Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2009-09-30 (ITC-9271)
Certification No.	C0249
Sponsor	Fuji Xerox Co., Ltd.
Name of TOE	Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570/C4470/C3370/C2270 Series Controller Software for Asia Pacific
Version of TOE	Controller ROM Ver.1.101.12
PP Conformance	None
Conformed Claim	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.
2010-03-12

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 Revision 2
- Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2

Evaluation Result: Pass

"Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570 /C4470/C3370/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

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570/C4470/C3370/C2270 Series Controller Software for Asia Pacific " (hereinafter referred to as "the TOE") conducted by Information Technology Security Center Evaluation Department (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Fuji Xerox Co., Ltd. and provides information to the users and system operators who are interested in this TOE.

The reader of the Certification Report is advised to read the corresponding ST. The operational conditions, details of usage assumptions, corresponding security objectives, security functional and assurance requirements needed for its enforcement, their summary of security specifications and rationale of sufficiency are specifically described in ST.

This certification report assumes the above persons(sponsor, system operators and users of the TOE) to be a reader. Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

1.1.1 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

1.1.2 PP Conformance

There is no PP to be conformed.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows;

Name of Product:	Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570/C4470/C3370/C2270 Series
ROM Version:	Controller ROM Ver.1.101.12
Developer:	Fuji Xerox Co., Ltd.

1.2.2 Product Overview

Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570/C4470 /C3370/C2270 Series is the Multi Function Device (hereinafter referred to as "MFD") that has copy, print, scan and FAX functions.
The MFD is assumed to be used at general office by clients (general user client and system administrator client), which are connected to the internal network or public

telephone line, and by a general user client which is directly connected to the MFD. TOE is stored on the controller ROM, which is on the controller board, and provides the following two functions:

-General functions to control the entire MFD.
-Security functions to protect the document data etc. in relation to the use of the above general functions against threats.

TOE provides the following general functions:

*Copy function
*Print function
*Scan function
*FAX function
*Direct FAX function
A FAX function to send data via public telephone line. The data is first sent to MFD as a print job and then to the destination without being printed out.
*Internet FAX function
A FAX function to send or receive data via the Internet without using public telephone line.
*CWIS function
CWIS is a function for general users to instruct scanning from the control panel and to retrieve the scanned document stored in the MFD's mailbox from the general user client using Web browser. Also, CWIS enables system administrators to confirm and rewrite TOE setting data via Web browser.
*Network Scanning Function
A function to transmit the scanned document data to the FTP server, SMB server, or Mail server according to the information set in the MFD. A general user can request this function from the control panel.

1.2.3 Scope of TOE and Security Functions

In addition to the general functions described in 1.2.2, TOE provides the following security functions (1)-(8).

The following TOE security functions are to protect the document data and used document data in relation to the use of the above general functions against threats of leakage, and to protect TOE setting data and security audit log data in relation to the use of TOE security functions against threats of alteration or leakage. Also, TOE provides a security function to protect against unauthorized access from the public telephone line or internal network. This function is required in Organizational Security Policies. (See 2.1.2)

(1) Hard Disk Data Overwrite
This function is to completely delete the used document data stored in the internal HDD. The data is overwritten with new data after any of copy, print, scan, etc. functions is completed.
(2) Hard Disk Data Encryption
This function is to encrypt the document data before being stored into the internal HDD when any of copy, print, scan, etc. functions is operated.
(3) User Authentication
This function allows only the authorized general user to use the TOE functions. A user needs to enter his/her ID and password from MFD control panel or general user client for identification/authentication. In addition, this function allows only a system administrator to refer to and change the TOE security functions. A system administrator needs to enter his/her ID and password from MFD control panel or system administrator client for identification/authentication.

