Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	March 30, 2005 (ITC-5043)
Certification No.	C0032
Sponsor	Canon Inc.
Name of TOE	Canon iR6570/iR5570 Series iR Security Kit-B3 (International version) iR Security Kit-B3 (Japanese version)
Version of TOE	Version 1.03
PP Conformance	None
Conformed Claim	EAL3
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.
October 18, 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

"Canon iR6570/iR5570 Series iR Security Kit-B3 Version 1.03 (International version) iR Security Kit-B3 Version 1.03 (Japanese 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 iR6570/iR5570 Series iR Security Kit-B3 Version 1.03 (International version) iR Security Kit-B3 Version 1.03 (Japanese 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 iR6570/iR5570 Series iR Security Kit-B3 (International version) iR Security Kit-B3 (Japanese version)
Version:	1.03
Developer:	Canon Inc.

1.2.2 Product Overview

This product is a software program to be installed for use on the Canon iR6570/iR5570 series multifunction products (hereafter referred to collectively as the “multifunction product”).

The multifunction product is a digital copier that offers the combined functionality of Copy, Send (Universal Send), Fax Reception, Mail Box, Print, Remote UI (a Web browser interface for operating the multifunction product), plus many others. When the Copy, Send (Universal Send), Fax Reception (fax/I-fax reception) or Print function is used, temporary image data is created on the hard drive of the multifunction product. Also, when the Mail Box function is used (for document storage) or the Fax Reception function is used (for “in-memory reception” of faxes/I-faxes or forwarding of faxes/I-faxes), image data is stored in the receiving inbox on the multifunction product. Furthermore, when the Remote UI function is used, image data is exchanged over the

network between the Web browser on the user's PC and the multifunction product.
By installing this product, security enhancements are added to the multifunction product, helping counter the threat of disclosure of temporary image data created on the hard drive, permanent image data stored in the inboxes, and image data that is transmitted over the Remote UI communication path.

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.

