Certification Report

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

IT Product (TOE)

Reception Date of Application (Reception Number)	2022-02-28 (ITC-2807)
Certification Identification	JISEC-C0766
Product Name	Xerox VersaLink B7135 / B7130 / B7125 with Fax and Disk Overwrite
Version and Release Numbers	Controller ROM Ver. 1.1.16, Fax ROM Ver. 2.2.1
Product Manufacturer	FUJIFILM Business Innovation Corp.
Evaluation Sponsor	Xerox Corporation
Conformance of Functionality	PP conformant functionality, CC Part 2 Extended
Protection Profile Conformance	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)
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.

2022-10-27

YANO Tatsuro, 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 5
- Common Methodology for Information Technology Security Evaluation
  Version 3.1 Release 5

Evaluation Result: Pass

"Xerox VersaLink B7135 / B7130 / B7125 with Fax and Disk Overwrite, Version Controller ROM Ver. 1.1.16, Fax ROM Ver. 2.2.1" 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 VersaLink B7135 / B7130 / B7125 with Fax and Disk Overwrite, Version Controller ROM Ver. 1.1.16, Fax ROM Ver. 2.2.1" (hereinafter referred to as the "TOE") developed by FUJIFILM Business Innovation Corp., and the evaluation of the TOE was completed on 2022-09-30 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 this 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 below. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Protection Profile or Assurance Package

The TOE conforms to the following Protection Profile [14][15] (hereinafter referred to as the "Conformance PP").

Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015
(Certification Identification: JISEC-C0553)

1.1.2 TOE and Security Functionality

The TOE is a multifunction device (hereinafter referred to as "MFD"), which has functions such as copy, scan, print, and fax.

The TOE provides security functions required by the Conformance PP to prevent the document data processed by the MFD and the setting data etc. affecting security from unauthorized disclosure and alteration.

For these security functions, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance requirements of the Conformance PP.

Threats and assumptions assumed for the TOE are described in the following sections.

1.1.2.1 Threats and Security Objectives

The following threats are assumed for the TOE.

There are threats that document data of users and data affecting security functions, which are assets to be protected by the TOE, may be disclosed or altered by unauthorized operation of the TOE or unauthorized access to the network to which the TOE is connected.

There are also threats that security functions of the TOE may be compromised by the failure of the TOE itself or installation of unauthorized software.

The TOE provides security functions required by the Conformance PP such as identification and authentication, access control, encryption, and digital signature to counter these threats.

1.1.2.2 Configuration and Assumptions

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

The TOE is assumed to be operated in an environment where unauthorized physical access to the TOE is restricted and connected to a LAN separated from the Internet.

The setting, administration and maintenance of the TOE must be performed in accordance with the guidance documents by a trusted administrator. Users of the TOE must have been trained in order to use the TOE securely.

1.1.3 Disclaimers

The following operation is not ensured by this evaluation:

- An environment different from that described in "4.2 Environmental Assumptions"
- TOE with settings different from those described in "7.5 Evaluated Configuration"

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 in 2022-09, 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 Reports 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. The Certification Body confirmed that those concerns pointed out by the Certification Body were fully resolved, and 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 and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	Xerox VersaLink B7135 / B7130 / B7125 with Fax and Disk Overwrite
TOE Version:	Controller ROM Ver. 1.1.16, Fax ROM Ver. 2.2.1

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

Users confirm the following information displayed on the control panel of the TOE as described in the guidance document.

- Vendor name: "Xerox"

- Model name: One of the following:
  VersaLink B7135, VersaLink B7130, VersaLink B7125

- Functions:
  Button for fax function is displayed.
  Disk Overwrite function is displayed.

- Version: Version of Controller ROM and FAX ROM

3. Security Policy

The TOE provides the basic functions of the MFD such as copy, scan, print, and fax. It has the functionality to store the user document data in the TOE and to communicate with user terminals and various servers via a network.

The TOE provides security functions that satisfy the requirements of the Conformance PP, to protect the document data processed by the MFD and setting data etc. affecting security.

As the background of the security functions provided by the TOE, the user roles, assets, threats, and organizational security policies assumed for the TOE are described in following Section 3.1 to 3.4. Details of the security functions of the TOE are described in Chapter 5.

3.1 Users

The user roles assumed for the TOE are shown in Table 3-1.

