Document ID:
CANON-Device06-001

Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 V2

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 1.03
Nov 17, 2005

Canon Inc.

Revision History

Version	Date	Changes Made	Author	Reviewer	Approver
Ver.1.00	Sep 28, 2005	Original.	Hirota	Miyahara	Makitani
Ver.1.01	Oct 03, 2005	Changed the TOE name.	Hirota	Miyahara	Makitani
Ver.1.02	Oct 25, 2005	Revised the description of the security function SF.COMP_ERASE.	Hirota	Miyahara	Makitani
Ver.1.03	Nov 17, 2005	Changed the TOE version.	Hirota	Miyahara	Makitani

English translation by Teruhiko Suzuki

Table of Contents

1. ST Introduction 5
1.1. ST Identification 5
1.2. ST Overview 5
1.3. CC Conformance 6
1.4. Abbreviations and Terms 6

2. TOE Description 8
2.1. Product Type 8
2.2. Overview 8
2.3. Operating Environment 10
2.4. Scope 11
2.4.1. Physical Scope 11
2.4.2. Logical Scope 12
2.5. Users 12
2.6. Assets 13

3. TOE Security Environment 14
3.1. Assumptions 14
3.1.1. Personnel Assumptions 14
3.1.2. Connectivity Assumptions 14
3.2. Threats 14
3.3. Organizational Security Policies 15

4. Security Objectives 16
4.1. Security Objectives for the TOE 16
4.2. Security Objectives for the Environment 16

5. Security Requirements 17
5.1. TOE Security Requirements 17
5.1.1. TOE Security Functional Requirements 17
5.1.2. Minimum Strength of Function Level 22
5.1.3. TOE Security Assurance Requirements 22
5.2. Security Requirements for the IT Environment 23
5.2.1. IT Environment Security Functional Requirements 23

6. TOE Summary Specification 24
6.1. TOE Security Functions 24
6.1.1. Security Function Details 24
6.2. Assurance Measures 26

7. PP Claims 27
7.1. PP Reference 27
7.2. PP Tailoring 27
7.3. PP Additions 27

8. Rationale 28
8.1. Security Objectives Rationale 28
8.1.1. Rationale for Organizational Security Policies 28
8.1.2. Rationale for Threats 29
8.1.3. Rationale for Assumptions 29
8.2. Security Requirements Rationale 30
8.2.1. Rationale for Security Functional Requirements 30
8.2.2. Rationale for Security Assurance Requirements 31
8.2.3. Dependencies of Security Functional Requirements 32
8.2.4. Mutually Supportive Security Requirements 32
8.2.5. Rationale for Minimum Strength of Function Level 33

8.3. TOE Summary Specification Rationale 33
8.3.1. Rationale for TOE Security Functions 33
8.3.2. Rationale for Strength of Function 36
8.3.3. Rationale for Combination of Security Functions 37
8.3.4. Rationale for Assurance Measures 37

Trademark Notice

- Canon, the Canon logo, imageRUNNER, MEAP and the MEAP logo are trademarks of Canon Inc.
- Macintosh, Mac OS and QuickTime are trademarks of Apple Computer Inc., registered in the United States and other countries.
- Active Directory, 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.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.
- 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 V2 Security Target
Document ID:	CANON-Device06-001
Date:	Nov 17, 2005
ST Version:	Version 1.03
Authors:	Canon Inc.
TOE:	Canon iR4570/iR3570/iR2870/iR2270 Series iR Security Kit-B2 Version 2.03 (Japanese version) iR Security Kit-B2 Version 2.03 (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 V2".*
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-0407
Assurance Level:	EAL3

1.2. ST Overview

This document is the Security Target that provides a specification of the security required of the "iR Security Kit-B2 V2" 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 V2". 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 the added security of the multifunction product.

