



Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	January 28, 2005 (ITC-5039)
Certification No.	C0029
Sponsor	Fuji Xerox Co., Ltd.
Name of TOE	Fuji Xerox ApeosPort C4535 I / C3626 I / C2521 I DocuCentre C4535 I / C3626 I / C2521 I Series Data Security Kit
Version of TOE	Controller ROM Ver1.3.0
PP Conformance	None
Conformed Claim	EAL2
TOE Developer	Fuji Xerox Co., Ltd.
Evaluation Facility	Japan Electronics and Information Technology Industries Association, Information Technology Security Center

This is to report that the evaluation result for the above TOE is certified as follows.
July 6, 2005

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center
Information-Technology Promotion Agency, Japan

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "General Requirements for IT Security Evaluation Facility".

- Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations-0407

Evaluation Result: Pass

"Fuji Xerox ApeosPort C4535 I / C3626 I / C2521 I DocuCentre C4535 I / C3626 I / C2521 I Series Data Security Kit Controller ROM Ver1.3.0" has been evaluated in accordance with the provision of the "General Rules for IT Product Security Certification" by Information-Technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:

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

Table of Contents

1. Executive Summary.....	1
1.1 Introduction.....	1
1.2 Evaluated Product.....	1
1.2.1 Name of Product.....	1
1.2.2 Product Overview.....	1
1.2.3 Scope of TOE and Overview of Operation	2
1.2.4 TOE Functionality	3
1.3 Conduct of Evaluation	4
1.4 Certificate of Evaluation	5
1.5 Overview of Report	5
1.5.1 PP Conformance	5
1.5.2 EAL.....	5
1.5.3 SOF.....	5
1.5.4 Security Functions	5
1.5.5 Threat	7
1.5.6 Organisational Security Policy	7
1.5.7 Configuration Requirements	7
1.5.8 Assumptions for Operational Environment.....	7
1.5.9 Documents Attached to Product.....	8
2. Conduct and Results of Evaluation by Evaluation Facility	9
2.1 Evaluation Methods.....	9
2.2 Overview of Evaluation Conducted	9
2.3 Product Testing.....	9
2.3.1 Developer Testing	9
2.3.2 Evaluator Testing	11
2.4 Evaluation Result.....	12
3. Conduct of Certification.....	13
4. Conclusion	14
4.1 Certification Result	14
4.2 Recommendations	14
5. Glossary.....	15
6. Bibliography	18

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 C4535 I / C3626 I / C2521 I DocuCentre C4535 I / C3626 I / C2521 I Series Data Security Kit” (hereinafter referred to as “the TOE”) conducted by Japan Electronics and Information Technology Industries Association, 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: Fuji Xerox ApeosPort C4535 I / C3626 I / C2521 I DocuCentre C4535 I / C3626 I / C2521 I Series Data Security Kit
Version: Controller ROM Ver. 1.3.0
Developer: Fuji Xerox Co., Ltd.

1.2.2 Product Overview

This product is firmware that is provided as an optional product of ApeosPort C4535 I, ApeosPort C3626 I, ApeosPort C2521 I, DocuCentre C4535 I, DocuCentre C3626 I, and DocuCentre C2521 I (Fuji Xerox’s digital multifunction machines with copy, printer, scanner, and facsimile functions. Hereafter “ApeosPort/DocuCentre.”)

This product protects document data that is stored on the hard disk drive when ApeosPort/DocuCentre performs processings of copy, print, scan, and facsimile from being illicitly disclosed. The following are the security functions provided by this product:

- HDD overwriting for residual data
- HDD data encryption
- Key-operator authentication
- Customer-engineer operation restriction

1.2.3 Scope of TOE and Overview of Operation

ApeosPort/DocuCentre consists of three board-units: controller board, control panel, and facsimile card. TOE is a set of programs that are recorded in the system ROM mounted on the controller board. TOE's physical configuration image and functions are shown in Figure 1-1.

