# Certification Report

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

**IT Product (TOE)**

| | |
|---|---|
| Reception Date of Application (Reception Number) | 2017-09-04 (ITC-7651) |
| Certification Identification | JISEC-C0619 |
| Product Name | Xerox D136 Copier/Printer |
| Version and Release Numbers | Controller+PS ROM Ver. 1.200.15 |
| Product Manufacturer | Fuji Xerox Co., Ltd. |
| Evaluation Sponsor | Xerox Corporation |
| Conformance of Functionality | PP conformant functionality, CC Part 2 Extended |
| Protection Profile Conformance | U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009) |
| Assurance Package | EAL2 Augmented by ALC_FLR.2 |
| Name of IT Security Evaluation Facility | Information Technology Security Center, Evaluation Department |

This is to report that the evaluation result for the above TOE has been certified as follows.
2018-09-28

Tatsuro Yano, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

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

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

**Evaluation Result: Pass**

"Xerox 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

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. 1.200.15" (hereinafter referred to as the "TOE") developed by Fuji Xerox Co., Ltd., and the evaluation of the TOE was finished on 2018-09-21 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Xerox Corporation, and provide security information to procurement entities and consumers who are interested in the TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") described in Chapter 10. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

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

## 1.1 Product Overview

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

### 1.1.1 Assurance Package

Assurance Package of the TOE is EAL2 augmented by ALC_FLR.2.

### 1.1.2 TOE and Security Functionality

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

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

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

#### 1.1.2.1 Threats and Security Objectives

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

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

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

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

#### 1.1.2.2 Configuration and Assumptions

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

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

### 1.1.3 Disclaimers

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

1) The following operations are not guaranteed in this evaluation:
- Use of the maintenance function for customer engineers, and operations after those functions are used.
- Use of the PostScript on the print function.

## 1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2018-09, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

## 1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and the Observation Report prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

## 2. Identification

The TOE is identified as follows:

| | | |
|---|---|---|
| TOE Name: | Xerox D136 Copier/Printer | |
| TOE Version: | Controller+PS ROM | Ver. 1.200.15 |
| Developer: | Fuji Xerox Co., Ltd. | |

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

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

- Model name: Xerox D136

- Version of Controller+PS ROM

# 3. Security Policy

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

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

When those MFD functions are used, the TOE provides security functions that fulfill the security functional requirements required by the Protection Profile for MFDs, U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009) [14][15] (hereinafter referred to as the "PP"). The security functions that the TOE provides include identification/authentication and access control of users, encryption of the document data stored in HDD, data overwrite at deleting the document data in HDD, and encryption communication. The TOE prevents the user's document data and the setting data affecting security that are assets to be protected from being disclosed or altered by unauthorized persons.

The TOE assumes the following user roles:

- General User
  Any person who uses the basic MFD functions, such as copy, print, scan, and network scan, 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 job to be processed by the TOE.

- 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 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 excluding TSF Confidential Data. For example, TSF Protected Data include user IDs, information on user permission for the basic functions, information on the owners of document data, etc.

## 3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Section 3.1.1, and to satisfy the organizational security policies shown in Section 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. Details of each security function are described in Chapter 5.

1) Countermeasures against threat "T.DOC.DIS," "T.DOC.ALT" and "T.FUNC.ALT"

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

The User Authentication function of the TOE is to allow only identified and authenticated users to use the TOE. When successfully identified and authenticated users attempt to use MFD's basic functions such as copy, print, scan, and network scan, the TOE checks the identification information of authorized users set for each basic function of the MFD and allows only authorized users to use them. In addition, when users who are permitted to use the basic functions of the MFD attempt to manipulate user data, the TOE allows only users with access rights to access the data.

The Hard Disk Data Overwrite function of the TOE is to overwrite the internal HDD area where the document data are stored when the data are deleted. This function prevents the residual information of the deleted document data from being read out.

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

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

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

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

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

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

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

### 3.1.2 Organizational Security Policies and Security Function Policies

#### 3.1.2.1 Organizational Security Policies

Organizational security policies required in use of the TOE are shown in Table 3-2. These organizational security policies are the same as those described in the PP, except that P.CIPHER is added.

