Certification Report

Kazumasa Fujie, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2010-07-09 (ITC-0303)
Certification No.	C0280
Sponsor	Fuji Xerox Co., Ltd.
Name of TOE	Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific
Version of TOE	Controller ROM Ver. 1.103.0
PP Conformance	None
Assurance Package	EAL3
Developer	Fuji Xerox Co., Ltd.
Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE is certified as follows.
2010-12-21

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

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

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

Evaluation Result: Pass

"Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

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

Table of Contents

1. Executive Summary

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific, Version Controller ROM Ver. 1.103.0" (hereinafter referred to as "the TOE") developed by Fuji Xerox Co., Ltd., and evaluation of the TOE was finished on 2010-12-10 by Information Technology Security Center Evaluation Department (hereinafter referred to as "Evaluation Facility"). It reports to the sponsor, Fuji Xerox Co., Ltd. and provides information to consumers and system operators who are interested in this TOE.

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

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

1.1 Product Overview

Overview of the TOE functions and operational conditions are as follows. Refer to and after Chapter 2 for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

This TOE is the controller software installed in the Multi Function Device (hereinafter referred to as "MFD"), which controls the entire MFD that has copy, print, scan, and FAX functions. This TOE operates in the following MFDs of Fuji Xerox Co., Ltd.:
Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 Series, and DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series.

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

About these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package.

1.1.2.1 Threats and Security Objectives

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

The document data of users which is an asset to be protected and the setting data affecting security may be disclosed or altered illegally by the following: unauthorized operation of TOE, direct data read-out from HDD in TOE, and access to the communication data on the network where TOE is installed.

Thus, the TOE prevents unauthorized operations of the TOE by identifying and authenticating TOE users and permitting the available operations only to the corresponding users. Also, the TOE prevents a direct data read-out from HDD by encrypting the protected asset at storing it to the HDD, and by overwriting the data at deleting the protected asset. Furthermore, the TOE prevents unauthorized read-out and alteration of the communication data by applying encryption protocol at network communication.

1.1.2.2 Configuration and Assumptions

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

The MFD in which this TOE is installed is assumed to be used at general office, linked to the internal network protected from threats on the external network by firewall, etc.

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

1.1.3 Disclaimers

In this evaluation, only the configuration, to which the setting condition such as restriction for customer engineer operation is applied, is evaluated as TOE. If the setting of those configuration conditions is changed, the configuration will not be subject to the guarantee assured by this evaluation.

The TOE has Remote Authentication function and S/MIME function which are valid in ApeosPort-IV series only and not provided in DocuCentre-IV series. (In DocuCentre-IV series, E-mail and Internet FAX functions are not included as standard specifications, and thus not included in the configuration subject to this evaluation.)

The TOE provides Direct FAX function and the function corresponding to Network Scan Utility of user client; however, those functions are limited to Local Authentication and not subject to evaluation at Remote Authentication.

1.2 Conduct of Evaluation

Evaluation Facility conducted IT security evaluation, and completed on 2010-12 based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme"[1], "IT Security Certification Procedure"[2], "Evaluation Facility Approval Procedure"[3] provided by Certification Body.

1.3 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Reports prepared by Evaluation Facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification oversight reviews are also prepared for those concerns found in the certification process.

Those concerns pointed out by the Certification Body are fully resolved, and the Certification Body confirmed that the TOE evaluation is appropriately conducted in accordance with CC ([4][5][6] or [7][8][9]) and CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by Evaluation Facility and concluded fully certification activities.

2. Identification

The TOE is identified as follows;

Name of TOE:	Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific
Version of TOE:	Controller ROM Ver. 1.103.0
Developer:	Fuji Xerox Co., Ltd.

This TOE is the controller software part of Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 or DocuCentre-IV C5570/C4470/C3370/C3371/C2270 series, which is the MFD targeted for Asia Pacific with an option of "Data Security Kit" installed.

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

Users operate on the control panel according to the procedure written in the guidance document, and confirm the version information displayed on the screen or that written in the print output of the configuration setting list.

Whether "Data Security Kit" is available or not can be confirmed by referring to "License" enclosed in the product, and by whether the settings are possible as specified in the guidance document regarding the overwrite and encryption functions for hard disk data that are enabled by the corresponding option.

3. Security Policy

This chapter describes whether this TOE realizes functions as security service under what kind of policy or rule.

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

The TOE can prevent the user's document data that is an asset to be protected and the setting data affecting security from being exposed or altered illegally, by applying the following security functions at using the MFD functions:
Identification/authentication and access control of user, encryption of the data stored in HDD, data overwrite at deleting the data in HDD, and encryption communication protocol.

The TOE provides access control function according to each role assuming the following roles:

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

- System Administrator (Key Operator + System Administrator Privilege [SA])
  An authorized administrator who configures TOE security functions settings and other device settings. This term covers both key operator and SA (System Administrator). Key operator can use all management functions, and SA can use a part of management functions. The role of SA is set by the key operator as required by the corresponding organization.

- Customer Engineer
  Customer service engineer who maintains and repairs MFD

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

3.1 Security Function Policies

The TOE provides the security functions to counter the threats shown in Chapter 3.1.1 and to meet the organisational security policy shown in Chapter 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threats shown in Table 3-1 and provides the functions to counter them.

