Certification Report

Target of Evaluation

Application date/ID	June 11, 2004 (ITC-4029)
Certification No.	C0020
Sponsor	Canon Inc.
Name of TOE	Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 (Japanese version) iR Security Kit-B2 (International version)
Version of TOE	Version 1.04
PP Conformance	None
Conformed Claim	EAL2
TOE Developer	Canon Inc.
Evaluation Facility	Electronic Commerce Security Technology Laboratory Inc. Evaluation Center

This is to report that the evaluation result for the above TOE is certified as follows.
February 9, 2005

TABUCHI Haruki, 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-0210

Evaluation Result: Pass

“Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 1.04 (Japanese version) iR Security Kit-B2 Version 1.04 (International version)” 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 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 1.04 (Japanese version) iR Security Kit-B2 Version 1.04 (International version)” (hereinafter referred to as “the TOE”) conducted by Electronic Commerce Security Technology Laboratory Inc. Evaluation Center (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, Canon Inc..

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:	Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 (Japanese version) iR Security Kit-B2 (International version)
Version:	1.04
Developer:	Canon Inc.

1.2.2 Product Overview

This product is a software program to be installed for use on the Canon iR4570/iR3570/iR2870/iR2270-series multifunction products (hereafter referred to collectively as the “multifunction product”).
The multifunction product is an office machine with the combined functionality of Copy, Send (Universal Send), Fax Reception, Mail Box, Print, and many others. The use of the Copy, Universal Send, Fax Reception (fax/I-fax reception) or Print function involves creation of temporary image data on the HDD of the multifunction product. Likewise, the use of the Mail Box function (for document storage) or the Fax Reception function (for “in-memory reception” or forwarding of faxes/I-faxes) involves the process of saving image data to an inbox on the multifunction product.
By installing this product, security enhancements can be added to the multifunction product, helping users counter the threat of unauthorized disclosure of their temporary image data created on the HDD and image data stored in the inboxes.

1.2.3 Scope of TOE and Overview of Operation

Figure 1-1 depicts a typical operating environment of the multifunction product with the TOE installed.

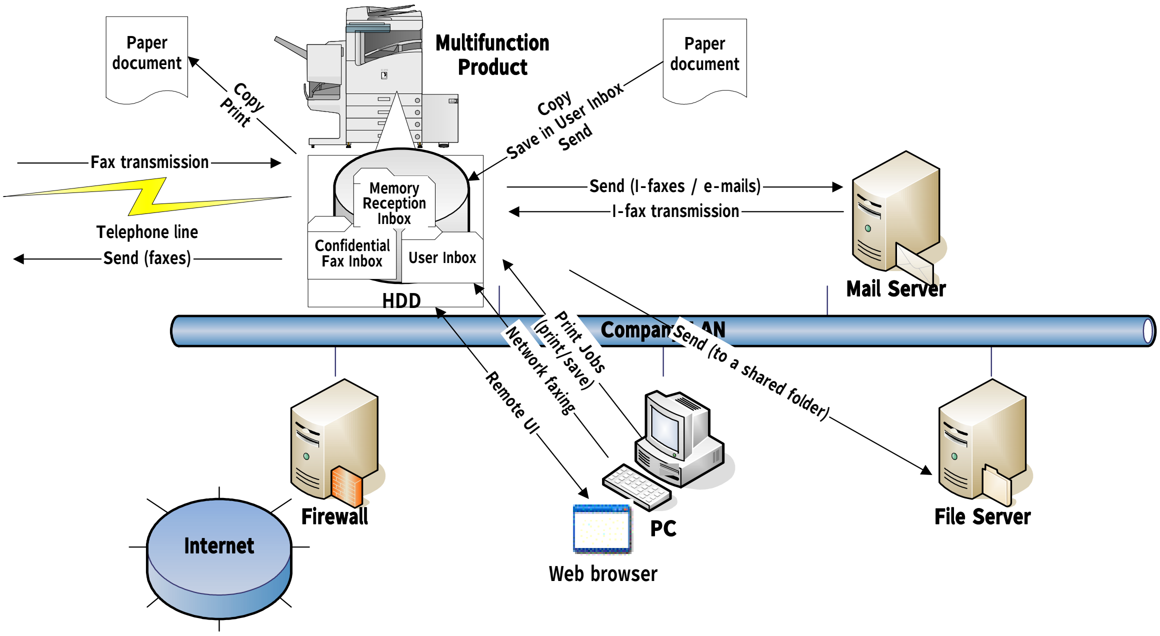

Figure 1-1: A typical operating environment of the multifunction product with the TOE installed

The scope of the TOE includes the whole of the software program that is installed on the multifunction product to control its entire functionality and the Web browser contents of the Remote UI. The assets to be protected are the temporary image data that will be created on the HDD of the multifunction product, and the image data that will be stored in any inbox on the multifunction product.

