Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2008-02-22 (ITC-8204)
Certification No.	C0183
Sponsor	Fuji Xerox Co., Ltd.
Name of TOE	Xerox WorkCentre 5225A/5230A
Version of TOE	Controller+PS ROM Ver.1.224.0 IOT ROM Ver.11.21.0 IIT ROM Ver.23.7.0 ADF ROM Ver.20.0.0
PP Conformance	None
Conformed Claim	EAL2
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.
2008-09-11

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

"Xerox WorkCentre 5225A/5230A" 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 "Xerox WorkCentre 5225A/5230A" (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..

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:	Xerox WorkCentre 5225A/5230A	
ROM Versions:	Controller + PS ROM	Ver.1.224.0
	IOT ROM	Ver.11.21.0
	IIT ROM	Ver.23.7.0
	ADF ROM	Ver.20.0.0
Developer:	Fuji Xerox Co., Ltd.	

1.2.2 Product Overview

This TOE is Xerox WorkCentre 5225A/5230A, the Multi Function Peripheral (hereinafter referred to as "MFP") that has copy, print, scan and fax functions.

The MFP is assumed to be used, at general office, from the control panel, public telephone line, clients (for general user and system administrator) and servers which are linked to the MFP via internal network, and general user client which is directly linked to the MFP.

The MFP provides the following functions:

- Hard Disk Data Overwrite
- Hard Disk Data Encryption
- User Authentication
- System Administrator's Security Management
- Customer Engineer Operation Restriction
- Security Audit Log
- Internal Network Data Protection
- FAX Flow Security

1.2.3 Scope of TOE and Overview of Operation

The physical scope of this TOE is the whole MFP and consists of the PWB units of controller board, control panel, ADF board, IIT board, and IOT board. Figure 1-1 shows TOE physical scope and configuration of each unit.