(4) System Administrator's Security Management
This function allows only system administrators to refer to and change the TOE security settings by identifying and authorizing a system administrator from the control panel or system administrator client.
(5) Customer Engineer Operation Restriction
This function allows only system administrators to inhibit CEs from changing the TOE security settings.
(6) Security Audit Log
This function enables tracing and recording of the important events (configuration management, etc.) based on when and who operated what function.
(7) Internal Network Data Protection
This function protects the communication data on the internal network (document data, security audit log data, and TOE setting data).
(8) FAX Flow Security
This function prevents unauthorized access to the inside of TOE or the internal network via FAX board from public telephone line.

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as "IT Security Evaluation and Certification Scheme"[2], "IT Security Certification Procedure"[3] and "Evaluation Facility Approval Procedure"[4].

Scope of the evaluation is as follow;

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined "Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570/C4470/C3370/C2270 Series Controller Software for Asia Pacific Security Target" as the basis design of security functions for the TOE (hereinafter referred to as "the ST")[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex A of CC Part 1 (either of [5] or [8]) and Functional Requirements of CC Part 2 (either of [6] or [9]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7] or [10]) as its rationale. Such evaluation procedure and its result are presented in "Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570/C4470/C3370/C2270 Series Controller Software for Asia Pacific Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [13]. Further, evaluation methodology shall comply with the CEM (either of [11] or [12]).

1.4 Certification

The Certification Body verified the Evaluation Technical Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. There were no

concerns found in the certification process. Evaluation was completed with the Evaluation Technical Report dated 2009-02 submitted by the evaluation facility and the Certification Body confirmed that the TOE evaluation was appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

2. Summary of TOE

2.1 Security Problem and assumptions

Problems should be solved by TOE and necessary assumptions are as follows.

2.1.1 Threat

This TOE assumes such threats presented in Table 2-1 and provides functions for countermeasure to them.

An attacker is considered to have public knowledge of how the TOE operates and low-level attack capability.

Table 2-1 Assumed Threats

Identifier	Threat
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, security audit log data from the HDD without authorization.
T.CONFDATA	An attacker may access, read, or alter, from control panel or system administrator client, the TOE setting data which only a system administrator is allowed to access. (Note: This threat is based on the assumption that general users, who are allowed to use the TOE, perform unauthorized actions which only a system administrator is allowed to do.)
T.DATA_SEC	An attacker may read document data and security audit log data from control panel or Web browser without authorization. (Note: This threat is based on the assumption that users, who are allowed to use the TOE, use the TOE beyond the authority given to the users 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.
T.CONSUME	An attacker may access TOE and use TOE functions without authorization. (Note: This threat is based on the assumption that users, who are not allowed to use the TOE, use the TOE without authorization.)

2.1.2 Organisational Security Policy

Organizational security policy required in use of the TOE is presented in Table 2-2.

Table 2-2 Organizational Security Policy

Identifier	Organizational 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.

2.1.3 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 2-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 2-3 Assumptions in Use of the TOE

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 the TOE as follows. • Use of password entered from MFD control panel in user authentication: enabled. • Length of system administrator password: 9 characters or more • Access denial due to authentication failure of system administrator: enabled • Allowable number of system administrator's

	authentication failures before access denial: 5 • Customer Engineer Operation Restriction: enabled • User authentication setting: enabled (select Local Authentication) • Length of user password (for general user and SA): 9 characters or more • Private Print setting: store authenticated jobs to Private Print area • Audit Log setting: enabled • SNMP v3 communication: enabled • SNMP v1/v2c communication: disabled • Length of authentication password for SNMP v3 communication: 8 characters or more • SSL/TLS communication: enabled • IPSec communication: enabled • S/MIME communication: enabled • SMB communication: NetBEUI disabled • Hard Disk Data Overwrite: enabled • Hard Disk Data Encryption: enabled • Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters

2.1.4 Documents Attached to Product

The identification of documents attached to the TOE is listed below. TOE users are required full understanding of following documents and compliance with descriptions.