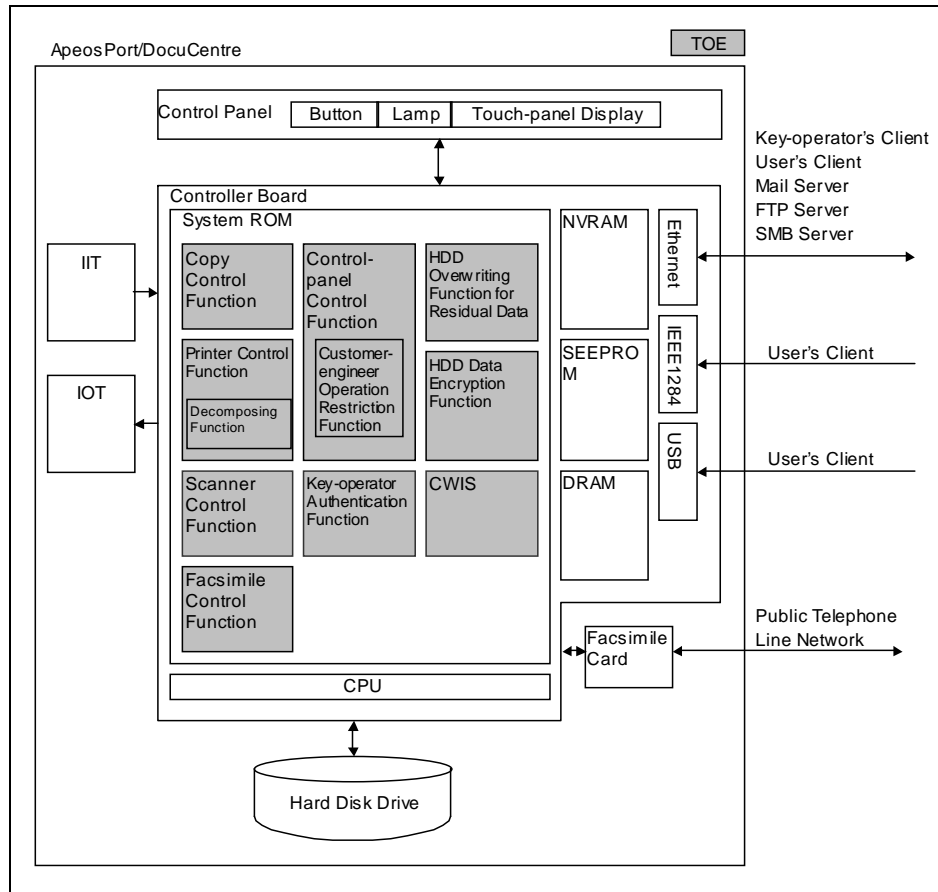


Figure 1-1: TOE's Physical Configuration Image

Usage environment of ApeosPort/DocuCentre with TOE security functions and operation overview is shown below.

