Document ID:

CANON-Device03-001

Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2

Security Target

This document is a translation of the security target written in Japanese, which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

Version 1.11

Jan 11, 2005

Canon Inc.

Revision History

Version	Date	Changes Made	Author	Reviewed by	Approved by
Ver.1.00	Jun 09, 2004	Original.	Sekita	Asai, Miyahara	Makitani
Ver.1.01	Jul 07, 2004	Addressed VCE-EOR-0001 thru 0005. Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.02	Jul 12, 2004	Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.03	Aug 02, 2004	Addressed VCE-EOR-0006 thru 0009. Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.04	Aug 17, 2004	Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.05	Aug 26, 2004	Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.06	Sep 01, 2004	Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.07	Nov 02, 2004	Addressed VCE-EOR-0022. Reflected internal review results. Modified due to additional supported devices.	Sekita	Miyahara	Makitani
Ver.1.08	Nov 15, 2004	Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.09	Dec 09, 2004	Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.10	Dec 10, 2004	Reflected internal review results.	Sekita	Miyahara	Makitani
Ver.1.11	Jan 11, 2005	Addressed VCE-EOR-0025 thru 0026.	Sekita	Miyahara	Makitani

English translation by Teruhiko Suzuki

Table of Contents

Trademark Notice

- Canon, the Canon logo, imageRUNNER, MEAP and the MEAP logo are trademarks of Canon Inc.
- Lotus Notes is a registered trademark of Lotus Development Corporation.
- Macintosh, Mac OS and QuickTime are trademarks of Apple Computer Inc., registered in the United States and other countries.
- Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States and other countries.
- Netscape, Netscape Communicator and Netscape Navigator are trademarks of Netscape Communications Corporation.
- All other company names and product names mentioned in this document are trademarks or registered trademarks of their respective owners.

1. ST Introduction

This chapter presents security target (ST) identification information, an overview of the ST, and claims of CC conformance for the TOE.

1.1. ST Identification

ST Title:	Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Security Target
Document ID:	CANON-Device03-001
Date:	Jan 11, 2005
ST Version:	Version 1.11
Authors:	Canon Inc.
TOE:	Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 1.04 (Japanese version) iR Security Kit-B2 Version 1.04 (International version) ***Note:*** *In this ST, the Japanese and the International versions of the TOE are referred to collectively as the "iR Security Kit-B2". The interface language to be evaluated is Japanese for the Japanese version, and English for the international version.*
Keywords:	Canon, imageRUNNER, iR, iR4570, iR3570, iR2870, iR2270, multifunction product, copy, print, fax, send, facsimile, residual information protection, overwrite, complete erase, encryption, Mail Box, Security Kit
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version2.1, August 1999 CCIMB Interpretations-0210
Assurance Level:	EAL2

1.2. ST Overview

This document is the Security Target that provides a specification of the security required of the "iR Security Kit-B2" software program that runs embedded in the Canon iR4570/iR3570/iR2870/iR2270-series multifunction products (hereafter referred to collectively as the "multifunction product" except where otherwise specified) to add security enhancements.

The TOE is provided to users as an optional product called "iR Security Kit-B2". Users contact their service providers to have the TOE installed on the hard disk drive of their multifunction product to replace the device control software, so that they can benefit from more secure multifunction products.

The TOE offers the security functions listed below to provide protection for every image data that will be created on the hard disk drive of the multifunction product, including both temporary image data and image data stored in the inboxes.

- HDD Data Encryption
- HDD Data Complete Erase
- Inbox User Identification and Authentication
- Inbox Management
- System Manager Identification and Authentication
- System Manager Management

1.3. CC Conformance

The TOE conforms with the following CC specifications:

- Security functional requirements – CC Part 2 Conformant
- Security assurance requirements – CC Part 3 Conformant
- Security assurance level – EAL2 Conformant

There are no Protection Profiles (PPs) claimed to which this ST is conformant.

1.4. Abbreviations and Terms

This ST uses the following abbreviations and terms.

Table 1-1: Abbreviations and terms

Abbrev and Terms	Description
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.
In-memory-reception	An act of receiving incoming faxes/I-faxes in memory for storage in the Memory Reception Inbox, without printing.
Mail Box	A function of the multifunction product that uses a dedicated portion of the HDD as the storage place for scanned documents, print jobs, and received faxes. It offers three types of storage places; User Inbox, Confidential Fax Inbox, and Memory Reception Inbox.
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	An inbox to store “in-memory-received” faxes/I-faxes for later printing or transfer to

Inbox	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.
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.

2. TOE Description

This chapter describes the product type, an overview and the scope of the TOE, as well as the assets to be protected.

2.1. Product Type

The TOE is optional software for the Canon iR4570/iR3570/iR2870/iR2270 series multifunction product to add security enhancements.
When installed, the TOE replaces the control software of the multifunction product.

2.2. Overview

The TOE is optional software for the Canon iR4570/iR3570/iR2870/iR2270-series multifunction product to add security enhancements. It is provided to users as an optional product called “iR Security Kit-B2”.

Users contact their service providers to have the TOE installed on the HDD of their multifunction product to replace the device control software, so that they can not only add the new HDD Data Encryption and Complete Erase functions to the multifunction product, but also increase the security of the already existing Inbox User and System Manager Identification and Authentication functions.

The multifunction product is a digital copier that offers the combined functionality of Copy, Send (Universal Send), Fax Reception, Mail Box, Print, and many others. It is equipped with a large-capacity HDD as the storage place for temporary image data that will be created through the use of the Copy, Print, and other functions.
The Mail Box function offers document storage functionality that saves scanned documents and documents received from external PCs to special disk space called “User Inbox”. All inboxes, including User Inboxes, can be password-protected to limit access to authorized users only.

Any user wishing to access a password-protected inbox for the purpose of reprinting the documents therein or sending them to an outside e-mail address or a shared folder on an external PC must first be identified and authenticated in the Inbox Selection Screen as an authorized inbox user with privileges to perform an operation that will involve readout of image data from the inbox. In contrast, a user who is identified and authenticated as the System Manager is given permission to read any image data from any inbox.

The TOE is used for the purpose of protecting the security of inbox-stored image data and any residual information left behind on the HDD of the multifunction product by deleting temporary image data or inbox-stored image data, preventing their unauthorized disclosure through unauthorized attempts (of reprinting or sending).