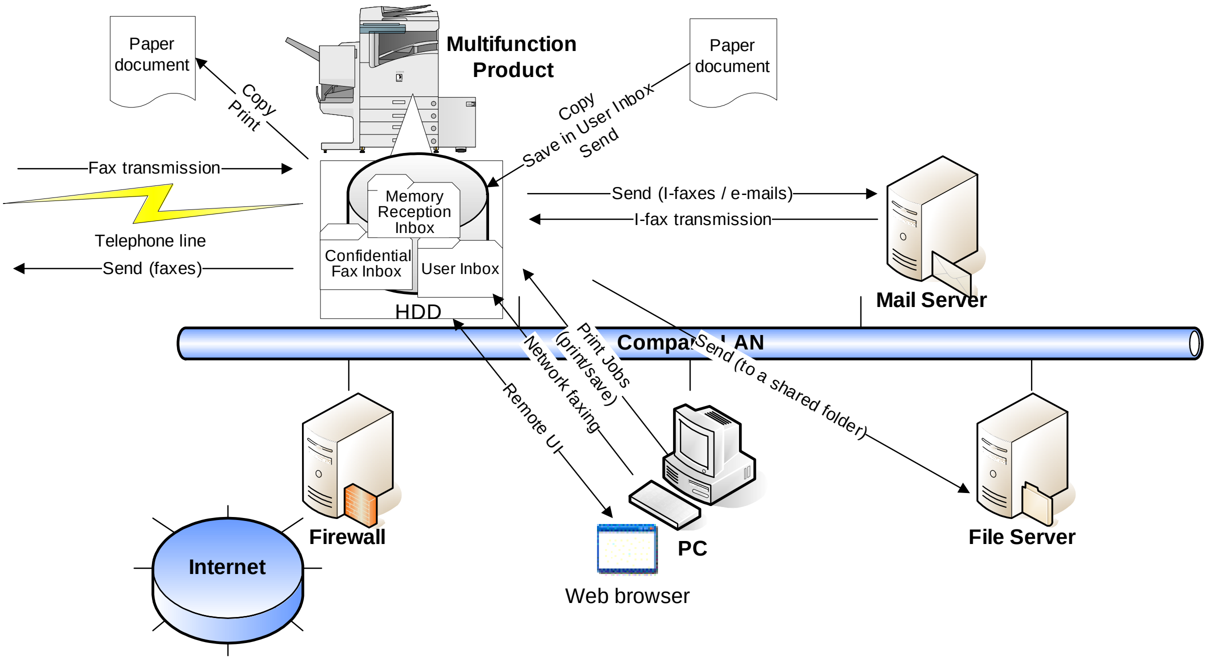


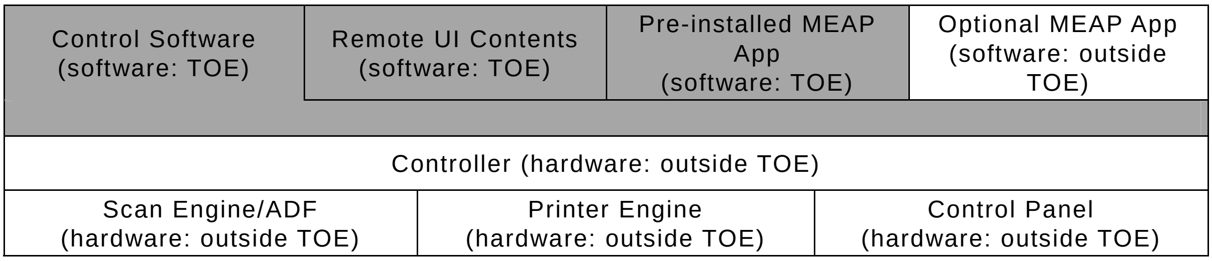
Figure 1-1: Typical operating environment of the multifunction product with the TOE installed

The physical scope of the TOE includes the whole of the software program that controls the functions of the multifunction product, the Web browser contents of the Remote UI, and the MEAP (Multifunctional Embedded Application Platform) authentication application that comes standard with the multifunction product.

The assets to be protected are temporary image data created on the HDD, permanent image data stored in the inboxes and image data that is transmitted over the Remote UI communication path.

The multifunction product control software is executed on the controller 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 multifunction product's hardware components, including the controller and the HDD 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 physical scope of the TOE on the multifunction product.



Note: The cross-hatched portion indicates the scope of the TOE (iR Security Kit-B3).

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, Authentication, System Manager Management and Secure Communication (Remote UI).

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, temporary image data is created and encrypted on the HDD of the multifunction product. Encrypted temporary image data is decrypted when read out by a user operation, and it is erased from the HDD by being overwritten with meaningless data at the completion of the operation. Encryption, decryption and overwrite erase of temporary image data are performed 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

Regular users are allowed to set passwords on inboxes 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, and is granted permission to use any image data stored in the inbox after successfully authorized.

Image data stored in inboxes can be previewed using the Remote UI, and image data transmissions exchanged between the user's Web browser and the multifunction product over the Remote UI communication path are protected by SSL.

(Related security functions: *Inbox Management, Inbox User Identification and Authentication, Secure Communication (Remote UI)*)

Inbox Password Management

Inbox users can modify or clear inbox passwords while authenticated as an authorized

user of the accessing inbox.
The System Manager can log in to the System Management Mode after identified and authenticated as the System Manager by entering the correct System Manager ID and System Password on the Control Panel of the multifunction product. 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. (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 save image data (temporary or permanent image data) to the HDD in an encrypted format.

HDD Data Complete Erase
A function to erase image data (temporary or permanent 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 user of an inbox by means of inbox password verification, prior to permitting readout of any image data.

Inbox Management
A function to password-protect an inbox.

System Manager Identification and Authentication
A function to identify and authenticate a user with the System Manager ID and the System Password as the System Manager, prior to permitting entry into the System Management mode.

System Manager Management
A function to define a System Manager ID and a System Password and activate/deactivate the Secure Communication (Remote UI) function.

Secure Communication (Remote UI)
A function to secure communications between the Remote UI and a user's Web browser using SSL.

(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 User Inboxes or the

Memory Reception Inbox as faxes or TIFF or PDF 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 using 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.
In-memory received faxes/I-faxes stored in the Memory Reception Inbox can be extracted at a later time for printing or outbound transfer. Fax forwarding settings can be configured to automatically redirect received faxes/I-faxes to a specified external destination or 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 external PCs 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 from its Control Panel or remotely via the Remote UI software. The Remote UI software allows remote PC users to access the multifunction product through their Web browser and network connection, enabling them to view device status information, manipulate jobs, perform inbox management operations, configure settings, and so on.
The Web server functionality is already embedded in the multifunction product, and hence users do not need 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 iR6570/iR5570 Series iR Security Kit-B3 Security Target Version 1.05” 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 iR6570/iR5570 Series iR Security Kit-B3 Version 1.03 (International version) iR Security Kit-B3 Version 1.03 (Japanese 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 （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 September, 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 EAL3 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.

When 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.