* ApeosPort-IV C5570/C4470/C3370/C2270 DocuCentre-IV C5570/C4470/C3370 /C2270 Administrator Guide
* ApeosPort-IV C5570/C4470/C3370/C2270 DocuCentre-IV C5570/C4470/C3370 /C2270 User Guide
* ApeosPort-IV C5570/C4470/C3370/C2270 DocuCentre-IV C5570/C4470/C3370 /C2270 Security Function Supplementary Guide

2.1.5 Configuration Requirements

The TOE is controller software of MFD that has copy, print, scan, and FAX functions.

Other than the MFD installed with this TOE, a FAX board is necessary as an option for using a FAX function, and installation of Windows 2000, Windows XP, or Windows VISTA is necessary as OS for the use from a remote client PC (general user client and

system administrator client).

For a general user client, the print driver, Network Scan Utility, and FAX driver shall be installed to general-purpose PC installed with the OS above.

For a system administrator client, Web browser and ApeosWare EasyAdmin shall be installed to general-purpose PC installed with the OS above.

This evaluation targets at the behavior on the above hardware and software. However the reliability of hardware and software described in the configuration is outside the scope of this evaluation.

2.2 Security Objectives

TOE counters threats described in 2.1.1 as follows by implemented security functions and fulfills the organizational security policies in 2.1.2.

Hard Disk Data Overwrite and Hard Disk Data Encryption functions, both of them are TOE security functions, are provided to cope with threats of unauthorized retrieve/use of document data stored in the internal HDD.

When Hard Disk Data Encryption function is enabled by a system administrator, the document data is encrypted before stored into the internal HDD when any of copy, print, scan, Network Scan, FAX, Internet FAX, or Direct FAX functions is operated.

For example, when copying of more than one set of the same document is instructed, the scanned document data is stored in the internal HDD of a MFD, and retrieved from the HDD for the number of specified sets and then printed. In this case, the scanned/stored document data are encrypted, and are encoded every time when retrieved from the internal HDD to be printed. Printed used document data are encrypted, and stored in the internal HDD.

When Hard Disk Data Overwrite function is enabled by a system administrator, the used document data stored in the internal HDD is deleted by overwriting the document data area in the internal HDD when each of copy, print, scan, Network Scan, FAX, Internet FAX, or Direct FAX jobs is completed.

When each of the above jobs is completed, used document data are stored in the internal HDD after being encrypted using Hard Disk Data Encryption function. Overwriting, therefore, is performed on encrypted used document data.

User Authentication is provided to cope with the threat of unauthorized access to MFD functions and document data. To allow only the authorized general user to use MFD functions and to access the document data within the scope of his/her authority, the user ID and password entered from MFD control panel or general user client are required for identification and authentication.

User Authentication and System Administrator's Security Management are provided to cope with the threat of unauthorized access to TOE setting data. To accord a privilege to a system administrator, the User Authentication function requires the system administrator's ID and password entered from MFD control panel or system administrator client for identification and authentication. Only the authenticated system administrator can refer to and change the TOE security function settings with System Administrator's Security Management.

When Customer Engineer Operation Restriction function is enabled, a system administrator can restrict CE's operation in the system administrator mode to inhibit CE from changing the settings related to System Administrator's Security Management. With this function enabled, the threat of unauthorized access to the TOE setting data is countered.

Internal Network Data Protection is provided to cope with the threats of interception and alteration of the document data, TOE setting data, and security audit log data that are on the internal network. This function establishes the secure data transmission between TOE and the remote (general user client, system administrator client, server) with the encryption communication protocol (IPSec, SSL/TLS, etc.) and protects the communication data including document data, TOE setting data, and security audit log data from the threats of interception and alteration.

Security Audit Log is provided to cope with the unauthorized access. This function traces and records the information when and who logged in and operated what operation as well as the important events (configuration change, user operation, etc.). Only the authenticated system administrator can read out the security audit log data. The security audit log data obtained is encrypted and protected by Hard Disk Data Encryption before being stored into the MFD internal HDD.

FAX Flow Security function prevents passing public phone line data from the public phone line to the TOE or the internal network via the FAX board, which is connected to the controller board via USB interface, at any case except the regular FAX receive. This is to meet a requirement in the organizational security policies, which requires inhibiting unauthorized access to the internal network from the public telephone line.