The Canon iR4570/iR3570/iR2870/iR2270-series multifunction product is intended for general use in office and business professional environments, and its assumed operating environment is shown in Figure 2-1. It should be noted however that Figure 2-1 is based on a use case where the multifunction product is fully-optioned as required by user needs, and thus may not be applicable to other environments where those options are partly or entirely not needed.

The multifunction product can also be used as a standalone copier or a fax machine by connecting to a telephone line, depending on the purpose of use.

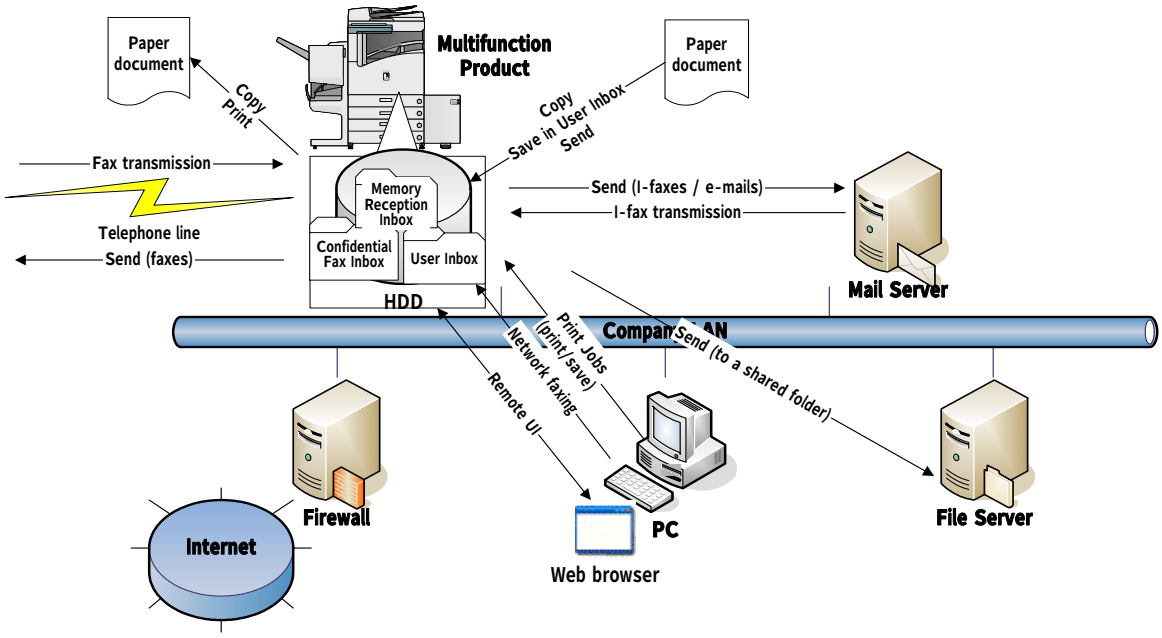

Figure 2-1: Assumed operational environment of Canon iR4570/iR3570/iR2870/iR2270

As depicted in Figure 2-1, the multifunction product has the following functions:

- **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.

- **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.
  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.

  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, whereas faxes/I-faxes received in a Confidential Fax Inbox are available for later printing only. Either way, inbox user identification and authentication must precede any attempt to read image data for printing or outbound transfer purposes. In contrast, user identification and authentication is not required before fax/I-fax reception, because in which case, no image data needs to be read out from the Memory Reception Inbox or a Confidential Fax Inbox.

- **User Inbox**
  A function to store documents scanned or received from an external PC as image data in a specified User Inbox.

  Inbox user identification and authentication must precede any attempt to read image data from a password-protected User Inbox for printing or outbound transfer purposes. In contrast, user identification and authentication is not required before storing image data in a User Inbox, because in which case, no image data needs to be read out.

  User Inbox-stored image data stored 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.

- **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 by using a fax driver.
  The Universal Send 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.

By installing the TOE, new functions are added to the Canon iR4570/iR3570/iR2870/iR2270-series multifunction product to ensure encryption of every temporary image data created on the HDD by the abovementioned functions and every inbox-stored image data created by the Fax Reception and User Inbox functions, and their complete removal upon deletion.
With these new security enhancements, it is possible to efficiently protect not only the image data stored in the inboxes, but also any residual information that will be left behind on the HDD by deleted temporary image data and/or inbox-stored image data.

2.2.1. Operating Environment

The operating environment of the TOE is described below.

Table 2-1: 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 options are available for the Japanese market models only, and hence their product names are quoted in Japanese language.
Canon iR4570F	
Canon iR3570	
Canon iR3570F	
Canon iR2870	
Canon iR2870F	
Canon iR2270	
Canon iR2270F	

Table 2-2: 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 print or fax from a user's PC, a printer driver or a fax driver needs to be installed on the user's PC. The following is a list of major printer drivers and fax drivers supporting this TOE.

- Canon LIPS IV/LIPS LX Printer Driver (Japanese version)
- Canon PCL5e/PCL6 Printer Driver (International version)
- Canon FAX Driver (Japanese and International versions)

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

- **Web browser**
  Any of the Web browsers shown in the following table is fine. Note however that the assumed Web browser is Microsoft Internet Explorer 6.0 for Windows.

Table 2-3: Web browsers that can run the Remote UI

OS	Web Browser	Version	Required SP
Windows	Microsoft Internet Explorer	5.01	SP2 or later
		5.5	SP2 or later
		6.0	-
	Netscape Communicator	4.75	-
		6.2.1	-
		7.1	-
Macintosh	Microsoft Internet Explorer	5.0	-
		5.2	-

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

For using the I-fax and the Universal Send functions, a mail server, an FTP server, or a file server is required.

2.3. Scope

This section describes the scope of the TOE from physical and logical points of view.

2.3.1. Physical Scope

The physical scope of the TOE includes the whole of the software program that controls the functions of the multifunction product identified in section 2.2 and the Web browser contents of the Remote UI. These are both to be installed on the HDD of the multifunction product.

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.

The TOE comprises one executable module and language files. Although the TOE allows MEAP applications to run on top of it and there are pre-installed MEAP authentication applications on the multifunction product, they are outside the scope of the TOE.
The TOE will prohibit addition of other MEAP applications.

Figure 2-2 illustrates the physical scope of the TOE on the multifunction product.

