CRP-C0165-01

Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2007-11-19 (ITC-7184)
Certification No.	C0165
Sponsor	Fuji Xerox Co., Ltd.
Name of TOE	ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software
Version of TOE	Controller ROM Ver.1.0.10
PP Conformance	None
Conformed Claim	EAL3
Developer	Fuji Xerox Co., Ltd.
Evaluation Facility	Information Technology Security Center

This is to report that the evaluation result for the above TOE is certified as follows.
2008-05-30

Hideji Suzuki, 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 2.3 (ISO/IEC 15408:2005)
- Common Methodology for Information Technology Security Evaluation Version 2.3 (ISO/IEC 18045:2005)

Evaluation Result: Pass

"ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software" 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 "ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software" (hereinafter referred to as "the TOE") conducted by Information Technology Security Center (hereinafter referred to as "Evaluation Facility"), and it reports to the sponsor, Fuji Xerox Co., Ltd..

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to "1.5.9 Documents Attached to Product" for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

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.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software
ROM Versions:	Controller ROM Ver.1.0.10
Developer:	Fuji Xerox Co., Ltd.

1.2.2 Product Overview

This Product is ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software including Data Security Kit Option, Which is the digital Multi Function Peripheral (hereinafter referred to as "MFP") that has copy, print, scan and FAX functions.

The data security kit is an option which protects, from unauthorized disclosure, the document data which is stored in the internal HDD after being processed by the MFP.

The document data and TOE configuration data on the internal network are protected from unauthorized access via FAX line using public telephone line.

The Controller Software provides the following security functions:
- Hard Disk Data Overwrite
- Hard Disk Data Encryption
- System Administrator's Security Management
- Customer Engineer Operation Restriction

- FAX Flow Security

1.2.3 Scope of TOE and Overview of Operation

The physical scope of this TOE is the controller software recorded on the controller ROM which is mounted on the controller board.Figure 1-1 shows TOE physical scope and configuration of each unit.