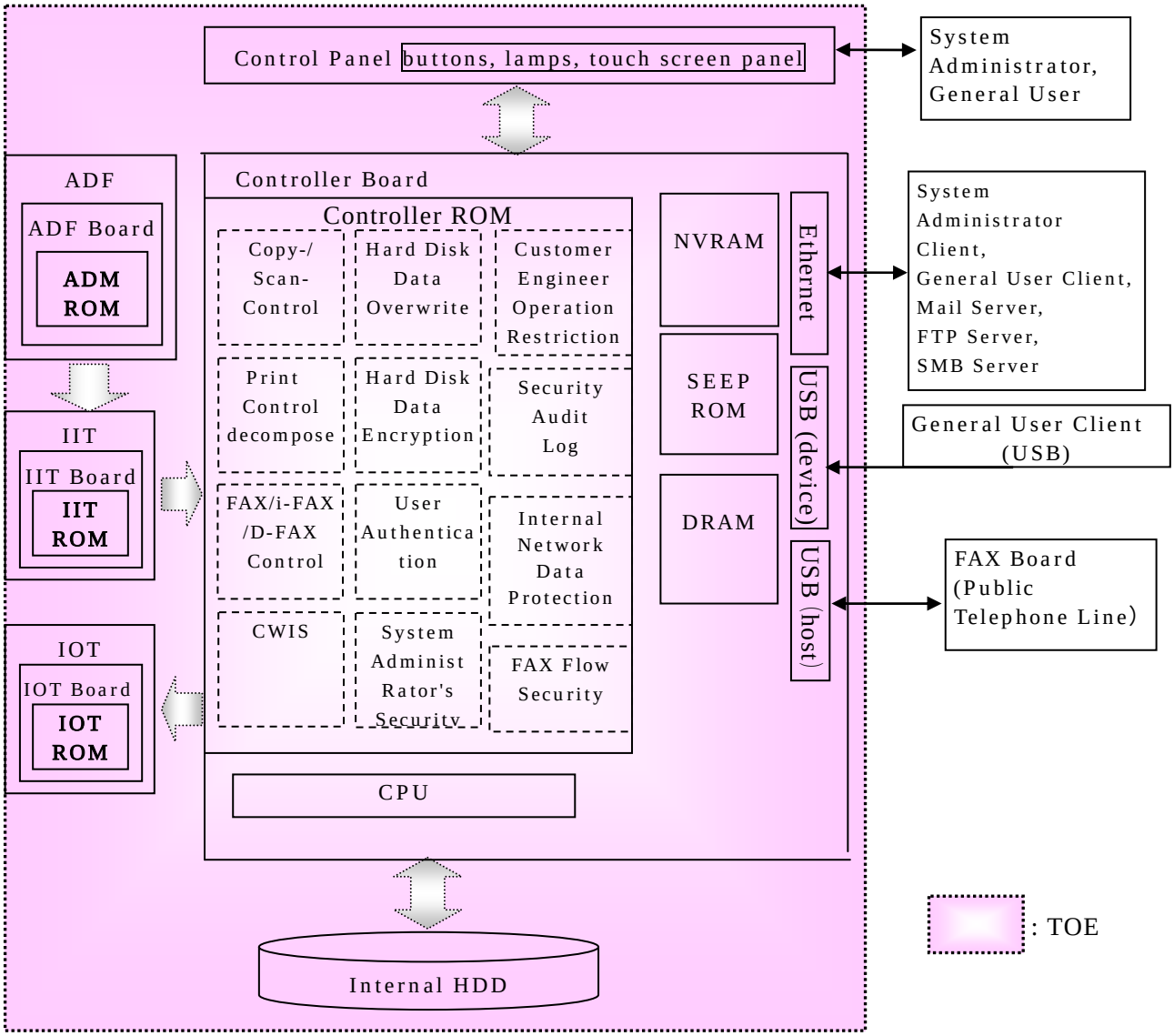

Figure 1-1 TOE Physical Scope and Configuration

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

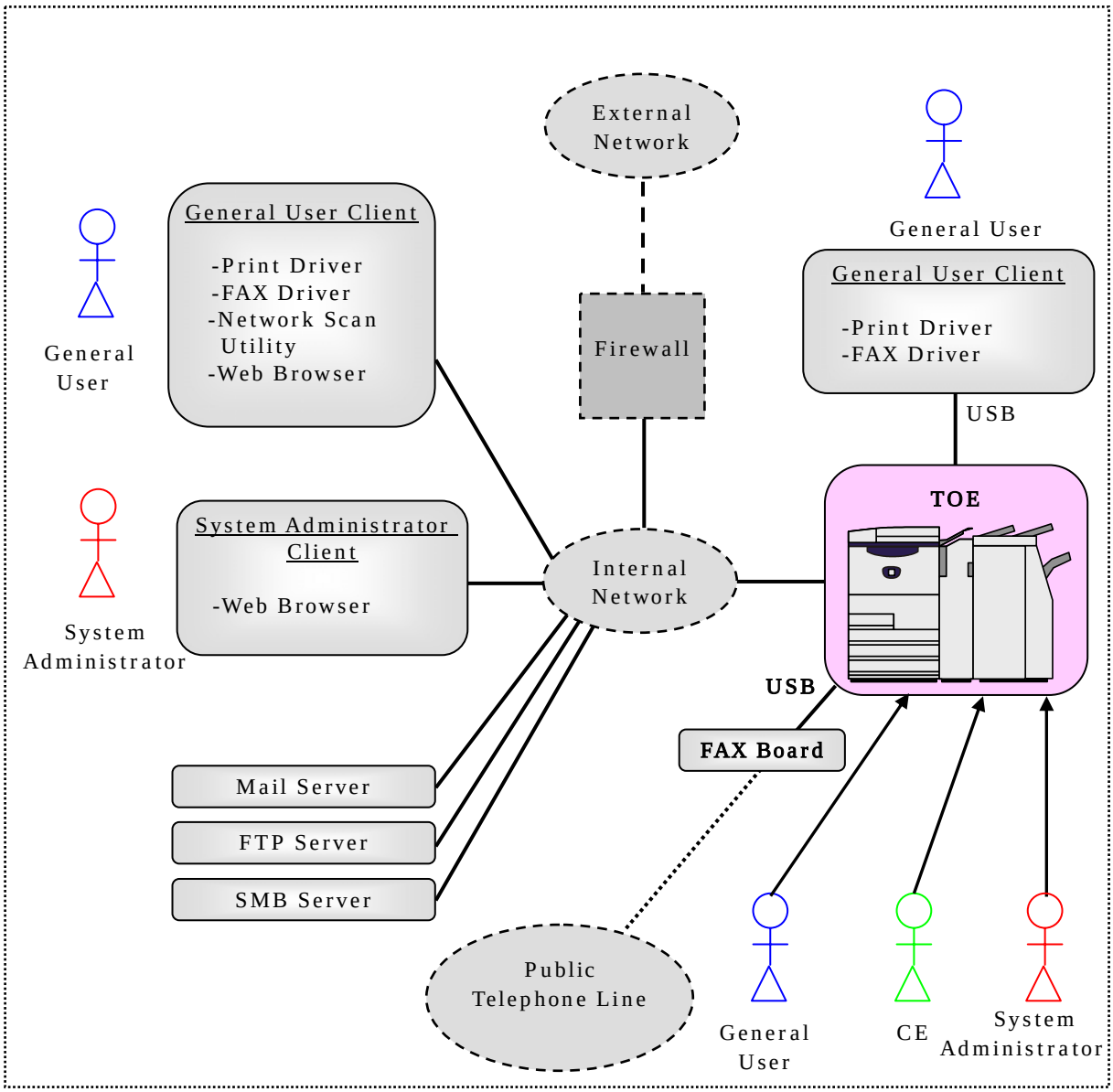

Figure 1-2 Operational Environment

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 and 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, i-FAX / 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
- User Authentication
- System Administrator's Security Management
- Customer Engineer Operation Restriction
- Security Audit Log
- Internal Network Data Protection
- 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 "Xerox WorkCentre 5225A/5230A 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 "Xerox WorkCentre 5225A/5230A 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 verified the Evaluation Technical Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is 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 2008-8 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.

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 EAL2 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.

- User Authentication
  This TOE restricts access to the TOE functions to authenticated general user. To use TOE, a user needs to enter his/her ID and password from the control panel, Web browser, or Network Scan Utility.

- System Administrator's Security Management
  This TOE restricts access to the tool mode to system administrator for according a privilege to a specific user. Thus, only the authenticated system administrator can configure and change the configurations of TOE security functions and can download the security audit log data from the control panel or Web browser.

- 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.

- Security Audit Log

  This TOE enables a system administrator to monitor unauthorized use of the TOE or attempt to it. The important events of TOE such as device failure, configuration change, and user operation are traced and recorded based on when and who operated what function.

- Internal Network Data Protection

  This TOE protects the security of communication data (document data, security audit log data, and TOE configuration data). To enable secure data transmission between TOE and the remote, the TOE supports general encryption communication protocols such as SSL/TLS, IPSec, SNMPv3, and S/MIME.

- 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 and security audit log 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 stored document data, used document data, and security audit log data.