<table>
<tr><td colspan="2" rowspan="2"></td><td>MEAP Authentication Applications
(software: outside TOE boundary)</td></tr>
<tr><td colspan="3">iR Security Kit-B2
(software, TOE)</td></tr>
<tr><td colspan="4">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 colspan="2">Control Panel
(hardware: outside TOE boundary)</td></tr>
</table>

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

Figure 2-2: TOE boundary on the multifunction product and hardware/software outside the TOE

2.3.2. Logical Scope

The TOE is a replacement for the control software of the multifunction product and hence its logical scope includes the entire functions of the multifunction product identified in section 2.2, plus the security functions described below.

The user authentication and directory service linking functions of the MEAP authentication applications are not covered by the logical scope of the TOE.

- **HDD Data Encryption**
  A function to encrypt image data upon saving to the HDD.
- **HDD Data Complete Erase**
  A function to clear image data on the HDD by overwriting its disk space with meaningless data.
- **Inbox User Identification and Authentication**
  A function to identify and authenticate authorized inbox users 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.

2.4. Users

This section describes the type of TOE users.

- **Regular user**
  A user of the multifunction product.
- **System Manager**
  A user of the multifunction product who is responsible for device configuration and management and has the right to reset inbox passwords in the case of password loss, etc.
- **Inbox user**
  A regular user of an inbox. Each inbox user can password-protect his desired inbox to prevent access by other regular users.

2.5. Assets

In This ST, the TOE assets and other non-protected general data are identified as follows:

The assets to be protected are the image data portion of every document that will be saved to the HDD by the TOE, not including the document management information.

- **Temporary image data**
  Temporary image data that is created through copying, printing or any other user action needs to be protected from unauthorized disclosure.
- **Inbox-stored image data**
  Image data that is stored in an inbox through scanning, fax reception or any other user action needs to be protected from unauthorized disclosure. Any image data that is stored in a non-password-protected inbox is not considered as an asset to be protected.

In this ST, the following types of document-related data and image data are not considered as assets to be protected.

- Document management information (i.e., document information that is not image data, e.g., title, author, date of creation, etc.)
- Image data that is being transmitted or received over a network connection or a telephone line
- Image data stored in a non-password-protected inbox
- Form images (image data registered for use in overlay printing)

3. TOE Security Environment

This chapter describes the assumptions, threats and organizational security policies that are applicable to the TOE.

3.1. Assumptions

This section describes the assumptions about the TOE operating environment.

3.1.1. Intended Usage

A.OUT_OF_TOE: Image Data Outside the TOE
Each TOE user shall keep in mind that image data that has been sent outside the TOE and image data that has not yet been received by the TOE are both outside the scope of the TOE and thereby are not assets to be protected.

3.1.2. Personnel 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 protected with a password.
The System Manager ID and the System Password shall already be set.

3.1.3. Connectivity Assumptions

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.

3.2. Threats

This section identifies the threats to the TOE.

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.

3.3. Organizational Security Policies

This ST identifies no organizational security policies.

4. Security Objectives

This chapter describes the security objectives for the TOE and the environment.

4.1. Security Objectives for the TOE

O.CRYPTO: Image Data Encryption
The TOE shall encrypt temporary image data and inbox-stored image data upon saving to the HDD.

O.RESIDUAL: Residual Information Protection for Image Data
The TOE shall prevent any residual information from being left behind on the HDD upon deletion of temporary image data or inbox-stored image data.

O. AUTH: Identification and Authentication
The TOE shall require any user attempting to read image data from a password-protected inbox to be first identified and authenticated as an authorized user of the inbox or the System Manager, before allowing any inbox-stored image data to be read out, in order to restrict the ability to read image data from that inbox to the authorized user of the inbox and the System Manager only.

4.2. Security Objectives for the Environment

OE.OUT_OF_TOE: Image Data Outside the TOE
Each TOE user shall keep in mind that image data that has been sent outside the TOE and image data that has not yet been received by the TOE are both outside the scope of the TOE and thereby are not assets to be protected.

OE.ADMIN: Trusted System Manager
The administrative personnel of each department using the multifunction product shall assign a competent individual as the System Manager.

OE.PWD_MANAGE: Password Management
Each inbox user and the System Manager shall set passwords that cannot easily be guessed by others, keep them secret from others, and change them on a regular basis.

OE.PWD_SET: Password Registration
Any inbox user wishing to store valuable image data in an inbox for protection shall set a password on the inbox at the first use of it, and shall at all times use the TOE with the password enabled.

Any inbox user wishing to quit the use of an inbox (by password removal) shall first confirm that the inbox contains no valuable image data that requires protection.

The System Manager shall register a System Manager ID and a System Password immediately after completion of installation of the TOE, and shall at all times use the TOE with the System Manager ID and System Password enabled.

OE.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 due to security measures such as a firewall.

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.

5. Security Requirements

This chapter provides the TOE security functional requirements as well as security requirements for the IT environment.

5.1. TOE Security Requirements

This section describes the security requirements that the TOE needs to satisfy.

5.1.1. TOE Security Functional Requirements

This section describes the security functional requirements for the TOE.
All of these requirements consist of functional components from CC Part 2 and are tailored using the conventions described below.

Selections and assignments are both indicated by underlined text.
Refinements are indicated by italicized text inside parentheses.
Iterated components are indicated by appending a lowercase alphabet to the component name.

5.1.1.1. Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: the Canon iR cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: 168 bits] that meet the following: [assignment: nothing].

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: the Canon iR cryptographic key destruction algorithm] that meets the following: [assignment: nothing].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [assignment: encryption and decryption of inbox-stored image data and temporary image data] in accordance with a specified cryptographic algorithm

[assignment: Tripe DES] and cryptographic key sizes [assignment: 168 bits] that meet the following: [assignment: FIPS PUB 46-3].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.1.2. User Data Protection

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] the following objects: [assignment: inbox-stored image data and temporary image data].

Dependencies: No dependencies.

5.1.1.3. Identification and Authentication

FIA_AFL.1a Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1a The TSF shall detect when [assignment: one] unsuccessful authentication attempts occur related to [assignment: inbox user authentication].

FIA_AFL.1.2a When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: impose a 1-second wait time before allowing the next inbox user authentication attempt].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1b Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1b The TSF shall detect when [assignment: one] unsuccessful authentication attempts occur related to [assignment: System Manager authentication].