3. Conduct and Results of Evaluation by Evaluation Facility

3.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are reported in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

3.2 Overview of Evaluation Conducted

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

Evaluation has started on 2009-09 and concluded by completion of the Evaluation Technical Report dated 2010-02. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development site on 2009-12 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and instructions, etc. and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on 2009-12 and 2010-2.

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

There were no concerns indicated during evaluation process by the Certification Body.

3.3 Product Testing

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

3.3.1 Developer Testing

The evaluator evaluated the integrity of developer testing that the developer executed and the test documentation of actual test results
The overview of evaluated tests performed by the developer is shown as follows;

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 3-1.

0

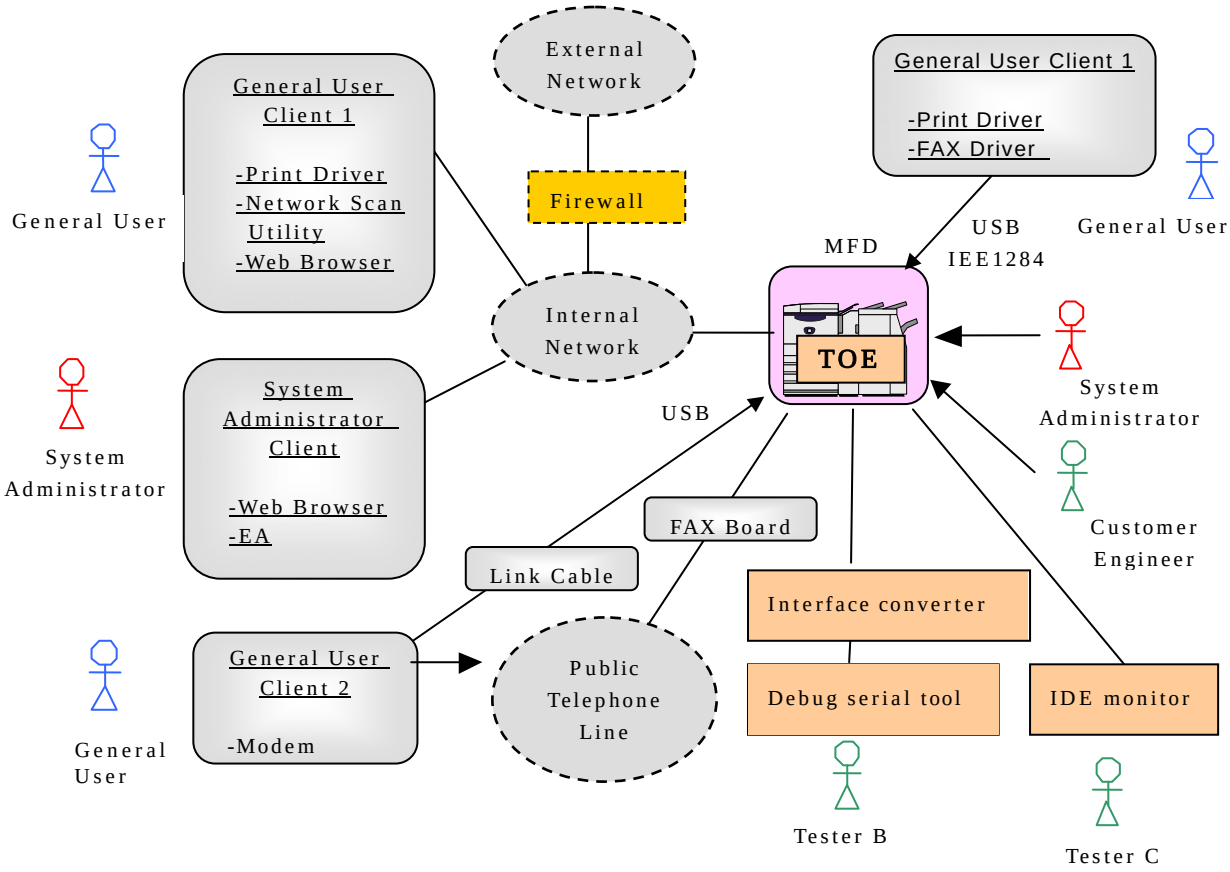

Figure 3-1 Configuration of Developer Testing

The developer testing is conducted in almost the same TOE operational environment (configuration for using the TOE, including the TOE itself) as identified in the ST.