Table 3-2 Organizational Security Policies

| Identifier | Organizational 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. |
| P.CIPHER | To prevent unauthorized reading-out, the document data in the internal HDD will be encrypted by the TOE. |

#### 3.1.2.2 Security Function Policies to Organizational Security Policies

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

1) Means of organizational security policy "P.USER.AUTHORIZATION"

The TOE realizes this policy by the User Authentication function.

The User Authentication function of the TOE is to allow only identified and authenticated users to use the TOE. When successfully identified and authenticated users attempt to use MFD's basic functions such as copy, print, scan, and network scan, the TOE checks the identification information of authorized users set for each basic function of the MFD and allows only authorized users to use them.

2) Means of organizational 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+PS 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 of organizational 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 record security relevant events as audit logs. Only identified and authenticated system administrators can read out the stored audit logs. It is not possible to delete and modify the audit logs.

4) Means of organizational 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 is to allow 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 external interfaces of the TOE cannot be transferred to the internal network unless the data are processed by the TOE, thereby preventing unauthorized data transfer from external interfaces to the internal network.

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

The TOE realizes this policy by the Hard Disk Data Encryption function.

The Hard Disk Data Encryption function of the TOE is to encrypt data to be written to the internal HDD. The cryptographic algorithm is 256-bit AES.

# 4. Assumptions and Clarification of Scope

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

## 4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. 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 | 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 Environmental Assumptions