The TOE offers the security functions listed below to provide protection for image data on the hard disk drive of the multifunction product, including both temporary data and permanent 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
- Secure Communication (Remote UI)

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 – EAL3 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 that stores incoming faxes/I-faxes 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 operation of the multifunction product.
Department ID	A unique ID assigned to each multifunction product user, who can be an individual or a department. When the Department ID Management function is active, any user must be identified and authenticated before operating the multifunction product. The System Manager is a user who is assigned a special department ID called the System Manager ID.
Department ID Management	A function of the multifunction product that assigns a department ID and a password to each multifunction product user, so as to keep track and control of usage information, e.g. the number of printed copies, on a per-department basis. When the Department ID Management function is active, any user must be identified and authenticated by providing the correct department ID and password before using the multifunction product.
Document	User data handled within the multifunction product. A document consists of management information and image data.
Form image	Image data stored in the multifunction product for use for overlay printing.
HDD	The hard disk drive of the multifunction product. It is the place 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 as a result of scanning, printing and fax reception operations.
In-memory-reception	Refers to storing received faxes/I-faxes in the Memory Reception Inbox without printing them.
Mail Box	A function of the multifunction product that offers storage space for scanned documents, print jobs and received faxes. Three types of storage inboxes are available; User Inbox, Confidential Fax Inbox, and Memory Reception Inbox.
MEAP	Short for Multifunctional Embedded Application Platform, which is an application platform for the multifunction product. It can run “MEAP applications” developed with the Java language.
MEAP applications	Special applications developed with the Java language for use in Canon digital multifunction products. They can be used in conjunction with a Canon digital multifunction product’s functions, e.g. print, copy, fax, scan, etc., to customize the user interface, simplify the document flow and automate routine tasks.

MEAP authentication application	A MEAP application that authenticates regular users of the multifunction product using Active Directory. It can substitute the Department ID Management function of the multifunction product for identification and authentication of regular users.
Memory Reception Inbox	An inbox that stores "in-memory-received" faxes/I-faxes for later printing or transfer to an external destination.
Multifunction product	A collective name for the Canon iR4570/iR3570/iR2870/iR2270 series copiers that offer the combined functionality of copying, faxing, printing and transmission (Universal Send). The multifunction product is equipped with a large-capacity HDD to perform these functions, and allows the TOE to run embedded in it.
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, tailoring device 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 the accessing user is given System Manager privileges on the multifunction product. Any operations attempted in this mode will be executed 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 charge of device configuration and management tasks. The System Manager may also be put in charge of inbox management on behalf of inbox users. The multifunction product regards a user with the System Manager ID as the System Manager.
User Inbox	An inbox that stores documents scanned by regular users and documents sent for storage from external PCs. 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 V2”.

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 HDD Data Encryption and Complete Erase functions to the multifunction product, but also increase the security of the 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, plus many others. It is equipped with a large-capacity hard drive and stores image data there temporarily when performing copying, printing, etc.
The Mail Box function is a document storage function that allows saving 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 documents 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 read image data from that 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 some or all of those options are 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.