Since this TOE is controller software common to ApeosPort-IV C5570/C4470/ C3370/C2270, DocuCentre-IV C5570/C4470/C3370/C2270 Series, ApeosPort-IV C5570 are used as MFD for this developer test.

Although installation of Windows2000, WindowsXP, or WindowsVista is required as OS of the user client (general user client and system administrator client) in the ST, this developer test is conducted using only the user client installed with Windows XP. That is because is it is judged that if the link between standard communication protocol and TOE security functions works without any problems on Windows XP environment, there shall be no problems on the other two OSs, because the TOE runs security functions on the standard communication protocol, and the standard communication protocol function is common to the above three OSs. Another developer test is conducted and confirmed that standard communication protocol of the other two OSs work without any problems.

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follows:

a. Test outline

The testing conducted by the developer is outlined as follows.

(1) Access to TSFI of TOE is enabled from the control panel of MFD and Web browser of system administrator client. When a general user uses a TOE's general function from the control panel and general user client (ex. Printer driver), the TOE security function (Hard Disk Data Overwrite) automatically operates. The TOE security functions are tested by stimulating the TOE, namely entering data to TSFI using the control panel, Web browser and printer driver.

(2) Debug serial tool and IDE monitor shown in Figure 3-1 are used to observe the test results of TOE security functions. The debug serial tool was connected to the MFD via the unique interface-converter and is used to check the final status of data in the HDD, i.e. the overwritten/encrypted data by Hard Disk Data Overwrite / Hard Disk Data Encryption.

The IDE monitor was connected to the controller board and the HDD within the MFD. The IDE monitor was used to check the contents of data transmitted through IDE bus, i.e. the data to be overwritten/encrypted by Hard Disk Data Overwrite / Hard Disk Data Encryption.

(3) The test on the operation error of Hard Disk Data Overwrite was conducted by generating HDD pseudo errors (After turning off the HDD, the HDD is turned on again.) This is enabled by connecting the trunk cable which has a HDD-power-off switch to the HDD.

(4) To conduct a test on sending/receiving FAX between the TOE and general user client, a general user client in Figure 3-1 is connected to the public phone line, and sent/received a FAX.

(5) To observe a testing result of internal network data protection (encryption protocol such as IPSec) of the TOE, the tool for confirming communication packets in the internal network was used.

b. Scope of Testing Performed

Testing is performed about 60 items by the developer. The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

c. Result

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

3.3.2 Evaluator Independent Testing

Evaluator executed the independent testing to reconfirm that Security functions are certainly implemented from the evidence shown by the process of the evaluation. Outlining of the independent testing performed by the developer is as follow;

1) Evaluator Independent Test Environment

The evaluator used almost the same test configuration which was used by the developer. Figure 3-2 shows its configuration. Test configuration performed by the evaluator shall be almost the same configuration with TOE configuration identified in ST.