The multifunction product control software is executed on the controller hardware of the multifunction product, and the Web browser contents of the Remote UI are executed on each user's desktop via a Web browser. The hardware components of the multifunction product, including the controller and the HDD, and its embedded MEAP authentication application software are outside the scope of the TOE. Also outside the scope of the TOE are the hardware components of a user's PC and its installed operating system, Web browser, printer drivers, fax drivers and image viewer plug-ins.

Figure 1-2 illustrates the TOE boundary.

<table>
<tr><td colspan="2"></td><td>MEAP Authentication Applications
(software: outside TOE boundary)</td></tr>
<tr><td colspan="3"><b>iR Security Kit-B2
(software, TOE)</b></td></tr>
<tr><td colspan="3">Controller (hardware: outside TOE boundary)</td></tr>
<tr><td>Scan Engine/ADF
(hardware: outside TOE boundary)</td><td>Printer Engine
(hardware: outside TOE boundary)</td><td>Control Panel
(hardware: outside TOE boundary)</td></tr>
</table>

Note: *The cross-hatched portion indicates the scope of the TOE.*

Figure 1-2: TOE boundary on the multifunction product

The security functions of the TOE are; HDD Data Encryption, HDD Data Complete Erase, Inbox User Identification and Authentication, Inbox Management, System Manager Identification and Authentication, System Manager Management.

The following provides an operational overview of these TOE security functions.

Copy, Send (Universal Send), Fax Reception, Print

When a regular user operates the multifunction product to perform the Copy, Send (Universal Send), Fax Reception (for receiving faxes/I-faxes) or Print function, encrypted temporary image data is created on the HDD of the multifunction product. This temporary image data is decrypted when it needs to be read out by a user operation, and at the completion of the operation, it is erased from the HDD by being overwritten with meaningless data. Encryption, decryption and overwrite erase of temporary image data are all done silently in the background, without bothering the TOE user. (Related security functions: *HDD Data Encryption*, *HDD Data Complete Erase*)

Mail Box, Fax Reception

When a regular user operates the multifunction product to perform the Mail Box function (for saving scanned documents or documents printed from the PC) or Fax Reception function (for “in-memory reception” or forwarding of faxes/I-faxes), encrypted image data is created in the appropriate inbox on the multifunction product, and it can be accessed from the Inbox Selection Screen by selecting its containing inbox. This inbox-stored image data is decrypted when it needs to be read out by a user operation, and if it is selected for deletion, it is erased from the inbox by being overwritten with meaningless data at the completion of the operation. Encryption, decryption and overwrite erase of inbox-stored image data are all done silently in the background, without bothering the TOE user. (Related security functions: *HDD Data Encryption*, *HDD Data Complete Erase*)

Inbox Password-based Document Management

A regular user can set a password on any desired inbox by operating the Control Panel of the multifunction product or the Remote UI. When such a password-protected inbox is selected in the Inbox Selection Screen, the accessing user is required to provide the password for that inbox. If successfully authorized, the user is granted access and allowed to use any image data stored in the inbox. (Related security functions: *Inbox Management, Inbox User Identification and Authentication*)

Inbox Password Management

A regular user who is authenticated as an authorized user of an inbox can modify or clear the password for that inbox. The user assigned as the System Manager can log in to the System Management Mode by entering the System Manager ID and the System Password on the Control Panel of the multifunction product. While in the System Management mode, the System Manager can not only modify or clear any inbox’s password, but also can modify the System Manager ID and the System Password themselves. (Related security functions: *Inbox User Identification and Authentication*, *Inbox Management*, *System Manager Identification and Authentication*, *System Manager Management*)

1.2.4 TOE Functionality

This section describes the functionality of the TOE.

(1) Security Functions
The TOE has the following security functions.

HDD Data Encryption
A function to encrypt image data (temporary or inbox-stored image data) upon saving to the HDD.