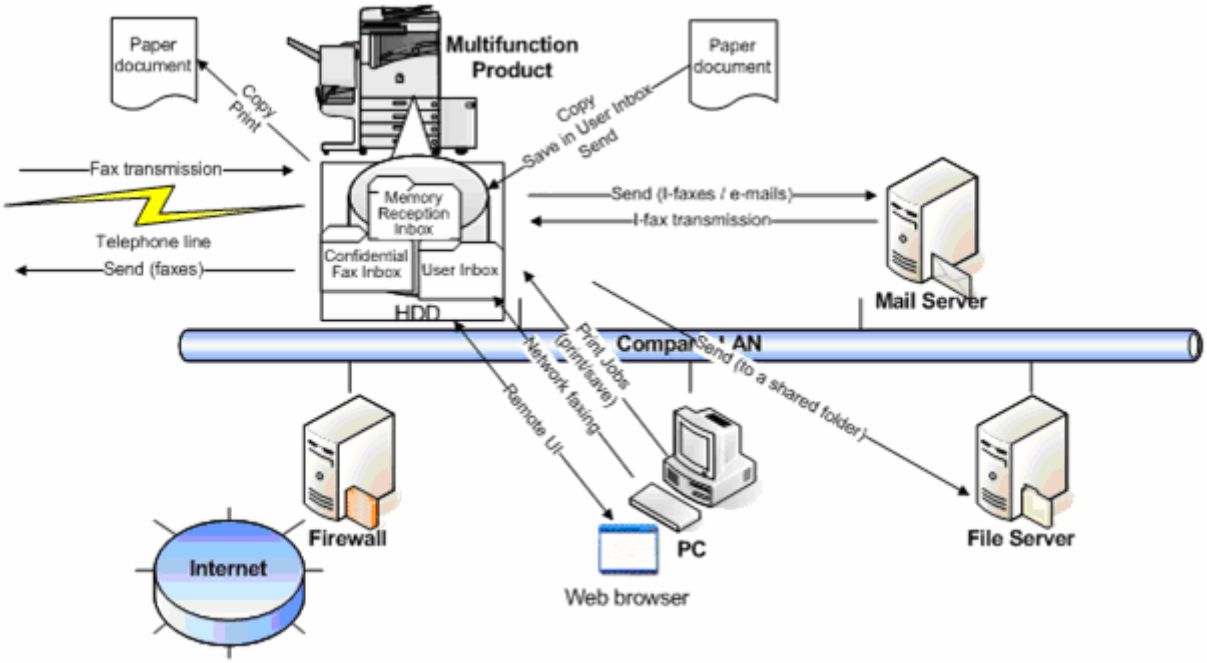


Figure 2-1: Assumed operational environment of Canon iR4570/iR3570/iR2870/iR2270 series

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.
  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.

  In-memory-received faxes/I-faxes stored in the Memory Reception Inbox can be extracted at a later time for printing or outbound transfer, whereas faxes/I-faxes received in Confidential Fax Inboxes are available for later printing only. In either case, user identification and authentication must precede any attempt to print or transmit them. In contrast, user identification and authentication is not required when receiving faxes/I-faxes, because in which case there is no need to read image data from the Memory Reception Inbox or 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.

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

  User Inbox-stored image data can be merged with other documents or overlaid with form images 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 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.

- **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.

- **MEAP**
  Optional MEAP applications can be installed on the multifunction product to add new functions.

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 respective functions described above and every inbox-stored image data created by the Fax Reception and User Inbox functions, as well as their complete removal upon deletion.

With these new security enhancements, efficient protection can be provided not only for inbox-stored image data, but also for any residual information left behind on the HDD by deleted temporary image data and/or inbox-stored image data.

2.3. 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)
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 (Int'l models)

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

Canon iR2870	
Canon iR2270	

For using the Print and Fax functions of the multifunction product, printer and fax drivers that are compatible with the multifunction product must be installed on the user's PC.

To operate the multifunction product using the Remote UI, the following software programs must be installed on the user's PC.

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

Table 2-3: 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)

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

2.4. Scope

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

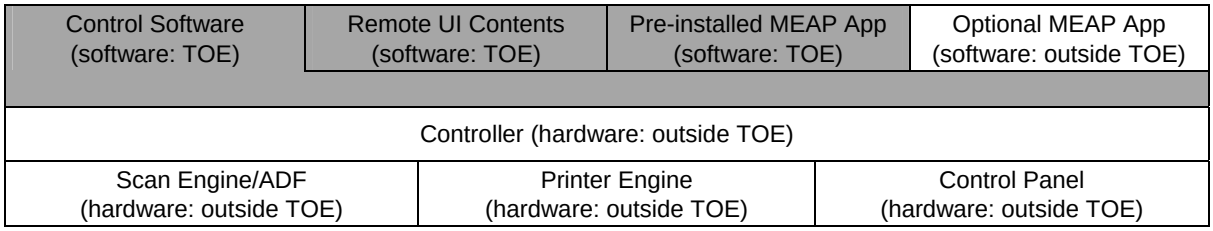
2.4.1. Physical Scope

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, the Web browser contents of the Remote UI, and the MEAP authentication application that comes standard with the multifunction product.
These are all pre-installed on the HDD of the multifunction product.

The hardware components of the multifunction product, including the controller and the HDD, are outside the scope of the TOE. Also outside the TOE scope 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 allows MEAP applications to run on top of it. The pre-installed MEAP authentication application is included in the scope of the TOE, but not any other optionally installed MEAP applications.