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

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

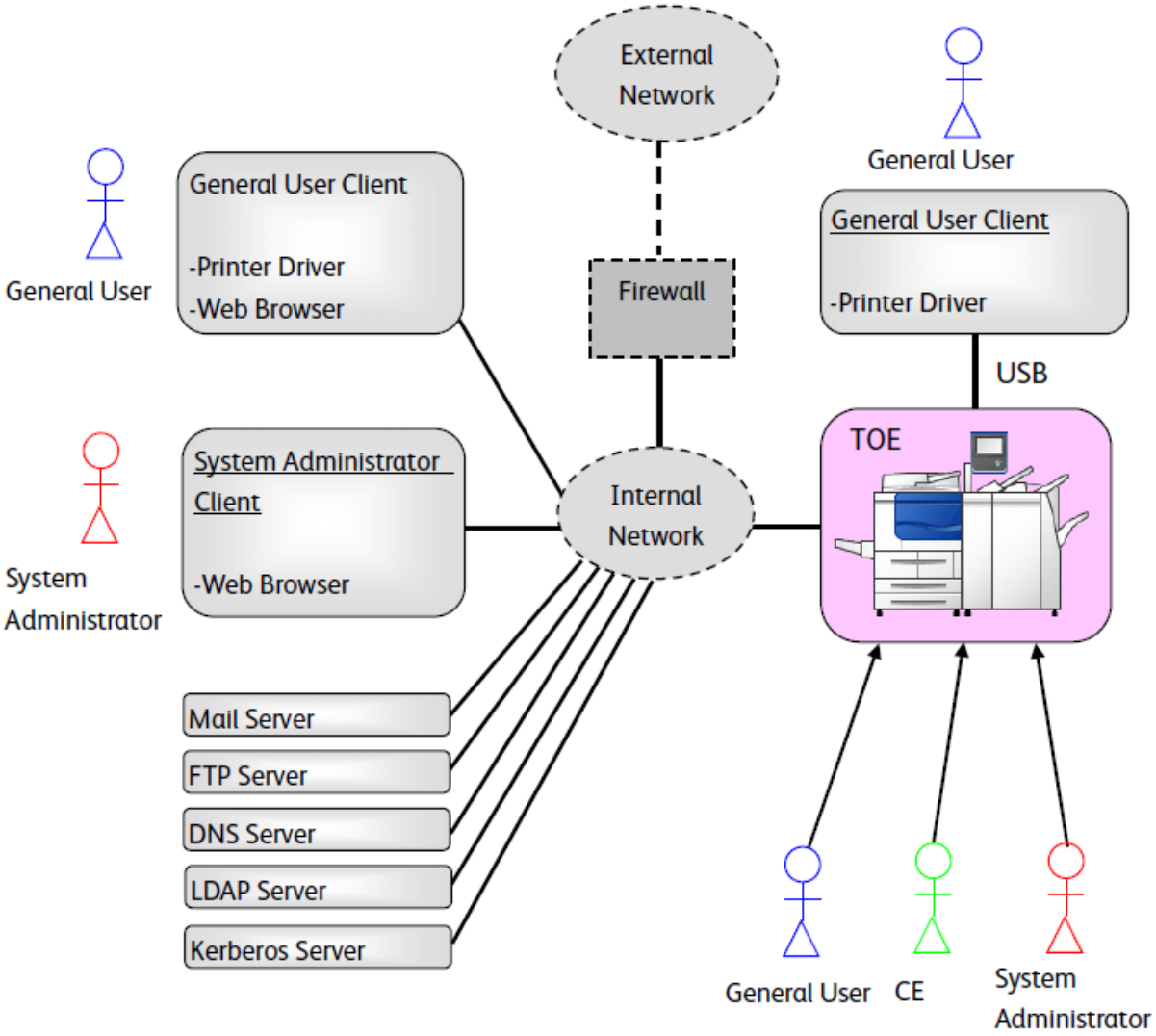


**Figure 4-1 Operational Environment of the TOE**

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

1) General User Client

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

- OS: Windows 7 or Windows 8.1
- Printer driver:
  PCL6 Driver - 64bit, Xerox User Interface - Microsoft Certified

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

- Web browser (included with OS)

2) System Administrator Client

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

connected to the TOE via the internal network. The following software is required:

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

3) LDAP Server, Kerberos Server

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

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

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

- Windows Active Directory

4) Mail Server, FTP Server

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

5) DNS Server

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

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

## 4.3 Clarification of Scope

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

1) Restrictions for Remote Authentication

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

2) IPsec for IPv6

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

3) Printer driver for PostScript

The TOE was evaluated with only PCL6 printer Driver. The operation with Postscript Printer Driver is not assured by this evaluation.