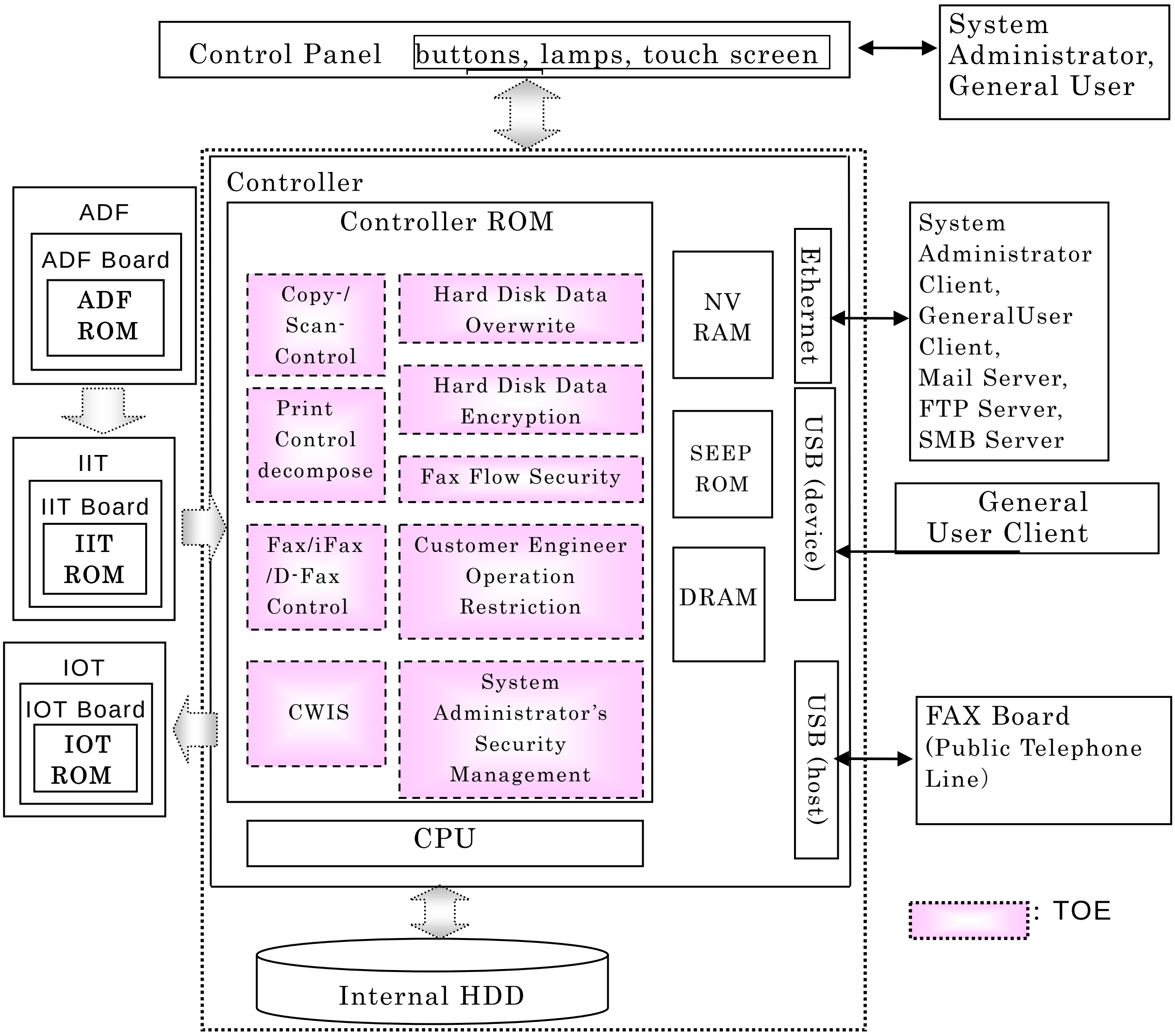

Figure 1-1 TOE Physical Scope and Configuration

Figure 1-2 shows the MFP operational environment to use TOE functions.

