Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2

Security Target

Version 1.01
Aug 08, 2008

Canon Inc.

This document is a translation of the evaluated and certified security target written in Japanese

Revision History

Version	Date	Changes Made
Ver.1.00	May 13, 2008	Original.
Ver.1.01	Aug 08, 2008	Made changes to the description of the TOE Security function.

Table of Contents

Trademark Notice

- Canon, the Canon logo, imageRUNNER, MEAP, and the MEAP logo are trademarks of Canon Inc.
- Microsoft, Windows, Windows XP, and Active Directory are registered trademarks of Microsoft Corporation in the United States.
- Macintosh, Mac OS, and QuickTime are trademarks of Apple Computer Inc., registered in the United States.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S.
- 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 iR3225/iR3230/iR3235/iR3245Series HDD Data Erase Kit-B2 Security Target
Date:	Aug 08, 2008
ST Version:	Version 1.01
Authors:	Canon Inc.
TOE:	Canon iR3225/iR3230/iR3235/iR3245 Series HDD Data Erase Kit-B2 Version 1.00
Keywords:	Canon, imageRUNNER, iR, iR3225/iR3230/iR3235/iR3245, 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, Version 2.3 Interpretations-0512 Japanese version of these documents, which are published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme, are referenced.
Assurance Level:	EAL3

1.2. ST Overview

This document is a Security Target (ST) that defines the security specifications for the HDD Data Erase Kit-B2 software program that adds security enhancements to the Canon multifunction product series iR3225/iR3230/iR3235/iR3245 (hereafter referred to as the “Multifunction Product” except where otherwise indicated).

The TOE is available to users as an optional product called “HDD Data Erase Kit-B2”. Users contact their service providers to have the TOE installed on the built-in hard disk drives of their Multifunction Products to replace the system software, so that they can benefit from the enhanced security.

The TOE offers the security functions listed below in order to prevent reuse of any residual information of temporary image data in the Multifunction Product.

- HDD Data Complete Erase
- 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 – 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 and I-faxes for later printing or transmission.
Controller	A platform for the TOE to run on; a hardware device with a CPU and memory.
Department ID	A unique ID assigned to each multifunction product user, who can be an individual or a department. A multifunction product running with the Department ID Management function enabled will require any user be identified and authenticated before operating the multifunction product. The System Manager refers to a user who is assigned a special department ID called System Manager ID.
Document	User data handled within a multifunction product, consisting of management information and image data.
Form image	Image data saved to a multifunction product for use in overlay printing.
HDD	The hard disk drive of a multifunction product. It is the storage place for the TOE and its assets.
I-fax	An Internet faxing service that allows transmission and reception of faxes using the Internet instead of telephone lines.
Image data	Image data that is created on the HDD of a multifunction product through document scanning, printing, or fax reception.
In-memory reception	The capability that automatically saves received faxes/I-faxes to the Memory Reception Inbox with no printouts.
Mail Box	A function of a multifunction product that offers storage space for scanned documents, print jobs, and received faxes. Three types of storage inboxes are provided: User Inbox, Confidential Fax Inbox, and Memory Reception Inbox.
MEAP	Short for Multifunctional Embedded Application Platform; a platform that allows software to run embedded in a multifunction product. It allows running “MEAP applications”, special software programs developed in the Java language for embedded use in multifunction products.
MEAP application	An application developed in the Java language for embedded use in multifunction products. MEAP applications can be used in conjunction with multifunction product functions, e.g., printing, copying, faxing, and scanning, to customize the device user interface, simplify the document flow, and automate routine tasks, and so on.
MEAP Authentication Application	A MEAP application that is capable of authenticating regular users of a multifunction product, integration with Active Directory, etc.
Memory Reception Inbox	An inbox that stores “in-memory-received” faxes and I-faxes for later printing.
Multifunction product	A digital copier with the combined functionality of copying, faxing, printing, and document transmission (Universal Send). Multifunction products are usually equipped with a large-capacity HDD to perform these functions, allowing the TOE to reside and run on it.
Operation Panel	A hardware component of a multifunction product, comprising operation keys and a touch panel display, that is used for operating the multifunction product.
Printer Engine	A hardware component of a multifunction product that prints image data on paper.