FIA_AFL.1.2b When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: impose a 1-second wait time before allowing the next System Manager authentication attempt].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_SOS.1a Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1a The TSF shall provide a mechanism to verify that secrets (*inbox passwords*) meet [assignment: a 7-digit number].

Dependencies: No dependencies.

FIA_SOS.1b **Verification of secrets**

Hierarchical to: No other components.

FIA_SOS.1.1b The TSF shall provide a mechanism to verify that secrets (*System Password*) meet [assignment: a 7-digit number].

Dependencies: No dependencies.

FIA_UAU.1 **Timing of authentication**

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [assignment: listing of inboxes] on behalf of the user to be performed before the user (*inbox user*) is authenticated.

FIA_UAU.1.2 The TSF shall require each user (*inbox user*) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2 **User authentication before any action**

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each user (*System Manager*) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 **Timing of identification**

Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [assignment: listing of inboxes] on behalf of the user to be performed before the user (*inbox user*) is identified.

FIA_UID.1.2 The TSF shall require each user (*inbox user*) to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 **User identification before any action**

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall require each user (*System Manager*) to identify itself before allowing any other TSF-mediated actions on behalf of the user.

Dependencies: No dependencies

5.1.1.4. Security Management

FMT_MTD.1a **Management of TSF data**

Hierarchical to: No other components.

FMT_MTD.1.1a The TSF shall restrict the ability to [selection: modify and clear] the [assignment: the password for an inbox] to [assignment: the authorized user of the inbox and the System Manager].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1b Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1a The TSF shall restrict the ability to [selection: modify and clear] the [assignment: System Manager ID and System Password] to [assignment: the System Manager].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: the management security functions underlined in the "Actions to Manage" column in Table 5-1 presented below].

Dependencies: No dependencies.

Table 5-1: Management security functions referenced by functional requirements

SFR	Actions to Manage	Addressed by
FCS_CKM.1	The following actions could be considered for the management functions in FMT: a) the management of changes to cryptographic key attributes. Examples of key attributes include key type (e.g. public, private, secret), validity period, and user (e.g. digital signature, key encryption, key agreement, data encryption).	None
FCS_CKM.4	The following actions could be considered for the management functions in FMT: a) the management of changes to cryptographic key attributes. Examples of key attributes include key type (e.g. public, private, secret), validity period, and user (e.g. digital signature, key encryption, key agreement, data encryption).	None
FCS_COP.1	There are no management activities foreseen for these components.	None
FDP_RIP.1	The following actions could be considered for the management functions in FMT Management: a) The choice of when to perform residual information protection (i.e., upon allocation or deallocation) could be made configurable within the TOE.	None
FIA_AFL.1a	The following actions could be considered for the management functions in FMT: a) management of the threshold for unsuccessful authentication attempts. b) management of actions to be taken in the event of an authentication failure.	None
FIA_AFL.1b	The following actions could be considered for the management functions in FMT: a) management of the threshold for unsuccessful authentication attempts. b) management of actions to be taken in the event of an authentication failure.	None
FIA_SOS.1a	The following actions could be considered for the management functions in FMT: a) the management of the metric used to verify the secrets.	None
FIA_SOS.1b	The following actions could be considered for the management functions in FMT:	None

SFR	Actions to Manage	Addressed by
	a) the management of the metric used to verify the secrets.	
FIA_UAU.1	The following actions could be considered for the management functions in FMT: a) management of the authentication data by an administrator; b) management of the authentication data by the associated user; c) managing the list of actions that can be taken before the user is authenticated.	FMT_MTD.1a
FIA_UAU.2	The following actions could be considered for the management functions in FMT: a) management of the authentication data by an administrator; b) management of the authentication data by the user associated with this data.	FMT_MTD.1b
FIA_UID.1	The following actions could be considered for the management functions in FMT: a) the management of the user identities; b) if an authorized administrator can change the actions allowed before identification, the managing of the action lists.	None
FIA_UID.2	The following actions could be considered for the management functions in FMT: a) the management of the user identities.	FMT_MTD.1b
FMT_MTD.1a	The following actions could be considered for the management functions in FMT Management: a) managing the group of roles that can interact with the TSF data.	None
FMT_MTD.1b	The following actions could be considered for the management functions in FMT Management: a) managing the group of roles that can interact with the TSF data.	None
FMT_SMF.1	There are no management activities foreseen for this component.	None
FMT_SMR.1	a) managing the group of users that are part of a role.	None
FPT_RVM.1	There are no management activities foreseen.	None

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: authorized inbox user, System Manager].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.1.5. Protection of the TSF

FPT_RVM.1 Non-bypassibility of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

5.1.2. Minimum Strength of Function Level

The TOE claims to have a minimum strength of function level of SOF-basic.

5.1.3. TOE Security Assurance Requirements

This section describes the security assurance requirements of the TOE.
The target assurance level for the TOE is EAL2. All the assurance requirements consist of the requirements for EAL2 defined in CC Part 3.
Also, although the ASE class is missing in the table below, it defines “must” assurance requirements for evaluation of the TOE.

Table 5-2: EAL2 assurance requirements

Assurance Class	Assurance Components
ACM	ACM_CAP.2
ADO	ADO_DEL.1, ADO_IGS.1
ADV	ADV_FSP.1, ADV_HLD.1, ADV_RCR.1
AGD	AGD_ADM.1, AGD_USR.1
ATE	ATE_COV.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_SOF.1, AVA_VLA.1

5.2. Security Requirements for the IT Environment

This section describes the security requirements that the IT environment of the TOE needs to satisfy.

5.2.1. IT Environment Security Functional Requirements

This TOE does not require any security functional requirements for the IT environment.

6. TOE Summary Specification

This chapter describes the TOE summary specification.

6.1. TOE Security Functions

This section describes the TOE security functions.

6.1.1. Security Function Details

In this ST, the password-based security functions implemented by SF.BOX_AUTH and SF.BOX_MANAGE and those implemented by SF.ADM_AUTH and SF.ADM_MANAGE are realized by a probabilistic or permutation mechanism, and the strength of these functions is SOF-basic.