Table 3-1 Assumed Threats

Identifier	Threat
T.CONSUME	A user may access TOE and use TOE functions without authorization.

T.DATA_SEC	A user who is authorized to use TOE functions may read document data and security audit log data exceeding the permitted authority range.
T.CONFDATA	A user who is authorized to use TOE functions may read or alter the TOE setting data without authorization although only a system administrator is allowed to access the TOE setting data.
T.RECOVER	An attacker may remove the internal HDD and connect it to commercial tools so that he/she can read out and leak the document data, used document data, and security audit log data from the HDD without authorization.
T.COMM_TAP	An attacker may intercept or alter document data, security audit log data, and TOE setting data on the internal network.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threats shown in Table 3-1 by the following security function policies.

1) Countermeasures to threat "T.CONSUME" "T.DATA_SEC" "T.CONFDATA"

The TOE counters the threats by the following functions: "User Authentication", "System Administrator's Security Management", "Customer Engineer Operation Restriction", and "Security Audit Log".

"User Authentication" allows only the authorized user who succeeds in identification/authentication to use the TOE functions. In addition, the authorized user can conduct the permitted operations only at operating Mailbox and document data.

"System Administrator's Security Management" allows only the authorized system administrator to refer to and change the setting data of security functions, and to change the Enable/Disable setting of security functions.

"Customer Engineer Operation Restriction" allows only the authorized system administrator to refer to and change the setting data that controls Enable/Disable status of operation restriction for customer engineer.

"Security Audit Log" allows only the authorized system administrator to acquire and read the audit log such of user log-in/out, job end, and setting changes. When the area to store the audit log becomes full, the oldest stored audit log is overwritten and a new audit log is stored.

With the above functions, only the operations permitted per valid TOE user can be conducted, thus unauthorized TOE use and access to protected assets can be prevented.

2) Countermeasures to threat "T.RECOVER"

The TOE counters the threat by the following functions: "Hard Disk Data Overwrite" and "Hard Disk Data Encryption".

"Hard Disk Data Overwrite" is to encrypt the document data upon storing the data into the internal HDD when any of MFD basic functions such as copy, print, scan, network

scan, FAX, and direct FAX is operated. Also, it encrypts the audit log data at storing the audit log data created by Security Audit Log function into the internal HDD.

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

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

3) Countermeasures to threat "T.COMM_TAP"

The TOE counters the threat by the function "Internal Network Data Protection".

"Internal Network Data Protection" is to apply the encryption communication protocol when TOE communicates with client terminals and various servers. The supported encryption protocols are SSL/TLS, IPSec, SNMPv3, and S/MIME.

With the above function, the encryption communication protocol is applied to the document data transmitted in the internal network, security audit log data, and TOE setting data to prevent interception and alternation of the data.

3.1.2 Organisational Security Policy and Security Function Policy

3.1.2.1 Organisational Security Policy

Organisational security policy imposed on use of the TOE is shown in Table 3-2.

Table 3-2 Organisational Security Policy

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

3.1.2.2 Security Function Policy to Organisational Security Policy

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

1) Countermeasure to organizational security policy "P.FAX_OPT"

"FAX Flow Security" function of TOE has a mechanism that the data received from public telephone line will not be passed to be sent to the internal network in any circumstances. This is to meet a requirement in the organizational security policy, which requires inhibiting unauthorized access to the internal network from the public telephone line.

4. Assumptions and Clarification of Scope

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

4.1 Usage Assumptions

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

Table 4-1 Assumptions

Identifier	Assumptions
A.ADMIN	A system administrator shall have the necessary knowledge of TOE security functions to perform the given role of managing the TOE and shall not operate the TOE with malicious intent.
A.SECMODE	A system administrator shall configure and set the TOE properly according to the security policy of organization and the product guidance document to manage the TOE and its external environment.