HDD Data Complete Erase
A function to clear image data (temporary or inbox-stored image data) on the HDD by overwriting its disk space with meaningless data.

Inbox User Identification and Authentication
A function to identify and authenticate an authorized inbox user by means of inbox password verification, before allowing any image data to be read out from the accessed inbox.

Inbox Management
A function to set a password on an inbox.

System Manager Identification and Authentication
A function to identify and authenticate an owner of the System Manager ID and the System Password as the System Manager, before allowing access to the System Management mode.

System Manager Management
A function to define a System Manager ID and a System Password.

(2) Control of the Multifunction Product's Functionality
The TOE controls the following functions of the multifunction product.

Copy
A function to duplicate hard-copy documents by scanning and printing.
The Copy function involves the process of creating temporary image data on the HDD of the multifunction product.

Universal Send (document transfer)
A function to send scanned documents or documents stored in a User Inbox or the Memory Reception Inbox as faxes or TIFF or PDF format files to an outside e-mail address or a shared folder on an external PC.
This function also allows network faxing from a user's desktop through the use of a fax driver.
The Universal Send function involves the process of creating temporary image data on the HDD of the multifunction product.

Fax Reception
A function to automatically print or forward received faxes/I-faxes.
The Fax/I-Fax Reception function involves the process of creating temporary image data on the HDD of the multifunction product.
Faxes/I-faxes received in memory and stored in the Memory Reception Inbox can be extracted at a later time for printing or outbound transfer. Received fax forwarding settings can be customized to automatically forward received faxes/I-faxes to an

external destination or a specific Confidential Fax Inbox before they are stored in the Memory Reception Inbox. Documents received in a Confidential Fax Inbox are available for later printing only.

User Inbox
A function to store documents scanned or received from an external PC as image data in a specified User Inbox. User Inbox-stored image data can be merged with other documents or overlaid with a form image before printing.

Print
A function to print documents received from an external PC by using the multifunction product as a network printer. The Print function involves the process of creating temporary image data on the HDD of the multifunction product.

Remote UI
The multifunction product can be operated directly via its Control Panel, as well as remotely via the Remote UI software. The Remote UI software allows remote access to the multifunction product from the Windows desktop via a Web browser and a network connection, enabling the user to view device status information, manipulate jobs, perform inbox management operations, configure various settings, and so on. The Web server functionality is already embedded in the multifunction product, so that users are not required to have any other software than a Web browser.

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 “Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Security Target Version 1.11” 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 “Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 (Japanese version) iR Security Kit-B2 (International version) 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[20] and [21].

1.4 Certificate of Evaluation

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 January, 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.

This claim is appropriate, because the TOE is a software program for use on the multifunction product that is a general commercial product intended for use in an office environment.

1.5.4 Security Functions

Security functions of the TOE are as follow.

HDD Data Encryption
The TOE generates 168-bit Triple DES cryptographic keys using the Canon iR cryptographic key generation algorithm. Whenever writing image data to the HDD, the TOE uses a FIPS PUB 46-3-compliant 168-bit Triple DES algorithm for encryption of the image data. Whenever reading out image data from the HDD, the TOE uses a FIPS PUB 46-3-compliant 168-bit Triple DES algorithm for decryption of the image data. The TOE destroys cryptographic keys using the Canon iR cryptographic key destruction algorithm.

HDD Data Complete Erase
When a document in an inbox is deleted, the TOE clears the corresponding image data from the HDD.
When the Copy, Print, Fax Reception or Universal Send function is executed, the TOE

creates temporary image data on the HDD and clears it upon completion of the function. When a complete image data erase is performed, the TOE overwrites the corresponding disk space with meaningless data so as to clear the image data. The TOE also automatically clears any residual temporary image data left on the HDD at startup (i.e., when the multifunction product is powered on), and this is achieved by overwriting the corresponding disk space with meaningless data.

Inbox User Identification and Authentication

The TOE requires any user attempting to access a password-protected inbox to provide the password for the inbox before allowing access (unless the user is trying to add image data there). If the inbox is not protected with a password, then the TOE does not require input of a password. The TOE identifies and authenticates the user as an authorized user of the inbox and displays the Inbox Operation Screen, only after verifying that the user-given password is the correct inbox password. Once authorized, the user, if accessing from the Control Panel, is maintained by the TOE as an authorized inbox user until the user returns to the Inbox Selection Screen from the Inbox Operation Screen. In contrast, if the user is accessing from the Remote UI, the TOE maintains the user as an authorized inbox user until some operation is attempted on a different inbox or the Web browser is closed. If an incorrect inbox password is given, the TOE imposes a 1-second wait time before redisplaying the Password Entry Screen.