Remote UI	An interface that allows remote access to a multifunction product from a desktop Web browser for viewing device status information, manipulating jobs, configuring Mail Box settings, customizing device settings, and so on.
Scan Engine/ADF	A hardware component of a multifunction product that scans paper documents into image data for storage in the multifunction product.
System Manager	The administrator of a multifunction product that is responsible for device configuration and management, as well as possibly management of inboxes on behalf of their users. A multifunction product identifies a user who logs in with a pre-registered System Manager ID as System Manager.
System Management mode	Operational mode of a multifunction product in which System Manager privileges are maintained on the multifunction product. Any operations specified in this mode are executed as System Manager actions. To enter this mode, a valid System Manager ID and System Password must be provided. System Management mode is exited when the ID key is pressed down on the multifunction product's Operation Panel.
User Inbox	An inbox that stores documents scanned by regular users as well as 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 roles and the assets to be protected by the TOE.

2.1. Product Type

The TOE is optional software to add security enhancements to the Canon multifunction product series iR3225/iR3230/iR3235/iR3245.
The system software of the Multifunction Product is replaced by the TOE when the TOE is installed.

2.2. Overview

The TOE is optional software to add security enhancements to the Multifunction Product, and is provided to users as an optional product named “HDD Data Erase Kit-B2”.
Users contact their service providers to have the TOE installed on the built-in HDDs of their Multifunction Products to replace the system software, so that they can benefit from the enhanced security.

The Canon iR3225/iR3230/iR3235/iR3245 series is a digital copier that offers a variety of functions including Copy, Send (Universal Send), Fax Reception, Mail Box, Print, and so on. It is also equipped with a large-capacity HDD and stores image data created during copying, printing, and other document handling operations temporarily on the HDD. In most standard multifunction products, such temporary image data is deleted only logically after use, i.e., upon completion of copying or printing, and residual information of deleted image data is not erased at all, being left exposed to the risk of reuse.
The TOE is used for protecting any residual information of temporary image data from being reused.

The Multifunction Product is intended for general use in office and business professional environments. Figure 2-1 depicts its assumed operating environment. It should be noted however that this is based on a use case where the Multifunction Product is fully-optioned to meet user needs and thus may not be applicable where required functions are limited.
There could also be cases where the Multifunction Product is used as a standalone copier or a mere fax machine connected only to a telephone line.

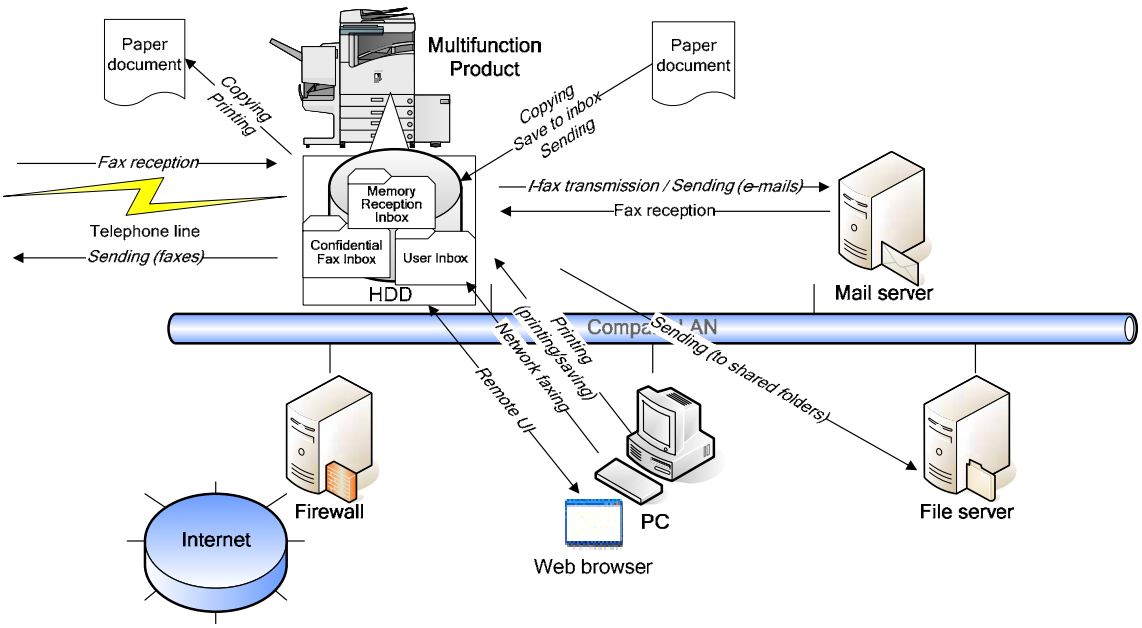


Figure 2-1: Assumed operating environment for the Canon iR3225/iR3230/iR3235/iR3245 series