Table 6-1: TOE security functions and functional components

Security Function	Functional Component
SF.CRYPTO	FCS_CKM.1, FCS_CKM.4, FCS_COP.1
SF.COMP_ERASE	FDP_RIP.1
SF.BOX_AUTH	FIA_UAU.1, FIA_UID.1, FIA_AFL.1a, FMT_SMR.1, FPT_RVM.1
SF.BOX_MANAGE	FIA_SOS.1a, FMT_MTD.1a, FMT_SMF.1, FPT_RVM.1
SF.ADM_AUTH	FIA_UAU.2, FIA_UID.2, FIA_AFL.1b, FMT_SMR.1, FPT_RVM.1
SF.ADM_MANAGE	FIA_SOS.1b, FMT_MTD.1b, FMT_SMF.1, FPT_RVM.1

SF.CRYPTO: HDD Data Encryption
The TOE generates 168-bit Triple DES cryptographic keys using the Canon iR cryptographic key generation algorithm.

For 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.
For 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.

SF.COMP_ERASE: 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 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). This is achieved by overwriting the corresponding disk space with meaningless data.

SF.BOX_AUTH: 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.

After verifying that the given password is the correct inbox password, the TOE identifies and authenticates

the user as an authorized user of the inbox and displays the Inbox Operation Screen.

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 another inbox is manipulated 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.

SF.BOX_MANAGE: 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.

SF.ADM_AUTH: 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.

After verifying that the given ID and password are the correct System Manager ID and System Password, the TOE identifies and authenticates the user as the System Manager. 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 inboxes 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 as the System Manager until the Web browser is closed.

SF.ADM_MANAGE: System Manager Management
The TOE restricts the right to modify and clear (remove) the System Manager ID and the System Password to the System Manager only.

The TOE limits the System Password to a 7-digit number.

6.2. Assurance Measures

This section describes the TOE security assurance measures.
The following assurance measures satisfy the assurance requirements identified in section 5.1.3.
Note that this ST is the assurance measure for the ASE class.

Table 6-2: Mapping of assurance components to assurance measures

Assurance Component	Assurance Measure
ACM_CAP.2	iR Security Kit-B2 Configuration Management Plan**(*)** iR Security Kit-B2 List of Configuration Items**(*)**
ADO_DEL.1	iR Security Kit-B2 Delivery Procedures**(*)**
ADO_IGS.1	iR Security Kit-B2 Installation Procedure (Japanese version) **(*)** iR Security Kit-B2 Installation Procedure (English version)
ADV_FSP.1	iR Security Kit-B2 Functional Specification**(*)**
ADV_HLD.1	iR Security Kit-B2 High-level Design**(*)**
ADV_RCR.1	iR Security Kit-B2 Analysis of Correspondence**(*)**
AGD_ADM.1	iR Security Kit-B2 Reference Guide (Japanese version) **(*)** iR Security Kit-B2 Reference Guide (English version)
AGD_USR.1	iR Security Kit-B2 Reference Guide (Japanese version) **(*)** iR Security Kit-B2 Reference Guide (English version)
ATE_COV.1	iR Security Kit-B2 Test Plan and Procedures**(*)**
ATE_FUN.1	iR Security Kit-B2 Test Plan and Procedures**(*)** iR Security Kit-B2 Test Results**(*)**
ATE_IND.2	TOE
AVA_SOF.1	iR Security Kit-B2 Strength of Function Analysis**(*)**
AVA_VLA.1	iR Security Kit-B2 Vulnerability Analysis**(*)**

(*) These document titles were translated from the original Japanese titles.

7. PP Claims

This chapter describes the PP claims.

7.1. PP Reference

There is no PP referenced by this ST.

7.2. PP Tailoring

There is no PP tailored by this ST.

7.3. PP Additions

There are no PP additions made by this ST.

8. Rationale

This chapter describes the rationale for the security objectives, requirements and TOE summary specifications.

8.1. Security Objectives Rationale

This section demonstrates that the security objectives are suitable to meet the threats and assumptions defined in the TOE security environment.

Table 8-1: Mapping of security objectives to threats, organizational security policies and assumptions

	A.OUT_OF_TOE	A.ADMIN	A.PWD_MANAGE	A.PWD_SET	A.NETWORK	T.HDD_ACCESS	T.UNAUTH
O.CRYPTO						X	
O.RESIDUAL						X	
O.AUTH							X
OE.OUT_OF_TOE	X						
OE.ADMIN		X					
OE.PWD_MANAGE			X				
OE.PWD_SET				X			
OE.NETWORK					X		

8.1.1. Rationale for Organizational Security Policies

There are no organization security policies in this ST.

8.1.2. Rationale for Threats

T.HDD_ACCESS: O.CRYPT ensures that every temporary image data and inbox-stored image data are encrypted upon saving to the HDD, thereby mitigating the threat T.HDD_ACCESS when the protected assets are stored on the HDD.

Furthermore, O.RESIDUAL ensures protection of any residual information left on the HDD by deleted temporary and inbox-stored image data, thereby removing the threat T.HDD_ACCESS when the protected assets are deleted from the HDD.

These security objectives contribute to mitigate the threat of the protected assets from being disclosed by means of direct HDD access.

T.UNAUTH: O.AUTH ensures that the TOE identifies and authenticates authorized inbox users and the System Manager, so as to prohibit unauthorized access attempts by unauthorized users (except the System Manager) to any password-protected inbox. This mitigates the threat of inbox-stored image data being disclosed by means of unauthorized access attempts via the Control Panel or the Remote UI.

8.1.3. Rationale for Assumptions

A.OUT_OF_TOE: OE.OUT_OF_TOE ensures that each TOE user keeps in mind that image data that has been sent outside the TOE and image data that has not yet been received by the TOE are both outside the scope of the TOE and thereby are not assets to be protected. Therefore, A.OUT_OF_TOE is satisfied.

A.ADMIN: OE.ADMIN ensures that the manager of the department using the multifunction product assigns a responsible individual as the System Manager. Therefore, A.ADMIN is satisfied.

A.PWD_MANAGE: OE.PWD_MANAGE ensures that every inbox user and the System Manager use passwords that cannot easily be guessed by others, keep them secret from others, and change them on a regular basis. Therefore, A.PWD_MANAGE is satisfied.

A.PWD_SET: OE.PWD_SET ensures that any inbox user wishing to store valuable image data in an inbox for protection sets a password on the inbox; that any inbox user wishing to quit the use of an inbox (by password removal) first confirms that the inbox contains no valuable image data that requires protection; and that the System Manager ID and the System Password are defined. Therefore, A.PWD_SET is satisfied.