Figure 2-2 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-B2 V2).*

Figure 2-2: TOE (iR Security Kit-B2 V2) and hardware/software outside the TOE

2.4.2. Logical Scope

Since the TOE will replace the control software of the multifunction product, its logical scope includes the entire functions of the multifunction product identified in section 2.2, plus the following security functions.

- **HDD Data Encryption**
  A function to save image data to the HDD in an encrypted format.
- **HDD Data Complete Erase**
  A function to erase 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.

2.5. Users

This section describes the type of TOE users.

- **Regular user**
  A normal user of the multifunction product.
- **System Manager**
  A special user of the multifunction product who is responsible for device configuration and management tasks 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 inbox to prevent access by other regular users.

2.6. 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 any document saved to the HDD by the TOE, with the document management information not included.

- **Temporary image data**
  Temporary image data created through the use of the Copy, Print, Fax Reception and Send (Universal Send) functions of the multifunction product needs to be protected from unauthorized disclosure.
  Print data received from a remote PC for printing (spooled data) is also regarded as temporary image data.
- **Image data stored in password-protected inboxes**
  Image data sent to inboxes by the User Inbox and Fax Reception functions of the multifunction product needs to be protected from unauthorized disclosure. Image data stored in inboxes can be previewed using the Remote UI.

The following general data is related with documents and image data both, but is not considered to be an asset in this ST.

- 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. 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 password-protected using the Control Panel or the Remote UI.
The System Manager ID and the System Password shall already be set.

3.1.2. 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.

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_USE: **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.

3.3. Organizational Security Policies

This ST identifies no organizational security policies.

4. Security Objectives

This chapter describes the security objectives for the TOE, security objectives for the TOE and environment, and security objectives for 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_BOX: Identification and Authentication upon Inbox Access
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 readout of any inbox-stored image data, 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.

O.TRUSTED_PATH: Protection of Data En Route
The TOE shall protect data transmissions over the Remote UI communication path from eavesdropping.

4.2. Security Objectives for the Environment

OE.ADMIN: Trusted System Manager
The administrative personnel of each department using the multifunction product shall assign a responsible 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 sensitive image data in an inbox for protection shall set a password on the inbox using the Control Panel or the Remote UI.

The System Manager shall register a System Manager ID and a System Password.

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.

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.
Hierarchical components such as FIA_UID.1 and FIA_UID.2 may be indicated by appending a lowercase alphabet to the component name for easy comprehension.

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 method] 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: Triple 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 [selection: [assignment: one]] unsuccessful authentication attempts occur related to [assignment: inbox user authentication using the Control Panel or the Remote UI].

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 [selection: [assignment: one]] unsuccessful authentication attempts occur related to [assignment: System Manager authentication using the Control Panel or the Remote UI].

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.1a Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1a 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.1.2a 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.2b User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1b 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.1a Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1a 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.1.2a 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.2b User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1b 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_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: determine the behavior of] the functions [assignment: the Secure Communication (Remote UI)] to [assignment: the System Manager].

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

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.1.1b The TSF shall restrict the ability to [selection: modify] 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 user, key type (e.g. public, private, secret), validity period, and use (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 user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).	None
FCS_COP.1	There are no management activities foreseen for these components.	None

SFR	Actions to Manage	Addressed by
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: a) the management of the metric used to verify the secrets.	None
FIA_UAU.1a	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.2b	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.1a	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.2b	The following actions could be considered for the management functions in FMT: a) the management of the user identities.	FMT_MTD.1b
FMT_MOF.1	The following actions could be considered for the management functions in FMT Management: a) managing the group of roles that can interact with the functions in the TSF.	None
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	The following actions could be considered for the management functions in FMT Management: a) managing the group of users that are part of a role.	None
FPT_RVM.1	There are no management activities foreseen.	None
FTP_TRP.1	The following actions could be considered for the management functions in FMT:	FMT_MOF.1

SFR	Actions to Manage	Addressed by
	a) Configuring the actions that require trusted path, if supported.	

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.

5.1.1.6. Trusted Path/Channels

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FPT_TRP.1.1 The TSF shall provide a communication path between itself and [selection: remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FPT_TRP.1.2 The TSF shall permit [selection: remote users] to initiate communication via the trusted path.