Inbox Management

The TOE restricts the right to modify and clear (remove) an inbox password only to authorized inbox users and the System Manager. The TOE gives the System Manager the ability to modify and clear any inbox’s password using the Control Panel. The TOE gives authorized inbox users the ability to modify and clear their inbox passwords using the Control Panel or the Remote UI. The TOE limits the length of an inbox password to a maximum of 7 numeric characters. If a password-protected inbox is re-registered with no password defined, the TOE removes the current password from the inbox.

System Manager Identification and Authentication

The TOE requires any user attempting to perform System Manager actions using the TOE to provide the correct System Manager ID and System Password in order to be identified and authenticated as the System Manager. At this time, if the Department ID Management function is active on the multifunction product, the System Manager Identification and Authentication function is invoked before allowing the user to operate the multifunction product via the Control Panel or the Remote UI. If the Department ID Management function is not active, the function is invoked when the System Settings Screen is displayed on the Control Panel or in the Remote UI window. The TOE identifies and authenticates the user as the System Manager only after verifying that the user-given ID and password are the correct System Manager ID and System Password. If they are incorrect, the TOE imposes a 1-second wait time before redisplaying the Password Entry Screen. Once authorized, the user, if accessing from the Control Panel, is maintained by the TOE as the System Manager with permissions to configure system management settings, manipulate any inbox and execute inbox management functions, until the System Management mode is canceled with the ID key on the Control Panel. If the user is accessing from the Remote UI, the TOE maintains the user the System Manager until the Web browser is closed.

System Manager Management

The TOE restricts the right to modify and clear (remove) the System Manager ID and the System Password only to the System Manager. The TOE limits the System Password to a maximum of 7 numeric characters.

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

Identifier	Threat
T.HDD_ACCESS: Direct Access to HDD Data	A malicious individual may attempt to disclose temporary image data or inbox-stored image data on the HDD by removing the HDD from the multifunction product and directly accessing the HDD using disk editor tools, etc.
T.UNAUTH: Operation Attempts by Unauthorized Users	An unauthorized inbox user (except the System Manager) may attempt to disclose inbox-stored image data by operating the Control Panel or the Remote UI.

1.5.6 Organisational Security Policy

There are no organizational security policies required for using the TOE.

1.5.7 Configuration Requirements

The TOE comprises the software product to be provided by Canon Inc. for installation on the multifunction product and the Web browser contents of the Remote UI.

The operating environment of the TOE is indicated below.

Table 1-2: Multifunction products supporting this TOE and necessary options (Japanese models)

Model Name	Necessary Options
Canon iR4570	Expansion Bus-B1(*) , USB Application Interface Board-D1(*) , additional memory (512MB or more in total, including onboard memory) (*)These option names were translated from the original Japanese names.
Canon iR4570F	
Canon iR3570	
Canon iR3570F	
Canon iR2870	
Canon iR2870F	
Canon iR2270	
Canon iR2270F	

Table 1-3: Multifunction products supporting this TOE and necessary options (International models)

Model Name	Necessary Options
Canon iR4570	Expansion Bus-B1, USB Application Interface Board-D1
Canon iR3570	
Canon iR2870	
Canon iR2270	

In order to operate the multifunction product using the Remote UI, the following software programs need to be installed on the user’s computer.

Web browser
Microsoft Internet Explorer 6.0 (for Windows)

Image viewer plug-in (required for document previewing from the Remote UI)
Canon JBIG Image Viewer Plug-in software (bundled with the multifunction product)

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 1-4 Assumptions in Use of the TOE