As depicted in Figure 2-1, the Multifunction Product has the following functions:

- **Copy**
  A function that creates copies of paper documents by scanning and printing.
  Temporary image data is created on the HDD at the time of document scanning.
- **Fax Reception**
  A function that automatically prints or forwards faxes/I-faxes received.
  Temporary image data is created on the HDD at the time of fax reception.
- **User Inbox**
  A function that automatically saves scanned documents and documents received from external PCs for User Inbox storage to their destination inboxes in the form of image data.
  Image data stored in a User Inbox can be edited, e.g., to be merged with other documents or overlaid with form images, before printing.
- **Print**
  A function that turns the Multifunction Product into a network printer for printing documents received from external PCs. Temporary image data is created on the HDD at the time of document printing.
- **Universal Send (document transfer)**
  A function that allows faxing scanned documents and documents stored in User Inboxes and the Memory Reception Inbox, or sending them as TIFF or PDF files to outside e-mail addresses or shared folders on external PCs. This function also allows network faxing from a user's PC using a fax driver.
  Temporary image data is created on the HDD at the time of document transmission.
- **Memory Media Function**
  A function that takes a scanned document image (ScanToMemory) or a document stored in the inbox (BoxToMemory), converts to a format such as PDF, and stores on the memory media inserted by the user. This function also prints documents stored in the memory media. Temporary image data is created in the HDD, when scanning or printing.
- **Remote UI**
  The Multifunction Product can be operated not only via the Operation Panel but also via the Remote UI software. The Remote UI allows remote PC users to access the Multifunction Product through a Web browser and a network connection, enabling them to view device status information, manipulate jobs, perform inbox management operations, configure device settings, and so on.
- **MEAP**
  Optional MEAP applications can be installed to add new functions to the Multifunction Product.

By installing the TOE on the Multifunction Product, new functionality is added that will not only logically delete temporary image data created through the use of the abovementioned device functions, but will also completely erase any residual information of such temporary image data.
Accordingly, these functions jointly make it possible to protect any residual information of temporary image data on the HDD of the Multifunction Product from unauthorized reuse.

2.3. Operating Environment

The TOE can be put into action by installing it on the Multifunction Product.
Also, in order to be able to perform the following operations using the Multifunction Product, additional servers and software will be required.

Operating the Multifunction Product via the Remote UI requires the installation and use of a Web browser on the user's PC.

Desktop printing or faxing requires the installation and use of an appropriate printer driver or fax driver on the user's PC.

Sending I-faxes or documents using the Universal Send function requires a mail server, an FTP server, and a file server.

The PC environment used for testing the TOE is as follows:

- Operating system: Microsoft Windows XP Professional SP2
- Web browser: Microsoft Internet Explorer Version 6.0 SP2

2.4. Scope

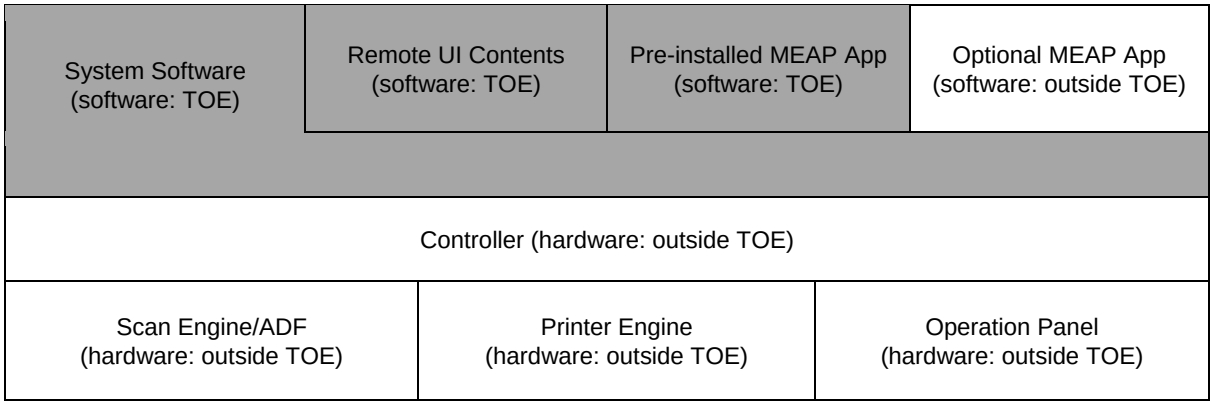
The physical scope and logical scope of the TOE are as described below.