Table 3-1 User Roles

Designation	Definition
Normal User	A User who has been identified and authenticated and does not have an administrative role
Administrator	A User who has been identified and authenticated and has an administrative role

Note that "administrator" is called as "system administrator" in the TOE, so the terms "administrator" and "system administrator" have the same meaning in this report.

3.2 Assets

The assets assumed to be protected by the TOE are shown in Table 3-2, Table 3-3 and Table 3-4. There are two categories of the assets, User Data and TSF Data, as shown in Table 3-2. Furthermore, User Data is classified as shown in Table 3-3 and TSF Data is as shown in Table 3-4.

Table 3-2 Assets

Designation	Category	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF

Table 3-3 Assets (User Data)

Designation	Type	Definition
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job

Table 3-4 Assets (TSF Data)

Designation	Type	Definition
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

3.3 Threats

The threats assumed for the TOE are shown in Table 3-5.

Table 3-5 Threats

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4 Organizational Security Policies

The organizational security policies required for the TOE are shown in Table 3-6.

Table 3-6 Organizational Security Policies

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.

P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.

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 whether to use the TOE.

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE. The effective performances of the TOE security functions are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

4.2 Environmental Assumptions

Figure 4-1 shows the operational environment assumed for the TOE. The TOE is installed in a general office and used in an environment connected to the PSTN and a LAN which is the internal network of the organization. Users operate the control panel of the TOE or a client PC (i.e. General User Client or System Administrator Client) connected to the LAN to use the TOE.