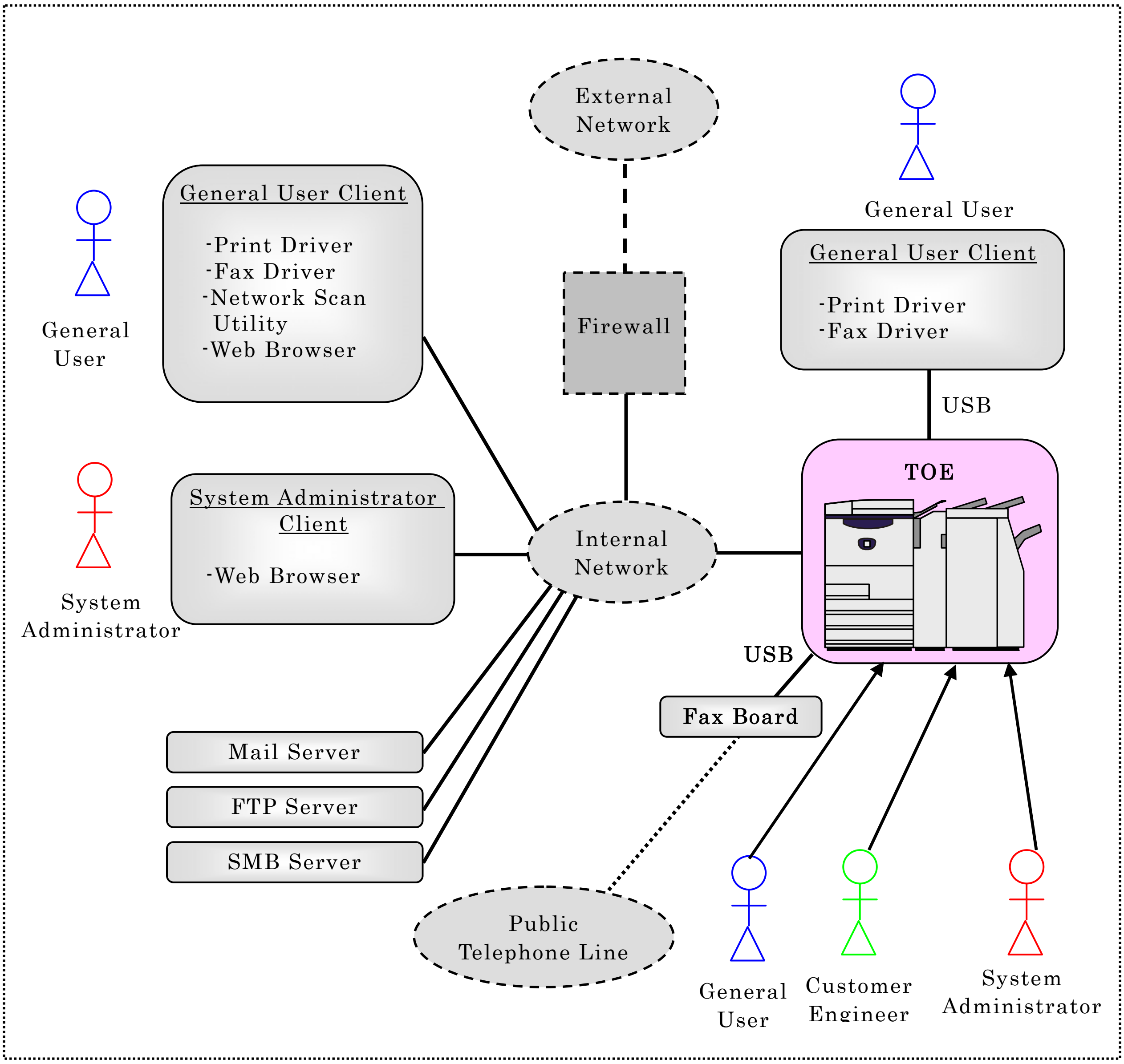

Figure 1-2 Operational Environment

The following are the overview of MFP operation and operational environment to use TOE functions.

(1) Control panel:
A general user can use such functions as copy, FAX, scan, and print.
A system administrator can configure, refer to, and change TOE configuration data.

(2) General user client:
When a client is linked to the MFP via the internal network and print driver, Network Scan Utility, and FAX driver are installed to the client, the general user can request the MFP to print, FAX and retrieve the document data.

The user can also request the MFP to retrieve the scanned document data via Web browser. Additionally, the user can change the configurations which user registered to the MFP: Mailbox name, password, access control, and automatic deletion of document.

When the client is linked to the MFP directly via USB, print/FAX driver is installed to the client, the user can request the MFP to print/FAX the document data.

(3) System administrator client:
A system administrator can configure, refer to, and change TOE configuration data and download security audit log data via Web browser.

(4) Mail server:
The MFP can send the document data to Mail server via mail protocol. (The document data was created by a general user using scan function of MFP.)

(5) FTP server:
The MFP can send the document data to FTP server via FTP. (The document data was created by a general user using scan function of MFP.)

(6) SMB server:
The MFP can send the document data to SMB server via SMB (a network file sharing protocol for Windows). (The document data was created by a general user using scan function of MFP.)

(7) FAX board:
The FAX board is connected to external public telephone line and supports G3/G4 protocols (the international standard for FAX communication). The FAX board is connected to the MFP via USB interface to enable FAX communication.

1.2.4 TOE Functionality

The TOE provides the basic functions of control panel, copy, print, scan, FAX, iFAX / D-FAX, and CWIS to general user.

Regarding the above basic functions, the TOE also provides the following functions to ensure the security of assets to be protected:
- Hard Disk Data Overwrite
- Hard Disk Data Encryption
- System Administrator's Security Management
- Customer Engineer Operation Restriction
- FAX Flow Security

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 "ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software 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 B of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) 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], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in "ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated 2008-05 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is 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.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

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

1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function.
This TOE assumes the attackers have "low-level" attack-ability. Thus, it is adequate to claim the SOF-Basic as the minimum strength of TOE functions.