Identifier	Assumptions
A.OUT_OF_TOE: Image Data Outside the TOE	Each TOE user shall keep in mind that image data sent outside the TOE and image data not yet received by the TOE are both outside the TOE and thereby are not assets to be protected.
A.ADMIN: Trusted System Manager	The System Manager shall be trusted not to abuse his privileges.
A.PWD_MANAGE: Password Management	Every inbox password and the System Password shall be kept secret from and difficult to be guessed by other users.
A.PWD_SET: Password Protection	Every inbox containing image data that requires protection shall be protected with a password. The System Manager ID and the System Password shall already be set.
A.NETWORK: Connection of the Multifunction Product	The multifunction product running the TOE, upon connection to a network, shall be connected to the internal network that is inaccessible directly from outside networks such as the Internet. The Remote UI, upon use, shall be executed via the internal network that is using appropriate network equipment and a robust communication method, e.g., encryption, to prohibit unnecessary data transfer to unspecified destinations and is properly managed by the network administrator to refuse connection attempts by unauthorized devices to prevent packet sniffing.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

(1) Documents attached to the iR Security Kit B2 (Japanese version)
- Canon iR Security Kit-B2 Reference Guide (FA7-6498), 000
- Reference Guide (FA7-7164), 000
- Copying and Box Guide (FA7-7165), 000
- Remote UI Guide (FA7-7167), 000
- Network Guide (FA7-7168), 000
- MEAP SMS Administrator Guide (FA7-7169), 000
- MEAP Authentication System Setting Guide (FA7-7170), 000
- Sending and Facsimile Guide (FA7-7166)

Note: These document titles were translated from the original Japanese titles.

(2) Documents attached to the iR Security Kit B2 (International version)
- Canon iR Security Kit-B2 Reference Guide (FA7-6500), 000
- Reference Guide (FA7-7171), 000

- Copying Guide (FA7-7172), 000
- Mail Box Guide (FA7-7173), 000
- Remote UI Guide (FA7-7175), 000
- Network Guide (FA7-7176), 000
- MEAP SMS Administrator Guide (FA7-7177), 000
- Sending and Facsimile Guide (FA7-7174), 000

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 June, 2004 and concluded by completion the Evaluation Technical Report dated January, 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 December, 2004 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 November, 2004.

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

As for problem 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 Table 2-1.

Table 2-1: Developer test configuration

TOE	Version
TOE	Japanese version: Ver.1.04, International version: Ver.1.04
Sample TOE	Japanese version: Ver.0.00, International version: Ver.0.00
Equipment	**Major Specification**
Multifunction product	iR2270F
Options for the multifunction product	- iR 256MB Expansion RAM·B1(*) - USB Application Interface Board-D1(*) - Expansion Bus-B1(*) - Send Expansion Kit(*) - Super G3 FAX Board-Q1(*) (*)These options are available for the Japanese market models only, and hence their product names are quoted in Japanese language.
PC	- HP Compaq Business Desktop d530 USDT (Remote UI PC) - Toshiba Dynabook Satellite J10 SA200P/5 (Log monitoring PC)
HUB	100Mbps switching HUB
Network cable x 2	UTP cable (category 5)
Facsimile apparatus	Canon Laser Class 9000 (Model H12124)
Central Office simulator	EXCEL-7000 (Nishiyama Corporation)
Software	**Major Specification**
OS	- Microsoft Windows 2000 Professional Service Pack 4 (Remote UI PC) - Microsoft Windows XP Professional Service Pack 1 (Log monitoring PC)
Communications software	HyperTerminal (of Windows)
Printing software	Microsoft Word 2000 SR-1
Web browser	Microsoft Internet Explorer Version 6.0 Service Pack 1
Printer driver	- Windows LIPS LX Version 1.11 Printer Driver (Japanese version) - PCL5e Printer Driver for Windows v6.50 (English version)

2) Outlining of Developer Testing

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

a. Test configuration

The testing was conducted using only some of the product models identified as TOE platforms in the ST (only one used, out of eight). However, these models all sport the same controller hardware, which is the very place where the TOE runs, and the difference between the scanner engine and the print engine is known to have no impact on the TOE. Furthermore, all these models are equipped with the same Control Panel to display the TOE interfaces. Therefore, these facts collectively verify that the test configuration was appropriate for the TOE operating environment, despite not all of the targeted multifunction product models being used.

The sample TOE used for the testing is a limited-feature version of the TOE Ver.1.04 with no HDD data readout logging functionality in order to suppress the amount of log output. The sample TOE and the TOE Ver.1.04 are exactly the same in terms of security functions and thus it is obvious that there was no problem in the use of the sample TOE.