# 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 components of the TOE. The scope of the TOE is the MFD.

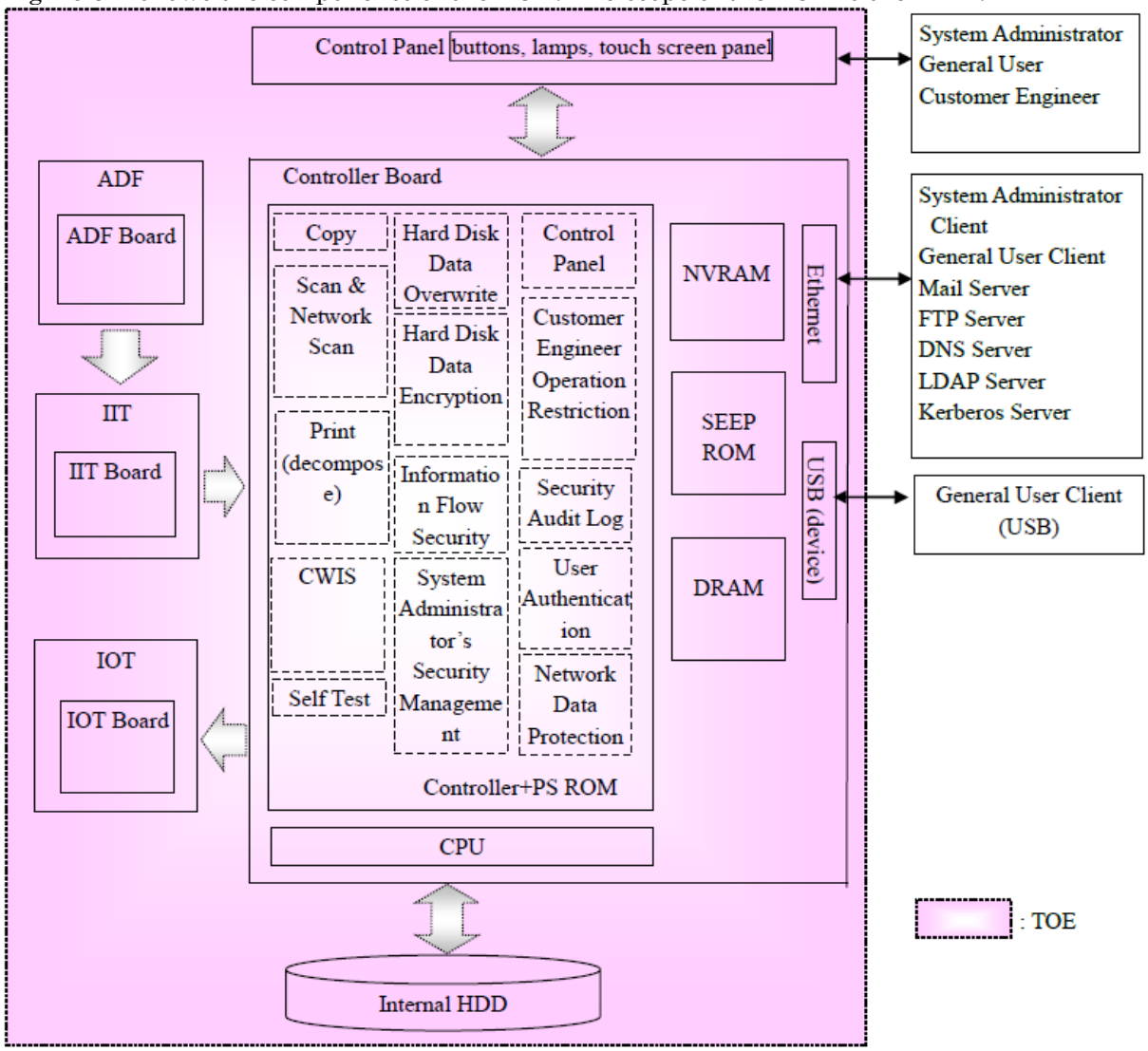


**Figure 5.1 Components of the TOE**

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

1) User Authentication

This function includes the following three functions: identification and authentication of users, access control for MFD's basic functions, and access control for user data.

a) Identification and authentication of users

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

- Control panel
- Client PCs (Web browsers, printer drivers)

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

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

- For Local Authentication, users are required to use passwords of nine or more characters.
- For Local Authentication, if a system administrator fails to be authenticated for five times in a row, the authentication process is suspended. This restriction is not applied to general users.
- If no user operation is confirmed for a specified amount of time after a user has been successfully authenticated, the session is terminated.

b) Access control for MFD's basic functions

This is the function to restrict the use of the MFD's basic functions such as copy, scan, network scan, and print.

When a user attempts to use a MFD's basic function, the TOE refers to the identification information of authorized users set for each basic function of the MFD and determines whether to restrict or allow the use of the function.

c) Access control for user data

This is the function to restrict the access to document data and job information used in MFD's basic functions to only authorized users.

As to the document data stored in the Mailbox or the Private Print, or the job information, only the user who is verified to be the owner of the data can perform operations on the document data or job information.

As to the document data generated in the process of the network scan function, only those users who performed the functions are allowed to send the data via network. No access means to such data is provided to other users.

2) System Administrator's Security Management

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

3) Customer Engineer Operation Restriction

This is the function with which system administrators restrict the operation by customer engineers. Only identified and authenticated system administrators are permitted to

refer to and change the setting data that control enabling and disabling of customer engineer operation restriction. If customer engineer operation is restricted, customer engineers are required to enter the password set by a system administrator in order to operate the MFD.