1.5.4 Security Functions

This TOE provides the following security functions:

- Hard Disk Data Overwrite
  This TOE prevents unauthorized disclosure of used document data. The document data created during each job processing is temporarily stored in the internal HDD. After each job is completed, the used data is overwritten with new data.

- Hard Disk Data Encryption
  This TOE prevents unauthorized disclosure of the document data which was created during each job processing. The document data is encrypted before stored into the internal HDD.

- System Administrator's Security Management

  To accord a privilege to a specific user, this TOE allows only the authenticated system administrator to access the system administrator mode which enables him/her to configure the following security functions from the control panel:

  Enable or disable Hard Disk Data Overwrite
  Enable or disable Hard Disk Data Encryption
  Configure the cryptographic seed key for Hard Disk Data Encryption
  Enable or disable use of password entered from MFP control panel in user authentication
  Change the ID and password of key operator
  Change the password of system administrator
  Set the allowable number of system administrator's authentication failures before access denial
  Enable or disable Customer Engineer Operation Restriction

  Additionally, this TOE allows only the system administrator authenticated from Web browser to configure the following security functions via CWIS:

  Change the ID and password of key operator;
  Change the password of system administrator;
  Set the allowable number of system administrator's authentication failures before access denial.

- Customer Engineer Operation Restriction

  This TOE enables a system administrator to inhibit CSE from configuring the TOE security functions. Thus, an attacker who is impersonating CSE cannot configure or change the configurations.

  Hard Disk Data Overwrite
  Hard Disk Data Encryption
  Setting of the ID and password of key operator
  Setting of the password of system administrator
  Setting of access denial due to authentication failure of system administrator identification
  Customer Engineer Operation Restriction

- FAX Flow Security

  This TOE prevents unauthorized access to the internal network via telephone line or a modem which are used for FAX function. The data other than FAX data cannot flow into the internal network so that unauthorized access is blocked.

1.5.5 Threat

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

Table 1-1 Assumed Threats

Threat (Identifier)	Description
Unauthorized retrieval of document data stored in the internal HDD	
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 used document data.
Unauthorized access to document data and TOE configuration data	
T.CONFDATA	An attacker may access, read, or alter, from control panel or

Threat (Identifier)	Description
	Web browser, the TOE configuration data which only a system administrator is allowed to access.

1.5.6 Organisational Security Policy

Organisational security policy required in use of the TOE is presented in Table 1-2.

Table 1-2 Organisational Security Policy

Organizational Policy (Identifier)	Description
Request from the U.S. agency	
P.FAX_OPT	At the behest of the U.S. Department of Defense, it must be ensured that the internal network cannot be accessed via public telephone line.

1.5.7 Configuration Requirements

This TOE is ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software including Data Security Kit Option, which is the digital Multi Function Peripheral that has copy, print, scan and FAX functions.

Besides the MFP, a FAX board should be adopted as an option for FAX function. One of the OSs (Windows 2000, Windows XP, or Windows VISTA) should be also installed for TOE use from the remote clients of general user and system administrator.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumptions in Use of the TOE

Assumption (Identifier)	Description
Personnel Confidence	
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 it viciously.
Protection Mode	
A.SECMODE	A system administrator shall configure the TOE as follows: *Use of password entered from MFP control panel in user authentication: enabled *Length of system administrator password: 7 characters or more *Access denial due to authentication failure of system administrator ID: enabled *Allowable number of system administrator's authentication failures before access denial: 5 *Customer Engineer Operation Restriction: enabled *Hard Disk Data Overwrite: enabled *Hard Disk Data Encryption: enabled

Assumption (Identifier)	Description
	*Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters
Network Connection Assumption	
A.NET	*Interception on the internal network of the MFP with the TOE installed shall be disabled. *When the internal network of the MFP with the TOE installed is linked to the external network, access to the MFP from the external network shall be disabled.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

*ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 System Administrator Guide
Version: DE3826J1-1 edition 1.2

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 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 report 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.

2.2 Overview of Evaluation Conducted

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

Evaluation has started on 2007-11 and concluded by completion the Evaluation Technical Report dated 2008-05. 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 sites on 2008-02 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating instructions and records 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 2008-02.