The communications software, the printing software, and the log monitoring PC were used as the equipment for retrieving necessary information for the testing, and they were all confirmed to have no impact on the TOE security functions. A Central Office simulator was used for data exchange with the facsimile apparatus, however, the TOE security functions are not impacted by the difference between an actual phone line and the Central Office simulator.

Other configuration components all match the TOE operating environment described in the ST.

b. Testing Approach

For the testing, following approach was used.

1. The developer stimulated each security function at each external interface by operating the multifunction product’s Control Panel or the Remote UI, and observed its behavior.

2. As for the security functions whose behavior could not be observed at the external interfaces, the developer verified the behavior using logs.

Table 2-2 describes the testing approach adopted for each security function.

Table 2-2: Testing approach

Security Function	Testing Approach
Inbox User Identification and Authentication Inbox Management System Manager Identification and Authentication System Manager Management	Operate the multifunction product’s Control Panel or the Remote UI and verify that the TSF behaves as described in the functional specification.
HDD Data Encryption HDD Data Complete Erase	Observe the behavior of the TSF using the terminal software and verify the invocation of the TSF with the output of a specific type of operation log as evidence. Then, verify the behavior of the TSF by capturing a hard disk dump at the time of the log output using the terminal software and/or by comparing the original image data with the result of printing/output by the multifunction product.

c. Scope of Testing Performed

Testing is performed about 57 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface.

d. Result

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

2.3.2 Evaluator Testing

1) Evaluator Test Environment

Test configuration performed by the evaluator is showed in the Table 2-3.

Table 2-3: Evaluator test configuration

TOE	Version	
TOE	Japanese version: Ver.1.04, International version: Ver.1.04	
Sample TOE	Japanese version: Ver.0.00, International version: Ver.0.00	
Equipment	Major Specification	
Multifunction product	iR2270F	iR3570
Options for the multifunction product	IR 256MB Expansion RAM-B1(*) USB Application Interface Board-D1(*) Expansion Bus-B1(*) Saddle Finisher-Q4(*) Puncher Unit-L1(*) Buffer Pass Unit-E1(*) Cassette Feeding Unit-Y2(*) (*) These options are available for the Japanese market models only, and hence their product names are quoted in Japanese language.	iR 256MB Expansion RAM-B1 USB Application Interface Board-D1 Expansion Bus-B1 Saddle Finisher-Q2 Puncher Unit-L1 Buffer Pass Unit-C1 Cassette Feeding Unit-Y1
PC	One for log monitoring, one for the Remote UI, one for the TOE, one for vulnerability analysis	
HUB	100Mbps switching HUB	
Network cable x 2	UTP cables (category 5)	
Facsimile apparatus	Canon Laser Class 9000 (Model H12124)	
Central Office simulator	EXCEL-7000 (Nishiyama Corporation)	
Software	Major Specification	
OS	Microsoft Windows 2000 Professional Service Pack 4, Microsoft Windows XP Professional Service Pack 1, Turbo Linux Serve V8	
Communications software	HyperTerminal Version 5.1	
Printing software	Microsoft Word 2000 SR-1	
Web browser	Microsoft Internet Explorer Version 6.0 Service Pack 1	
Printer driver	Windows LIPSLX Version 1.11 Printer Driver (Japanese version) PCL5e Printer Driver for Windows v6.50 (English version)	
Vulnerability analysis software	Nmap v3.75, Nessus v2.2	
Packet capturing software	Ethereal v0.10.7	

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

Test configuration performed by the evaluator is showed in the table 2-3.

The testing was conducted using only some of the product models identified as TOE platforms in the ST (only one used, out of eight). However, these models all sport the same controller hardware, which is the very place where the TOE runs, and the difference between the scanner engine and the print engine is known to have no impact on the TOE. Furthermore, all these models are equipped with the same Control Panel to display the TOE interfaces. Therefore, these facts collectively verify that the test configuration was appropriate for the TOE operating environment, despite not all of the targeted multifunction product models being used. The evaluator used an extra PC and software for the penetration testing, however, they also have no impact on the TOE security functions.

Other configuration components are the same as those of the developer testing.

b. Testing Approach

The evaluator confirmed that the developer's testing methodology was appropriate for examination of the expected behavior of the security functions and thus adopted the same testing approach.

c. Scope of Testing Performed

The evaluator performed 37 tests in total; 4 independent tests, 24 sampled developer tests, and 9 penetration tests. As for selection of the test subset, the following factors are considered.

