Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application date/ID	2013-04-10 (ITC-3451)
Certification No.	C0411
Sponsor	Fuji Xerox Co., Ltd.
Name of the TOE	Xerox D136 Copier/Printer
Version of the TOE	Controller+PS ROM Ver. 1.200.6, IOT ROM Ver. 113.27.0, IIT ROM Ver. 13.1.0, ADF ROM Ver. 13.17.1
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.
2013-10-30

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

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

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

Evaluation Result: Pass

"Xerox D136 Copier/Printer" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

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

Table of Contents

1. Executive Summary 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 7
1.3 Certification 7
2. Identification 8
3. Security Policy 9
3.1 Security Function Policies 10
3.1.1 Threats and Security Function Policies 10
3.1.1.1 Threats 10
3.1.1.2 Security Function Policies against Threats 10
3.1.2 Organisational Security Policies and Security Function Policies 12
3.1.2.1 Organisational Security Policies 12
3.1.2.2 Security Function Policies to Organisational Security Policies 12
4. Assumptions and Clarification of Scope 14
4.1 Usage Assumptions 14
4.2 Environmental Assumptions 14
4.3 Clarification of Scope 16
5. Architectural Information 17
5.1 TOE Boundary and Components 17
5.2 IT Environment 19
6. Documentation 20
7. Evaluation conducted by Evaluation Facility and Results 21
7.1 Evaluation Approach 21
7.2 Overview of Evaluation Activity 21
7.3 IT Product Testing 22
7.3.1 Developer Testing 22
7.3.2 Evaluator Independent Testing 25
7.3.3 Evaluator Penetration Testing 27
7.4 Evaluated Configuration 30
7.5 Evaluation Results 31
7.6 Evaluator Comments/Recommendations 31
8. Certification 32
8.1 Certification Result 32

8.2 Recommendations 32
9. Annexes 33
10. Security Target 33
11. Glossary 34
12. Bibliography 37

1. Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "Xerox D136 Copier/Printer, Version Controller+PS ROM Ver. 1.200.6, IOT ROM Ver. 113.27.0, IIT ROM Ver. 13.1.0, ADF ROM Ver. 13.17.1" (hereinafter referred to as the "TOE") developed by Fuji Xerox Co., Ltd., and the evaluation of the TOE was finished on 2013-10-24 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Fuji Xerox Co., Ltd., and provide information to procurement personnel and consumers who are interested in this TOE.

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

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

1.1 Product Overview

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

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3 augmented with ALC_FLR.2.

1.1.2 TOE and Security Functionality

The TOE is the multi-function device (hereinafter referred to as "MFD"), which has such functions as copy, print, and scan. The TOE does not provide the fax function.

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

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

1.1.2.1 Threats and Security Objectives

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

The document data of users and the setting data affecting security, which are assets to be

protected, may be disclosed or altered by unauthorized operation of the TOE or by unauthorized access to the communication data on the network to which the TOE is connected.

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

1.1.2.2 Configuration and Assumptions

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

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

1.1.3 Disclaimers

The following operation and functions will not be assured by this evaluation.

In this evaluation, only the configuration, to which the setting condition such as restriction for customer engineer operation is applied, is evaluated as the TOE. If the TOE settings shown in "7.4 Evaluated Configuration" are changed, the configuration will not be assured by this evaluation.

The user authentication that is subject to this evaluation is not performed when sending print data from the printer driver of user clients. Though the TOE performs user authentication upon sending print data when Local Authentication is used, this user authentication is not subject to this evaluation.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2013-10, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and evaluation evidential materials, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

Name of the TOE:	Xerox D136 Copier/Printer	
Version of the TOE:	Controller+PS ROM	Ver. 1.200.6
	IOT ROM	Ver. 113.27.0
	IIT ROM	Ver. 13.1.0
	ADF ROM	Ver. 13.17.1
Developer:	Fuji Xerox Co., Ltd.	

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

Users operate on the control panel according to the procedure written in the guidance document, and confirm 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 written in the print output of the configuration setting list.

3. Security Policy

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

The TOE provides MFD functions such as copy, print, and scan, 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 and the setting data affecting security that are assets to be protected from being disclosed or altered by unauthorized persons.

The TOE assumes the following roles when it is used:

- General User
  Any person who uses copy, print, and scan functions provided by the TOE.