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.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1) Developer Test Environment

Test configuration performed by the developer is showed in the Figure 2-1.

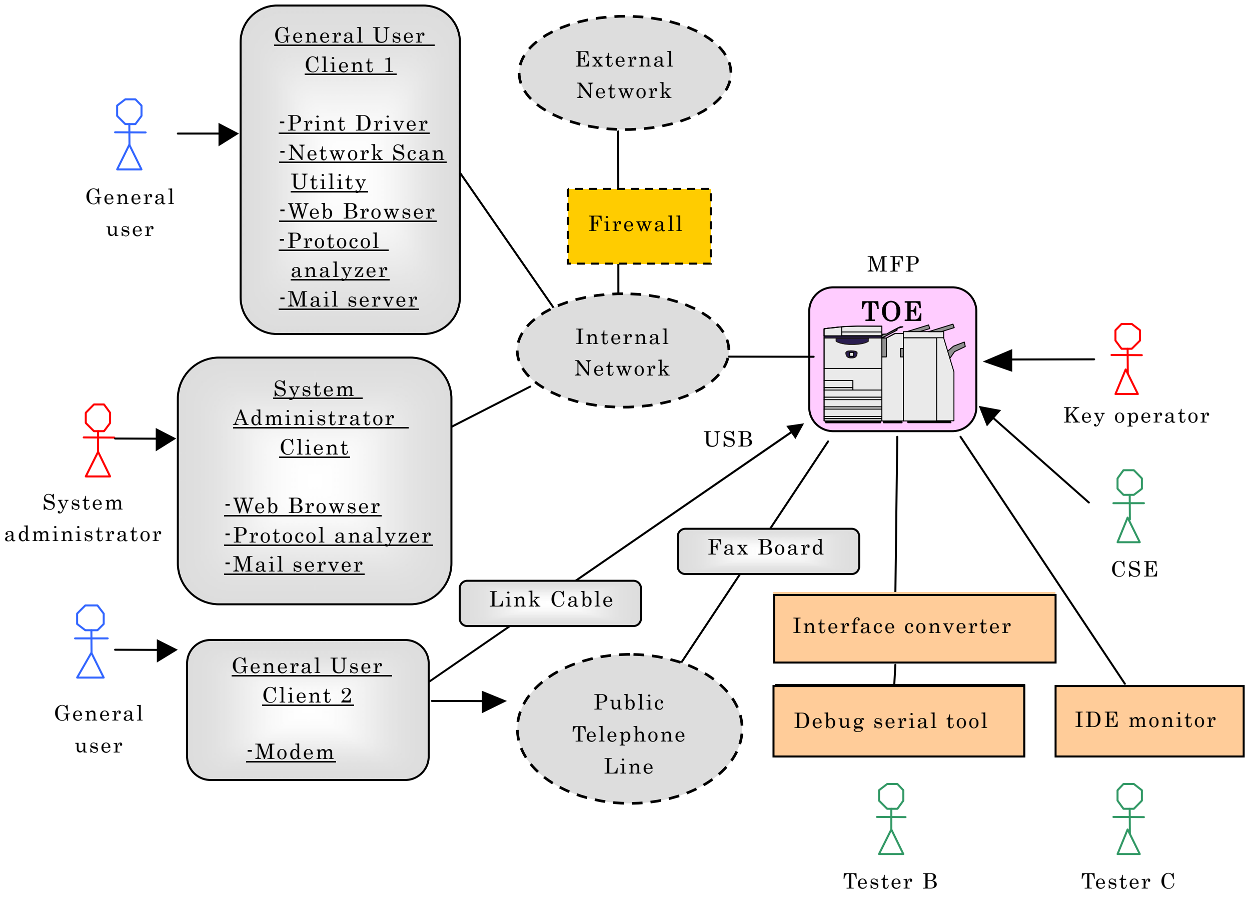

Figure 2-1 Configuration of Developer Testing

2) Outline of Developer Testing

The testing conducted by the developer is outlined as follows.

a. Test Configuration

The test configuration used by the developer is shown in Figure 2-1. The developer conducted the testing in almost the same TOE operational environment as identified in the ST.

b. Testing Approach

For the testing, following approach was used.