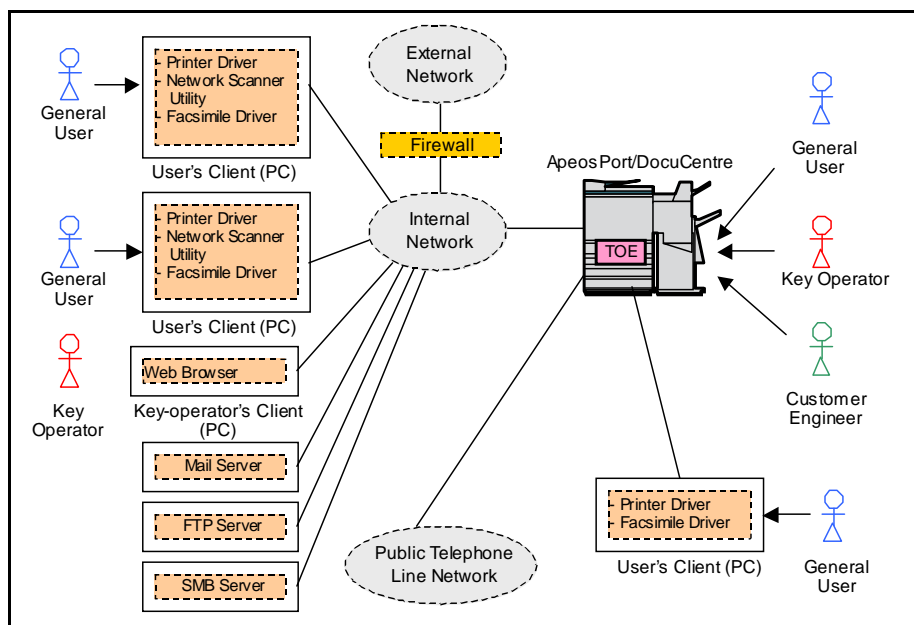


Figure 1-2: Usage Environment

<Overview of TOE operation related to key operator>

Identification and authentication are performed at the control panel of ApeosPort/DocuCentre or the key-operator's client. Key operator makes settings described in Table 1-1 after being identified and authenticated as key operator.

Table 1-1: Setting Data

Item number	Setting data
1	Setting for HDD overwrite function
2	Setting for using password
3	Key-operator's password
4	Setting for customer-engineer operation restriction function
5	Access denial due to failure in authentication of key-operator's ID
6	Setting for HDD data encryption function
7	Cryptographic seed key for data stored on the hard disk drive

<Overview of TOE operation related to general user>

By operating the control panel of ApeosPort/DocuCentre or the user's client and performing copy, print, scan, or facsimile, used document data is stored on the hard disk drive built into ApeosPort/DocuCentre. At this time, security functions automatically operate according to the setting data in Table 1-1 before general user knows (when the "setting for HDD overwriting function for residual data" and the "setting for HDD data encryption function" are enabled, used document data is stored after being encrypted, and then overwritten and erased at the time of completion of each processing).

1.2.4 TOE Functionality

TOE has the security functions described below:

<HDD overwriting function for residual data>

After the operation of copy, printer, scanner, and facsimile functions, this function overwrites and erases used document data stored on the hard disk drive.

<HDD data encryption function>

At the time of the operation of copy, printer, scanner, and facsimile functions, this function encrypts document data when storing it on the hard disk drive.

<Key-operator authentication function>

This function identifies and authenticates key operator at the control panel or the key-operator's client, and enables only the key operator to make settings on the TOE security functions described below:

- Setting for HDD overwriting function for residual data
- Setting for using password
- Key-operator's password
- Access denial due to failure in authentication of key-operator's ID
- Setting for HDD data encryption function
- Cryptographic seed key for data stored on the hard disk drive

<Customer-engineer operation restriction function>

This function enables only the key operator to make the setting for customer-engineer operation restriction function.

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 "Guidance for IT Security Certification Application, etc." [2], "General Requirements for IT Security Evaluation Facility" [3] and "General Requirements for Sponsors and Registrants of IT Security Certification" [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 C4535 I / C3626 I / C2521 I DocuCentre C4535 I / C3626 I / C2521 I Series Data Security Kit 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 C of CC Part 1 (either of [5], [8], [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9], [12] or [15]) 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], [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in "Fuji Xerox ApeosPort C4535 I / C3626 I / C2521 I DocuCentre C4535 I / C3626 I / C2521 I Series Data Security Kit Evaluation Technical Report" (hereinafter referred to as "the Evaluation Technical Report") [22]. Further, evaluation methodology should comply with the CEM Part 2 (either of [17], [18] or [19]). In addition, the each part of CC and CEM shall include contents of interpretations (either of [20] and [21]).

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 problems found in the certification process. Evaluation is completed with the Evaluation Technical Report dated June, 2005 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 EAL2 conformance.

1.5.3 SOF

This ST claims "SOF-basic" as its minimum strength of function. Attack level of the attackers assumed for this TOE is low level. Therefore, the claim of "SOF-basic" as the minimum function strength is appropriate.

1.5.4 Security Functions

Security functions of the TOE are as follow.

<HDD overwriting function for residual data (SF.OVERWRITE)>

According to the "setting for HDD overwriting function for residual data" that is set by key operator, this function overwrites and erases the used document data on the hard disk drive using the way described in Table 1-2.

If overwriting of the used document data is not finished such as due to power shutdown, this function overwrites and erases the data at the next system booting because a list of the used document data that is to be overwritten and erased is in the hard disk drive.

