Communication	Set to [Enabled]
13	Customer Engineer Operation Restriction	Set to [Enabled]
14	Direct Fax	Set to [Disabled] at Remote Authentication. (Note: For Local Authentication, evaluation is performed with setting of [Enabled])
15	Network Scan utility (WebDAV setting)	Set to [Disabled]
16	Minimum password length for general user and SA	Set to [9] characters. (Note: For Remote Authentication, at least 9 characters password shall be set on LDAP and Kerberos server side.)

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.
- PP Conformance:
  2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
  (IEEE Std 2600.1-2009)

  SFR packages conformance defined in the above PP:
  - 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A: Conformant
  - 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A: Conformant
  - 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A: Conformant
  - 2600.1-FAX, SFR Package for Hardcopy Device FAX Functions, Operational Environment A: Conformant
  - 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A: Conformant
  - 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A: Augmented

- Security functional requirements: Common Criteria Part 2 Extended
- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.
- All assurance components of EAL3 package
- Augmented assurance component ALC_FLR.2

The result of the evaluation is applied only to the evaluated configuration described in this report, in regard to the TOE identified in the 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 each materials submitted by Evaluation Facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

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

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

8.1 Certification Result

As a result of verification of submitted Evaluation Technical Report, Observation Reports and related evaluation deliverables, Certification Body determined that the TOE satisfies all components of the EAL3 augmented with ALC_FLR.2 in the CC part 3.

8.2 Recommendations

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

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

In this evaluation, it is considered that SFR required by the PP does not require identification and authentication upon print request from the printer driver of user client, and it requires identification and authentication when a user actually prints out document data. Thus, it should be noted that the TOE may not be able to satisfy the needs of consumers who expect identification and authentication upon print request from the printer driver of user client.

When using the printer driver of user client, operation from the control panel is required to output printed documents. However, document data stored by using such functions as scan and fax-receive can be output as printed documents by operation from web browser of user client as well as from the control panel. Thus, it should be noted that the TOE may not be able to satisfy the needs of consumers who expect that document data can be printed out only when they operate from the control panel to ensure the security of paper documents.

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 Color 550/560 Printer Security Target Version 1.1.8, June 6 2011, Fuji Xerox Co., Ltd.

11. Glossary

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

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

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

ADF	Auto Document Feeder
IIT	Image Input Terminal
IOT	Image Output Terminal
MFD	Multi Function Device
NVRAM	Non Volatile Random Access Memory
SEEPROM	Serial Electronically Erasable and Programmable Read Only Memory

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

CWIS Function	CWIS (CentreWare Internet Service) is to retrieve the document data stored in Mailbox via Web browser. CWIS also enables management of the setting data by System Administrator.
SA	See the description of "System Administrator".
TOE Owner	Any person or organizational entity responsible for protecting TOE assets and establishing related security policies for the TOE operating environment.
U.ADMINISTRATOR	A user who has been specifically granted the authority to configure settings of TOE security functions. It is equivalent to system administrators (key operator and system administrator privilege [SA]).
U.NORMAL	Any person who uses copy, print, scan, and fax functions provided by TOE. It is equivalent to general users.
User Document Data	Document data of user. All the data including image information that are passed through MFD when general user uses MFD functions such as copy, print, scan, and fax.
User Function Data	The information about a user's document or job to be processed by the TOE. Job Flow sheet and Mailbox are included.

TSF Confidential Data	Among the data used for security functions, the data whose integrity and confidentiality are required. All the data used for security functions are defined as TSF Confidential Data in this TOE.
TSF Protected Data	Among the data used for security functions, the data whose integrity only is required to be maintained. In the definition of this TOE, these data do not exist.
Cryptographic Seed Key	The 12 alphanumeric characters to be set by system administrators. When data in the internal HDD are encrypted, a cryptographic key is generated based on this data.
General User	Any person who uses copy, print, scan, and fax functions provided by TOE.
Auto Clear Function	A function to automatically logout authentication when the state that a user does not perform any operations continues for the specified amount of time.
Key Operator	See the description of "System Administrator".
Customer Engineer (CE)	Customer service engineer who maintains and repairs 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.
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). 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 organization.
Job Flow sheet	A series of registered actions to the device, such as scanner setting information, conversion format, and data delivery process / destination, to process the scanned document and received fax document.
Mailbox	Logical box that is created in the internal HDD to store the document data scanned by scan function or fax-receive function.
Scan Function	Scan function is to read the original data from IIT and then store it into the Mailbox inside the MFD according to the general user's instruction from the control panel. The stored document data can be retrieved via CWIS using Web browser or control panel function.

Control Panel Function	Control panel function is a user interface function for general user, system administrator, and CE to operate MFD functions.
Direct Fax Function	Direct Fax function is to directly fax document data to the destination. According to the instruction from a general user client, the print data are sent to the MFD as a print job, and then sent to the destination via public telephone line without being printed out.
Store Print	See the description of "Print Function".
Normal Print	See the description of "Print Function".
Network Scan Function	Network scan function is to read the original data from IIT and automatically transmit it to FTP server, Mail server, or SMB server according to the information set in the MFD. A general user can request this function from the control panel.
Network Scan Utility	Software for a general user client to retrieve the document data stored in Mailbox of MFD.
Fax Function	Fax function is to send and receive fax data. According to the general user's instruction from the control panel, the original data are 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 are received, and the data are printed by the recipient's IOT.
Private Print	An area in the internal HDD to store print data sent from printer driver to MFD.
Print Function	Print function is to print out the data, which is sent to the MFD via printer driver, from IOT according to the instruction from a general user client. There are two types of the print function: "Normal Print" in which the data are printed out immediately from IOT when the MFD receives the data, and "Store Print" in which the print data are temporarily stored in the HDD inside the MFD and then printed out from IOT according to the general user's instruction from the control panel. In this evaluation, only the "Store Print" is subject to the evaluation.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[2] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[3] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

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

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

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

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

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

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

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

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

[12] Xerox Color 550/560 Printer Security Target Version 1.1.8, June 6 2011, Fuji Xerox Co., Ltd.

[13] Xerox Color 550/560 Printer Evaluation Technical Report Version 1.9, June 8 2011, Information Technology Security Center Evaluation Department

[14] IEEE Std 2600.1-2009, IEEE Standard for a Protection Profile in Operational Environment A, Version 1.0, June 2009