When 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 method.

HDD Data Complete Erase

When a document is deleted from an inbox, 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 at the completion of the function.

When performing a complete image data erase, the TOE overwrites the corresponding disk space with meaningless data so as to clear the image data.

The TOE clears any residual temporary image data left on the HDD at the request of the System Manager or at startup time (i.e. when the multifunction product is powered on). This is accomplished 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 enter the password for the inbox before allowing access (unless the user is trying to add image data).

If the inbox is not protected with a password, then the TOE does not require the input of a password.

The TOE identifies and authenticates the accessing user as an authorized user of the inbox and displays the Inbox Operation Screen only after verifying that the given password is the correct inbox password.

If the user is accessing from the Control Panel, the TOE maintains the user's role as an authorized inbox user until the user returns to the Inbox Selection Screen from the Inbox Operation Screen.

If the user is accessing from the Remote UI, then the TOE maintains the user's role as an authorized inbox user until the user manipulates another inbox or closes the Web browser.

If an incorrect inbox password is entered through the Control Panel or the Remote UI, the TOE imposes a 1-second wait time before redisplaying the Password Entry Screen.

Inbox Management

The TOE restricts the ability to modify and clear (remove) the password for an inbox to the authorized user of the inbox and the System Manager only.

The TOE gives the System Manager the ability to modify and clear any inbox password using the Control Panel. The TOE gives authorized inbox users the ability to modify and clear their own inbox passwords using the Control Panel or the Remote UI.

The TOE limits the inbox password to a 7-digit number. If a password-protected inbox is unregistered and re-registered with no password, the TOE removes the 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 of the multifunction product

is active, the System Manager Identification and Authentication function is invoked before allowing the user to operate the multifunction product from the Control Panel or via 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 accessing user as the System Manager only after verifying that the given ID and password are the correct System Manager ID and System Password.
If an incorrect System Manager ID or System Password is entered from the Control Panel or via the Remote UI, the TOE imposes a 1-second wait time before redisplaying the Password Entry Screen.
If the user is accessing from the Control Panel, the TOE maintains the user's role as the System Manager with the right to configure system management settings, manipulate inboxes and execute inbox management functions until the user exits the System Management mode with the ID key on the Control Panel.
If the user is accessing from the Remote UI, then the TOE maintains the user's role as the System Manager until the user closes the Web browser.

System Manager Management
The TOE assigns the following privileges to the System Manager only:
The System Manager can modify the System Manager ID and System Password, and can also delete (unset) the System Manager ID. The System Password is limited to a 7-digit number by the TOE. The TOE limits the System Password to a 7-digit number.
The System Manager can activate or deactivate the Secure Communication (Remote UI) function.

Secure Communication (Remote UI)
The TOE uses SSL for secure communications between the Remote UI and a user's Web browser in order to protect the transmitted data from unauthorized modification and disclosure.

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 of the multifunction product 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.
T.NETWORK_TAP: Eavesdropping of Data En Route	A malicious individual may attempt to disclose passwords and image data by intercepting data transmissions over the Remote UI communication path.

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 iR6570	Expansion Bus-C1,USB Application Interface Board-D1, additional memory (512MB or more in total, including onboard memory)
Canon iR6570N	
Canon iR5570	
Canon iR5570N	

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

Model Name	Necessary Options
Canon iR6570	Expansion Bus-C1, USB Application Interface Board-D1
Canon iR5570	

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
Any of the Web browsers shown in the following table can be used.

Table 1-4: Web browsers that can run the Remote UI

OS	Web Browser	Required SP
Windows	Microsoft Internet Explorer	5.01 SP2 or later
	Netscape Communicator	4.6 or later
Macintosh	Microsoft Internet Explorer	5.0 or later

Netscape Communicator 5.x and Netscape 6.x are not in the scope of evaluation.

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 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
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 password-protected using the Control Panel or the Remote UI. 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.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

(1) Documents attached to the Canon iR6570/iR5570 Series iR Security Kit-B3 Version 1.03 (International version)

- iR Security Kit-B3 Reference Guide, FA7-8992
- 6570/5570 Reference Guide, FA7-8997
- 6570/5570 Copying Guide, FA7-8998
- 6570/5570 Mail Box Guide, FA7-8999
- 6570/5570 Sending and Facsimile Guide, FA7-9000
- 6570/5570 Remote UI Guide, FA7-9001
- 6570/5570 Network Guide, FA7-9002
- MEAP SMS Administrator Guide, FA7-9003