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

- 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 the 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. In the definition of the TOE, they include passwords of users, the cryptographic seed key used to generate a cryptographic key, the setting values of encryption communication protocol, and the 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 the TOE, they include the setting values of security functions except for TSF Confidential Data.

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Chapter 3.1.1, and to satisfy the 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 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.PROT.ALT	TSF Protected 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

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 basic MFD 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 for 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 function to store the copy data 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, preview, deletion, network transmission of the document data stored by the scan function, and edition of the document data stored by the function to store copy data

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

The Internal Network Data Protection function of the TOE is to use encryption communication protocol when the TOE communicates with client terminals and various servers. The supported encryption communication protocols are SSL/TLS (SSL 3.0, TLS 1.0), IPSec, SNMPv3, and S/MIME. This function prevents communication data from being disclosed 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.PROT.ALT", "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 required in 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 satisfy 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 9 or more upon the password registration to strengthen the identification and authentication function.

Note that 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 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 basic MFD functions as copy, print, scan, or network scan, 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 basic MFD 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 the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. These assumptions are the same as those described in the PP. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions in Use of the TOE

Identifier	Assumptions
A.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 Environmental Assumptions

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

The TOE users use the TOE by operating the control panel of the TOE, general user clients, or system administrator clients.

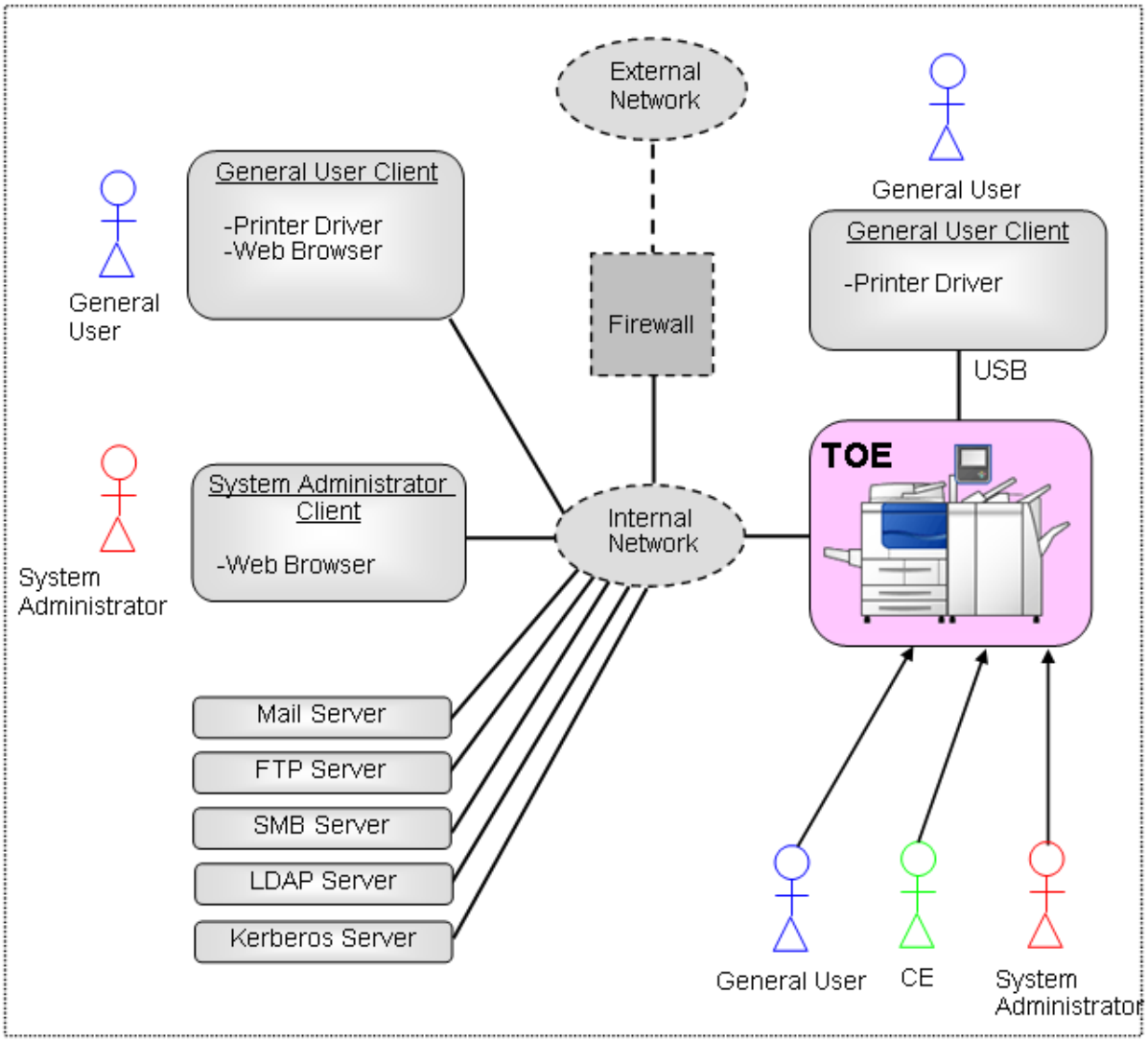

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following:

1) General User Client

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

- OS: Windows XP, Windows Vista, or Windows 7
- Printer driver

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

- Web browser (included with OS)

2) System Administrator Client

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

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

3) LDAP Server, Kerberos Server

When Remote Authentication is set for 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.

4) 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.

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

4.3 Clarification of Scope

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

1) Restrictions for Remote Authentication
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.

- The TOE function that restricts the number of characters of password to be 9 or more is not applied to user password stored in the Remote Authentication server. An administrator is responsible for ensuring that user password stored in the remote authentication server is long enough not to be predicted.

2) Identification and Authentication upon sending print data
In this evaluation, the evaluator evaluates that the security functional requirements of the identification and authentication specified in the PP are not applied to the operation of sending print data from the printer driver of user client to the MFD. Therefore, the following function is out of scope of the evaluated security functions.

- Printer driver requires a user to enter user ID and password. This authentication which uses user password is not the target of 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. This implementation of identification is necessary for the TOE, and included in the security functions to be evaluated.

5. Architectural Information

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

5.1 TOE Boundary and Components

Figure 5-1 shows the configuration of the MFD, 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.