FPT_TRP.1.3 The TSF shall require the use of the trusted path for [selection: [assignment: communication with the Remote UI]].

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 EAL3. All the assurance requirements consist of the requirements for EAL3 defined in CC Part 3.
Please note that although the ASE class is omitted in the table below, it defines “must” assurance requirements for evaluation of the TOE.

Table 5-2: EAL3 assurance requirements

Assurance Class	Assurance Components
ACM	ACM_CAP.3, ACM_SCP.1
ADO	ADO_DEL.1, ADO_IGS.1
ADV	ADV_FSP.1, ADV_HLD.2, ADV_RCR.1
AGD	AGD_ADM.1, AGD_USR.1
ALC	ACL_DVS.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_MSU.1, 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 ST places no security functional requirements on 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.1a, FIA_UID.1a, 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.2b, FIA_UID.2b, FIA_AFL.1b, FMT_SMR.1, FPT_RVM.1
SF.ADM_MANAGE	FIA_SOS.1b, FMT_MOF.1, FMT_MTD.1b, FMT_SMF.1, FPT_RVM.1
SF.SSL	FTP_TRP.1

SF.CRYPTO: 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.

SF.COMP_ERASE: HDD Data Complete Erase

When clearing temporary image data or inbox-stored image data from the HDD, the TOE overwrites the corresponding disk space with meaningless data so as to clear the image data completely.
The security function SF.COMP_ERASE is executed–

(1) when the Copy, Print, Fax Reception or Universal Send function is completed — in order to clear the temporary image data created on the HDD.
(2) when a document is deleted from an inbox — in order to clear the corresponding image data on the HDD.
(3) when the TOE is started — in order to clear any residual temporary image data discovered on the HDD.
(4) when the TOE is restarted, if the System Manager has turned on the “Initialize All Data/Settings” function of the multifunction product — in order to clear all temporary image data and inbox-stored image data on the HDD.

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.

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.

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 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.

SF.ADM_MANAGE: System Manager Management
The TOE assigns the following privileges to the System Manager only:

(1) 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.
(2) The System Manager can activate or deactivate the Secure Communication (Remote UI) function.

SF.SSL: 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.

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.3	iR Security Kit-B2 V2 Configuration Management Plan **(*)**
ACM_SCP.1	iR Security Kit-B2 V2 List of Configuration Items **(*)**
ADO_DEL.1	iR Security Kit-B2 V2 Delivery Procedures **(*)**
ADO_IGS.1	iR Security Kit-B2 V2 Installation Procedure (Japanese version) **(*)** iR Security Kit-B2 V2 Installation Procedure (English version)
ADV_FSP.1	iR Security Kit-B2 V2 Functional Specification **(*)**
ADV_HLD.2	iR Security Kit-B2 V2 High-level Design **(*)**
ADV_RCR.1	iR Security Kit-B2 V2 Analysis of Correspondence **(*)**
AGD_ADM.1	iR Security Kit-B2 V2 Reference Guide (Japanese version) **(*)** iR Security Kit-B2 V2 Reference Guide (English version)
AGD_USR.1	iR Security Kit-B2 V2 Reference Guide (Japanese version) **(*)** iR Security Kit-B2 V2 Reference Guide (English version)
ALC_DVS.1	IR Security Kit-B2 V2 Development Security Rules **(*)**
ATE_COV.2	iR Security Kit-B2 V2 Analysis of Test Coverage and Depth of Testing **(*)**
ATE_DPT.1	iR Security Kit-B2 V2 Analysis of Test Coverage and Depth of Testing **(*)**
ATE_FUN.1	iR Security Kit-B2 V2 Test Plan and Procedures **(*)** iR Security Kit-B2 V2 Test Results **(*)**
ATE_IND.2	TOE
AVA_MSU.1	iR Security Kit-B2 V2 Reference Guide (Japanese version) **(*)** iR Security Kit-B2 V2 Reference Guide (English version) iR Security Kit-B2 V2 Installation Procedure (Japanese version) **(*)** iR Security Kit-B2 V2 Installation Procedure (English version)
AVA_SOF.1	iR Security Kit-B2 V2 Strength of Function Analysis **(*)**
AVA_VLA.1	iR Security Kit-B2 V2 Vulnerability Analysis **(*)**

(*) These documents are available in Japanese only.

