RICOH

Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B Security Target
08 May, 2007
Document No. 2007-001

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite N
Columbia, MD 21046-2587

Phone: 301-498-0150

Fax: 301-498-0855

The information in this document is subject to change. COACT, Inc. assumes no liability for any errors or omissions that may appear in this document.

DOCUMENT INTRODUCTION

Prepared By:

COACT, Inc.
9140 Guilford Road, Suite N
Columbia, Maryland 21046-2587

Prepared For:

Ricoh Company, Ltd.
3-6, Nakamagome 1-chome, Ohta-ku
Tokyo 143-8555, Japan

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Hard Disc Security Module version 1. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
	08 May, 2007 Initial Publication

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC	Common Criteria
CCT	Cluster Count Table
CSM	Common Service Module
EAL3	Evaluation Assurance Level 3
HDD	hard disk drive
HSM	Hard Disk Security Module
IMH	Image Memory Handler
IT	Information Technology
MCS	Memory Control Service
MFP	Multi-Function Printer
NIAP	National Information Assurance Partnership
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B Security Target. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.2*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) and international interpretations through January 26, 2006. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B Security Target version 2007-001, revision 4, dated 08 May, 2007.

1.2 TOE Reference

Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B

1.3 Evaluation Assurance Level

Assurance claims conform to EAL3 (Evaluation Assurance Level 3) from the *Common Criteria for Information Technology Security Evaluation, Version 2.2*.

1.4 Keywords

Ricoh, HSM, overwrite, random data, random data generation, null, null generation, copy, print, data remanence, MFP, HDD

1.5 TOE Overview

This Security Target defines the requirements for the Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B version 1 TOE. The TOE is the software that once loaded is always resident in memory and constructs buffers containing two passes of random data and a single pass of nulls for use in overwriting copy and print residual data located in the Temporary Area of the MFP (Multi-Function Printer) hard disk drive (HDD). During print and copy job processing, the MFP stores images as files in the Temporary Area of the hard disk drive. There is a risk that these images could be disclosed during subsequent jobs. When initialized, the TOE performs an inspection of a table resident in memory and if copy or print residual data is present on the HDD, the TOE begins the random data and null buffer generation which is used to overwrite those portions of the HDD. The MFP displays an icon indicating whether or not the HDD is "clean" (this functionality is provided by MFP firmware not included in the TOE boundary).

1.5.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.6 Common Criteria Conformance

The Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B version 1 is compliant with the Common Criteria (CC) Version 2.2, functional requirements (Part 2) conformant or extended and assurance requirements (Part 3) conformant, augmented or extended for EAL3.

1.7 Protection Profile Conformance

The Hard Disc Security Module with imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B version 1 does not claim conformance to any registered Protection Profile.

1.8 Conventions

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

<u>Selection: indicated in underlined text</u>

<u>*Assignments within selections: indicated in italics and underlined text*</u>

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Hard Disk Security Module (TOE) Description

The Hard Disk Security Module (HSM) is a software module executed on MFP hardware and is contained on an SD memory card or DIMM-ROM providing adaptability to various MFP devices. The HSM is delivered in a kit and each kit is adaptable to a suitable MFP device. The kit contains the software either on a SD memory card or DIMM-ROM, an Operating Instruction Booklet or a CD-ROM containing the Operating Instruction Booklet and a Keytop version for each type of MFP device. Table 1 identifies and describes the HSM kit, the item, and the MFP devices suitable for each HSM kit type.

The HSM software executes exactly the same for each HSM kit type. The HSM creates buffers with two passes of random digits and a third pass of nulls. The HSM sends these buffers to the OS. The OS uses this data to overwrite the Temporary Area of MFP's hard disk drive (HDD) upon completion of each copy or print job thereby removing residual data. Copy and print jobs use the Temporary Area of the MFP HDD as a temporary staging area, and upon completion of the copy or print function the HSM creates buffers which the OS uses to overwrite the clusters of the Temporary Area of the HDD used by the copy or print function, thereby removing residual data. The OS uses the HSM created buffers to overwrite the clusters of the Temporary Area of the HDD used by the copy or print function employing a three-pass method. HSM first creates a buffer of random digits and through system calls sends this pass of random digits to the OS. The OS uses this pass of random digits to overwrite the targeted clusters in the Temporary Area of the HDD. This process is repeated a second time using a second buffer of random digits. Finally the HSM creates a buffer of nulls and sends this buffer to the OS. The OS then writes these nulls to the targeted clusters in the Temporary Area of the HDD.