(1) MFP used for a test is ApeosPort-III C3300/C2200.
Although this product have the composition of CP model (copy function and printer functional), CPF model (copy function, printer function and FAX functional), and CPFS model (copy function, printer function, FAX function and scanner functional), all the models were summarized and it is named generically ApeosPort-III C3300/C2200 series.
The tests were conducted by the CPFS model equipped with all interfaces.

(2) The MFP for testing is connected, via the network (Ethernet) for testing, to the user client 1 (PC) on which print driver, network scan utility, and Web browser are installed.

(3) The user client 2 (PC) is connected to public telephone line and sends/receives a FAX to/from the TOE.

(4) The system administrator client accesses the MFP for testing via the network (Ethernet) for testing from Web browser.

(5) The debug serial tool is connected to the MFP 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.

(6) The IDE monitor is connected to the controller board and the HDD within the MFP. The IDE monitor is used to check the contents of data transmitted between the board and HDD, *i.e.* the data to be overwritten/encrypted by Hard Disk Data Overwrite / Hard Disk Data Encryption.

(7) The test on the operation error of Hard Disk Data Overwrite is conducted by generating HDD pseudo errors. This is enabled by connecting the trunk cable which has an HDD-power-off switch to the HDD.

c. Scope of Testing Conducted

The developer conducted 30 tests.

The following show the number of tests conducted for each security function:

Hard Disk Data Overwrite: 19 tests
Hard Disk Data Encryption: 4 tests
System Administrator's Security Management: 4 tests
Customer Engineer Operation Restriction: 1 test
FAX Flow Security: 2 tests

The scope of testing covers all behavior of each function. The quantity and scope of testing conducted are satisfactory as a whole.

d. Result

The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The evaluator confirmed that the developer testing approach and tested items were legitimate and that the approach and results of actual tests matched those described in the test plan.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator shall be almost the same configuration with developer testing. Figure 2-2 shows its schematic.

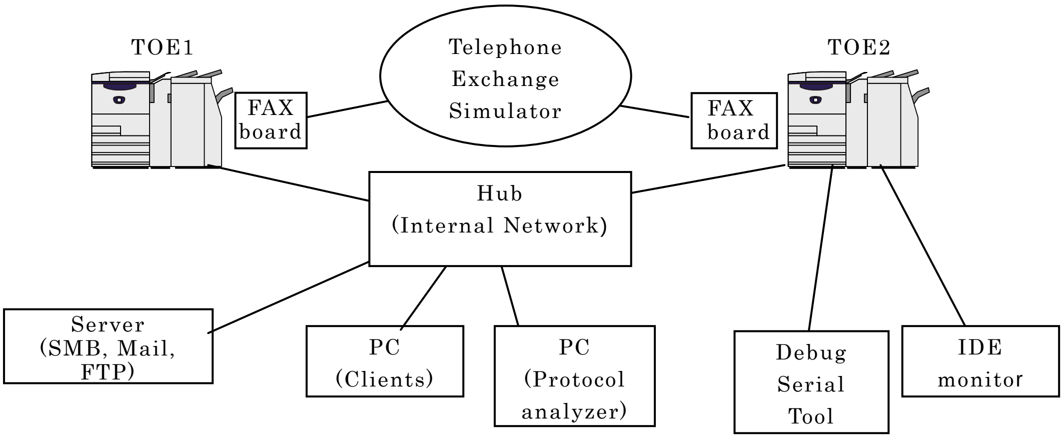

Figure 2-2 Evaluator Test Configuration

2) Outline of Evaluator Testing

Outline of testing performed by the evaluator is as follow.

a. Test configuration

The test configuration used by the evaluator is shown in Figure 2-2. The evaluator conducted testing in almost the same TOE operational environment as identified in the ST.

b. Testing Approach

The evaluator conducted testing in almost the same approach and TOE operational environment as those used in the developer testing.

c. Scope of Testing Conducted

The evaluator conducted 33 tests in total: 3 independent tests and 30 tests sampling the developer tests. The following were considered as the selection criteria of the tests.