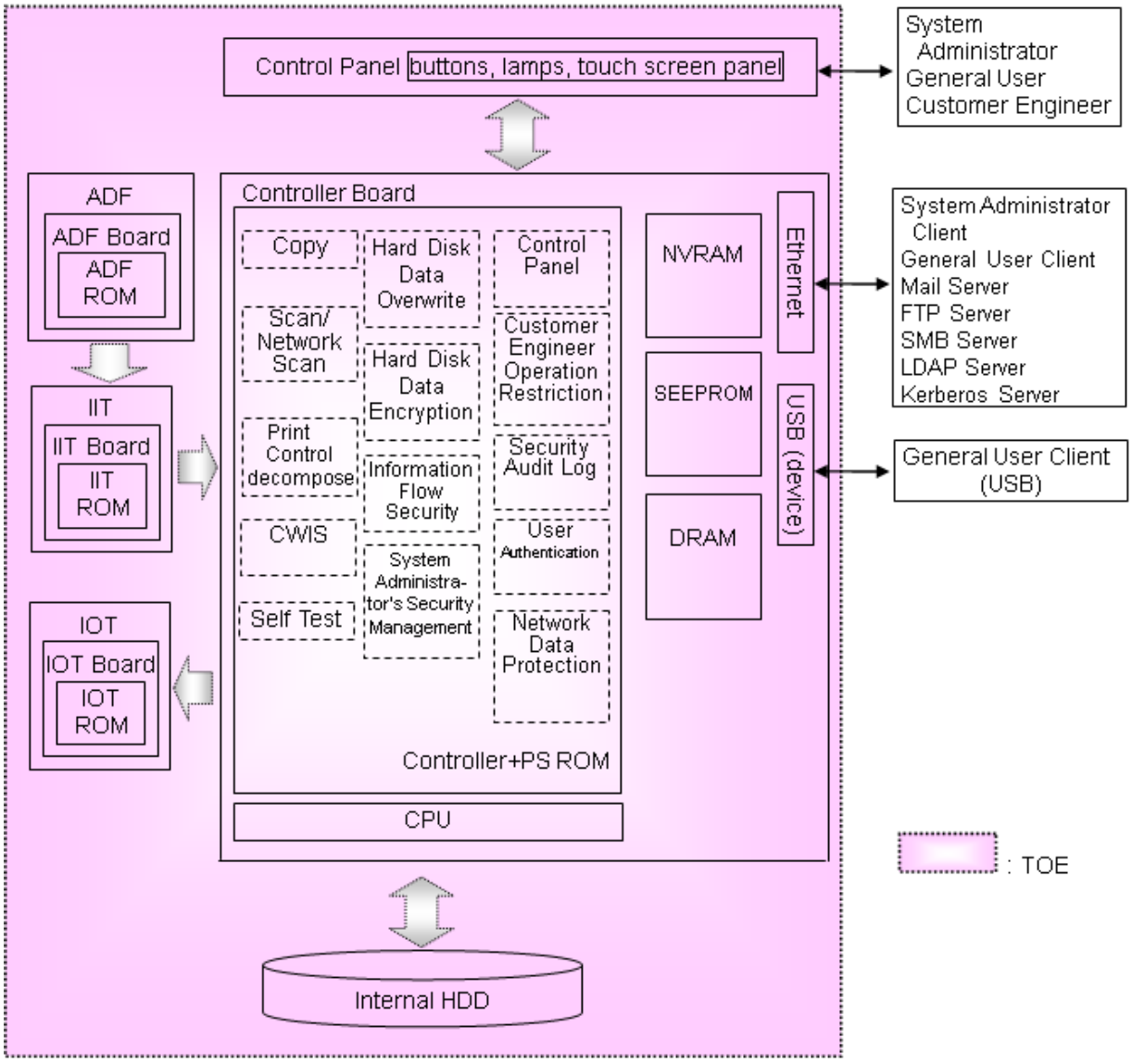

Figure 5.1 TOE boundary

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

When a user uses basic TOE functions such as copy, print, scan, and network scan, 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 function to store copy data 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.

3) 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 by using the scan function 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.

4) Internal HDD data protection

In the above cases 1) to 3), 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.

5) Network protection

In the above cases 1) to 3), 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.

6) Generation of audit logs

The Security Audit Log function generates audit logs when security functions are used in the above cases 1) to 3), and when the establishment of encryption communication protocol fails in the above case 5).

5.2 IT Environment

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

For various servers and clients that are connected to the MFD via the internal network, the TOE communicates using various encryption communication protocols. First of all, the TOE uses IPSec for these servers and clients. Furthermore, SSL/TLS is used for web browser of clients, S/MIME is used for mails transmitted with Mail server, and SNMPv3 is used for network management. When the TOE communicates with the authentication server, LDAP (SSL/TLS) protocol and Kerberos protocol are used to encrypt the data related to identification and authentication.

6. Documentation

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

- Xerox D95/D110/D125/D136 Copier/Printer User Guide
  (Version 3.0, September 2013)

- Xerox D95/D110/D125/D136 Copier/Printer System Administration Guide
  (Version 3.0, September 2013)

- Xerox D136 Copier/Printer Security Function Supplementary Guide
  (Version 1.0, September 2013)

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 were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.2 Overview of Evaluation Activity

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

The evaluation has started on 2013-04 and concluded upon completion of the Evaluation Technical Report dated 2013-10. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2013-07, 2013-08 and 2013-09, and examined procedural status conducted in relation to each work unit for configuration management, delivery and development security, 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 conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2013-08.

7.3 IT Product Testing

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

7.3.1 Developer Testing

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

1) Developer Testing Environment

Figure 7-1 shows the testing configuration performed by the developer.