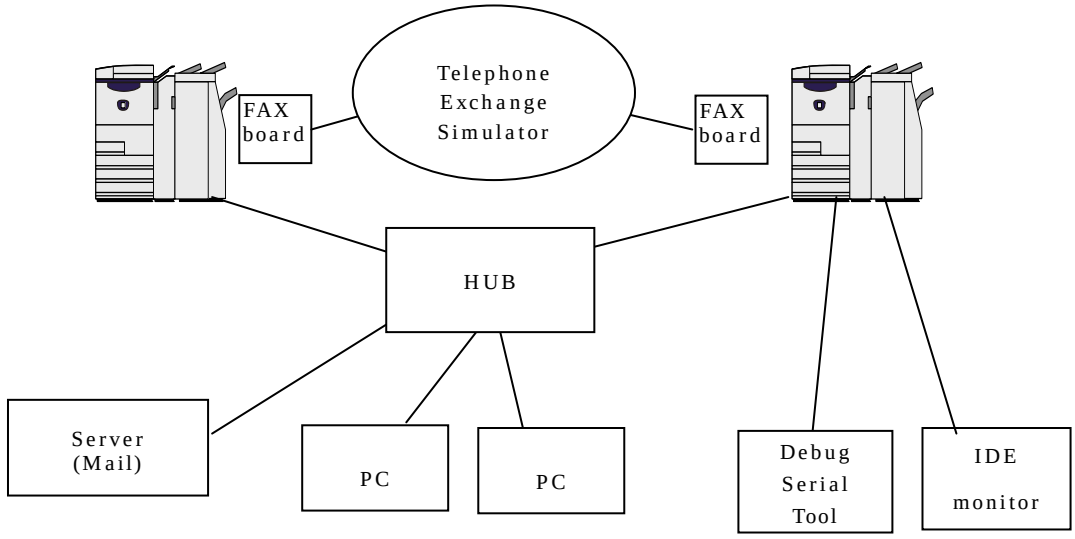

Figure 3-2 Evaluator Testing Configuration

This evaluator testing was conducted by using only ApeosPort-IV C3370 as MFD and Windows XP as OS. The basis for the validity of not conducting testing on all types of OS identified in the ST is the same as descriptions in Developer Testing (3.3.1 1)).

2) Outlining of Evaluator Independent Testing

Independent testing performed by the evaluator is as follows;

a. In terms of Evaluator Independent Testing

Evaluator devised the independent testing from the developer testing and the provided documentation in terms of followings.

(1) From a viewpoint of sampling of developer testing, tested all the items tested by the developer.
(2) Selected 6 items as independent testing from a view point of analysis of parameter limit values since some of the interfaces are not strictly tested on the performance of security functions in the developer testing.

b. Outlining of Evaluator Independent Testing

Outlining of evaluator independent testing performed by the evaluator is as follows:

(1) Almost the same test method (e.g. debug serial, IDE monitor) as the developer testing, written in 3.3.1 2) a., is used for sampling test of the developer testing.
(2) As for the evaluator independent testing, to analyze parameter limit values of the interface of User Authentication function, validity was tested on the performances at data input of ID and password, and at the change of password of general users and system administrators in other than the settable range.

c. Result

All evaluator independent testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

3.3.3 Evaluator Penetration Testing

Evaluator devised and conducted the necessary penetration testing about the possibility of exploitable concern at assumed environment of use and attack level. Outlining of Evaluator penetration testing is as follows:

1) Outlining of Evaluator Penetration Testing

Outlining of penetration testing performed by the evaluator is as follows:

a. Vulnerability of concern

Evaluator searched the potential vulnerability from information which is within the public domain and provided evidence to identify the following vulnerability that requires penetration testing.

From the searched information within the public domain, the evaluator identified 16 potential vulnerability points (SSL/TLS/IPSec communication, bypassing of authentication from client, password remaining before reboot, cross-site scripting through Web, and unauthorized access through port forwarding) in the use of this TOE. The evaluator also identified 43 potential vulnerability points from the provided evidence document in the use of this TOE. Based on the above, the evaluator confirmed that penetration testing is

necessary to judge the abuse possibility.

The 43 vulnerability points identified from the evidence document are as follows:
*Unauthorized penetration from local interface for maintenance
*Security weakness due to the invalid TOE settings and data input
*Bypassing of authentication process (system administrator client / general user client)
*Penetration to initialization process
*Security weakness in simultaneous operations by multiple system administrators
*Unauthorized input in the entry form (system administrator client / general user client)
*Penetration from USB ports
*Unauthorized use of print requirement interface from CWIS
*Unauthorized operation/settings on the control panel
*Unauthorized settings from CWIS
*Conflict by simultaneous access to mailbox

b. Scope of Test Performed

Evaluator conducted the following penetration testing to determine the exploitable potential vulnerability.