Table 1-2: Control of Overwriting

Number of overwritings	Data to overwrite with
One time	0
Three times	First time: random number Second time: random number Third time: 0

<HDD data encryption function (SF.ENCRYPTION)>

According to the "setting for HDD data encryption function" that is set by key operator, this function encrypts document data stored on the hard disk drive. At the time of booting, TOE generates cryptographic key using the "cryptographic seed key for data stored on the hard disk drive" that is set by key operator.

When storing document data on the hard disk drive, TOE stores the document data after performing encryption using the cryptographic key generated at the time of booting. When reading the stored document data, TOE also performs decryption using the cryptographic key generated at the time of booting.

Cryptographic key is lost when the power of the mainframe of ApeosPort/DocuCentre is shut down.

<Key-operator authentication function (SF.MANAGE)>

This function controls the operation of TOE setting data so that the operation can be performed by the authenticated key-operator. Before allowing the operation of TOE setting data, this function identifies and authenticates key operator with "key-operator's user ID" and "key-operator's password" entered at the control panel or through the Web browser of key-operator's client.

While "key-operator's password" is being entered at the control panel or through the Web browser of key-operator's client, asterisks ("*") of the same number as the characters of the entered password are displayed in the "password" input field of the control panel or the Web browser of key-operator's client.

When the "key-operator's user ID" and "key-operator's password" entered at the control panel or through the Web browser of key-operator's client are correct and the identification/authentication of key operator succeeds, this function allows the operation of TOE setting data. When either of the "key-operator's user ID" or "key-operator's password" entered at the control panel or through the Web browser of key-operator's client is incorrect and the identification/authentication of key operator fails, this function displays identification/authentication error. When authentication fails the same number of times as that set in the "access denial due to failure in authentication of key-operator's ID," this function denies authentication. Only the key operator who is authenticated in the above-described way can set:

- "HDD overwriting function for residual data" to "Not perform," "Perform (one time)," or "Perform (three times)."
- "setting for using password" to "Not perform" or "Perform."
- "HDD data encryption function" to "Not perform" or "Perform."
- "key-operator's password" to 7 to 12 alphanumeric characters.
- "access denial due to failure in authentication of key-operator's ID" to "Not perform" or "Perform (1 to 10 times)."
- "cryptographic seed key for data stored on the hard disk drive" to 12 alphanumeric characters.

<Customer-engineer operation restriction function (SF.CEREST)>

This function controls the operation of the TOE setting data for "setting for customer-engineer operation restriction function" so that the operation can be performed by the authenticated key-operator. Although "setting for customer-engineer operation restriction function" can be set to "Not perform" or "Perform," "Perform" must be set when using TOE. By setting to "Perform," customer engineer can be restricted from referring to / changing settings on TOE security functions.

1.5.5 Threat

This TOE assumes such threats presented in Table 1-3 and provides functions for countermeasure to them.

Table 1-3 Assumed Threats

Identifier	Threat
T.RECOVER <Illicit recovery of used document data>	General user and the person who is not related to TOE might recover used document data such as by removing the hard disk drive and connecting it directly to a tool.
T.CONFDATA <Illicit access to TOE setting data>	General user and the person who is not related to TOE might change settings by accessing TOE setting data from the control panel or key-operator's client. This setting data is allowed to be accessed only by key operator.

1.5.6 Organisational Security Policy

No organizational security policies to comply with are required of the TOE utilized in organizations.

1.5.7 Configuration Requirements

This product is offered as an optional product that is installed on Fuji Xerox's digital multifunction machines, "ApeosPort C4535 I," "ApeosPort C3626 I," "ApeosPort C2521 I," "DocuCentre C4535 I," "DocuCentre C3626 I," and "DocuCentre C2521 I."

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-4. The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-4 Assumptions in Use of the TOE

Identifier	Assumptions
A.SECMODE <Protection mode>	When operating TOE, key operator makes settings as follows: <ul style="list-style-type: none"> - Key-operator's password: 7 to 12 characters - Setting for customer-engineer operation restriction function: "Perform" - Setting for using password: "Perform" - Access denial due to failure in authentication of key-operator's ID: "Perform" and five times Additionally, key-operator's password is managed so that it is prevented from being guessed or disclosed.
A.ADMIN <Trust in key operator>	Key operator has knowledge necessary to fulfill the assigned role and does not conduct improperly with malicious intention.
A.NET <Network connection condition>	ApeosPort/DocuCentre that TOE is installed on is connected to an internal network. This internal network constitutes an environment where interceptions are not made. Even when this internal network is connected to an external network, ApeosPort/DocuCentre cannot be accessed from the external network.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- User Guides for ApeosPort C4535 I / C3626 I / C2521 I, and DocuCentre C4535 I / C3626 I / C2521 I 2nd Edition
- Delivery, Introduction, and Operation Procedure Description K1.04

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM Part 2 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 Part 2.