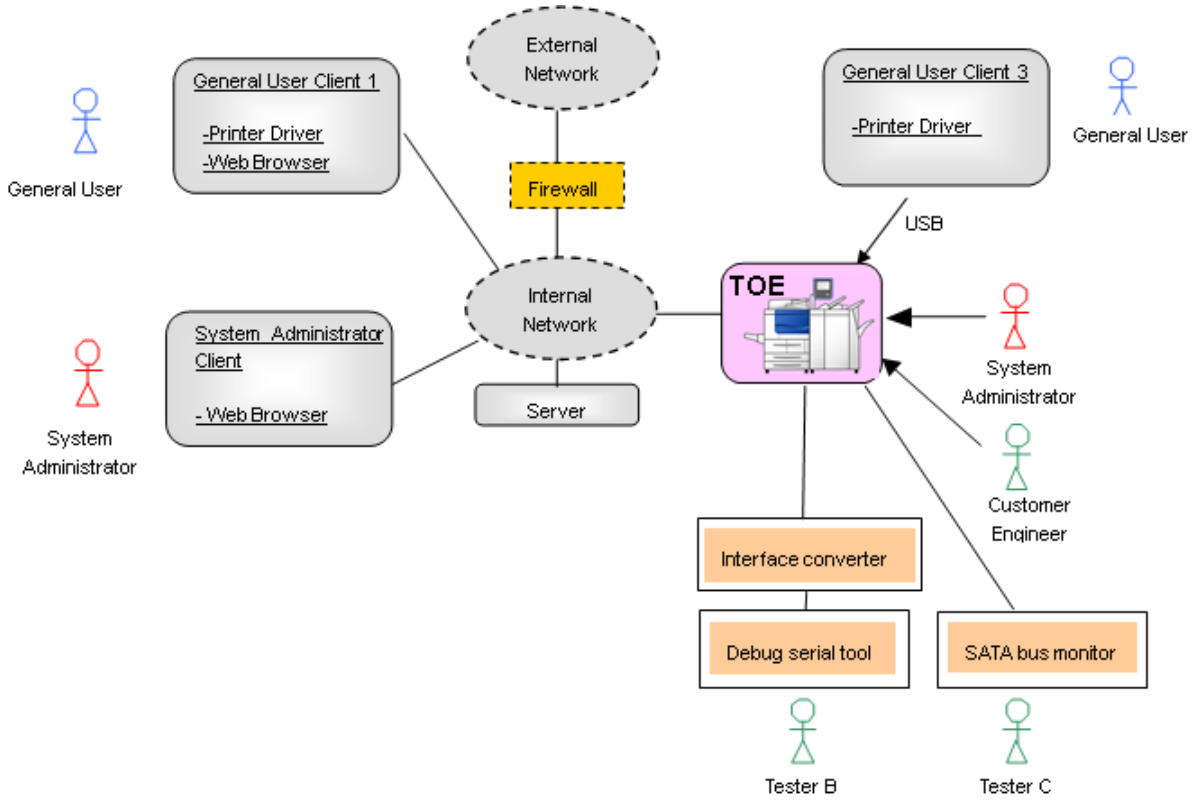

Figure 7-1 Configuration of the Developer Testing

The TOE tested by the developer is Xerox D136 Copier/Printer, and is the same TOE as in TOE identification of Chapter 2.

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

Table 7-1 Configuration Items for the Developer Testing

Items	Description
Server	Used as various servers. The testing is performed with the following two models a) PC with Microsoft Windows Server 2008 R2 - Mail Server: Xmail Version 1.27 - FTP/SMB/LDAP servers: Standard software in OS b) PC with Microsoft Windows Server 2012 - Kerberos server: Standard software in OS
System Administrator Client	Used as system administrator client. The testing is performed with the following three models. a) PC with Microsoft Windows 7 professional SP1 (Web browser: Internet Explorer 8) b) PC with Microsoft Windows XP professional SP3 (Web browser: Internet Explorer 6) c) PC with Microsoft Windows VISTA business SP2 (Web browser: Internet Explorer 7)
General User Client 1	Used as general user client (connected via internal network). The testing is performed with the following three models. a) PC with Microsoft Windows 7 professional SP1 (Web browser: Internet Explorer 8) b) PC with Microsoft Windows XP professional SP3 (Web browser: Internet Explorer 6) c) PC with Microsoft Windows VISTA business SP2 (Web browser: Internet Explorer 7) Additionally, the following software is used. - Printer driver: PCL6 5.303.15
General User Client 3	Used as general user client (connected via USB port for printer). - PC with Microsoft Windows XP professional SP3 - Printer driver: PCL6 5.303.15
SATA Bus Monitor	A tool to monitor the SATA bus data transferred to and from the internal HDD. - PC with Windows XP to which the dedicated device, ST2-32-2-A by Catalyst Enterprises, is connected - Dedicated software: Serial ATA Analyzer V1.984.0401
Debug Serial	Debugging terminal of the MFD, i.e. PC whose serial port is connected to the terminal port of the MFD for debugging via interface converter. - PC with Windows XP professional - Software: Tera Term Pro Version 2.3
Interface converter	Fuji Xerox-unique conversion board to connect the MFD and debug serial.