4) Security Audit Log

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

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

5) Hard Disk Data Encryption

This is the function that encrypts data to be stored in the internal HDD. The cryptographic algorithm is 256-bit AES. A cryptographic key is generated upon booting the TOE using the proprietary algorithm of Fuji Xerox Co., Ltd., based on the cryptographic seed key of 12 alphanumeric characters set by system administrators when the TOE is installed. The same value of the cryptographic key is generated every time the power is turned on and stored in the volatile memory, while it is deleted when the power is turned off.

6) Hard Disk Data Overwrite

This is the function that overwrites the internal HDD area where document data were stored when the data are deleted. This overwrite operation is performed in the following cases.

- When document data have become unnecessary after a user finishes using MFD's basic functions. Unnecessary data include those temporarily generated in the TOE while the TOE is executing some processing.

- When a user has requested to delete document data.

- When the power of the MFD is turned on. If the overwrite operation has not been completed when the power is turned off, the operation resumes when the power is turned on.

- When "On Demand Overwrite function" is executed; the function deletes the stored data at the specified time according to the setting by a system administrator.

System administrators can select one pass overwrite (overwriting with zero) or three pass overwrite (overwriting with a random number, a random number, and zero). It should be noted that the data actually overwritten on the internal HDD are encrypted. Therefore, the data actually overwritten is different from the overwrite pattern.

7) Internal Network Data Protection

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

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

8) Information Flow Security

This is the function that prevents unauthorized data transfer from external interfaces to the internal network. Data received from external interfaces of the TOE cannot be transferred to the internal network unless the data are processed by the TOE.

9) Self Test

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

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

## 5.2 IT Environment

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

# 6. Documentation

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

- Xerox D95/D110/D125/D136 Copier/Printer
  System Administration Guide; Version 3.1 January 2014
  (SHA256 hash value:
  16e971b5953d5fa38676016260cf0aed61a14f291fdbf2543056bad01c0a42b1)

- Xerox D95/D110/D125/D136 Copier/Printer
  User Guide; Version 3.0 September 2013
  (SHA256 hash value:
  4524d4c91d5002b543dd1ebe4bc0310c7704db8146b86198d5fefbc8b73ada6c)

- Xerox D95/D110/D125/D136 Copier/Printer
  Security Function Supplementary Guide; Version 1.0 September 2018
  (SHA256 hash value:
  0a4b5a995a9b414b354bfde243842f80fff4f89be79b3ebed2734cdea0decce2)

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

# 7. Evaluation conducted by Evaluation Facility and Results

## 7.1 Evaluation Facility

Information Technology Security Center, Evaluation Department that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

## 7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

## 7.3 Overview of Evaluation Activity

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

The evaluation started on 2017-09 and concluded upon completion of the Evaluation Technical Report dated 2018-09. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted.

Additionally, the evaluator directly visited the development site on 2017-10, and examined procedural status conducted in relation to each work unit for configuration management and delivery, by investigating records and interviewing staff. For some manufacturing sites, site visits were omitted as the Evaluation Facility determined that the examination details of the past CC-certified products could be reused.

Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2017-10 and 2018-06.

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, it was reflected in the Evaluation Technical Report.