2.2 Overview of Evaluation Conducted

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

Evaluation has started on January, 2005 and concluded by completion the Evaluation Technical Report dated June, 2005. 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 and manufacturing sites on April, 2005 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records 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 April, 2005.

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

System configuration for the test that was conducted by developer is shown in Figure 2-1.

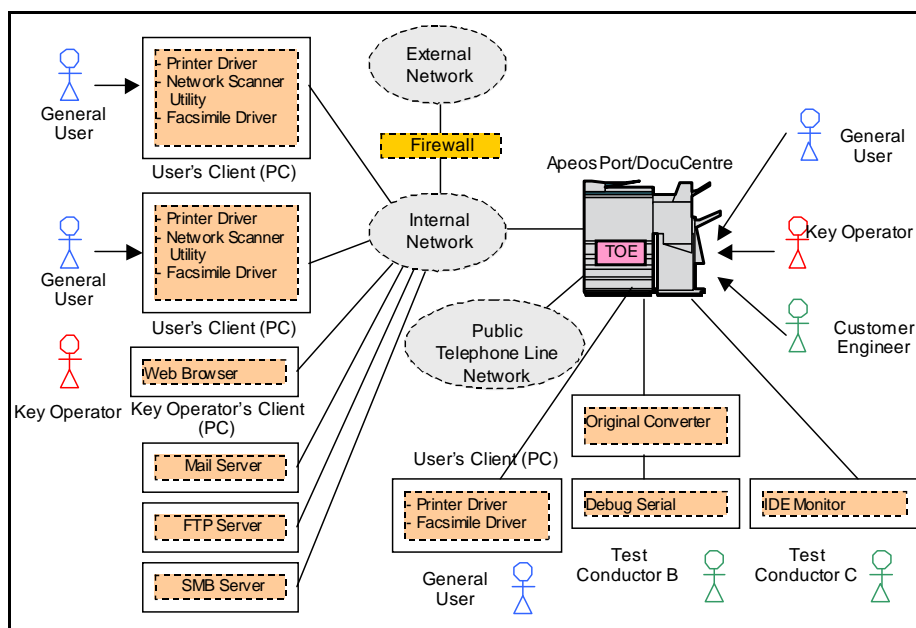


Figure 2-1 Configuration of Developer Testing

2) Outlining of Developer Testing

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

a. Test configuration

System configuration for the test that was conducted by developer is shown in Figure 2-1. Developer testing was conducted in the same TOE test environment as the TOE configuration identified in ST.

b. Testing Approach

For the testing, following approach was used.

1. Method of directly observing the behavior of security functions from the external interfaces by stimulating the external interfaces of these functions by operating ApeosPort/DocuCentre and PCs.
2. Method of checking the behavior of the security functions of which behavior cannot be directly observed from the external interfaces (“HDD overwriting function for residual data” and “HDD data encryption function”) using the tools (debug serial and IDE monitor).
 Debug serial was connected via the original converter to ApeosPort/DocuCentre, and used for checking the condition of the data in the hard disk drive. IDE monitor was used for checking the contents of the data communicated between the controller board and the hard disk drive in ApeosPort/DocuCentre by monitoring the communicated data. By generating pseudo-errors of the hard disk drive by connecting the trunk cable, which has a switch to turn off the power of the hard disk drive, to the hard disk drive, the test on the operation errors of the overwriting and erasing function was conducted.

c. Scope of Testing Performed

Total number of test items was 21.