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. Note that the physical scope of the TOE includes the MEAP Authentication Application that comes pre-installed on the Multifunction Product's built-in HDD, 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 region indicates the scope of the TOE.*

Figure 2-2: TOE (HDD Data Erase Kit-B2) and hardware/software outside the TOE

2.4.2. Logical Scope

Since the TOE will replace the system 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 Complete Erase**
  A function that erases residual information of temporary image data on the HDD upon the deletion of temporary image data by overwriting the corresponding disk space with meaningless data.
- **System Manager Identification and Authentication**
  A function that identifies and authenticates the claimed identity of an authorized System Manager via the System Manager ID and System Password, prior to permitting entry into System Management mode.
- **System Manager Management**

A function that allows registration of a System Manager ID and System Password as well as the various settings of the HDD Data Complete Erase function.

2.5. Users

This section describes the types of TOE users.

- **Regular user**
  An ordinary user of the Multifunction Product.
- **System Manager**
  A special user of the Multifunction Product who is responsible for device configuration and management, and authorized to use the System Manager Management function.

2.6. Assets

The TOE assets are identified as follows in this ST.

- **Residual information of temporary image data**
  Temporary image data refers to any image data that is temporarily created by document copying, document printing, fax reception, or document transmission (Universal Send). Print data received from remote PCs for printing (spooled data) is also regarded as temporary image data.

  In most standard multifunction products, such temporary image data is deleted only logically after use, i.e., upon completion of copying or printing, and residual information of deleted image data is not erased at all, being left exposed to the risk of reuse.

  The assets of the TOE are any residual information of temporary image data that is typically left undeleted in most standard multifunction products.

3. TOE Security Environment

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

3.1. Assumptions

The assumptions in this ST are described below.

3.1.1. Personnel Assumptions

A.ADMIN: Trusted System Manager
The System Manager shall be trusted not to abuse his privileges.

A.ADMIN_PWD: System Password
The System Manager shall set a non-guessable 7-digit number as the System Password.

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 not accessible 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 remove the HDD of the Multifunction Product and reuse residual information of temporary image data by directly accessing the HDD using disk editor tools, etc.

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 security objectives for the environment.

4.1. Security Objectives for the TOE

O.RESIDUAL: Residual Data Protection for Image Data
The TOE shall completely erase any residual information of temporary image data upon the deletion of temporary image data.

O.ADMIN_AUTH: System Manager Identification and Authentication
The TOE shall identify and authenticate the claimed identity of an authorized System Manager in order to restrict the System Manager Management function to the System Manager only.

4.2. Security Objectives for the Environment

OE.ADMIN: Trusted System Manager
The administrative personnel of an organization that uses the Multifunction Product shall assign a responsible individual as System Manager.

OE.ADMIN_PWD: System Password
The System Manager shall set a non-guessable 7-digit number as the 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 and security requirements for the IT environment.
All requirements were drawn from the functional components defined in CC Part 2 and operated using the following conventions: Selections and assignments are denoted by underlined text, refinements by parenthesized italicized text, and iterations by lowercase alphabets following the component name.

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.

5.1.1.1. User Data Protection

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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: temporary image data].

5.1.1.2. Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

FIA_AFL.1.2 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].

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 Timing of identification

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.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

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.

5.1.1.3. Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

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

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: disable, enable, modify] the functions [assignment: the HDD Data Complete Erase function] to [assignment: the System Manager].

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

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

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

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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].