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

	T.HDD_ACCESS	T.UNAUTH_USE	T.NETWORK_TAP	A.ADMIN	A.PWD_MANAGE	A.PWD_SET	A.NETWORK
O.CRYPTO	X						
O.RESIDUAL	X						
O.AUTH_BOX		X					
O.TRUSTED_PATH			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 temporary image data and inbox-stored image data are always saved to the HDD in an encrypted format, thereby mitigating the threat T.HDD_ACCESS while 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 after protected assets are removed from the HDD.

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

T.UNAUTH_USE: O.AUTH_BOX 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.

T.NETWORK_TAP: O.TRUSTED_PATH ensures that the TOE protects data transmissions over the Remote UI communication path from eavesdropping.
This mitigates the threat of passwords and image data being disclosed by a malicious individual intercepting data transmissions over the Remote UI communication path.

8.1.3. Rationale for Assumptions

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 sensitive image data in an inbox for protection sets a password on the inbox using the Control Panel or the Remote UI; 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. 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_BOX	O.TRUSTED_PATH
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.1a			X	
FIA_UAU.2b			X	
FIA_UID.1a			X	
FIA_UID.2b			X	
FMT_MOF.1				X
FMT_MTD.1a			X	
FMT_MTD.1b			X	
FMT_SMF.1			X	
FMT_SMR.1			X	
FPT_RVM.1			X	
FTP_TRP.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_BOX: FIA_UID.1a and FIA_UAU.1a ensure that any attempt to read image data from a password-protected inbox is always preceded by inbox user identification and authentication.
FIA_UID.2b and FIA_UAU.2b ensure that any attempt to perform System Manager actions on any inbox is always preceded by System Manager identification and

authentication.

In case of success of the authentication, FMT_SMR.1 ensures that the user's role as an authorized inbox user or the System Manager is maintained.
In case of failure of the authentication via the Control Panel or the Remote UI, 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 a certain time period, helping reduce 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 an 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 an 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 and the System Manager Identification and Authentication functions from being bypassed.

Therefore, O.AUTH_BOX is achieved.

O.TRUSTED_PATH: FTP_TRP.1 ensures that all communications between the TOE and a user's Web browser are protected. FMT_MOF.1 ensures that the ability to activate and deactivate the Secure Communication (Remote UI) function is restricted to the System Manager only.
Therefore, O.TRUSTED_PATH is satisfied.

8.2.2. Rationale for Security Assurance Requirements

In this ST, the EAL3 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, and the multifunction product, the operating environment for the TOE, is a standard commercial product and intended for use in general offices. 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, EAL3 is an appropriate assurance level for the TOE, taking the time and cost of evaluation 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 two columns show the components that are dependent upon. Removed components are enclosed in parentheses.

Table 8-3: Security functional requirements dependencies

SFR	Dependencies Identified in CC	Dependencies Met in the ST
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1, FCS_CKM.4, (FMT_MSA.2)
FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1, FMT_MSA.2	FCS_CKM.1, (FMT_MSA.2)
FCS_COP.1	FDP_ITC.1 or FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4, (FMT_MSA.2)
FDP_RIP.1	–	–
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.1a
FIA_AFL.1b	FIA_UAU.1	FIA_UAU.2b
FIA_SOS.1a	–	–
FIA_SOS.1b	–	–
FIA_UAU.1a	FIA_UID.1	FIA_UID.1a
FIA_UAU.2b	FIA_UID.1	FIA_UID.2b
FIA_UID.1a	–	–
FIA_UID.2b	–	–
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1a	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1b	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	–	–
FMT_SMR.1	FIA_UID.1	FIA_UID.1a、FIA_UID.2b
FPT_RVM.1	–	–
FTP_TRP.1	–	–

As for the security assurance requirements, they are conformant to the EAL3 level and thus all dependencies are satisfied.