4.2 Environment Assumptions

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

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

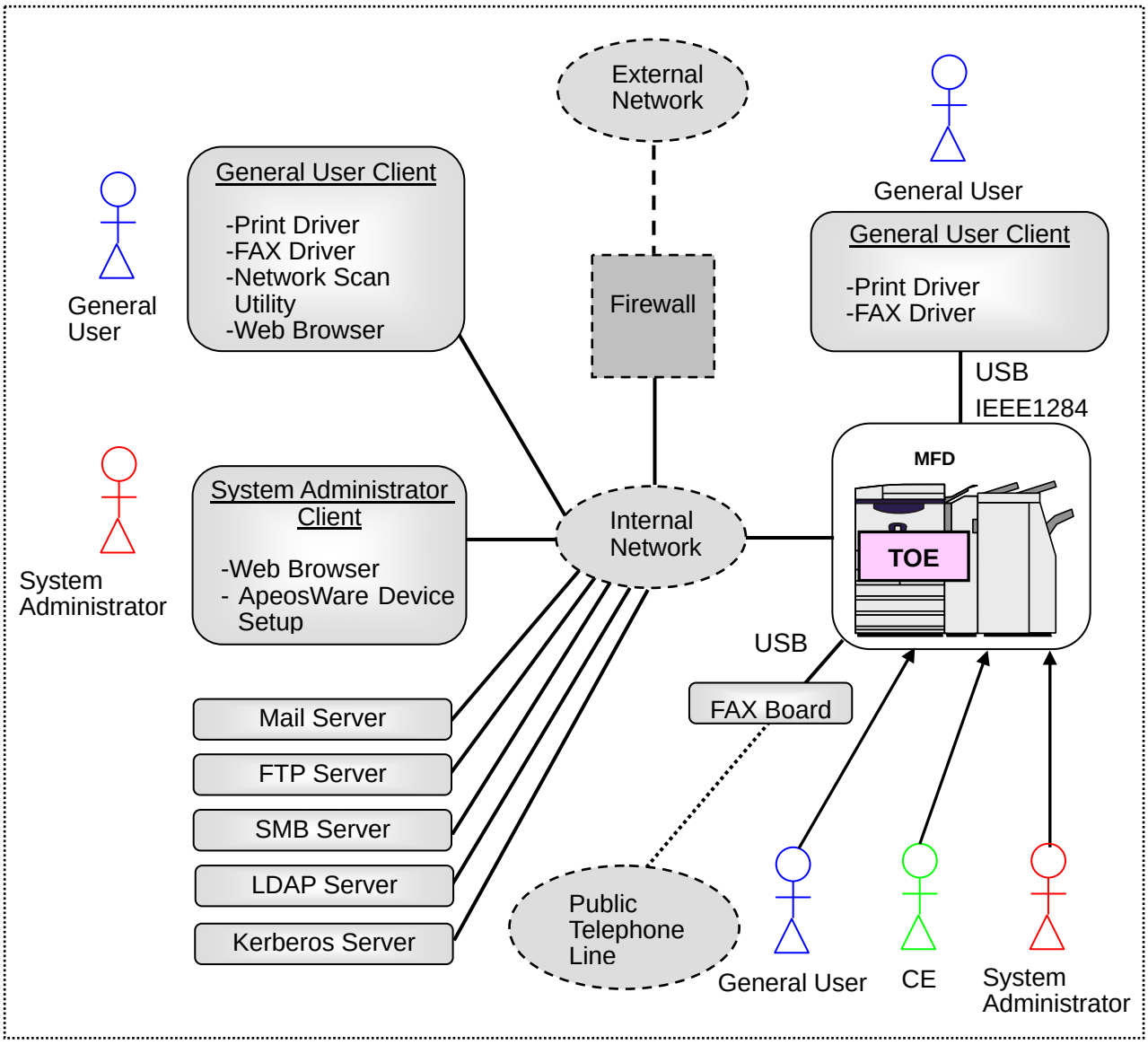

Figure 4-1 Operational Environment of TOE

The operational environment of TOE consists of the following:

1) MFD

Multi Function Device in which TOE is to be installed. This TOE can be installed in the following MFD series:

- Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 Series
- Fuji Xerox DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series

Among the series, some MFDs do not have scan and FAX functions as standard specifications and provide them as an option only. All the following configurations are subject to this evaluation: Series with scan and FAX functions provided as standard specifications, Series without scan and FAX functions, and Series without scan and FAX functions but with optional scan and FAX functions added.

However, E-mail and Internet FAX functions of DocuCentre-IV series are not subject to this evaluation since these functions are not provided in all DocuCentre-IV series as

standard specifications.

2) FAX Board
Even when MFD has a FAX function, FAX Board connected to MFD by USB is still sold separately. A user who wants to use FAX function needs to select the MFD series with FAX function provided and also purchase the FAX Board specified by Fuji Xerox Co., Ltd.

3) General User Client
General User Client is a general-purpose PC for general user and linked to the TOE via USB and IEEE1284 port or the internal network. The following software is required:
- OS: Windows XP, Windows Vista, or Windows 7
- Print/FAX driver

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

4) System Administrator Client
System Administrator Client is a general-purpose PC for system administrator and connected to TOE via internal network. The following software is required:
- OS: Windows XP, Windows Vista, or Windows 7
- Web browser (included with OS)
- ApeosWare Device Setup

5) LDAP Server, Kerberos Server
When "Remote Authentication" is set for user authentication function, either authentication server, LDAP server or Kerberos server will be necessary. When "Local Authentication" is set, neither authentication server is necessary.

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

6) Mail Server, FTP Server, SMB Server
A server is installed as necessary at using MFD basic functions.

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

4.3 Clarification of Scope

1) The print function of TOE is of two types: "Store Print" in which the print data received from the general user client is temporarily stored in the HDD and then printed out according to the general user's instruction from the control panel, and "Normal Print" in which the data is printed out immediately when the MFD receives the data. In this evaluation, only the "Store Print" is subject to the evaluation.

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

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

3) "Remote Authentication" and S/MIME function are not provided in DocuCentre-IV series. (S/MIME function is used for E-mail and Internet FAX functions. However, it is not included in the configuration subject to this evaluation since E-mail and Internet FAX functions are not provided as standard specifications.)