## 7.4 IT Product Testing

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

### 7.4.1 Developer Testing

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

#### 1) Developer Testing Environment

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

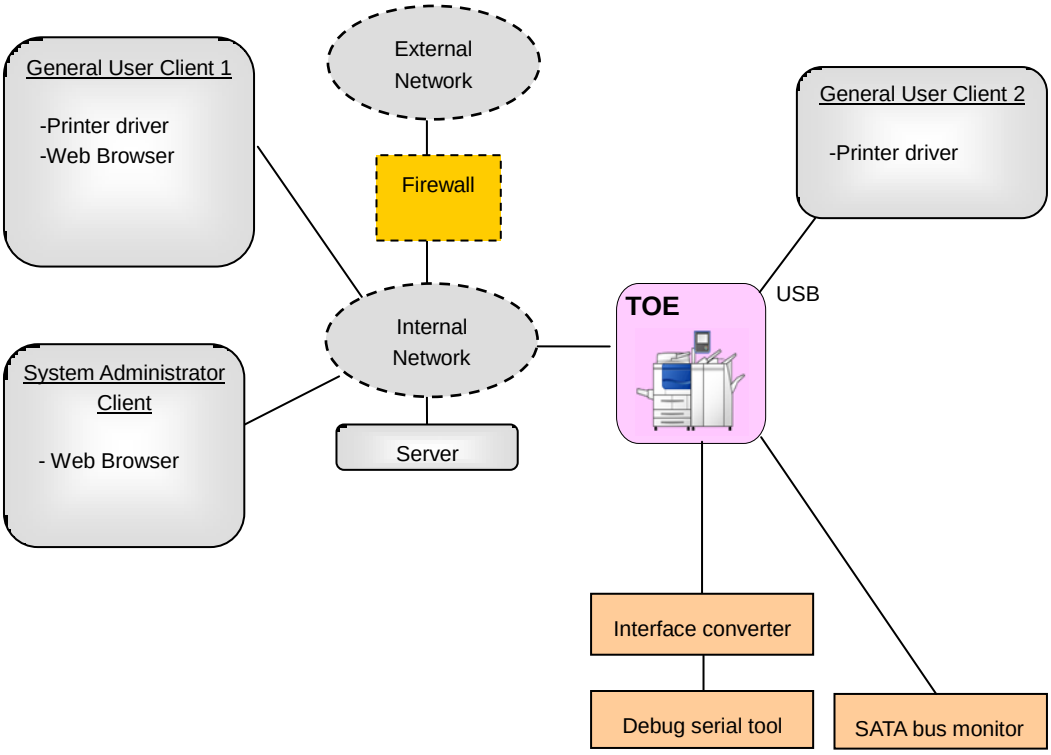


**Figure 7-1 Configuration of the Developer Testing**

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

**Table 7-1 Configuration Items for the Developer Testing**

| Items | Description |
|---|---|
| TOE | Xerox D136 Copier/Printer<br>(Controller+PS ROM Ver. 1.200.15) |
| Server | Used as various servers.<br>- PC with Microsoft Windows Server 2008 R2 SP1<br>- Mail server: Xmail Version 1.27<br>- FTP server: Standard software in OS<br>- DNS server: Standard software in OS<br>- LDAP server: Standard software in OS<br>- Kerberos server: Standard software in OS |
| System Administrator Client | Used as system administrator client.<br>The testing is performed with the following two models:<br>a) PC with Microsoft Windows 7 Professional SP1<br>(Web browser: Microsoft Internet Explorer 11)<br>b) PC with Microsoft Windows 8.1<br>(Web browser: Microsoft Internet Explorer 11) |
| General User Client 1 | Used as general user client (connected via internal network).<br>The testing is performed with the following two models:<br>a) PC with Microsoft Windows 7 Professional SP1<br>(Web browser: Microsoft Internet Explorer 11)<br>b) PC with Microsoft Windows 8.1<br>(Web browser: Microsoft Internet Explorer 11)<br><br>Additionally, the following software is used.<br>- Printer driver: PCL6 Driver - 64bit, Xerox User Interface - Microsoft Certified Version 5.337.3 |
| General User Client 2 | Used as general user client (connected via USB port for printer).<br>- PC with Microsoft Windows 8.1<br>- Printer driver: PCL6 Driver - 64bit, Xerox User Interface - Microsoft Certified Version 5.337.3 |
| SATA Bus Monitor | A tool to monitor the SATA bus data transferred to and from the internal HDD.<br>- PC with Microsoft Windows 7 Professional SP1 to which the dedicated device,<br>ST2-31-2-A by Catalyst Enterprises, is connected<br>- Dedicated software: stx sata protocolsuite V4.20 |
| Debug Serial | Debugging terminal of the MFD; i.e., PC whose serial port is connected to the terminal port of the MFD for debugging via interface converter.<br>- PC with Microsoft Windows 7 Professional SP1<br>- Terminal Software: Tera Term Pro Version 2.3 |
| Interface converter | Fuji Xerox-unique conversion board to connect the MFD and debug serial. |

The TOE tested by the developer has the same TOE identification of Chapter 2.