Rationale for Not Satisfying All Dependencies:

The reason why the dependencies of FCS_CKM.1, FCS_CKM.4 and FCS_COP.1 on FMT_MSA.2 are not satisfied is as follows:

In this TOE, only one common key is used for encryption of the HDD data and thus there are no key attributes, e.g. key type and expiration period, that need to be managed at the time of key generation. 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, and user identification and authentication data is managed by the security management (FMT) so that it can be modified or cleared.
These functions are mutually supportive, as the security management (FMT) functional requirements prevent impersonation of authorized inbox users.

Furthermore, FDP_RIP.1 ensures residual information protection and FCS_COP.1 ensures image data protection, which jointly ensure that all inbox-stored image data and temporary image data are protected 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 Identification and Authentication and the System Manager Identification and Authentication functions (FIA_UID.1a, FIA_UID.2b, FIA_UAU.1a, and FIA_UAU.2b) 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 enhances the non-bypassibility of these identification and authentication functions (FIA_UID.1a, FIA_UID.2b, FIA_UAU.1a, and FIA_UAU.2b), as FMT_MTD.1a and FMT_MTD.1b ensure that only limited users can modify and clear the identification and authentication data and FMT_MOF.1 ensures that only the System Manager can activate or deactivate the Secure Communication (Remote UI) function.

As such, FPT_RVM.1 supports the TOE in restricting the ability to read image data from a password-protected inbox to an 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, and the multifunction product, the operating environment for the TOE, is a standard commercial product and intended for use in general offices. 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.1a	FIA_UAU.2b	FIA_UID.1a	FIA_UID.2b	FMT_MOF.1	FMT_MTD.1a	FMT_MTD.1b	FMT_SMF.1	FMT_SMR..1	FPT_RVM.1	FTP_TRP.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		X	
SF.SSL																			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 redisplay of the Password Entry Screen if an incorrect inbox password is entered from the Control Panel or via the Remote UI.

FIA_AFL.1b:
This requirement is addressed by SF.ADM_AUTH, which imposes a 1-second wait time before the redisplay of the Password Entry Screen if an incorrect System Password is entered from the Control Panel or via the Remote UI.

FIA_SOS.1a:
This requirement is addressed by SF.BOX_MANAGE, which limits every 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.1a:
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 inbox-stored image data.

FIA_UAU.2b:
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 in the System Settings Screen if the Department ID Management function is not active.

FIA_UID.1a:
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 inbox-stored image data.

FIA_UID.2b:
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 in the System Settings Screen if the Department ID Management function is not active.

FMT_MOF.1:
This requirement is addressed by SF.ADM_MANAGE, which prohibits the activation/deactivation of

the Secure Communication (Remote UI) function without prior successful System Manager identification and authentication.

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.1a (the management of the authentication data by the associated user) is addressed by SF.BOX_MANAGE, which permits inbox users to manage only their own passwords for their own inboxes.
The management action of FIA_UAU.2b (the management of the authentication data by an administrator) and the management action of FIA_UID.2b (the management of the user identities) are addressed by SF.ADM_MANAGE, which permits only the System Manager to manage the System Manager ID and System Password.
The management action of FTP_TRP.1 (configuring the actions that require trusted path) is also addressed by SF.ADM_MANAGE, which permits only the System Manager to activate or deactivate the Secure Communication (Remote UI) function.
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.1a	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_MOF.1	a) managing the group of roles that can interact with the functions in the TSF. There is no action to manage because the role is automatically maintained after authentication.
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 user's role as an authorized inbox user until the Inbox Operation Screen is exited if the accessing user was identified and authenticated via the Control Panel; or until another inbox is manipulated or the Web browser is closed if the accessing user was identified and authenticated via the Remote UI.
This requirement is also addressed by SF.ADM_AUTH, which maintains the user's role as the System Manager until the System Management mode is exited if the accessing user was identified and authenticated via the Control Panel; or until the Web browser is closed, if the accessing user was 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.

FTP_TRP.1:

This requirement is addressed by SF.SSL, which secures the Remote UI communication path using SSL.

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 when they are created on the HDD, and are completely erased by SF.COMP_ERASE when they are deleted 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 an authorized inbox user or 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_AUTH are always invoked and cannot be bypassed.

8.3.4. Rationale for Assurance Measures

Table 8-5 shows the mapping of assurance measures to EAL3 assurance components.