5. Architectural Information

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

5.1 TOE Boundary and Component

The MFD configuration with TOE and the IT environment other than MFD are shown in Figure 5-1 below. In Figure 5-1, MFD corresponds to controller board, control panel, internal HDD, ADF, IIT, and IOT. The TOE corresponds to a software part that realizes various functions and is stored in Controller ROM of the controller board.

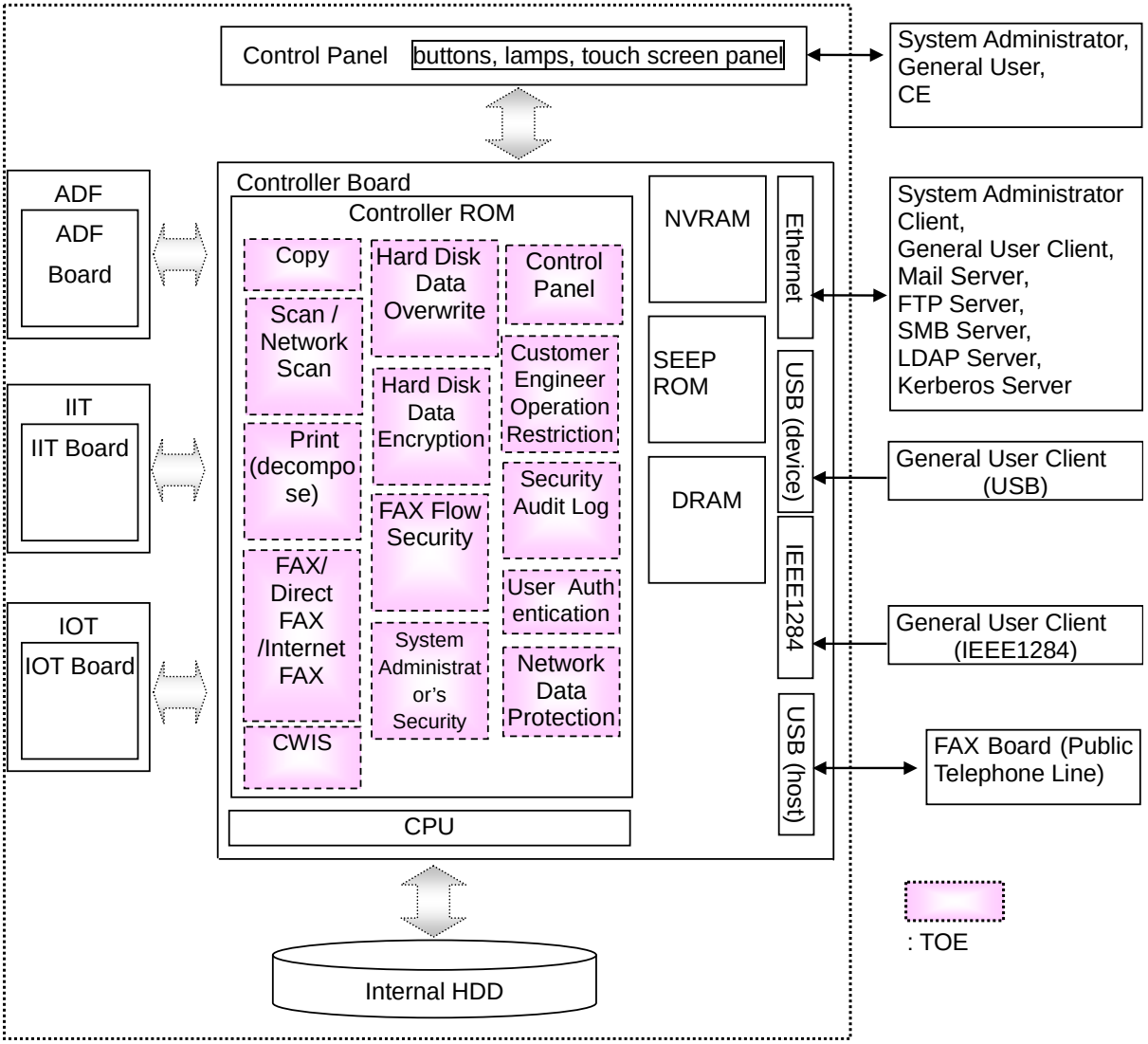

Figure 5-1 TOE Boundary

The TOE consists of the security function described in Chapter 3 and other MFD basic functions. Regarding the MFD basic functions, refer to Terminology in Chapter 11.

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

1) When a user uses functions that refer to the audit log in MFD basic functions, System Administrator Security, and Security Audit Log functions, User Authentication function is applied and the authorized user is allowed to perform operations according to his/her role. Also, when these functions are used, audit log is created by Security Audit Log function.

2) For the document data and audit log to be stored in the internal HDD at the use in 1) above, Hard Disk Data Encryption function is applied, and Hard Disk Data Overwrite function is applied at deleting the document data. These processing are also applied not only to the document data stored or deleted intentionally by user, but also to the document data stored temporarily in HDD by user without intention due to the processing of copy function, etc.

3) When the MFD with TOE and other IT devices communicate via Ethernet at the use in 1) above, Internal Network Data Protection function is applied. Also, Fax Flow Security function is applied for FAX.

5.2 IT Environment

The TOE shall be installed to MFD to operate.