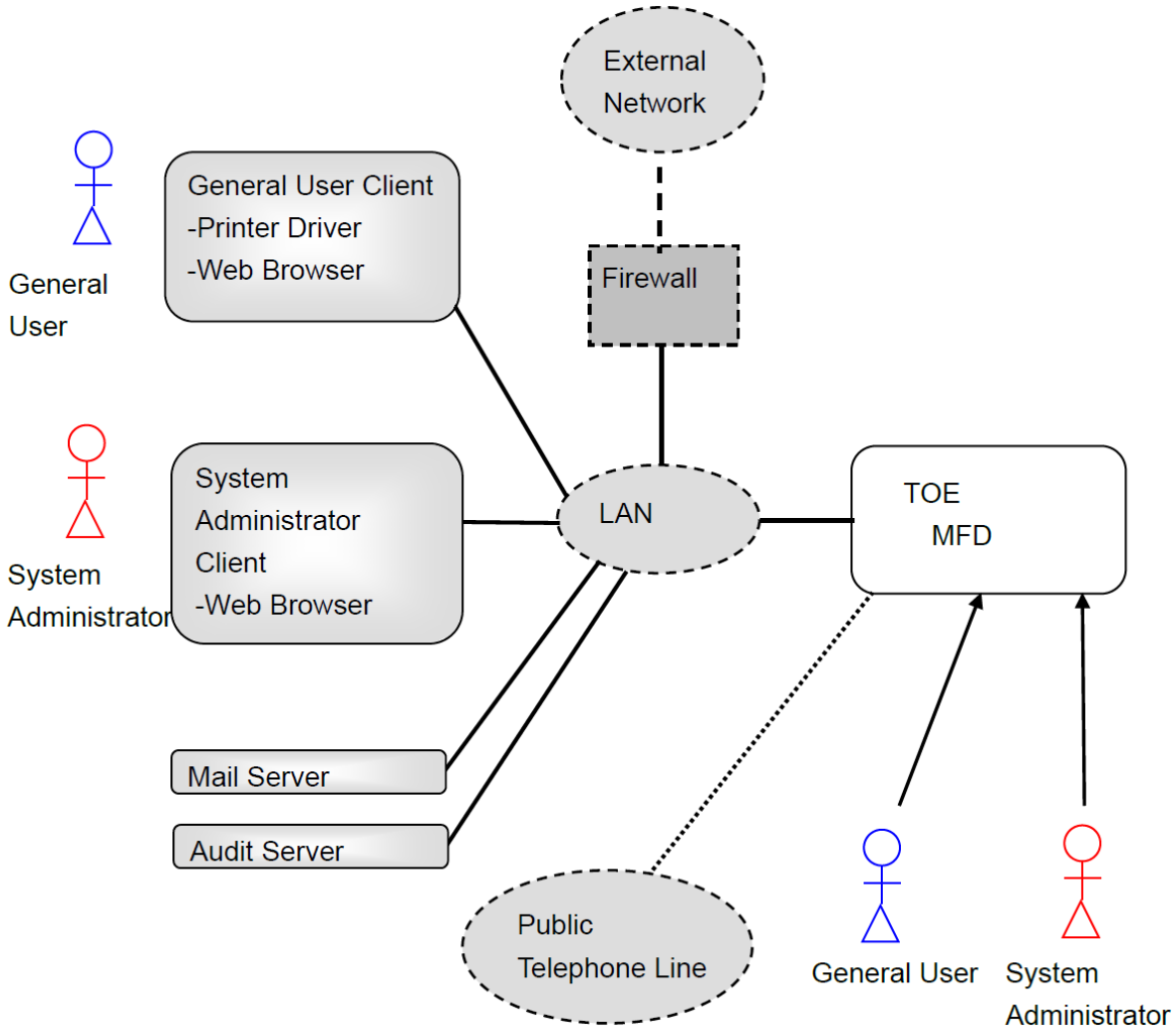

Figure 4-1 Operational Environment of the TOE

The operational environment of the TOE consists of the following components.

1) General User Client

A general user client is a general-purpose PC for general users. The following software is required:

- OS: Windows 10
- Web browser: Microsoft Edge
- Printer driver (Provided by Xerox Corporation)
  PCL6 Print Driver Version:5.860.1.0

2) System Administrator Client

A system administrator client is a general-purpose PC for system administrators. The following software is required:

- OS: Windows 10

- Web browser: Microsoft Edge

3) Mail Server

A mail server is used to send user document data from the TOE. The following software is required:

- Software supporting SMTP protocol with TLS 1.2.
  (Postfix version 2.10.1 was used in this evaluation.)

4) Audit Server

An audit server is a server to store audit logs generated by the TOE. The following software is required:

- OS: Windows 10
- PowerShell script to retrieve audit logs from the TOE (described in the TOE guidance)
- PowerShell Version 5.1 (OS built-in tool)

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

4.3 Clarification of Scope

There are the following restrictions on the security functions provided by the TOE or ensured by this evaluation.

1) Servers and client PCs

System administrators are responsible for operating servers and client PCs cooperating with the TOE securely.

2) Audit server operation

An audit server polls the TOE periodically to read out audit logs stored on the TOE. The TOE sends all the stored audit logs on the polling, regardless of whether they have already been read out. System administrators are responsible for distinguishing newly generated audit logs from duplicated data and extracting necessary audit logs.

5. Architectural Information

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

5.1 TOE Boundary and Components

The TOE is the entire MFD with the necessary option.

The functions provided by the TOE consist of the basic functions of the MFD and the security functions. Regarding the basic functions of the MFD such as copy, scan, print, and fax, please refer to Chapter 11. The security functions of the TOE are described below.

1) Identification and Authentication

This function is to identify and authenticate users of the TOE with their IDs and passwords. This function is applied when the TOE is used as follows:

- When users use the TOE with the control panel of MFD, or Web browser on client PC, or printer driver on client PC. (Only the identification of a user ID is performed when using printer driver on client PC.)

- When an audit server retrieves the audit logs from the TOE. (The ID and password of System Administrator is used.)

This function has the following functionality to strengthen the identification and authentication.

- Restriction on the minimum password length.

- Suspending the identification and authentication on continuous unsuccessful authentication attempts.

- Termination of the session if there is no operation for a certain time after the successful authentication.

2) Access Control

This function is to control the access to the user data when users operate the basic functions of the MFD on them. The access control is based on the owner information of the user data and on the user's identification information and role.

3) Data Encryption

This function is to encrypt the data stored in the TOE and the communication data. The encryption of the stored data uses AES CBC mode with a 256-bit key. The encryption of communication data is used in the encryption communication protocol described in "4) Trusted Communication. "

Encryption keys are generated using a random bit generator with enough entropy that is difficult to guess.

4) Trusted Communication

This function is to protect communication data between the TOE and IT devices using

encryption communication protocol, TLS 1.2.

5) Security Management

This function is to restrict the setting, etc. of the security functions to system administrators. For general users, it permits them to change their own passwords.