A total of 14 penetration tests were prepared based on the 59 potential vulnerability points given in the above a., and detailed tests were conducted.

The following are the major items of the penetration test:
*Port scan survey about forwarding unnecessary ports from MFD LAN ports.
*Unauthorized access to the TOE from USB ports.
*Unauthorized access from Web browser of system administrator client (bypassing of authentication by recording user authentication URL, simultaneous settings using control panel and other system administrator client, inputting of unauthorized data such as script to the entry form, and inputting of types/values exceeding the limit to the parameter).
*Change of the media in which TOE setting data is stored.
*Unauthorized access from the Web browser of general user client (bypassing of authentication process by recording URL, entering of unauthorized program upon print request, TOE access during initialization processing)
*Security weakness in communication at failure in the communication negotiation of SSL/TLS and IPSec.

c. Result

In the conducted evaluator penetration testing, the exploitable vulnerability that attackers who have the assumed attack potential could not be found.

3.4 Evaluation Result

3.4.1 Evaluation Result

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

3.4.2 Evaluator comments/Recommendations

None.

4. Conduct of 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.

There were no concerns found in certification process.

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

5. Conclusion

5.1 Certification Result

The Certification Body verified the Evaluation Technical Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 were conducted appropriately to the TOE. The Certification Body determined the TOE was satisfied the assurance requirements of EAL3 prescribed in CC Part 3.

5.2 Recommendations

None.

6. 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
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

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

CWIS	CentreWare Internet Service
EA	ApeosWare EasyAdmin
IIT	Image Input Terminal
IOT	Image Output Terminal
MFD	Multi Function Device Indicate Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570/C4470/C3370/C2270 Series in this report.
PDL	Page Description Language

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

Term	Definition
General User	Any person who uses copy, scan, FAX, and print functions of MFD.
System Administrator	An authorized user who manages MFD maintenance and configures TOE security functions.
Customer Engineer	Customer service engineer, an engineer who maintains and repairs MFD.
Attacker	A malicious user of TOE
Control Panel	A panel of MFD on which buttons, lamps, and a touch screen panel are mounted to operate the MFD
General User Client	A client for general user to operate the MFD.

Term	Definition
System Administrator Client	A client for system administrator. An administrator can refer to and rewrite TOE setting data of MFD via Web browser.
User Client	This term covers both System Administrator Client and General User Client.
System Administrator Mode	An operation mode that enables a system administrator to refer to and rewrite TOE setting for device operation and that for security functions according to the operational environment. This mode is distinguished from the operation mode that enables a general user to use the MFD functions
CentreWare Internet Service (CWIS)	A service to retrieve the document data scanned by MFD from Mailbox. It also enables a system administrator to refer to and rewrite TOE configuration data via Web browser.
ApeosWare EasyAdmin	Software for the system administrator to conduct settings and management to multiple MFDs from a system administrator client. EasyAdmin enables reference and editing of registration information such as user information (ID and password of general user and system administrator), mailbox, address book, and job flow, and also the basic device information in a list. EasyAdmin is different from CWIS that it enables the TOE settings for multiple MFDs, although CWIS enables the TOE settings of system administrator security management function only for one MFD. However, EasyAdmin enables only a part of TOE settings that can be set from the operation panel and CWIS.
Print Driver	Software for a general user to convert the data on a general user client into print data written in page description language (PDL), a readable format for MFD.
FAX Driver	Software for Direct FAX function, which enables a general user to FAX data to the destination directly from a general user client through MFD. The user can send the FAX data just as printing