Various servers, system administrator client, and general use client that are connected to MFD via Ethernet perform communication using the encryption communication protocol IPsec. Furthermore, SSL/TLS is used for Web browser to be installed to client, and S/MIME is used for mails transmitted with Mail server. Also, SNMPv3 is used for network management.

When "Remote Authentication" via LDAP server is selected in TOE settings, User ID and password are verified in LDAP server and its result is used by TOE. When "Remote Authentication" via Kerberos server is selected, identification/authentication is performed by the coordinated operation of Kerberos server and TOE. In either case, password of more than 9 characters needs to be set.

In addition, when "Remote Authentication" is selected in TOE settings, even with either LDAP server or Kerberos server, the TOE uses the user attribute acquired from LDAP server to determine if the user is SA role.

6. Documentation

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

- ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Administrator Guide (ME4564E2-3)

- ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 User Guide (ME4563E2-3)

- ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Security Function Supplementary Guide (DE4552E2-1)

7. Evaluation conducted by Evaluation Facility and results

7.1 Evaluation Approach

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

7.2 Overview of Evaluation Activity

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

Evaluation has started on 2010-07 and concluded by completion the Evaluation Technical Report dated 2010-12. The evaluator received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluator directly visited the development and manufacturing sites on 2010-09 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff interview. Further, the evaluator executed the sampling check of the developer testing and the evaluator testing by using developer testing environment at developer site on 2010-09.

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

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

7.3 IT Product Testing

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

7.3.1 Developer Testing

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

1) Developer Testing Environment

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

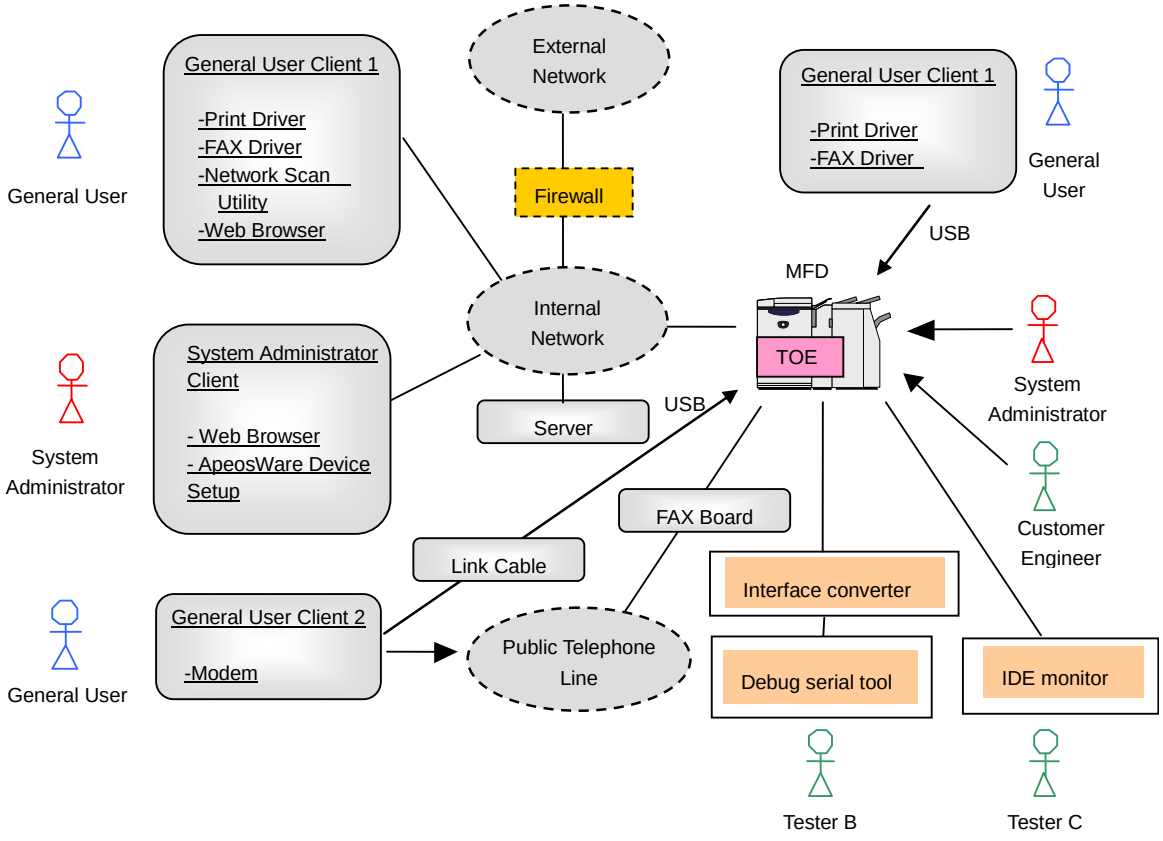

Figure 7-1 Configuration of Developer Testing

The TOE to be subject to evaluation is the same TOE as in TOE Identification of Chapter 2.

The MFDs used in testing are ApeosPort-IV C3370 and DocuCentre-IV C5570. The evaluator evaluated the testing by representative products of both series as sufficient, since the TOE is the controller software common to ApeosPort-IV C5570/C4470/C3370 /C3371/C2270 series and DocuCentre-IV C5570/C4470/C3370/C3371/C2270 series, and all functions including series-related differences are confirmed by testing them.