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

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

2) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

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

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

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

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

(5) To confirm the encryption communication protocol function such as IPSec, use the testing tools to be described later and check that the encryption communication protocol is used as specified.

<Developer Testing Tools>

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

Table 7-2 Developer Testing Tools

Tool Name	Outline and Purpose of Use
SATA Bus Monitor (PC and dedicated device) * See Table 7-1 for configuration.	Monitor the data in SATA bus for connecting the internal HDD in the MFD, and check the data to be written to the internal HDD, and also read out the data written in the internal HDD.

Protocol Analyzer (Wireshark Version 1.8.2)	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 and Interface Converter * See Table 7-1 for configuration.	Read out the data written on the internal HDD and check the contents.

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

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

b. Scope of the Performed Developer Testing

The developer testing was performed on 63 items by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested. By the depth analysis, it was verified that all the subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

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

7.3.2 Evaluator Independent Testing

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

1) Independent Testing Environment

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

Although the testing tools such as the developer's proprietary debug environment (debug serial and interface converter) are the same as those used in the developer testing, the validity verification and operation tests for the testing tools were performed by the evaluator.

2) Summary of the Independent Testing

A summary of the Independent testing is as follows.

a. Viewpoints of the Independent Testing

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

<Viewpoints of the Independent Testing>

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

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

b. Independent Testing Outline

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

<Independent Testing Approach>
The evaluator used the same method as the developer testing and performed the same testing and the testing with changed parameters.

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

<Content of the Performed Independent Testing>
The evaluator performed the sampling testing of 49 items and the additional testing of 7 items, based on the viewpoints of the independent testing.

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

Table 7-3 Major Independent Testing Performed

Viewpoint	Outline of the Independent Testing
Viewpoint (1)	Confirm that the behavior of the TOE is as specified when the entry for changing or entering passwords exceeds the limit values.
Viewpoint (1)	Confirm that access control to Mailbox for system administrators is as specified.
Viewpoint (1)	Test whether or not the account lock is performed as specified, and also test whether the account lock is performed as specified even when different user accounts exist.
Viewpoint (1)	Confirm that the behavior of the TOE is as specified when users who own document data are unregistered while their document data exist in the TOE.

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.3.3 Evaluator Penetration Testing

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

1) Summary of the Penetration Testing

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

a. Vulnerability of Concern

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

(1) There is a concern corresponding to the TOE regarding the publicly available vulnerability information, such as the possibility of unauthorized use of network service, various vulnerabilities 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 document data as protected assets become inconsistent when multiple users access the document data in Mailbox, from the analysis of vulnerability on the provided evidence.

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

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

b. Penetration Testing Outline

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

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

Table 7-4 Penetration Testing Tools

Tool Name		Purpose of use
PC for Penetration Testing		Client with Windows XP, Windows Vista or Windows 7, which operates the following penetration testing tools.
	Nmap Ver.6.25	A tool to detect available network service ports.
	Fiddler2 V2.4.4.5	A tool to refer to and change the communication data between web browser (Client) and web server (TOE). The tool enables to send any data to web server without any restriction of web browser by using Fiddler2.
	ContentsBridge Utility Version 7.3.0	Printer software for PC by Fuji Xerox.

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

Table 7-5 Outline of the Penetration Testing

Vulnerability	Penetration Testing Outline
(1)	- Executed Nmap for the TOE and confirmed that the open port cannot be misused. - Conducted various entries to web server (TOE) using web browser and 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, it 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 the operation by others when multiple users access document data in Mailbox.
(6)	- Confirmed that operation is rejected during initialization processing of the MFD right after the power-on. - Confirmed that an error is displayed and the MFD cannot be used when the power is turned on while the battery for the system clock of the MFD has run down.

c. Result

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

7.4 Evaluated Configuration

TOE configuration conditions for this evaluation are described in the guidance "Xerox D136 Copier/Printer Security Function Supplementary Guide". To enable security functions of the TOE and use them safely, system administrators need to configure the TOE settings to satisfy the configuration conditions as described in the guidance.