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

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.	FMT_MOF.1
FIA_AFL.1	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_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.1
FIA_UID.2	The following actions could be considered for the management functions in FMT: a) the management of the user identities.	FMT_MTD.1
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.1	The following actions could be considered for the management functions	None

	in FMT Management: a) managing the group of roles that can interact with the TSF data.	
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

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: System Manager].

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

5.1.1.4. Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

5.1.2. Minimum Strength of Function Level

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

The TOE uses a probabilistic or permutational mechanism to identify and authenticate the System Manager, and hence claims a strength of function that can counter low-level attacks for the security functional requirements FIA_UAU.2 and FIA_UID.2.

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.

Table 5-2: EAL3 assurance requirements

Assurance Class	Assurance Components
ASE	ASE.1
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

There are no security functional requirements that the IT environment needs to satisfy.

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 authentication mechanism in the security function SF.ADM_AUTH is the only probabilistic or permutational mechanism in this ST, and the strength of this function is SOF-basic.

Table 6-1: TOE security functions and functional components

Security Function	Functional Component
SF.COMP_ERASE	FDP_RIP.1
SF.ADM_AUTH	FIA_UAU.2, FIA_UID.2, FIA_AFL.1, FMT_SMR.1, FPT_RVM.1
SF.ADM_MANAGE	FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

SF.COMP_ERASE: HDD Data Complete Erase
When temporary image data is deleted on the HDD, the TOE overwrites the corresponding disk space with meaningless data in order to ensure that no residual information remains.
The security function SF.COMP_ERASE runs at the following times:

(1) Upon completion of a copying, printing, fax reception, or sending (Universal Send) operation, any residual information of temporary image data created on the HDD is completely erased.

(2) Upon startup of the TOE: any residual information of previously deleted temporary image data detected on the HDD is completely erased.

(3) Upon restart of the TOE, due to the System Manager having executed the Initialize All Data/Settings function of the Multifunction Product: any residual information of previously deleted temporary image data detected on the HDD is completely erased.

SF.ADM_AUTH: System Manager Identification and Authentication
The TOE requires any user accessing the System Manager Management function to enter a System Manager ID and System Password in order to restrict the System Manager Management function to the System Manager only.

The TOE identifies and authenticates the accessing user as System Manager only if the entered System Manager ID and System Password both match the registered ones.

If the entered System Manager ID or System Password does not match the registered one, the TOE does not identify nor authenticate the accessing user as System Manager and imposes a 1-second wait time before allowing a retry.

SF.ADM_MANAGE: System Manager Management
The TOE grants the following privileges only to the authorized System Manager role:

(1) The System Manager can modify or delete the System Manager ID and System Password.

(2) The following settings can be made for the HDD Data Complete Erase function.

a) Enabling or disabling the function itself

b) Changing the Erase mode

① Single write operation of 0 data

② Single write operation of random data

③ Triple write operation of random data

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.

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

Assurance Component	Assurance Measure
ASE.1	This ST.
ACM_CAP.3	HDD Data Erase Kit-B2 Configuration Management Plan
ACM_SCP.1	HDD Data Erase Kit-B2 List of Configuration Items
ADO_DEL.1	HDD Data Erase Kit-B2 Delivery Procedures
ADO_IGS.1	HDD Data Erase Kit-B2 Installation Procedure
ADV_FSP.1	HDD Data Erase Kit-B2 Functional Specification
ADV_HLD.2	HDD Data Erase Kit-B2 High-level Design
ADV_RCR.1	HDD Data Erase Kit-B2 Analysis of Correspondence
AGD_ADM.1 AGD_USR.1	HDD Data Erase Kit-B2 Reference Guide iR Series User Documentation
ALC_DVS.1	HDD Data Erase Kit-B2 Development Security Rules
ATE_COV.2	HDD Data Erase Kit-B2 Analysis of Test Coverage and Depth of Testing
ATE_DPT.1	HDD Data Erase Kit-B2 Analysis of Test Coverage and Depth of Testing
ATE_FUN.1	HDD Data Erase Kit-B2 Test Plan and Procedures HDD Data Erase Kit-B2 Test Results
ATE_IND.2	TOE
AVA_MSU.1	HDD Data Erase Kit-B2 Reference Guide iR Series User Documentation HDD Data Erase Kit-B2 Installation Procedure
AVA_SOF.1	HDD Data Erase Kit-B2 Strength of Function Analysis
AVA_VLA.1	HDD Data Erase Kit-B2 Vulnerability Analysis