The number of test items for testing each security function was as follows:

- HDD overwriting function for residual data: 12 items
- HDD data encryption function: 4 items
- Key-operator authentication function: 4 items
- Customer-engineer operation restriction function: 1 item

The test covered the behavior of each function, and the overall test volume and scope were appropriate.

d. Result

As for the result of developer testing, the actual test-result was confirmed to match the expected test-result. Evaluator checked the validity of the methods to conduct developer testing and the test items, and confirmed that the methods and the result match those described in the “Test Plan and Report.”

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator is shown in Figure 2-2.

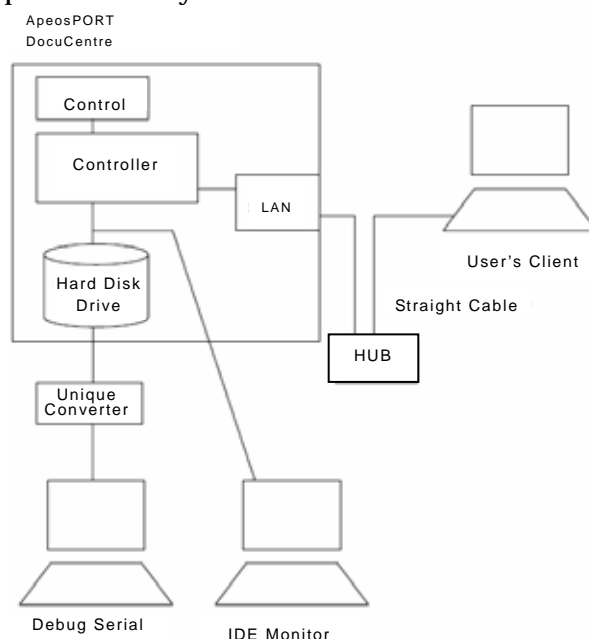


Figure 2-2: System Configuration for Evaluator Testing

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

System configuration for the test that was conducted by evaluator is shown in Figure 2-2. Evaluator testing was conducted in the same TOE test environment as the TOE configuration identified in ST.

b. Testing Approach

Evaluator conducted the test in the same methods as those for developer testing based on the judgment that the testing methods implemented by developer are suitable to verify the expected behavior of security functions.

c. Scope of Testing Performed

Evaluator conducted the 20-item test (3 items created uniquely by evaluator, 12 items conducted by sampling evaluator testing, and 5 items of intrusion test). The test created uniquely by evaluator was conducted by considering the accuracy of the developer testing for security functions.

For sampling test, 12 items, which are 57 % of the 21 items of the test conducted by developer, were selected.

For intrusion test, vulnerability analysis was conducted based on the result of developer vulnerability analysis, and 5-item test was conducted based on this analysis result.

d. Result

Evaluator was able to check the behavior of TOE by correctly completing all the tests conducted by evaluator, and confirmed that all the test results match the expected behavior.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM Part 2 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 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 glossaries used in this report are listed below.

General User:	One who uses copy and printer functions of ApeosPort/DocuCentre.
Key Operator:	One who manages ApeosPort/DocuCentre.
Customer Engineer:	Fuji Xerox's engineer who maintains and repairs ApeosPort/DocuCentre.
Control Panel:	Panel on which the buttons, lamps, and touch panel display that are necessary for operating ApeosPort/DocuCentre are arranged.
User's Client:	Client that is used by general user. General user uses printer functions of ApeosPort/DocuCentre by using printer driver that is installed on the user's client.
Key-operator's Client:	Client that is used by key operator. Key operator checks and rewrites TOE setting data for ApeosPort/DocuCentre using the Web browser.
Printer Driver:	Software that converts data on user's client to print data described in page description language (PDL) that can be interpreted by ApeosPort/DocuCentre. Used on user's client.
Printer Function:	Function to decompose and print out print data sent from user's client.
Storage Print:	Print method in printer function. In this method, bitmap data created by decomposing print data is once stored on the internal hard disk drive of ApeosPort/DocuCentre, and printed according to the general-user's instruction from the control panel or when the designated time comes. There are following five methods: <ul style="list-style-type: none"> - Security print - Sample print