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

Assurance Measures	ACM_CAP.3	ACM_SCP.1	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.2	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ALC_DVS.1	ATE_COV.2	ATE_DPT.1	ATE_FUN.1	ATE_IND.2	AVA_MSU.1	AVA_SOF.1	AVA_VLA.1
iR Security Kit-B2 V2 Configuration Management Plan **(*)**	X																
iR Security Kit-B2 V2 List of Configuration Items **(*)**		X															
iR Security Kit-B2 V2 Delivery Procedures **(*)**			X														
iR Security Kit-B2 V2 Installation Procedure (Japanese) **(*)** iR Security Kit-B2 V2 Installation Procedure (English)				X											X		
iR Security Kit-B2 V2 Functional Specification **(*)**					X												
iR Security Kit-B2 V2 High-level Design **(*)**						X											
iR Security Kit-B2 V2 Analysis of Correspondence **(*)**							X										
iR Security Kit-B2 V2 Reference Guide (Japanese) **(*)** iR Security Kit-B2 V2 Reference Guide (English)								X	X						X		
iR Security Kit-B2 V2 Development Security Rules **(*)**										X							
iR Security Kit-B2 V2 Test Plan and Procedures **(*)**													X				
iR Security Kit-B2 V2											X	X					

Analysis of Test Coverage and Depth of Testing **(*)**																
iR Security Kit-B2 V2 Test Results **(*)**												X				
TOE													X			
iR Security Kit-B2 V2 Strength of Function Analysis **(*)**															X	
iR Security Kit-B2 V2 Vulnerability Analysis **(*)**																X

(*) These documents are available in Japanese only.

ACM_CAP.3:

The documents "iR Security Kit-B2 V2 Configuration Management Plan" and "iR Security Kit-B2 V2 List of Configuration Items" describe the configuration management of the TOE.

ACM_SCP.1:

The document "iR Security Kit-B2 V2 List of Configuration Items" describes the configuration management of the TOE.

ADO_DEL.1:

The document "iR Security Kit-B2 V2 Delivery Procedures" ensures the secure transfer of the TOE to a user's site.

ADO_IGS.1:

The documents "iR Security Kit-B2 V2 Installation Procedure" (Japanese) and "iR Security Kit-B2 V2 Installation Procedure" (English) ensure secure installation of the TOE.

ADV_FSP.1:

The document "iR Security Kit-B2 V2 Functional Specification" provides the functional specification of the TOE.

ADV_HLD.2:

The document "iR Security Kit-B2 V2 High-level Design" provides the high-level design of the TOE.

ADV_RCR.1:

The document "iR Security Kit-B2 V2 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 V2 Reference Guide" (Japanese) and "iR Security Kit-B2 V2 Reference Guide" (English) provide the administrator user guidance.

AGD_USR.1:

The documents "iR Security Kit-B2 V2 Reference Guide" (Japanese) and "iR Security Kit-B2 V2 Reference Guide" (English) provide the regular user guidance.

ALC_DVS.1:

The document "iR Security Kit-B2 V2 Development Security Rules" maintains security in the TOE development environment.

ATE_COV.2:

The document "iR Security Kit-B2 V2 Analysis of Test Coverage and Depth of Testing" provides the

analysis of the test coverage.

ATE_DPT.1:

The document “iR Security Kit-B2 V2 Analysis of Test Coverage and Depth of Testing” provides the analysis of the depth of testing.

ATE_FUN.1:

The documents “iR Security Kit-B2 V2 Test Plan and Procedures” and “iR Security Kit-B2 V2 Test Results” provide the developer test plans and test results.

ATE_IND.2:

The TOE is provided.

AVA_MSU.1:

The documents “iR Security Kit-B2 V2 Reference Guide” (Japanese), “iR Security Kit-B2 V2 Reference Guide” (English), “iR Security Kit-B2 V2 Installation Procedure” (Japanese), and “iR Security Kit-B2 V2 Installation Procedure” (English) prevent misuse of the TOE.

AVA_SOF.1:

The document “iR Security Kit-B2 V2 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 V2 Vulnerability Analysis” describes the developer vulnerability analysis of the TOE.