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

Table 7-1 Devices for Developer Testing

Device Name	Description
Server	Used as Mail server, LDAP server, and Kerberos server. - PC with Windows Server 2003 sp2 - Various servers: Standard software in OS
System Administrator Client	Used as system administrator client. - PC with Windows XP professional sp2 - Web browser: Internet Explorer 6.0 sp2 - ApeosWare Device Setup Version 1.0.0.1
General User Client 1	Used as general user client (connected via internal network) and SMB server. - PC with Windows 7 - Web browser: Internet Explorer 8 - Network Scan Utility: Ver.1.7.3 - Print/FAX driver: Version 6.00 - SMB server: Standard software in OS
General User Client 2	Used to send/receive FAX and to confirm that USB port for connecting MFD FAX cannot be used for other use. - PC with Windows XP professional sp2 PC modem port is connected to public telephone line. PC USB port is connected to the USB port for MFD FAX board via link cable (USB cable).
General User Client 3	Used as general user client (connected via printer USB and IEEE1284 port). - PC with Windows VISTA sp2 - Print/FAX driver: Version 6.00
IDE Monitor	A tool to monitor the data transmitted through the connected IDE bus of HDD. - IDE-POCKET (by TOYO Corporation) of dedicated device is connected to the PC with Windows 2000 - Software: IDE-WinU V1.9.3 (by TOYO Corporation)
Debug Serial	Debugging terminal of MFD - Device for use: Serial port of PC for system administrator client is connected to the terminal port for MFD debugging via Fuji Xerox-unique conversion board. - Software: Tera Term Pro version 2.3
Public Telephone Line	Use an artificial exchange system as an alternative of public telephone line.
FAX Board	An option of MFD by Fuji Xerox - Fax ROM Ver 1.1.2

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

In the ST, Windows VISTA (Web browser: Internet Explorer 7) is listed as a user client in addition to Windows XP (Web browser: Internet Explorer 6.0 sp2) and Windows 7 (Web browser: Internet Explorer 8) that are used in the developer testing. The evaluator evaluated that there is no problem with the operations of Windows VISTA, since the TOE-dependent functions can be confirmed sufficiently by the testing of Windows XP and Windows 7.

2) Summary of Developer Testing

Summary of the developer testing is as follows;

a. Outline of Developer Testing
The testing performed by the developer is outlined as follows;

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

(2) To confirm the Hard Disk Data Overwrite function, use the IDE monitor as a testing tool and read out and observe the data to be written to HDD and the HDD contents.

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

(4) To confirm the encryption communication protocol function such as IPsec, use the testing tool to be described later and observe that the encryption communication protocol is applied as specified.

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

<Developer Testing Tools>
The tools used for the developer testing are shown in Table 7-2 below.

Table 7-2 Tools for Developer Testing

Tool Name	Description
IDE Monitor (See Table 7-1 for configuration.)	Monitor the data in IDE bus for connecting HDD in MFD, and observe the data to be written to HDD. Also, read out the data written in HDD.
Protocol Analyzer Wireshark Version 1.2.3	Monitor the communication data on the network, and confirm that the encryption communication protocol is IPsec, SSL/TLS, or SNMPv3 as specified.
Mailer Windows Live Mail Version 2009	Transmit mails via TOE and mail server, and confirm that the encryption by S/MIME and signature are as specified.

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

Also, the evaluator confirmed that the processing halt by MFD power off and its restart by MFD power on and the prevention of access to internal network from FAX are operated as specified.

b. Scope of Developer Testing Performed

The developer testing is performed about 74 items by the developer. By the coverage analysis, it was verified that all security functions and external interfaces described in the TOE functional specification had been tested. By the depth analysis, it was verified that all subsystems and subsystem interfaces described in the TOE high-level design had been tested enough.

c. Result

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

7.3.2 Evaluator Independent Testing

The evaluator executed the independent testing to reconfirm that security functions are certainly implemented based on the evidence shown in the process of the evaluation. The overview of the independent testing executed by the evaluator is described as follows;