6) Security Audit

This function is to generate audit logs on audit events relevant to the security functions and enable an audit server and system administrators to retrieve them.

Generated audit logs are stored in the TOE. When the stored logs exceed the storage capacity, the oldest one is deleted to store a new audit log.

7) Trusted Operation

This function consists of the following functionality:

- Verification of the check sum of the firmware and the correct operation of the random bit generation at start-up of the TOE.

- Verification of the digital signature of new firmware when the firmware is updated.

8) PSTN Fax-Network Separation

This function is to separate the Public Switched Telephone Network (PSTN) and the LAN. It prevents sending and receiving data from the PSTN to the LAN via the TOE.

9) Overwrite Hard Disk

This function is to overwrite the area of the hard disk drive in the TOE where user document data are stored when those data are deleted by completion of the basic function of the TOE or by deletion operation by users, etc.

5.2 IT Environment

The TOE communicates with servers and client PCs via LAN. The function of the TOE described in "4) Trusted Communication" works in cooperation with those IT devices and uses the following protocols:

- Client PC (Web browser): HTTP over TLS
- Client PC (Printer driver): IPP over TLS
- Audit Server: HTTP over TLS
- Mail Server: SMTP over TLS

6. Documentation

The identification of the guidance documents of the TOE is listed in Table 6-1. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

Table 6-1 Guidance

Name	Version
Xerox VersaLink B71XX Multifunction Printer User Guide	Version 1.1
Xerox VersaLink Series Multifunction and Single Function Printers System Administrator Guide	Version 2.0
Xerox VersaLink B7125/B7130/B7135 Quick Use Guide	Rev C
Xerox VersaLink B7135 / B7130 / B7125 Multifunction Printer Security Function Supplementary Guide	Version 1.0 (20220617)

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

The evaluation was conducted in accordance with the assurance requirements in the CC Part 3 required by the Conformance PP using the evaluation methods prescribed in the CEM and the assurance activities of the Conformance PP.

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 for each work unit in the CEM and assurance activity of the Conformance PP.

7.3 Overview of Evaluation Activity

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

The evaluation started in 2022-02 and concluded upon completion of the Evaluation Technical Report dated 2022-09. 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. Furthermore, the evaluator conducted the evaluator testing at the developer site in 2022-05 and 2022-06.

Concerns found in evaluation activities were issued as the Observation Reports and reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

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

7.4 IT Product Testing

As the verification results of the evidence shown in the evaluation process, the evaluator performed the evaluator independent testing to ensure that the security functions of the product are accurately implemented, and the evaluator penetration testing based on vulnerability assessments.

7.4.1 Developer Testing

The developer testing is not included in the assurance requirements of this evaluation.

7.4.2 Evaluator Independent Testing

The evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") based on the evidence shown in the evaluation process to ensure that the security functions of the product are accurately implemented. The independent testing performed by the evaluator is explained below.

1) Independent Testing Environment

The environment for the independent testing is based on the operational environment of the TOE shown in Figure 4-1. The components used in the independent testing environment are shown in Table 7-1.

Table 7-1 Components for the Independent Testing

Components	Description
TOE	Xerox VersaLink B7125 with Fax and Disk Overwrite Version: Controller ROM Ver. 1.1.16, Fax ROM Ver. 2.2.1
	Xerox VersaLink B7135 with Fax and Disk Overwrite Version: Controller ROM Ver. 1.1.16, Fax ROM Ver. 2.2.1
Client PC (General User Client)	- OS: Microsoft Windows 10, Microsoft Windows 10 Professional - Web browser: Microsoft Edge - Printer Driver: PCL6 Print Driver Version:5.860.1.0
Client PC (System Administrator Client)	- OS: Microsoft Windows 10, Microsoft Windows 10 Professional - Web browser: Microsoft Edge
Mail Server	- OS: Cent OS ver7.6 - Postfix version 2.10.1
Audit Server	- OS: Microsoft Windows 10, Microsoft Windows 10 Professional - PowerShell Version 5.1 - PowerShell Script (described in the guidance)

The TOE tested by the evaluator has the same identification as the TOE identification in Chapter 2.

The configuration of the independent testing except the TOE is different from the TOE

configuration identified in the ST in the points described below. The evaluator determined that there are no problems with the differences and that the security functions of the TOE configuration identified in the ST can be considered properly tested.