1. TSFI not tested by the developer
2. Security functions whose behavior could not be observed from outside
3. Security functions with changeable parameters

The evaluator randomly sampled 19 (one-third) of the developer's 57 tests. The sample testing comprises further 5 tests in terms of the types of interfaces and the types of inboxes to store assets (image data).

The penetration testing comprises 9 tests according to the outcome of the vulnerability analysis performed based on publicly-known vulnerabilities, multifunction product-specific vulnerabilities, and the evaluator's knowledge of the TOE gained during the evaluation.

d. Result

All evaluator testing conducted is completes correctly and could confirm the behavior of the TOE. The evaluator also confirmed that all the test results are consistent with the behavior, and that there are no obvious exploitable vulnerabilities in the TOE.

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.

Problems found in certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such problems 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.

Confidential Fax Inbox: An inbox to store incoming faxes/I-faxes as sorted by recipient for later printing.

Controller: The TOE platform. A hardware device with a CPU and memory.

Control Panel: A hardware component of the multifunction product consisting of operation keys and a touch panel display. It is used for operating the multifunction product.

Department ID: An ID assigned to each multifunction product user, who could be an individual or a department. When the Department ID Management function is active, every user must be identified and authenticated before operating the multifunction product.
The System Manager is a user who is given a special department ID called the System Manager ID.

Department ID Management: A function of the multifunction product that issues a department ID and a password to each multifunction product user, in order to keep track and control of the number of printed copies, etc., on a per-department basis. When the Department ID Management function is active, every user has to be identified and authenticated by providing the correct department ID and password before using the multifunction product.

Document: Form of user data handled within the multifunction product. A document consists of management information and image data.

Form image: Internal image data that is stored in the multifunction product and used for overlay printing.

HDD: The hard disk drive of the multifunction product, where the TOE and its assets will be stored.

I-fax: An Internet faxing service that allows transmission and reception of faxes using the Internet instead of telephone lines.

Image data: Data that is created on the HDD of the multifunction product through scanning, printing and fax reception.

Inbox user: A regular user of an inbox. Each inbox user can password-protect his desired inbox to prevent access by other regular users.

In-memory-reception: An act of receiving incoming faxes/I-faxes in memory for storage in the Memory Reception Inbox, without printing.

MEAP: Short for Multifunctional Embedded Application Platform, which is a platform for running applications on the multifunction product.

MEAP authentication application: A MEAP application that runs embedded in the multifunction product to authenticate regular users using device-side functionality or a directory service.
It can be used to substitute for the Department ID Management function of the multifunction product.

Memory Reception Inbox: An inbox to store “in-memory-received” faxes/I-faxes for later printing or transfer to an external destination.

Multifunction product: A digital copier with the combined functionality of copying, faxing, printing, and sending (Universal Send). The multifunction product is equipped with a large-capacity HDD to perform these functions.

Printer engine: A hardware component of the multifunction product that prints image data on paper.

Regular user: A user of the multifunction product.

Remote UI: An interface that allows remote access to the multifunction product from a desktop Web browser for viewing device status information, manipulating jobs, configuring Mail Box settings, configuring various settings, etc.

Scan engine/ADF: A hardware component of the multifunction product that scans paper documents and stores acquired image data in the multifunction product.

System Management mode: A mode in which System Manager privileges are maintained on the multifunction product. Any operations specified in this mode are performed as System Manager actions. To enter this mode, the System Manager ID and System Password must be provided. The System Management mode is canceled when the ID key is pressed down on the multifunction product’s Control Panel.

System Manager: A special user of the multifunction product who is in responsible for device configuration and management. The System Manager may also be put in charge of inbox management on behalf of inbox users. The multifunction product will identify a user who owns the System Manager ID as the System Manager.

User Inbox: An inbox to store documents scanned by regular users and documents sent for storage from a connected PC. Documents stored in a User Inbox can be extracted at a later time for printing or transfer to an external destination.

6. Bibliography

[1] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Security Target Version 1.11 (January 11, 2005) Canon Inc.

[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-0210 (February 2002)

[21] CCIMB Interpretations-0210 (February 2002) (Translation Version 1.0 October 2002)

[22] Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 (Japanese version) iR Security Kit-B2 (International version) Evaluation Technical Report Version 2.0, January 17, 2005, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center