- Authentication print
 - Time designation print
 - Print that uses mailbox
- Scanner Function:** Function to scan an original in IIT and print out from IOT, according to the general-user's instruction from the control panel. When multiple copies of the same original are instructed to be printed, the document data is
- scanned in IIT,
 - stored on the internal hard disk drive of ApeosPort/DocuCentre,
 - read from the internal hard disk drive for the same number of times as the number of designated copies, and printed out.
- Scanner Function:** According to the general-user's instruction from the control panel, scans an original in IIT and stores it in an expanded mailbox created in the internal hard disk drive of ApeosPort/DocuCentre. The stored document data is retrieved by network scanner utility on user's client.
- Facsimile Function:** Sends and receives facsimiles. When sending a facsimile, document data of an original scanned in IIT is sent to a remote machine connected to public telephone line network, according to the general-user's instruction from the control panel. When receiving a facsimile, document data sent via public telephone line network from a connected remote-machine is received and printed out from IOT.
- Expanded Mailbox:** Logical box created in the hard disk drive of ApeosPort/DocuCentre. The following can be stored in this box: the document data scanned by scanner function and the document data for the print that uses an expanded mailbox.
- Document Data:** In this ST, "document data" is used as a generic term for the data including all the image information that pass the inside of ApeosPort/DocuCentre when general user uses copy, printer, scanner, and facsimile functions of ApeosPort/DocuCentre.
The following are included:
- Bitmap data that is printed in IOT when using copy function.
 - Print data sent from user's client and bitmap data created by decomposing the data, when using printer function.
 - Bitmap data that is stored on the internal hard disk drive when using scanner function.
 - Bitmap data that is sent to a connected remote-machine and bitmap data that is received from a connected remote-machine and printed in IOT, when using facsimile function.
- Used Document Data:** Document data of which use is finished after being stored on the internal hard disk drive of ApeosPort/DocuCentre.
- To Overwrite and Erase:** To overwrite the data area with the specific data when document data stored on the hard disk drive is to be deleted.

Cryptographic Seed Key: 12-digit alphanumeric characters that are entered by user. Cryptographic key is generated from this key.

Cryptographic Key: 128-bit data that is automatically generated from cryptographic seed key. Encryption is performed using this cryptographic key.

6. Bibliography

- [1] Fuji Xerox ApeosPort C4535 I / C3626 I / C2521 I DocuCentre C4535 I / C3626 I / C2521 I Series Data Security Kit Security Target Version: 1.13 (May 31, 2005) Fuji Xerox Co., Ltd.
- [2] Guidance for IT Security Certification Application, etc. April 2004, Information-Technology Promotion Agency, ITQM-23 (Revised on November 5, 2004)
- [3] General Requirements for IT Security Evaluation Facility, April 2004, Information-Technology Promotion Agency, ITQM-07
- [4] General Requirements for Sponsors and Registrants of IT Security Certification, April 2004, Information-Technology Promotion Agency, ITQM-08 (Revised on November 5, 2004)
- [5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-00-031
- [6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- [7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
- [8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031 (Translation Version 1.2 January 2001)
- [9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (Translation Version 1.2 January 2001)
- [10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (Translation Version 1.2 January 2001)
- [11] ISO/IEC15408-1: 1999 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model JIS
- [12] ISO/IEC 15408-2: 1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- [13] ISO/IEC 15408-3:1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
- [14] JIS X 5070-1: 2000 - Security techniques - Evaluation criteria for IT security - Part 1: General Rules and general model
- [15] JIS X 5070-2: 2000 - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- [16] JIS X 5070-3: 2000 - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

- [17] Common Methodology for Information Technology Security Evaluation
CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999
- [18] Common Methodology for Information Technology Security Evaluation
CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999
(Translation Version 1.0 February 2001)
- [19] JIS TR X 0049: 2001 – Common Methodology for Information Technology Security
Evaluation
- [20] CCIMB Interpretations-0407 (December 2003)
- [21] CCIMB Interpretations-0407 (December 2003)
(Translation Version 1.0 August 2004)
- [22] Fuji Xerox ApeosPort C4535 I / C3626 I / C2521 I DocuCentre C4535 I / C3626 I /
C2521 I Series Data Security Kit Evaluation Technical Report Version 1.4, June 8,
2005, Japan Electronics and Information Technology Industries Association,
Information Technology Security Center