The “iR Series User Documentation” consists of the following guides:

- imageRUNNER 3225/3230/3235/3245 Reference Guide
- imageRUNNER 3225/3230/3235/3245 Copying and Mail Box Guide
- imageRUNNER 3225/3230/3235/3245 Sending and Facsimile Guide
- imageRUNNER 3225/3230/3235/3245 Remote UI Guide
- imageRUNNER 3225/3230/3235/3245 Network Guide
- MEAP SMS Administrator Guide

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	A.ADMIN	A.ADMIN_PWD	A.NETWORK
O.RESIDUAL	X			
O.ADMIN_AUTH	X			
OE.ADMIN		X		
OE.ADMIN_PWD			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.RESIDUAL ensures that any residual information of deleted temporary image data, which is a TOE asset, is completely erased in order to prevent its reuse, thereby removing the threat T.HDD_ACCESS once the asset has been completely wiped out.

Furthermore, any intentional attempt to deactivate the option that protects residual information of temporary image data via an unauthorized operation of the System Manager Management function must be prevented. Likewise, any unintentional attempt to activate this option that has been deliberately deactivated by the System Manager must also be prevented. To achieve these objectives, O.ADMIN_AUTH ensures that the System Manager Management function, which includes the ability to activate or deactivate the temporary image data residual information protection option, is restricted only to the authorized System Manager role.

8.1.3. Rationale for Assumptions

A.ADMIN

OE.ADMIN ensures that the administrative personnel of an organization that uses the Multifunction Product assigns a responsible individual as System Manager. Therefore, A.ADMIN is satisfied.

A.ADMIN_PWD

OE.ADMIN_PWD ensures that the System Manager uses a non-guessable 7-digit number as the

System Password. Therefore, A.PWD_MANAGE 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.RESIDUAL	O.ADMIN_AUTH
FDP_RIP.1	X	
FIA_AFL.1		X
FIA_UAU.2		X
FIA_UID.2		X
FMT_MOF.1		X
FMT_MTD.1		X
FMT_SMF.1		X
FMT_SMR.1		X
FPT_RVM.1		X

O.RESIDUAL

FDP_RIP.1 requires any residual information of temporary image data be completely erased to prevent its reuse. Therefore, O.RESIDUAL is satisfied.

O.ADMIN_AUTH

FIA_UID.2 and FIA_UAU.2 require that any operation of the System Manager Management function be preceded by the System Manager Identification and Authentication function.
In case of successful authentication, FMT_SMR.1 maintains the user's role as System Manager.
In case of unsuccessful authentication, FIA_AFL.1 imposes a 1-second wait time before allowing the next authentication attempt, in order to unfailingly maintain the maximum allowed number of authentication attempts in a certain time period, thereby not only helping reduce the chances of successful attacks on these identification and authentication functions, but also ensuring effective operation of these functions. Additionally, FPT_RVM.1 guarantees the non-bypassability of the System Manager Identification and Authentication function.

These functional requirements in combination ensure that only the authorized System Manager role can use the System Manager Management function.

FMT_MTD.1 and FMT_SMF.1 restrict the ability to modify or delete the System Manager ID and System Password only to the authorized System Manager role.

Furthermore, FMT_MOF.1 and FMT_SMF.1 restrict the ability to make the various settings of the HDD Data Complete Erase function only to the authorized System Manager role.

These functional requirements in combination prevent impersonation of an authorized System Manager.

Therefore, O.AUTH_BOX is achieved.

8.2.2. Rationale for Security Assurance Requirements

The EAL3 assurance package has been 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, being the TOE platform, is a standard commercial product intended for use in general offices where A.NETWORK ensures that the TOE is secure from direct attacks from outside networks such as the Internet.