(1) Tested models

In the models of the TOE described in Chapter 2 "TOE identification," there are multiple models due to the following differences:

- Difference in printing speed

The evaluator determined that the security functions of all the models of the TOE can be considered to have been tested by testing the representative two models considering the above differences, because the security functions of each models are the same

(2) Using a modified firmware for testing

In the independent testing, a firmware modified for testing was used to verify the encryption functions instead of the firmware of the TOE. The evaluator determined that the testing on the modified firmware is valid because its modules of the encryption functions are the same as that of the TOE, and the modification for testing does not affect the encryption functions.

(3) Using additional tools for testing

In the independent testing, some tools for testing were used to confirm and alter the communication data and to confirm the data written in the hard disk drive. Those tools for testing were validated by the evaluator.

2) Summary of the Independent Testing

A summary of the independent testing performed by the evaluator is described below.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing devised by the evaluator based on the requirements of the Conformance PP and on the provided evaluation documentation are as follows.

<Viewpoints of the Independent Testing>

(1) Confirm security functions for each Security Functional Requirement (SFR).

(2) Confirm if the implementation of the cryptographic algorithms is correct.

b. Independent Testing Outline

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

<Independent Testing Approach>
The behavior of the TOE on inputs using the control panel of the TOE, the client PC, the audit server and the testing tools was confirmed by following means:

- If the behavior can be confirmed from the external interfaces of the TOE, the external interfaces of the TOE are used.

- If the behavior cannot be confirmed from the external interfaces of the TOE, the developer interface of the TOE, the analyzer for the hard disk drive in the TOE and the firmware for testing are used.

<Content of the Performed Independent Testing>
The evaluator performed the independent testing of 20 items.

Table 7-2 shows contents of the independent testing corresponding to the viewpoints.

Table 7-2 Performed Independent Testing

Viewpoint	Outline of the Independent Testing
(1)	<Confirmation of security functions> Confirm that all security functions work as the specification with the test items created based on the assurance activities of the Conformance PP for each SFR or the requirements of the SFR.
(2)	<Confirmation of implementation of cryptographic algorithms> Confirm the following cryptographic algorithms are implemented as the specification. - RSA (key generation, signature generation/verification) - ECDSA (key generation, signature generation/verification) - AES-CBC-128, AES-CBC-256, AES-GCM-128, AES-GCM-256 - SHA-1, SHA-256, SHA-384, SHA-512 - HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 - CTR_DRBG (AES)

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 test 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 below.

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 unintended network ports of the TOE may be open, and known vulnerabilities may exist in the network services running on the TOE.

(2) There is a concern that known vulnerabilities may exist in the Web interface of the TOE.

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

(4) There is a concern that the identification and authentication function may be bypassed by the malicious input from the control panel of the TOE, printer driver or Web interface.

(5) There is a concern that USB ports of the TOE may be exploited.

b. Penetration Testing Outline

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

<Penetration Testing Environment>
The 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 7-3 shows the tools used in the penetration testing.

Table 7-3 Penetration Testing Tools

Name	Outline and Purpose of Use
Nmap Version 7.92	A tool to detect available network service ports.
Nessus Version 10.2.0	A tool to detect known vulnerabilities at network ports.
OWASP ZAP Version 2.11.1	A tool to detect known vulnerabilities at Web application.
Fiddler Version 5.0.20211.51073	The tool is used to refer to and alter the communication data between Web browser and Web server (TOE).
PRET Version 0.40	A tool to inspect various vulnerabilities in a printing processing.

<Content of the Performed Penetration Testing>
Table 7-4 shows contents of the penetration testing corresponding to the vulnerabilities of concern.

Table 7-4 Outline of the Penetration Testing

Vulnerability	Penetration Testing Outline
(1)	- Confirm that unexpected network ports of the TOE are not open using Nmap. - Confirm that there is no known vulnerability in the network services running on the TOE using Nessus.

(2)	- Confirm that there is no known vulnerability in the Web interface of the TOE using OWASP ZAP. - Confirm that the identification and authentication function and the access control function cannot be bypassed even if the data from Web browser to the TOE are altered using Fiddler.
(3)	- Confirm that there is no known vulnerability in print processing of the TOE using PRET and exploit codes available at the Internet.
(4)	- Confirm that unexpected behaviour is not observed even if the character strings that may cause buffer overflow or unauthrised processing are input for the user ID or password in the control panel, printer driver and Web interfaces of the TOE.
(5)	- Confirm that the USB port of the TOE cannot be used using the PC for the penetration tesing and bootable USB flash drive.