A.NETWORK: OE.NETWORK ensures that the multifunction product running the TOE is connected to the internal network that is inaccessible directly from outside networks; and that the Remote UI is 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 managed properly by the network administrator to refuse connection attempts by unauthorized devices to prevent packet sniffing. Therefore, A.NETWORK is satisfied.

8.2. Security Requirements Rationale

8.2.1. Rationale for Security Functional Requirements

Table 8-2 shows the mapping of security functional requirements to security objectives.

Table 8-2: Mapping of security functional requirements and security objectives

	O.CRYPTO	O.RESIDUAL	O.AUTH
FCS_CKM.1	X		
FCS_CKM.4	X		
FCS_COP.1	X		
FDP_RIP.1		X	
FIA_AFL.1a			X
FIA_AFL.1b			X
FIA_SOS.1a			X
FIA_SOS.1b			X
FIA_UAU.1			X
FIA_UAU.2			X
FIA_UID.1			X
FIA_UID.2			X
FMT_MTD.1a			X
FMT_MTD.1b			X
FMT_SMF.1			X
FMT_SMR.1			X
FPT_RVM.1			X

O.CRYPTO: FCS_CKM.1 ensures generation of cryptographic keys.
FCS_COP.1 ensures encryption of inbox-stored image data and temporary image data upon saving to the HDD using generated cryptographic keys.
FCS_CKM.4 ensures destruction of generated cryptographic keys.
Therefore, O.CRYPTO is achieved.

O.RESIDUAL: FDP_RIP.1 ensures that residual information on the HDD is protected upon deallocation of inbox-stored image data and temporary image data from disk space.
Therefore, O.RESIDUAL is satisfied.

O.AUTH: FIA_UID.1 and FIA_UAU.1 ensure that any attempt to read image data from a password-protected inbox is preceded by inbox user identification and authentication.
FIA_UID.2 and FIA_UAU.2 ensure that any attempt to perform System Manager actions on any inbox is preceded by System Manager identification and authentication.

In case of successful authentication, FMT_SMR.1 ensures that the accessing user is maintained as an authorized inbox user or the System Manager.

In case of unsuccessful authentication, FIA_AFL.1a and FIA_AFL.1b ensure that a 1-second wait time is imposed before another authentication attempt is accepted, so as to unfailingly limit the maximum allowed number of authentication attempts in the specified period, reducing the chances of success for attackers and ensuring effective operation of these authentication functions.

These functional requirements in combination ensure that the ability to read image data from a password-protected inbox is restricted to the authorized user of the inbox and the System Manager only.

FMT_MTD.1a and FMT_SMF.1 ensure that the ability to modify the password for an inbox is restricted to the authorized user of the inbox and the System Manager only. FIA_SOS.1a ensures that every inbox password is limited in length.

FMT_MTD.1b and FMT_SMF.1 ensure that the ability to modify the System Manager ID and the System Password is restricted to the System Manager only. FIA_SOS.1b ensures that the System Password is limited in length.

These functional requirements in combination prevent impersonation of authorized inbox users or the System Manager.

Furthermore, FPT_RVM.1 ensures that any attempt to read image data from a password-protected inbox is never be allowed without prior user identification and authentication, preventing the Inbox User Identification and Authentication function and the System Manager Identification and Authentication functions from being bypassed.

Therefore, O.AUTH is achieved.

8.2.2. Rationale for Security Assurance Requirements

In this ST, the EAL2 assurance package is selected to identify the TOE security assurance requirements.

The TOE is a software program to control the entire functionality of the multifunction product that is not only the platform for running the TOE but also is a general commercial product intended for use in an office environment. Therefore, it is required to provide assurance of security against low-level attackers.

Since A.NETWORK ensures that the TOE is secure from direct attacks from outside networks such as the Internet, EAL2 is an appropriate assurance level for the TOE, taking the time and cost of evolution into account.

8.2.3. Dependencies of Security Functional Requirements

Table 8-3 shows the dependencies of the security functional requirements.
The left column shows the components selected in this ST and the right column shows the components that are dependent upon. Removed components are indicated in parentheses.

Table 8-3: Security functional requirements dependencies

SFR	Dependencies
FCS_CKM.1	(FCS_CKM.2) or FCS_COP.1, FCS_CKM.4, (FMT_MSA.2)
FCS_CKM.4	(FDP_ITC.1) or FCS_CKM.1, (FMT_MSA.2)
FCS_COP.1	(FDP_ITC.1) or FCS_CKM.1, FCS_CKM.4, (FMT_MSA.2)
FDP_RIP.1	–
FIA_AFL.1a	FIA_UAU.1
FIA_AFL.1b	FIA_UAU.1: satisfied by FIA_UAU.2
FIA_SOS.1a	–
FIA_SOS.1b	–
FIA_UAU.1	FIA_UID.1
FIA_UAU.2	FIA_UID.1: satisfied by FIA_UID.2
FIA_UID.1	–
FIA_UID.2	–
FMT_MTD.1a	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1b	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	–
FMT_SMR.1	FIA_UID.1
FPT_RVM.1	–

As for the security assurance requirements, they are conformant to the EAL2 level and thus all dependencies are satisfied.

Rationale for Not Satisfying All Dependencies:

The dependency of FCS_CKM.1 on FCS_CKM.2 is not satisfied, because –
FCS_COP.1 is used.

The dependencies of FCS_CKM.4 and FCS_COP.1 on FDP_ITC.1 are not satisfied, because –
FCS_CKM.1 is used.

The dependency of FCS_CKM.1 on FMT_MSA.2 is not satisfied, because –
In this TOE, only one common key is used for encryption of HDD data and thus there are no key attributes, e.g. key type and expiration period, to be managed at the time of key generation. Therefore, the functional requirement for the management of security attributes is not needed.

The dependency of FCS_CKM.4 on FMT_MSA.2 is not satisfied, because –
In this TOE, only one common key is used for HDD data encryption and thus there are no key attributes, e.g. key type and expiration period, to be managed at the time of key destruction. Therefore, the functional requirement for the management of security attributes is not needed.

The dependency of FCS_COP.1 on FMT_MSA.2 is not satisfied, because –
In this TOE, only one common key is used for HDD data encryption and thus there are no key attributes, e.g. key type and expiration period, to be managed at the time of image data encryption. Therefore, the functional requirement for the management of security attributes is not needed.

8.2.4. Mutually Supportive Security Requirements

The security functional requirements selected in this ST are mutually supportive, as demonstrated below.