Therefore, it is required to provide assurance of security against low-level attackers, and 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 second 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

TOE/IT Environment	SFR	Dependencies identified in CC	Dependencies met in the ST
TOE	FDP_RIP.1	-	-
	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
	FIA_UAU.2	FIA_UID.1	FIA_UID.2
	FIA_UID.2	-	-
	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
	FMT_SMF.1	-	-
	FMT_SMR.1	FIA_UID.1	FIA_UID.2
	FPT_RVM.1	-	-
IT environment	-	N/A	N/A

Table 8-3 shows that the security requirements listed under the **Dependencies met in the ST** column satisfy those listed under the **Dependencies identified in CC** column.
As for the security assurance requirements, they are conformant to the EAL3 level and thus all dependencies are satisfied.

8.2.4. Mutually Supportive Security Requirements

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

The TOE counters the threat of reuse of residual information of temporary image data using the HDD Data Complete Erase function that satisfies FDP_RIP.1.

As for the non-bypassability, the System Manager Identification and Authentication function of the TOE, as required by FIA_UID.2 and FIA_UAU.2, prevents attackers from misuse of the System Manager Management function, whereby FPT_RVM.1 can ensure that the System Manager Identification and Authentication function is never bypassed.

FMT_MTD.1 restricts users that can modify or delete System Manager ID, Identification and Authentication Data. Furthermore, FMT_MOF.1 restricts the ability to make the various settings of the HDD Data Complete Erase function only to the authorized System Manager role.

Therefore, these respective functional requirements do not conflict nor contradict with each other and are mutually supportive.

8.2.5. Rationale for Minimum Strength of Function Level

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

The TOE is a software program that controls the entire functionality of the Multifunction Product, and the Multifunction Product, being the TOE platform, is a standard commercial product intended for use in general offices. For this reason, the objective O.ADMIN_AUTH is needed to counter the threat that a low-level attacker may impersonate an authorized System Manager to perform unauthorized operations. This justifies the assumption of low-level attacks as an appropriate strength of function rationale and hence the minimum strength of function required for the TOE is SOF-basic.

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

	FDP_RIP.1	FIA_AFL.1	FIA_UAU.2	FIA_UID.2	FMT_MOF.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1
SF.COMP_ERASE	X								
SF.ADM_AUTH		X	X	X				X	X
SF.ADM_MANAGE					X	X	X		

FDP_RIP.1

This requirement is fulfilled by SF.COMP_ERASE, which performs a complete erase of any residual information of every temporary image data.

FIA_AFL.1

This requirement is fulfilled by SF.ADM_AUTH, which imposes a 1-second wait time before a redisplay of the password entry screen in case of a mismatch between the given password string and the registered System Password.

FIA_UAU.2

This requirement is fulfilled by SF.ADM_AUTH, which authenticates the claimed identity of an authorized System Manager with the System Password in the initial screen that appears when the Department ID Management function is active, or in the system management configuration screen that appears when the Department ID Management function is not active.

FIA_UID.2

This requirement is fulfilled by SF.ADM_AUTH, which identifies the claimed identity of an authorized System Manager with the correct System Manager ID in the initial screen that appears when the Department ID Management function is active, or in the system management configuration screen that appears when the Department ID Management function is not active.

FMT_MOF.1

This requirement is fulfilled by SF.ADM_MANAGE, which restricts the ability to activate or deactivate, and change the Erase mode of the HDD Data Complete Erase function, only to the authorized System Manager role.

FMT_MTD.1

This requirement is fulfilled by SF.ADM_MANAGE, which restricts the ability to modify or delete the System Manager ID and System Password only to the authorized System Manager role.

FMT_SMF.1

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 fulfilled by SF.ADM_MANAGE, which restricts the ability to manage the System Manager ID and System Password only to the authorized System Manager role.
SF.ADM_MANAGE further ensures that the ability to make the various settings of the HDD Data Complete Erase function is restricted only to the authorized System Manager role.

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.

FIA_AFL.1	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.
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.1	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 fulfilled by SF.ADM_AUTH, which maintains the user's role as System Manager until System Management mode is exited if the user has identified and authenticated himself via the Operation Panel, or until the Web browser is closed if the user has identified and authenticated himself via the Remote UI.

FPT_RVM.1

This requirement is fulfilled by SF.ADM_AUTH. For details, see Section 8.3.3.