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

The conditions of the TOE configuration, that are prerequisites for this evaluation, are as described in the guidance documents listed in Chapter 6. In order to use the TOE securely as ensured by the evaluation, the TOE must be set as described in the guidance documents. Different settings are not subject to assurance by this evaluation.

7.6 Evaluation Results

The evaluator had concluded that the TOE satisfies all work units prescribed in the CEM and all assurance activities in the Conformance PP as per the Evaluation Technical Report.

In the evaluation, the following were confirmed.

- PP Conformance:

  Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015

  Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

  Guideline for Certification Application with HCD-PP Conformance [16]
  - Treatment regarding FCS_RBG_EXT.1 Test
  - Treatment regarding FCS_TLS_EXT.1.1 Test

- 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 required by the Conformance PP.

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1,
ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1,
ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1

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

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurement entities.

8. Certification

The Certification Body performed the certification from the following viewpoints 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 in the CEM and assurance activities of the Conformance PP 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 and the assurance activities of the Conformance PP.

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 Evaluation Technical Report, Observation Report and related evaluation documentation submitted by the Evaluation Facility, the Certification Body determined that the TOE evaluation satisfies the assurance requirements required by the Conformance PP.

8.2 Recommendations

Procurement entities who are interested in the TOE are advised to refer "4.2 Environmental Assumptions" and "7.5 Evaluated Configuration" to make sure the scope of the evaluation and the operational requirements of the TOE meet the operational conditions assumed by each user.

It is necessary that an audit server polls the TOE periodically to read out audit logs from the TOE. The system administrator for the TOE needs to determine the interval time of polling based on the consideration of your operational policy for audit logs and your usage of the TOE. Note that if the polling interval is too short, the audit server might run short of storage area because the TOE sends all stored audit logs every polling. Also note that if the polling interval is too long, audit logs might be lost.

9. Annexes

There is no annex.

10. Security Target

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

Title:	Xerox VersaLink B7135 / B7130 / B7125 with Fax and Disk Overwrite Security Target
Version:	V 1.07
Publication Date:	September 29, 2022
Author:	FUJIFILM Business Innovation Corp.

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
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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

MFD	Multi-Function Device
PSTN	Public Switched Telephone Network

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

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CTR_DRBG	Counter (CTR) mode block cipher algorithm DRBG
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
GCM	Galois/Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IPP	Internet Printing Protocol
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
TLS	Transport Layer Security

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

Copy Function	A function to scan paper documents by operating the control panel and duplicate them.
Fax Function (fax send, fax receive)	A function to send and receive fax data via Public Switched Telephone Network. Fax send functionality is to scan paper documents by operating the control panel and send the scanned user document data using the standard fax protocol. Fax receive functionality is to receive user document data using the standard fax protocol and print them by operating the control panel of the MFD.
Print Function	A function to receive user document data from the printer driver of a user client, and then print out them by operating control panel of the MFD.
Scan Function	A function to scan paper documents by operating the control panel and send the scanned user document data to a mail server.
Assurance Activity	Evaluation work to be performed by an evaluator in order to conform to a PP. It is a supplement of the CEM. In the case of the Conformance PP [14], it is described in the Conformance PP.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, October 2020, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2020, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2021, 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 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001, (Japanese Version 1.0, July 2017)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002, (Japanese Version 1.0, July 2017)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003, (Japanese Version 1.0, July 2017)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004, (Japanese Version 1.0, July 2017)

[12] Xerox VersaLink B7135 / B7130 / B7125 with Fax and Disk Overwrite Security Target, Version V1.07, September 29, 2022, FUJIFILM Business Innovation Corp.

[13] Xerox VersaLink B7135 / B7130 / B7125 with Fax and Disk Overwrite Evaluation Technical Report, Version 1.3, September 30, 2022, Information Technology Security Center, Evaluation Department

[14] Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Certification Identification: JISEC-C0553)

[15] Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

[16] Guideline for Certification Application with HCD-PP Conformance, Version 1.8, November 11, 2020, Information-technology Promotion Agency, Japan, JISEC-CERT-2020-A18