Term	Definition
Network Scan Utility	Software for a general user client to retrieve the document data stored in Mailbox of MFD.
Decompose Function	A function to analyze and convert the print data written in PDL into bitmap data
Decompose	To analyze and convert the data written in PDL into bitmap data by decompose function.
Print Function	A function to decompose and print out the print data transmitted by a user client.
Print Control Function	A function to control the device to enable print operation.
Copy Function	A function in which original is read from IIT and then printed out from IOT according to the general user's instruction from the control panel. When more than one copy is ordered for one original, the data read from IIT is first stored into the MFD internal HDD. Then, the stored data is read out from the HDD as needed so that required number of copies can be made.
Scan Function	According to the general user's instruction from the control panel, the original data is read from IIT and then stored into Mailbox within the MFD internal HDD. The stored document data can be retrieved via standard Web browser by CWIS or Network Scan Utility function.
Network Scan Function	A function in which original data is read from IIT and then transmitted to FTP server, SMB server, or Mail server according to the information set in the MFD. This function is operated according to the general user's instruction from the control panel.
FAX Function	A function 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 then sent to the destination via public telephone line. The document data is received from the sender's machine and then printed out from the recipient's IOT.
Direct FAX Function	A FAX function in which data is sent via public telephone line directly from a user client. The data

Term	Definition
	is first sent to MFD as a print job and then to the destination without being printed out.
Internet FAX Function	A FAX function in which the data is sent or received via the Internet, not public telephone line.
Mailbox	A logical box created in the MFD internal HDD. Mailbox stores the scanned document data or the data to be printed later. Mailbox is categorized into Personal Mailbox and Shared Mailbox.
Document Data	Document data means all the image data transmitted across the MFD when any of copy, print, scan or FAX functions is operated by a general user. The document data includes: • Bitmap data read from IIT and printed out from IOT (copy function), • Print data sent by general user client and its decomposed bitmap data (print function), • Bitmap data read from IIT and then stored into the internal HDD (scan function), Bitmap data read from IIT and sent to the FAX destination and the bitmap data faxed from the sender's machine and printed out from the recipient's IOT (FAX function).
Used Document Data	The remaining data in the MFD internal HDD even after deletion. The document data is first stored into the internal HDD, used, and then only its file is deleted.
TOE Setting Data	The data which is created by TOE or for TOE and may affect TOE operations. Specifically, it includes the information regarding the functions of Hard Disk Data Overwrite, Hard Disk Data Encryption, Customer Engineer Operation Restriction, Use of password entered from MFD control panel in user authentication, ID and password of system administrator, access denial due to authentication failure of system administrator ID, system administrator data, internal network data protection, security audit log, mailbox, and user authentication.
Security Audit Log	The chronologically recorded data of important

Term	Definition
Data	events of TOE. The events such as device failure, configuration change, and user operation are recorded based on when and who caused what event and its result.
Overwrite	To write over the area of the document data stored in the internal HDD when deleting the data.
External Network	The network which cannot be managed by the organization that manages TOE. This does not include the internal network.
Internal Network	Channels between MFD and highly reliable remote server / client PC. The channels are located in the network of the organization, the owner of TOE, and are protected from the security risks coming from the external network.

7. Bibliography

[1] Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570 /C4470/C3370/C2270 Series Controller Software for Asia Pacific Security Target Version 1.0.7 (January 27, 2010) Fuji Xerox Co., Ltd.

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

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

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

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 3.1 Revision 1, September 2006, CCMB-2006-09-001 (Translation Version 1.2, March 2007)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-002 (Translation Version 2.0, March 2008)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1 Revision 2, September 2007, CCMB-2007-09-003 (Translation Version 2.0, March 2008)

[11] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004

[12] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 3.1 Revision 2, September 2007, CCMB-2007-09-004 (Translation Version 2.0, March 2008)

[13] Fuji Xerox ApeosPort-IV C5570/C4470/C3370/C2270, DocuCentre-IV C5570 /C4470/C3370/C2270 Series Controller Software for Asia Pacific Evaluation Technical Report Version 1.2, February 10, 2010, Information Technology Security Center Evaluation Department