8.3.2. Rationale for Strength of Function

The strength of function level of SF.ADM_AUTH, which is a probabilistic or permutational mechanism in the TOE, is SOF-basic. The minimum strength of function level of the TOE is also SOF-basic.
As these strength of function levels do not conflict, the strength of function claim of SOF-basic for SF.ADM_AUTH is reasonable.

8.3.3. Rationale for Combination of Security Functions

In order to protect the assets from unauthorized direct HDD access, SF.COMP_ERASE performs a complete erase of residual information of temporary image data upon the deletion of temporary image data.

Also, although SF.ADM_MANAGE allows making the various settings of the HDD Data Complete Erase function as well as modifying or deleting the System Manager ID and System Password, access to these functions is restricted to the authorized System Manager role by SF.ADM_AUTH.
Hence, SF.ADM_AUTH cannot be bypassed in order for SF.ADM_MANAGE to run.

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	ASE.1	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
This ST	X																	
HDD Data Erase Kit-B2 Configuration Management Plan		X																
HDD Data Erase Kit-B2 List of Configuration Items			X															
HDD Data Erase Kit-B2 Delivery Procedures				X														
HDD Data Erase Kit-B2 Installation Procedure					X											X		
HDD Data Erase Kit-B2 Functional Specification						X												
HDD Data Erase Kit-B2 High-level Design							X											
HDD Data Erase Kit-B2 Analysis of Correspondence								X										
HDD Data Erase Kit-B2 Reference Guide, and iR Series User Documentation									X	X						X		
HDD Data Erase Kit-B2 Development Security Rules											X							
HDD Data Erase Kit-B2 Test Plan and Procedures														X				
HDD Data Erase Kit-B2 Analysis of Test Coverage and Depth of Testing												X	X					
HDD Data Erase Kit-B2 Test Results														X				
TOE															X			
HDD Data Erase Kit-B2 Strength of Function Analysis																	X	
HDD Data Erase Kit-B2 Vulnerability Analysis																		X

ASE.1

This ST provides necessary information for ASE.

ACM_CAP.3

The document “HDD Data Erase Kit-B2 Configuration Management Plan” describes the configuration management of the TOE.

ACM_SCP.1

The document “HDD Data Erase Kit-B2 List of Configuration Items” describes the configuration management of the TOE.

ADO_DEL.1

The document “HDD Data Erase Kit-B2 Delivery Procedures” ensures the secure transfer of the TOE to a user’s site.

ADO_IGS.1

The document “HDD Data Erase Kit-B2 Installation Procedure” ensures secure installation of the TOE.

ADV_FSP.1

The document “HDD Data Erase Kit-B2 Functional Specification” provides the functional specification of the TOE.

ADV_HLD.2

The document “HDD Data Erase Kit-B2 High-level Design” provides the high-level design of the TOE.

ADV_RCR.1

The document “HDD Data Erase 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 document “HDD Data Erase Kit-B2 Reference Guide” and “iR Series User Documentation” provide the administrator user guidance.

AGD_USR.1

The document “HDD Data Erase Kit-B2 Reference Guide” and “iR Series User Documentation” provide the regular user guidance.

ALC_DVS.1

The document “HDD Data Erase Kit-B2 Development Security Rules” maintains security in the TOE development environment.

ATE_COV.2

The document “HDD Data Erase Kit-B2 Analysis of Test Coverage and Depth of Testing” provides the analysis of the test coverage.

ATE_DPT.1

The document “HDD Data Erase Kit-B2 Analysis of Test Coverage and Depth of Testing” provides the analysis of the depth of testing.

ATE_FUN.1

The documents “HDD Data Erase Kit-B2 Test Plan and Procedures” and “HDD Data Erase Kit-B2 Test Results” provide the developer test plans and test results.

ATE_IND.2

The TOE will be provided.

AVA_MSU.1

The documents “HDD Data Erase Kit-B2 Reference Guide”, “iR Series User Documentation”, and “HDD Data Erase Kit-B2 Installation Procedure” prevent misuse of the TOE.

AVA_SOF.1

The document “HDD Data Erase Kit-B2 Strength of Function Analysis” provides a rationale for the

strength of function claim for the probabilistic or permutational mechanisms in the TOE.

AVA_VLA.1

The document “HDD Data Erase Kit-B2 Vulnerability Analysis” describes the developer vulnerability analysis of the TOE.