The TOE has identification and authentication functions (FIA) to prevent unauthorized access to password-protected inboxes. Identification information and authentication information are managed by the security management (FMT), so that they can be changed or cleared. These functions are mutually supportive owing to the security management (FMT) functional requirements, preventing impersonation of authorized inbox users.

Also, FDP_RIP.1 and FCS_COP.1 ensure protection and encryption of residual information on the HDD, jointly protecting all inbox-stored image data and temporary image data from unauthorized disclosure attempts by means of direct HDD access bypassing the TOE.

The non-bypassibility of the TOE is provided by FPT_RVM.1, as it ensures that the Inbox User and System Manager Identification and Authentication functions (FIA_UID.1, FIA_UID.2, FIA_UAU.1, and FIA_UAU.2) cannot be bypassed, by allowing no user to read image data from any password-protected inbox unless successfully identified and authenticated as an authorized user of the inbox or the System Manager.

FPT_RVM.1 further ensures the non-bypassibility of these identification and authentication functions (FIA_UID.1, FIA_UID.2, FIA_UAU.1, and FIA_UAU.2), for the security functions, specified by FMT_MTD.1a and FMT_MTD.1b, that restrict the ability to modify and clear identification and authentication data to specific users only.

As such, FPT_RVM.1 supports the TOE in restricting the ability to read image data from a password-protected inbox to the authorized user of the inbox and the System Manager only.

8.2.5. Rationale for Minimum Strength of Function Level

The TOE claims to have a minimum strength of function level of SOF-basic.

This claim is appropriate, because the TOE is a software program to control the entire functionality of the multifunction product that is not only the platform for running the TOE but also is a general commercial product intended for use in an office environment. Therefore, it is required to provide assurance of security against low-level attackers.

8.3. TOE Summary Specification Rationale

8.3.1. Rationale for TOE Security Functions

Table 8-4 shows the mapping of TOE security functions to TOE security functional requirements.

Table 8-4: Mapping of security functions to security functional requirements

	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_RIP.1	FIA_AFL.1a	FIA_AFL.1b	FIA_SOS.1a	FIA_SOS.1b	FIA_UAU.1	FIA_UAU.2	FIA_UID.1	FIA_UID.2	FMT_MTD.1a	FMT_MTD.1b	FMT_SMF.1	FMT_SMR..1	FPT_RVM.1
SF.CRYPTO	X	X	X														
SF.COMP_ERASE				X													
SF.BOX_AUTH					X				X		X					X	X
SF.BOX_MANAGE							X						X		X		X
SF.ADM_AUTH						X				X		X				X	X
SF.ADM_MANAGE								X						X	X		X

FCS_CKM.1:
This requirement is addressed by SF.CRYPTO, which generates cryptographic keys.

FCS_CKM.4:
This requirement is addressed by SF.CRYPTO, which destroys cryptographic keys.

FCS_COP.1:
This requirement is addressed by SF.CRYPTO, which encrypts/decrypts image data.

FDP_RIP.1:
This requirement is addressed by SF.COMP_ERASE, which performs a complete erase of image data on the HDD.

FIA_AFL.1a:
This requirement is addressed by SF.BOX_AUTH, which imposes a 1-second wait time before the Password Entry Screen is redisplayed if an incorrect inbox password is specified.

FIA_AFL.1b:
This requirement is addressed by SF.ADM_AUTH, which imposes a 1-second wait time before the Password Entry Screen is redisplayed if an incorrect System Password is specified.

FIA_SOS.1a:
This requirement is addressed by SF.BOX_MANAGE, which limits the inbox password to a 7-digit number.

FIA_SOS.1b:
This requirement is addressed by SF.ADM_MANAGE, which limits the System Password to a 7-digit number.

FIA_UAU.1:
This requirement is addressed by SF.BOX_AUTH, which requires each inbox accessing user to be

successfully authenticated by means of inbox password verification before reading out any inbox-stored image data.

FIA_UAU.2:

This requirement is addressed by SF.ADM_AUTH, which requires the System Manager to be successfully authenticated by entering the System Password in the Startup Screen at the multifunction product's startup if the Department ID Management function is active; or otherwise in the System Settings Screen.

FIA_UID.1:

This requirement is addressed by SF.BOX_AUTH, which requires each inbox accessing user to be successfully identified by means of inbox password verification before reading out any inbox-stored image data.

FIA_UID.2:

This requirement is addressed by SF.ADM_AUTH, which requires the System Manager to be successfully identified by entering the System Password in the Startup Screen at the multifunction product's startup if the Department ID Management function is active; or otherwise in the System Settings Screen.

FMT_MTD.1a:

This requirement is addressed by SF.BOX_MANAGE, which prohibits the changing/clearing of any inbox password without prior successful inbox user identification and authentication, or prior successful System Manager identification and authentication via the Control Panel.

FMT_MTD.1b:

This requirement is addressed by SF.ADM_MANAGE, which prohibits the changing of the System Manager ID and the System Password without prior successful System Manager identification and authentication.

FMT_SMF.1:

The management action of FIA_UAU.1 (the management of the authentication data by the associated user) is addressed by SF.BOX_MANAGE, which permits each inbox user to manage only their own password for their inbox. Also, the management action of FIA_UAU.2 (the management of the authentication data by an administrator) and the management action of FIA_UID.2 (the management of the user identities) are addressed by SF.ADM_MANAGE, which ensures that only the System Manager is allowed to manage the System Manager ID and System Password.
There are still other actions that should be considered for the management functions. The following clarifies the rationale for the TOE not providing security management functions for them.

FCS_CKM.1	a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption). Only one common key will be used and thus no cryptographic key attributes need to be managed.
FCS_CKM.4	a) the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption). Only one common key will be used and thus no cryptographic key attributes need to be managed.
FDP_RIP.1	a) the choice of when to perform residual information protection (i.e., upon allocation or deallocation) could be made configurable within the TOE.