Unauthorized access to document data and TOE configuration data	
T.CONFDATA	An attacker may access, read, or alter, from control panel or Web browser, the TOE configuration data which only a system administrator is allowed to access.
T.DATA_SEC	An attacker may read document data and security audit log data from control panel or Web browser without authorization.
Interception of document data and TOE configuration data	

Threat (Identifier)	Description
T.COMM_TAP	An attacker may intercept or alter document data, security audit log data, and TOE configuration data on the internal network.
T.CONSUME	An attacker may access TOE and use TOE functions without authorization.

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. agency, it must be ensured that the internal network cannot be accessed via public telephone line.

1.5.7 Configuration Requirements

This TOE is "Xerox WorkCentre 5225A/5230A", the MFP manufactured by Fuji Xerox Co.,Ltd.

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

Assumption (Identifier)	Description
	authentication: enabled • Length of system administrator password: 9 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 • Type of authentication: User Authentication enabled • Length of user password (for general user and SA): 9 characters or more • Private Print configuration: store an authenticated job to Private Print area • Security Audit Log: enabled • SNMPv3 communication: enabled • Length of authentication password for SNMPv3 communication: 8 characters or more • SSL/TLS communication: enabled • IPSec communication: enabled • S/MIME communication: enabled • SMB communication: disabled • Hard Disk Data Overwrite: enabled • Hard Disk Data Encryption: enabled • Size of cryptographic seed key for Hard Disk Data Encryption: 12 characters • Scheduled Image Overwrite: enabled

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

* WorkCentre 5225A/5230A System Administrator Guide
  Version: XE3022EN0-2

* WorkCentre 5225A/5230A Security Function Supplementary Guide
  Version: 897E01112

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 2008-02 and concluded by completion the Evaluation Technical Report dated 2008-08. 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 2008-07 and examined procedural status conducted in relation to each work unit for delivery and operation 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 2008-07.