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

### 2) Summary of the Developer Testing

A summary of the developer testing is as follows.

#### a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

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

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

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

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

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

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

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

<Developer Testing Tools>

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

**Table 7-2 Developer Testing Tools**

| Tool Name | Outline and Purpose of Use |
|---|---|
| SATA Bus Monitor<br>(PC and dedicated device)<br>* 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<br>(Wireshark<br>Version 1.10.6) | Monitor the communication data on the internal network, and confirm that the encryption communication protocol is IPsec or TLS as specified. |

| | |
|---|---|
| Mailer<br>(Microsoft Windows Live Mail 2011) | Transmit E-mails with the TOE via Mail server, and confirm that the encryption and signature by S/MIME are as specified. |
| HTTP debugger<br>(Fiddler 2.4.7.1) | A tool to mediate the communication between a Web browser (client PC) and a Web server (MFD) and to refer to and change the data communicated between them. |
| Debug Serial and Interface Converter<br>* See Table 7-1 for configuration. | Read out the data written on the internal HDD and check the contents. |
| Nmap Ver.7.31 | A tool to detect available network service ports. |

<Content of the Performed Developer Testing>

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

The variations of the input parameters include the rewrite of communication data between web browsers and the TOE, and power-on/off of the TOE while document data is overwritten.

b. Scope of the Performed Developer Testing

The developer testing was performed on 78 items by the developer.

By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been tested.

c. Result

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

### 7.4.2 Evaluator Independent Testing

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

### 1) Independent Testing Environment

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

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

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

### 2) Summary of the Independent Testing

A summary of the Independent testing is as follows.

#### a. Viewpoints of the Independent Testing

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

<Viewpoints of the Independent Testing>

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

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

#### b. Independent Testing Outline

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

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

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

<Content of the Performed Independent Testing>
The evaluator performed the sampling testing of 59 items and the additional testing of 6 items, based on the viewpoints of the independent testing.

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

**Table 7-3 Major Independent Testing Performed**

| Viewpoint | Outline of the Independent Testing |
|---|---|
| Viewpoint (1) | Confirm that the user roles and account lock are as specified when the Remote Authentication is used. |
| Viewpoint (1) | Confirm that the behavior of the TOE is as specified when users who own document data are unregistered while their document data exist in the TOE. |
| Viewpoint (1) | Confirm that the TOE accepts print jobs as the Store Print, even if an option other than the Store Print is specified for the print jobs from the printer driver. |
| Viewpoint (1) | Confirm that the restriction of the length, etc of an ID and password is as specified when it is set for not only a general user but also key operator. |

c. Result

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

### 7.4.3 Evaluator Penetration Testing

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

#### 1) Summary of the Penetration Testing

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

a. Vulnerability of Concern

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

(1)There is a concern that known vulnerabilities may exist in the network interfaces.

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

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

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

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

b. Penetration Testing Outline

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

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

**Table 7-4 Penetration Testing Tools**

| Tool Name | Outline and Purpose of Use |
|---|---|
| Nmap<br>Version 6.47 | A tool to detect available network service ports. |
| netcat<br>Version 1.11 | A tool to transfer data to network ports. |
| Fiddler<br>4.6.20173.34691 | A tool to mediate the communication between Web browser and Web server (TOE), which refers to and changes the communication data between them. |
| OWASP ZAP<br>Version 2.6.0 | A tool to inspect vulnerabilities of the Web application. |
| SSLScan<br>Version 1.8.2 | A tool to check whether SSL/TLS cipher suites are supported or not. |
| Metasploit<br>Version 4.6.2 and 4.13.0 | The tool is used for the creation of the testing data to inspect the vulnerabilities caused by PDF files. |
| PRET<br>Version 0.36 | A tool to inspect various vulnerabilities in a printing processing. |