	No such setting value is necessary because a complete erase will be performed immediately following the deallocation of the resource.
FIA_AFL.1a	a) management of the threshold for unsuccessful authentication attempts; b) management of actions to be taken in the event of an authentication failure. There is no action to manage because the threshold is fixed and there is only one action that is to be taken.
FIA_AFL.1b	a) management of the threshold for unsuccessful authentication attempts; b) management of actions to be taken in the event of an authentication failure. There is no action to manage because the threshold is fixed and there is only one action that is to be taken.
FIA_SOS.1a	a) the management of the metric used to verify the secrets. The metric used to verify the secrets is fixed and thus needs no management.
FIA_SOS.1b	a) the management of the metric used to verify the secrets. The metric used to verify the secrets is fixed and thus needs no management.
FIA_UID.1	a) the management of the user identities; b) if an authorized administrator can change the actions allowed before identification, the managing of the action lists. The user identities need no management because identification and authentication are performed together. Also, the actions allowed before identification are fixed and need no management.
FMT_MTD.1a	a) managing the group of roles that can interact with the TSF data. There is no action to manage because the role is automatically maintained after authentication.
FMT_MTD.1b	a) managing the group of roles that can interact with the TSF data. There is no action to manage because the role is automatically maintained after authentication.
FMT_SMR.1	a) managing the group of users that are part of a role. There is no action to manage because the role is automatically maintained after authentication.

FMT_SMR.1:

This requirement is addressed by SF.BOX_AUTH, which maintains the authorized inbox user role until the Inbox Operation Screen is exited, if the user has been identified and authenticated via the Control Panel; or until another inbox is manipulated or the Web browser is closed, if the user has been identified and authenticated via the Remote UI. It is also addressed by SF.ADM_AUTH, which maintains the System Manager role until the System Management mode is canceled, if the user has been identified and authenticated via the Control Panel; or until the Web browser is closed, if the user has been identified and authenticated via the Remote UI.

FPT_RVM.1:

This requirement is addressed by SF.BOX_AUTH and SF.ADM_AUTH, and by SF.BOX_MANAGE and SF.ADM_MANAGE. For details, see section 8.3.3.

8.3.2. Rationale for Strength of Function

The security functions implemented by SF.BOX_AUTH and SF.BOX_MANAGE and those implemented by SF.ADM_AUTH and SF.ADM_MANAGE are realized by a probabilistic or permutation mechanism and the strength of these security functions are SOF-basic. Also, the minimum strength of function of the TOE is SOF-basic. As these strength of function levels do not conflict, the strength of function claim of SOF-basic for the security functions realized by SF.BOX_AUTH and SF.BOX_MANAGE and by SF.ADM_AUTH and SF.ADM_MANAGE is reasonable.

8.3.3. Rationale for Combination of Security Functions

In order to protect the TOE assets on the HDD from unauthorized direct access, inbox-stored image data and temporary image data are encrypted by SF.CRYPTO upon saving to the HDD, and are completely erased by SF.COMP_ERASE upon deletion from the HDD.

Protection is ensured for inbox-stored image data by not allowing any readout attempts without prior invocation of SF.BOX_AUTH or SF.ADM_AUTH, which refuses access attempts by any other user than authorized inbox users and the System Manager.

Also, inbox passwords are managed by SF.BOX_MANAGE and the System Manager ID and the System Password are managed by SF.ADM_MANAGE. These management functions are restricted to authorized inbox users and the System Manager only, hence, SF.BOX_AUTH and SF.ADM_AUT are always invoked and cannot be bypassed.

8.3.4. Rationale for Assurance Measures

Table 8-5 shows the mapping of assurance measures to EAL2 assurance components.

Table 8-5: Mapping of assurance measures to assurance components

Assurance Measures	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ATE_COV.1	ATE_FUN.1	ATE_IND.1	AVA_SOF.1	AVA_VLA.1
iR Security Kit-B2 Configuration Management Plan**(*)**	X												
iR Security Kit-B2 List of Configuration Items**(*)**	X												
iR Security Kit-B2 Delivery Procedures**(*)**		X											
iR Security Kit-B2 Installation Procedure (Japanese) **(*)** iR Security Kit-B2 Installation Procedure (English)			X										
iR Security Kit-B2 Functional Specification **(*)**				X									
iR Security Kit-B2 High-level Design**(*)**					X								
iR Security Kit-B2 Analysis of Correspondence**(*)**						X							
iR Security Kit-B2 Reference Guide (Japanese) **(*)** iR Security Kit-B2 Reference Guide (English)							X	X					
iR Security Kit-B2 Test Plan and Procedures**(*)**									X	X			
iR Security Kit-B2 Test Results**(*)**										X			
TOE											X		
iR Security Kit-B2 Strength of Function Analysis**(*)**												X	
iR Security Kit-B2 Vulnerability Analysis**(*)**													X

(*) These document titles were translated from the original Japanese titles.

ACM_CAP.2:
The documents “iR Security Kit-B2 Configuration Management Plan” and “iR Security Kit-B2 List of Configuration Items” describe the configuration management of the TOE.

ADO_DEL.1:
The document “iR Security Kit-B2 Delivery Procedures” ensures the secure transfer of the TOE to a user’s site.

ADO_IGS.1:
The documents “iR Security Kit-B2 Installation Procedure” (Japanese) and “iR Security Kit-B2 Installation Procedure” (English) ensure secure installation of the TOE.

ADV_FSP.1:
The document “iR Security Kit-B2 Functional Specification” provides the functional specification of the TOE.

ADV_HLD.1:
The document “iR Security Kit-B2 High-level Design” provides the high-level design of the TOE.

ADV_RCR.1:
The document “iR Security Kit-B2 Analysis of Correspondence” describes the correspondence between the TOE summary specification and the functional specification, and the correspondence between the functional specification and the high-level design.

AGD_ADM.1:
The documents “iR Security Kit-B2 Reference Guide” (Japanese) and “iR Security Kit-B2 Reference Guide” (English) provide the administrator and regular user guidance.

AGD_USR.1:
The documents “iR Security Kit-B2 Reference Guide” (Japanese) and “iR Security Kit-B2 Reference Guide” (English) provide the administrator and regular user guidance.

ATE_COV.1:
The document “iR Security Kit-B2 Test Plan and Procedures” provides the analysis of the coverage.

ATE_FUN.1:
The documents “iR Security Kit-B2 Test Plan and Procedures” and “iR Security Kit-B2 Test Results” provide the developer test plans and test results.

ATE_IND.2:
The TOE is provided.

AVA_SOF.1:
The document “iR Security Kit-B2 Strength of Function Analysis” provides a rationale for the strength of function claim for the probabilistic or permutation mechanism.

AVA_VLA.1:
The document “iR Security Kit-B2 Vulnerability Analysis” describes the developer vulnerability analysis of the TOE.