There were no concerns found in evaluation activities for each work unit.

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

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

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

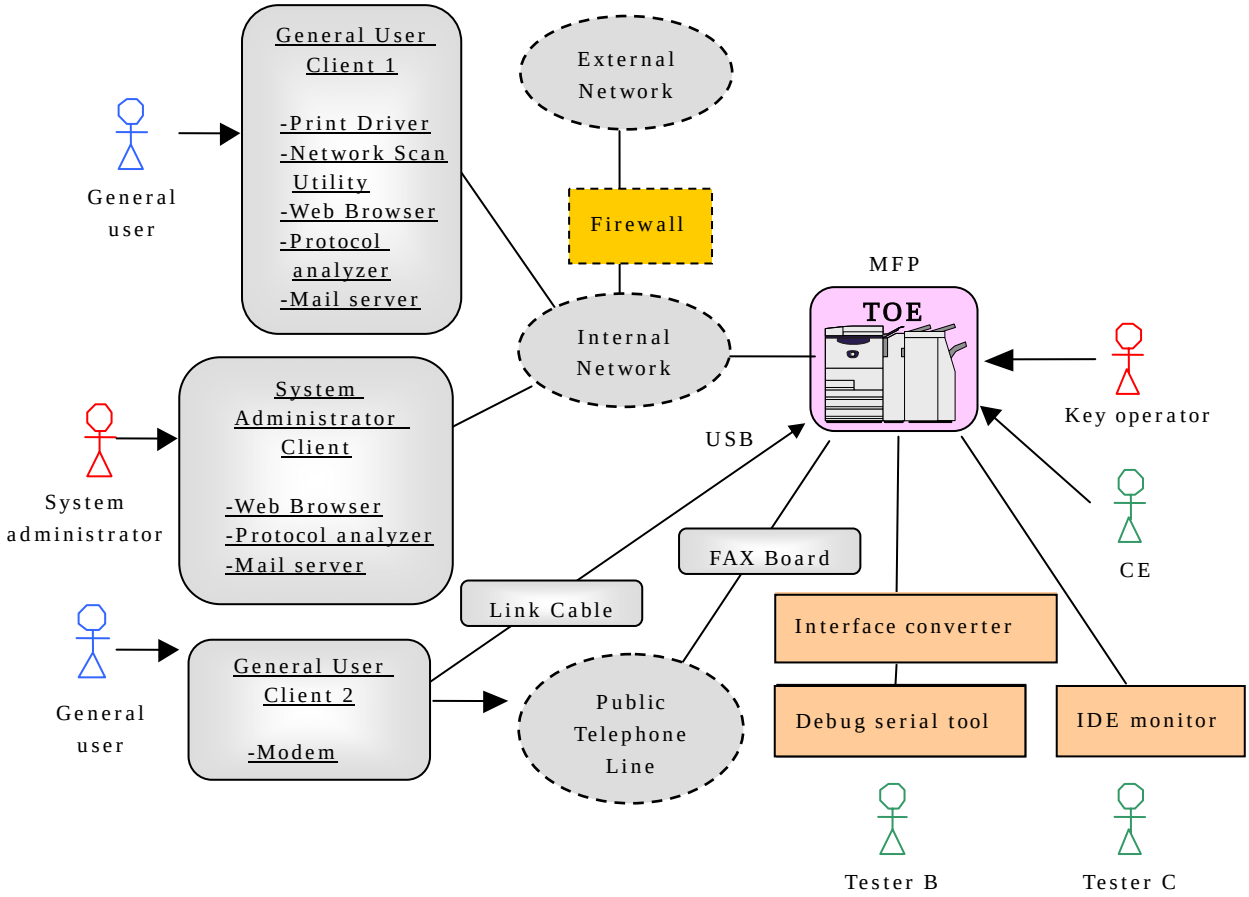

Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a. Test configuration

The test configuration performed by the developer is showed in the Figure 2-1. Developer testing was performed at almost the same TOE testing environment with the TOE configuration identified in ST.

b. Testing Approach

For the testing, following approach was used.