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

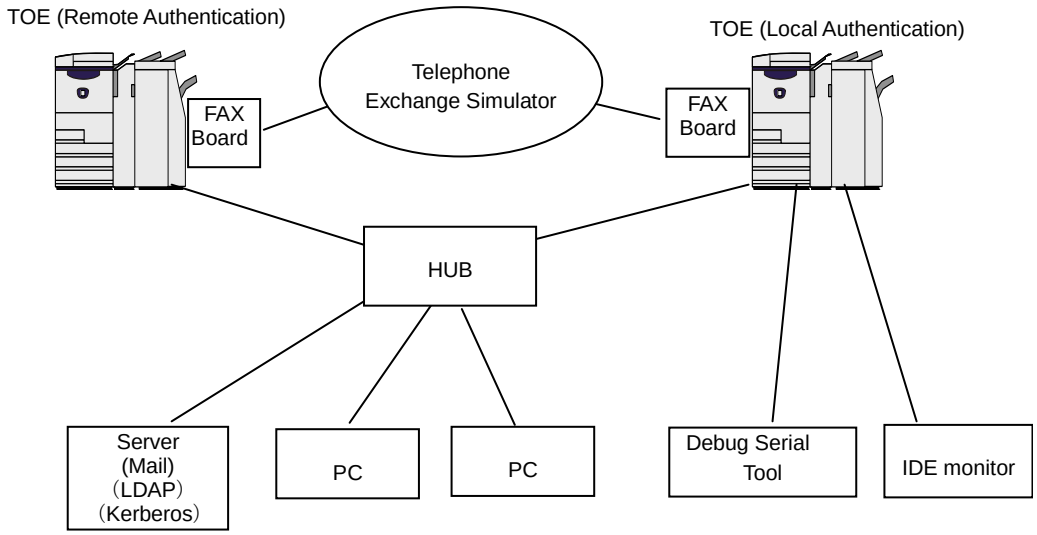

Figure 7-2 Configuration of Evaluator Testing

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

The target TOE and the MFD with TOE are the same as those in the developer testing, and ApeosPort-IV C3370 is used for the TOE (remote authentication), and DocuCentre-IV C5570 is used for the TOE (local authentication). The MFD is used instead of the PC used in the developer testing for sending/receiving FAX with MFD, and the evaluator evaluated that it does not affect the test of security function.

The evaluator independent testing is executed in the same environment as TOE configuration identified in ST.

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

a. Viewpoint of Independent Testing

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

<Viewpoint of Independent Testing>
(1) Conduct the same test on either of two MFD types regarding all test items performed by the developer, from the viewpoint of sampling of developer testing.

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

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

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

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

<Contents of Independent Testing Performed>
Table 7-3 shows outline of the independent testing conducted by the evaluator with corresponding viewpoints of independent testing.

Table 7-3 Conducted Independent Testing

Viewpoint of independent testing	Outline of independent testing
(1)	Test all the items tested by the developer on either MFD type and confirm that the same result as that by the developer can be obtained.
(2)	Confirm that that following are as specified:

	- Behavior of limit value for length upon password change and entry - Bahavior of accout lock when there are both cases mixed that identification/authentication of system administrator of different user IDs is successful and failed - Access control to Mailbox of system administrator
(2)	Confirm that the setting cannot be conducted in system administrator security management function for the functions that are not provided in DocuCentre series.
(2)	Confirm that the behavior of access control without using LDAP server that stores user attributes is as specified in Remote Authentication (Kerberos server). (Note: Recognized as general user, not as SA)

c. Result

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

7.3.3 Evaluator Penetration Testing

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

1) Summary of the Penetration Testing
Summary of the penetration testing conducted by the evaluator is as follows;

a. Vulnerability of concern

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

(1) There is a concern corresponding to this TOE regarding the publicly available vulnerability information, such as the possibility of unauthorized use of network service, various vulnerability of Web, and selection of insecure encryption upon SSL communication.

(2) There is a concern that the TOE operates unexpectedly for the entry exceeding the limit value or the entry of unexpected character code on the interface other than Web, such as control panel.

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

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

(5) There is a concern that the document as a protected asset becomes inconsistent when multiple users access the document in Mailbox, from the analysis of

vulnerability on the provided evidence.

b. Outline of Penetration Testing

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

< Penetration Testing Environment>

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

Table 7-4 Tools for Penetration Testing

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

<Contents of Penetration Testing Performed>

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

Table 7-5 Outline of Penetration Testing

Vulnerability of concern	Outline of penetration testing
(1)	- Executed Nmap for TOE and confirmed that the open port cannot be misused. - Conducted various entries to Web server (TOE) using Web browser and Fiddler2, and confirmed that there is no known vulnerability such as bypass of identification/authentication, buffer overflow, and various injections. - Confirmed that the communication cannot be enabled other than by the encryption communication protocol specified by the TOE even when the setting of the PC used as client is changed to the unrecommended value for the encryption communication protocol.
(2)	- Confirmed that it becomes an error when the character of out-of-spec length, character code, and special key are entered from control panel, system administrator client (ApeosWare Device Setup), or general user client (network scan utility, print driver).
(3)	- Confirmed that other than the intended functions such as print and FAX cannot be used even when attempting to access the TOE by connecting the PC for penetration testing to each USB port of

	the TOE.
(4)	- Confirmed that the TOE cannot be used with an error occurrence even after replacing NVRAM and SEEPROM with the new ones to which no setting is applied.
(5)	- Confirmed that the access is rejected during the operation by others when multiple users access the document in Mailbox.