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

**Table 7-5 Outline of the Penetration Testing**

| Vulnerability | Penetration Testing Outline |
|---|---|
| (1) | - Executed Nmap for the TOE and confirmed that the open port cannot be misused.<br><br>- Conducted various entries to Web server (TOE) using OWASP ZAP, Web browser and Fiddler, and confirmed that there is no known vulnerability. |

| | |
|---|---|
| | - Executed SSLScan for the TOE, and confirmed that weak encryption methods are not supported. |
| (2) | - Confirmed that the unauthorized processing is not executed even if print job commands and print files including unauthorized processing are input to the TOE. |
| (3) | - Confirmed that the character of out-of-spec length, character code, and special key cannot be entered from the control panel. |
| (4) | - Confirmed that, other than the intended functions such as print, it cannot be used even when attempting to access the TOE by connecting the client for the penetration testing to each USB port of the TOE. |
| (5) | - Confirmed that operation is rejected during initialization processing of the MFD after the power-on. |

c. Result

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

## 7.5 Evaluated Configuration

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

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

- Customer Engineer Operation Restriction: [Enabled]
- SNMP: [Disabled]
- Print from USB, Store to USB: [Disabled]
- SOAP: [Disabled] (Note: Job Flow function cannot be used because of this setting.)
- Shared Mailbox Creation: [Prohibited]

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

## 7.6 Evaluation Results

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

In the evaluation, the following were confirmed.

- PP Conformance:
  U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

  The TOE also conforms to the following SFR packages defined in the above PP:
  - 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
  - 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
  - 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
  - 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B
  - 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

- 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 EAL2 package
- Additional assurance component ALC_FLR.2

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

## 7.7 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

# 8. Certification

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

1. Contents pointed out in the Observation Report shall be adequate.

2. Contents pointed out in the Observation Report shall properly be solved.

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

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

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

Concerns found in the certification process were prepared as the certification oversight reviews, and those were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the 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 the submitted Evaluation Technical Report, Observation Report and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL2 augmented by ALC_FLR.2 in the CC Part 3.

## 8.2 Recommendations

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

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

When using the print function of the TOE, the print data from the client PC are stored in the TOE, and the operation from the control panel is required to output printed documents. However, document data stored in the Mailbox of the TOE can be output as printed documents by operation from the client PC. Thus, it should be noted that the TOE may not be able to satisfy the needs of procurement entities 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

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

Xerox D136 Copier/Printer EAL2 Security Target, Version 2.1.4, September 20, 2018, Fuji Xerox Co., Ltd.

# 11. Glossary

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

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

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

| | |
|---|---|
| ADF | Auto Document Feeder |
| 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.

| | |
|---|---|
| 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. |
| Customer Engineer (CE): | Customer service engineer who maintains and repairs the MFD. |
| CWIS Function: | CWIS function is a service used by general users and system administrators via the Web browser in order for them to confirm the status of the TOE, change settings of the TOE, and request the TOE to retrieve and print the documents. |
| Job flow: | Job Flow is a function to execute the registered processing to the document data scanned by the scan function, such as sending them to an external server or printing them. This function cannot be used in the evaluated configuration. |
| Key Operator: | Key operator is a system administrator who can use all the management functions. |

| | |
|---|---|
| Mailbox: | An area in the MFD to store the document data scanned by the scan function or the copy function. |
| Network Scan Function: | Network Scan function is to read the original data from IIT according to the general user's instruction from the control panel, and automatically send to FTP server or Mail server according to the setting of the MFD. |
| Print Function: | Print function is to print out the data from IOT, which are sent to the MFD from printer driver of a general user client. The received print data are stored into the Private Print inside the MFD, and printed out according to the general user's instruction from the control panel. |
| 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 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). |

## 12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, July 2018, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, September 2018, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, September 2018, 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 EAL2 Security Target, Version 2.1.4, September 20, 2018, Fuji Xerox Co., Ltd.

[13] Xerox D136 Copier/Printer Evaluation Technical Report, Version 1.8, September 21, 2018, Information Technology Security Center, Evaluation Department

[14] U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

[15] CCEVS Policy Letter #20, 15 November 2010, National Information Assurance Partnership