(2) Documents attached to the Canon iR6570/iR5570 Series iR Security Kit-B3 Version 1.03 (Japanese version)

- Canon iR Security Kit-B3 Reference Guide, FA7-8981
- iR6570/iR6570N iR5570/iR5570N Reference Guide, FA7-8985
- iR6570/iR6570N iR5570/iR5570N Copying / Mail Box Guide, FA7-8986
- iR6570/iR6570N iR5570/iR5570N Sending and Facsimile Guide, FA7-8987
- iR6570/iR6570N iR5570/iR5570N Remote UI Guide, FA7-8988
- iR6570/iR6570N iR5570/iR5570N Network Guide, FA7-8989
- iR6570/iR6570N iR5570/iR5570N MEAP SMS Administrator Guide, FA7-8990
- iR6570/iR6570N iR5570/iR5570N MEAP Authentication System Setting Guide, FA7-8991

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

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 April, 2005 and concluded by completion the Evaluation Technical Report dated September, 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 June and July, 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 August, 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

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.1.03, Int'l version: Ver.1.03
Equipment	**Major Specification**
Multifunction product	iR6570N (Japanese), iR6570N (Int'l)
Options for the multifunction product	▪ iR 256MB Expansion RAM-B1 ▪ USB Application Interface Board-D1 ▪ Expansion Bus-C1 ▪ Send Expansion Kit ▪ Super G3 FAX Board-R1 ▪ Web browser
PC	Three Windows-based PCs
HUB	100Mbps switching HUB
Network cable x 2	UTP cable (category 5)
Facsimile apparatus	A facsimile to communicate with the multifunction product
Central Office simulator	A device to connect the multifunction product and the facsimile with simulated telephone lines
Software	**Major Specification**
OS	Microsoft Windows 2000 Professional Service Pack 4
Communications software	Serial terminal software
Printing software	Printing software for windows
Web browser	Microsoft Internet Explorer Version 6.0 Service Pack 1
Printer driver	Windows LIPS LX Version 1.11 Printer Driver (Japanese version) PCL6 or PCL5e Printer Driver and PS Printer Driver (English version)

2) Outlining of Developer Testing

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

a. Test configuration

The developer test configuration is clarified in Table 2-1.
The testing was conducted using only some of the product models identified as TOE platforms in the ST (only one used, out of four). 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.
Communications software, printing software, and other software 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

(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 their behavior by means of monitoring the operating status of the TOE program, capturing hard disk dumps, and monitoring packets on the network.

c. Scope of Testing Performed

Testing is performed about 107 items by the developer.
A coverage analysis was performed and verified that the security functions and external interfaces described in the functional specification have been all tested.
A depth analysis was performed and verified that the subsystems and subsystem interfaces described in the high-level design have been all thoroughly tested.

d. Result

The developer testing results provide evidence that the expected test results match the actual test results. The evaluator confirmed the legitimacy of the developer testing approach and tested items, and consistencies between the testing approach described in the test plan and the actual test results.

2.3.2 Evaluator Testing

1) Evaluator Test Environment

The evaluator used the same test configuration as the test configuration used by the developer, plus an additional tool for penetration testing against the developer test configuration.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. 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.

b. Scope of Testing Performed
The evaluator performed 60 tests in total; 15 independent tests, 24 sampled developer tests, and 21 penetration tests.
The evaluator's independent testing took the following into account.
(1) Security functions whose behavior could not be observed from outside
(2) Security functions with changeable parameters
The evaluator sampled 24 (23%) of the developer's 107 tests for sample testing in a way that all the functions would be covered.
The penetration testing comprised 21 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.

c. Result
The evaluator successfully completed all the tests and observed the behavior of the TOE security functions. The evaluator confirmed that the actual test results match the expected test results, 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.

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

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

4. Conclusion

4.1 Certification Result

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

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC:	Common Criteria for Information Technology Security Evaluation
CEM:	Common Methodology for Information Technology Security Evaluation
EAL:	Evaluation Assurance Level
PP:	Protection Profile
SOF:	Strength of Function
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Functions

The 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 iR6570/iR5570 Series iR Security Kit-B3 Security Target Version 1.05 (September 5, 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-0407 (December 2003)

[21] CCIMB Interpretations-0407 (December 2003)
(Translation Version 1.0 August 2004)

[22] Canon iR6570/iR5570 Series iR Security Kit-B3 (International version) iR Security Kit-B3 (Japanese version) Evaluation Technical Report Version 1.1, September 27, 2005, Electronic Commerce Security Technology Laboratory Inc. Evaluation Center