(1) Independent testing

Exactitude of developer testing for security functions: the testing was conducted based on parameter-threshold analysis.

(2) Sampling of developer tests

The evaluator conducted all 30 tests conducted by the developer.

d. Result

All evaluator testing conducted was completed correctly. The evaluator confirmed the behavior of the TOE and that all the behavior shown in the test results matched the expected one.

2.4 Evaluation Result

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

3. Conduct of Certification

The following certification was conducted 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 review, which were sent to evaluation facility.

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

4. Conclusion

4.1 Certification Result

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

4.2 Recommendations

None

5. Glossary

The abbreviations 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 specific abbreviations for the TOE used in this report are listed below.

ADF	Auto Document Feeder
G3/G4	Group 3 Facsimile / Group 4 Facsimile
IIT	Image Input Terminal
IOT	Image Output Terminal
IPSEC	Security Architecture for Internet Protocol
MFP	Multi Function Peripheral
NVRAM	Non Volatile Random Access Memory
SEEPROM	Serial Electronically Erasable and Programmable Read Only Memory
SMB	Server Message Block

The glossaries used in this report are listed below. (Relevant terms are included for better understanding.)

Term	Definition
General User	Any person who uses copy, scan, FAX, and print functions of MFP.
Key Operator	An authorized user who manages MFP maintenance and

Term	Definition
	configures TOE security functions.
System Administrator Privilege (SA)	A user authorized by key operator to manage MFP maintenance and configure TOE security functions.
System Administrator	An authorized user who manages MFP maintenance and configures TOE security functions. This term covers both key operator and SA.
Customer Service Engineer (CSE)	A Fuji Xerox engineer who maintains and repairs MFP.
Attacker	A malicious user of TOE.
Control Panel	A panel of MFP on which buttons, lamps, and a touch screen panel are mounted to operate the MFP.
General User Client	A client for general user and SA to operate the MFP.
System Administrator Client	A client for system administrator. An administrator can refer to and rewrite TOE configuration data of MFP via Web browser.
CentreWare Internet Service (CWIS)	A service to retrieve the document data scanned by MFP from Mailbox. It also enables a system administrator to refer to and rewrite TOE configuration data via Web browser.
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 MFP.
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 MFP. The user can send the FAX data just as printing.
Network Scan Utility	Software for a general user client to retrieve the document data stored in Mailbox of MFP.
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.
Store Print	A print function in which bitmap data (decomposed print data) is temporarily stored in the MFP internal HDD and then printed out according to the general user's instruction from the control panel. There are three ways for the Store Print: *Security Print A user can start print operation by entering his/her

Term	Definition
	password from the control panel. The user password needs to be preset from the print driver of the general user client. *Sample Print When printing several copies, only one copy is printed out first as a sample document. A user can check its quality and print out the remaining copies by sending an instruction from the control panel. *Mailbox Print Decomposed bitmap data is stored in Mailbox and printed out according to the general user's instruction from the control panel.
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 MFP 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 MFP 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 MFP. 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 (D-FAX)Function	A FAX function in which data is sent via public telephone line directly from a user client. The data is first sent to MFP as a print job and then to the destination without being printed out.
Internet FAX (iFAX) 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 MFP 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 MFP 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

Term	Definition
	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 MFP internal HDD even after deletion. The document data is first stored into the internal HDD, used, and then only its file is deleted.
TOE Configuration 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, System Administrator's Security Management, Customer Engineer Operation Restriction, Internal Network Data Protection, Security Audit Log, Mailbox, and User Authentication.
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 MFP 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.

6. Bibliography

[1] ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller Software Security Target Version 1.0.5 (Feburary 28,2008) 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 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] ApeosPort-III C3300/C2200 DocuCentre-III C3300/C2200 Series Controller

Software Evaluation Technical Report Version 1.2, May 13, 2008, Information Technology Security Center