(1) 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.

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

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

(4) 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.

(5) 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.

(6) The protocol analyzer (ethereal) is installed on the system administrator client and general user client. The protocol analyzer is used to capture the network traffic and to check if the specified protocol and cryptography are used in the data transmission.

(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 Performed

Testing is performed about 53 items by the developer.
The following show the number of tests conducted for each security function:

- Hard Disk Data Overwrite: 18 tests
- Hard Disk Data Encryption: 4 tests
- System Administrator's Security Management: 4 tests
- User Authentication: 4 tests
- Customer Engineer Operation Restriction: 1 test
- Security Audit Log: 8 tests
- FAX Flow Security: 2 tests
- Internal Network Data Protection: 12 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

The test configuration performed by the evaluator shall be almost the same

configuration with developer testing. Figure 2-2 shows its schematic.

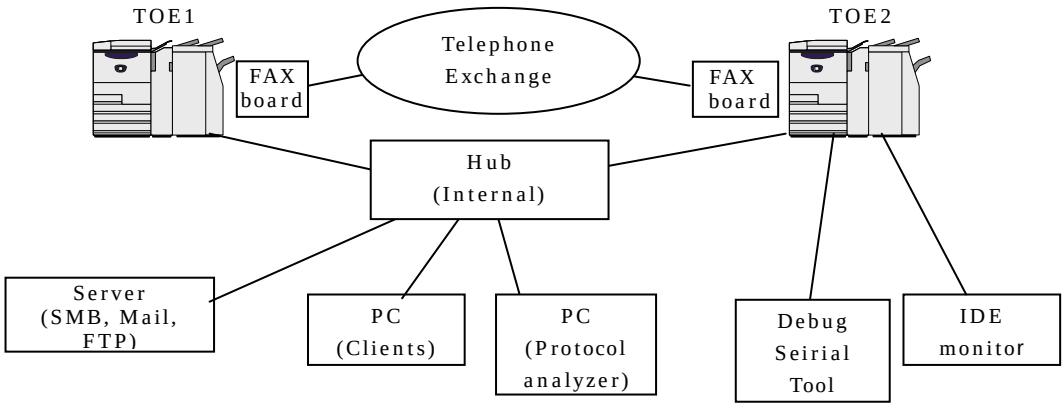

Figure 2-2 Evaluator Test Configuration

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

The test configuration performed by the evaluator is showed in the Figure 2-2. Evaluator testing was performed at almost the same TOE testing environment with the TOE configuration identified in 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 Performed

The evaluator conducted 59 tests in total: 6 independent tests and 53 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, and the detailed functions which were not tested by the developer were also tested.

(2) Sampling of developer tests

The evaluator conducted 53 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. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
2. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
3. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

There were no concerns found in evaluation activities and in certification process.

4. Conclusion

4.1 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 verified the TOE was satisfied the EAL2 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
SNMP	Simple Network Management Protocol
SSL/TLS	Secure Socket Layer / Transport Layer Security
S/MIME	Secure/Multipurpose Internet Mail Extensions

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 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 Engineer (CE)	A 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.
Tool Mode	An operation mode that enables a system administrator to refer to and rewrite TOE configuration 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 MFP functions.
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.

Term	Definition
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.
Private Print	In this print function, jobs are stored only when MFP authenticates a user with his/her ID and password which were preset in the print driver on a general user client. When the user is authenticated with his/her ID and password entered from the control panel, he/she can start print operation. (Private Print is one type of Store Print function in which 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.)
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

Term	Definition
	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 (i-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 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.
Personal Mailbox	The Mailbox privately used by a general user. Each user can create his/her own Personal Mailbox.
Shared Mailbox	The Mailbox shared by any general user. Key operator can create the 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 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.
Security Audit Log Data	The chronologically recorded data of important 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.
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,

Term	Definition
	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.
User Authentication	A function to limit the accessible TOE functions by identifying the user before he/she uses each TOE function.

6. Bibliography

[1] Xerox WorkCentre 5225A/5230A Security Target Version 1.0.4 (July 23,2008) 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] Xerox WorkCentre 5225A/5230A Evaluation Technical Report Version 1.0, August 6, 2008, Information Technology Security Center Evaluation Department