c. Result

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

7.4 Evaluated Configuration

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

Table 7-6 TOE Configuration Condition

Item No.	Setting Item	Setting Value
1	Hard Disk Data Overwrite	Set to [1 Overwrite] or [3 Overwrites].
2	Hard Disk Data Encryption	Set to [Enabled]
3	Passcode Entry from Control Panel	Set to [Enabled]
4	Maximum Login Attempts	Set to [5] Times
5	SSL/TLS Communication	Set to [Enabled]
6	IPSec Communication	Set to [Enabled]
7	S/MIME Communication	Set to [Enabled] for ApeosPort-IV series. (Note: This function is not provided for DocuCentre-IV series.)
8	User Authentication	Set to [Local Authentication] or [Remote Authentication] (Note: Both setting are evaluated. For Remote Authentication, either LDAP or Kerberos setting is mandatory.)
9	Store Print	Set to [Save As Private Charge Print]
10	Audit Log	Set to [Enabled]
11	SNMPv3 Communication	Set to [Enabled]
12	Customer Engineer Operation Restriction	Set to [Enabled]
13	Direct FAX	Set to [Disabled] at Remote Authentication. (Note: For Local Authentication, evaluation is conducted with setting of [Enabled])
14	Network Scan utility (WebDAV setting)	Set to [Disabled] at Remote Authentication. (Note: For Local Authentication, evaluation is conducted with the setting of [Enabled])
15	Minimum password length for general user and SA	Set to [9] characters. (Note: For Remote Authentication, at least 9-digit password shall be set on LDAP and Kerberos server side.)

7.5 Evaluation Results

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

In the evaluation, the following were confirmed.
- PP Conformance: none
- Security functional requirements: Common Criteria Part 2 Conformant
- Security assurance requirements: Common Criteria Part 3 Conformant

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

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

7.6 Evaluator Comments/Recommendations

The evaluator recommendations for users are not mentioned.

8. Certification

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

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

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

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

8.1 Certification Result

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

8.2 Recommendations

This TOE provides different functions depending on MFD types to which this TOE is installed. Also, Local Authentication and Remote Authentication are available as the user authentication function, but there are restrictions on the function subject to evaluation when the operation with Remote Authentication is selected, compared with the case of Local Authentication. A user who is interested in this TOE needs to select MFD type by considering if the presumed function and operation are possible, at purchasing the MFD products with TOE.

If the TOE setting is performed according to the attached document in operating this TOE, configuration conditions with which this evaluation is conducted are to be satisfied. If the setting value of TOE is set to other than that in the configuration conditions, it shall be noted that it will not be subject to the guarantee by this evaluation.

9. Annexes

There is no annex.

10. Security Target

Security Target [12] of the TOE is provided within a separate document of this certification report.

Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific Security Target Version V1.0.6 (November 29, 2010) Fuji Xerox Co., Ltd.

11. Glossary

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

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

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

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

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

ApeosWare Device Setup	Software for a key operator to perform settings and management to MFDs from the system administrator client.
CWIS Function	CWIS (CentreWare Internet Service) is to retrieve the document data stored in Mailbox via Web browser. CWIS also enables management of the setting data by System Administrator.
IEEE1284	Standard protocol of parallel port for printer.
SA	See the description of "System Administrator".
General User	Any person who uses copy, print, scan, and FAX functions of TOE.
Internet FAX Function	Internet FAX function is to send and receive FAX data via the Internet, not via public telephone line.
Key Operator	See the description of "System Administrator".
Customer Engineer (CE)	Customer service engineer who maintains and repairs MFD.
Copy Function	Copy function is to read the original data from IIT and print it out from IOT according to the general user's instruction

	from the control panel.
System Administrator	An authorized administrator who configures TOE security functions and other device settings. This term covers both key operator and SA (System Administrator). Key operator can use all management functions, and SA can use a part of management functions. The role of SA is set by key operator as required by the corresponding organization.
Mailbox	A logical box created in the MFD internal HDD. Mailbox can store the scanned document data and received FAX data by users and senders.
Scan Function	Scan function is to read the original data from IIT and then store it into the Mailbox inside the MFD according to the general user's instruction from the control panel. The stored document data can be retrieved via Network Scan Utility or CWIS using Web browser.
Control Panel Function	Control panel function is a user interface function for general user, system administrator, and CE to operate MFD functions.
Direct FAX Function	Direct FAX function is to directly FAX document data to the destination. According to the instruction from a general user client, the print data is sent to the MFD as a print job, and then sent to the destination via public telephone line without being printed out.
Store Print	See the description of "Print Function".
Normal Print	See the description of "Print Function".
Network Scan Utility	Software for a general user client to retrieve the document data stored in Mailbox of MFD.
FAX Function	FAX function is to send and receive FAX data. According to the general user's instruction from the control panel to send a FAX, the original data is read from IIT and sent to the destination via public telephone line. The document data sent from the sender's machine via public telephone line is received and printed out from the recipient's IOT.
Print Function	Print function is to print out the data, which is sent to the MFD via print driver, from IOT according to the instruction from a general user client. The print function is of two types: "Normal Print" in which the data is printed out immediately from IOT when the MFD receives the data, and "Store Print" in which the print data is temporarily stored in the HDD inside the MFD and then printed out from IOT according to the general user's instruction from the control panel. In this evaluation, only the "Store Print" is subject to the evaluation.

12. Bibliography

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

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

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

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

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

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

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

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

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

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

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

[12] Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific Security Target Version V1.0.6 (November 29, 2010) Fuji Xerox Co., Ltd.

[13] Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C3371/C2270 DocuCentre-IV C5570/C4470/C3370/C3371/C2270 Series Controller Software for Asia Pacific Evaluation Technical Report Version 1.5, December 10, 2010, Information Technology Security Center Evaluation Department