In addition to the settings that are required to enable security functions, there are other settings for the TOE as described below.

- Customer Engineer Operation Restriction: [Enabled]
- Store Print: [Save as Private Charge Print]
- Network Scan utility (WebDAV setting): [Disabled]

If these setting values are changed to the values different from those specified in the guidance, the configuration will not be assured by this evaluation.

Furthermore, the TOE does not include the optional functions of printing from USB and storing to USB, which are sold separately. The configuration of the TOE with these functions added will not be assured by this evaluation.

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 following were confirmed.

- PP Conformance:
  2600.1, Protection Profile for Hardcopy Devices, Operational Environment A
  (IEEE Std 2600.1-2009)

  The TOE also conforms to the following SFR packages 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-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: Conformant

- 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
- Additional assurance component ALC_FLR.2

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

7.6 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 during the evaluation process.

1. The submitted evidential materials were sampled, the contents were examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

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

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

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report and related evaluation deliverables, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 augmented with ALC_FLR.2 in the CC Part 3.

8.2 Recommendations

Procurement personnel who are interested in this TOE need to consider whether the scope of evaluation and the operational requirements of this TOE satisfy the operational conditions that they assume, by referring to the descriptions in "1.1.3 Disclaimers", "4.3 Clarification of Scope", and "7.4 Evaluated Configuration".

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

When using the copy and print functions of the TOE, operation from the control panel is required to output printed documents. However, document data stored by using scan function 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.

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 administrators 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 as a separate document along with this Certification Report.

Xerox D136 Copier/Printer Security Target, Version 1.0.3, August 23, 2013, Fuji Xerox Co., Ltd.

11. Glossary

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

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

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

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

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

Control Panel Function:	Control panel function is a user interface function for general user, system administrator, and CE to operate MFD functions.
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. Also, the data can be stored in Mailbox for reprint (the function to store copy data). The stored document data can be edited and printed from the control panel.
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 the data.
Customer Engineer (CE):	Customer service engineer who maintains and repairs the MFD.
CWIS Function:	CWIS is a service via the Web browser of the user client, to confirm the status of the TOE, change settings of the TOE, and request the TOE to retrieve and print the documents.

General User:	Any person who is allowed to use basic MFD functions of the TOE, such as copy, print, and scan.
Job Flow:	Job Flow is a feature for executing a series of registered actions such as sending documents scanned by the scan function to FTP server, Mail server, or SMB server and printing the scanned documents.
Job Flow Sheet:	Information required for the Job Flow function. A series of registered actions (a registered flow) to the device, such as the delivery process and destination of document data.
Key Operator:	Key operator is a system administrator who can use all the management functions.
Mailbox:	A logical box in the MFD to store the document data scanned by the scanner function or the function to store the copy data.
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, Mail server, and SMB server according to the setting of the MFD.
Normal Print:	In normal print, the data are printed out immediately when the MFD receives the data. See the description of "Print Function".
Print Function:	Print function is to print out the data from IOT, which are sent to the MFD from printer driver or web browser of 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.
Private Print:	An area in the MFD to store print data sent from a general user client to the MFD.
SA:	SA is a system administrator who can use a part of management functions. The role of SA is set by key operator as required by the corresponding organization.
Scan Function:	Scan function is to read the original data from IIT and then store them into the Mailbox inside the MFD according to the general user's instruction from the control panel. The stored document data can be retrieved via the control panel or Web browser.
Store Print:	In store print, the print data are 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 Owner:	Any person or organizational entity responsible for protecting TOE assets and establishing related security policies for the TOE operating environment.
TSF Confidential Data:	Among the data used for security functions, the data whose integrity and confidentiality are required.
TSF Protected Data:	Among the data used for security functions, the data whose integrity only is required.
User Document Data:	Document data of users. All the data including image information that are passed through the MFD when general users use MFD functions such as copy, print, and scan.
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.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme, March 2012, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, April 2013, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of Evaluation Facility, April 2013, Information-technology Promotion Agency, Japan, CCM-03

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

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

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

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

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

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

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

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

[12] Xerox D136 Copier/Printer Security Target, Version 1.0.3, August 23, 2013, Fuji Xerox Co., Ltd.

[13] Xerox D136 Copier/Printer Evaluation Technical Report, Version 1.3, October 24, 2013, 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