The HSM function is automatic. Once installed on the MFP device, the overwriting function becomes effective immediately. It cannot be turned off, unless the software is removed. There is, however, a priority scheme. For practical MFP usability, the HSM function will become suspended if another application job accesses the HDD for writing or reading data. Once that job is completed HSM resumes. If the MFP power is disrupted either during HSM execution or if HSM is idle, upon power restore HSM is executed before user functionality can begin.

Table 1 - HSM Kit and Target MFP

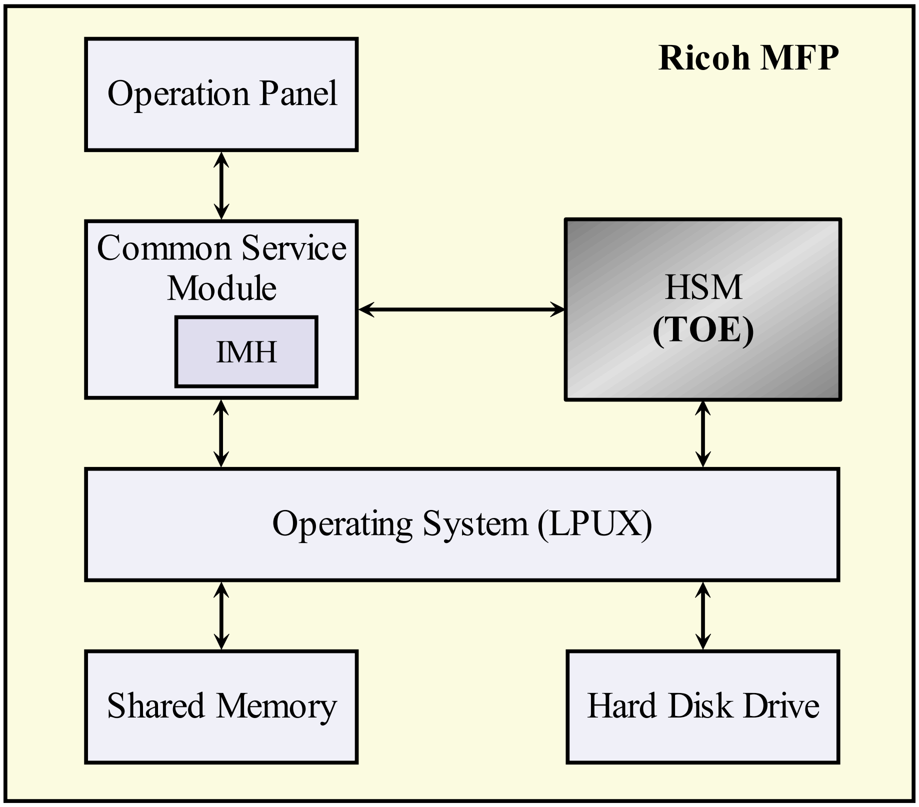
Kit Name	Item	Target MFP (Series)
DIMM ROM		
(Japan) imagio Security Module Type A [Model No.: B694-00] (Other Countries) DataOverwriteSecurity Unit Type A [Model No.: B694-01]	DIMM-ROM[P/N: B694-1500] Operating Instruction for users: Booklet (Japan) [P/N: B694-8600] CD ROM (Other Countries) [P/N: B692-8700] Keytop for model-1 [P/N:B027-1449] Keytop for model-2 [P/N:B077-1534]	**Model 1**
		(Japan) Ricoh imagio Neo 221/271 (Other Countries) Ricoh Aficio 2022/2027/2032 Infotec IS 2122/2127/2132 Savin 4022/4027 Nashutec DSm622/627/632 RexRotary DSm622/627/632 Gestetner DSm622/627/632 Lanier LD122/127/132
		Model 2
		(Japan) Ricoh imagio Neo 352/452 (Other Countries) Ricoh Aficio 2035e/2045e/2035eG/2045eG Infotec ISC 2135/2145 Savin 4035e/4045e/4035eG/4045eG Nashutec DSm635/645 RexRotary DSm635/645 Gestetner DSm635/645/635G/645G Lanier LD135/145

Kit Name	Item	Target MFP (Series)
SD Memory		
(Japan) imagio Security Card Type A [Model No.:B692-00] (Other Countries) DataOverwriteSecurity Unit Type B [Model no.:B692-01]	SD memory card [P/N:B692-1200] Operating Instructions for Users: Booklet (Japan) [P/N:B692-8501] CD-ROM (Other Countries) [P/N:B692-8700] Keytop for Model-3 [P/N:G570-1963] Keytop for Model-4 [P/N: B027-1449]	**Model 3**
		(Japan) Ricoh imagio Neo C325/C385 (Other Countries) Ricoh Aficio 2232C/2238C Infotec ISC 2432/2838 Savin C3224/3828 Nashutec DSc332/338 RexRotary DSc332/338 Gestetner DSc332/338 Lanier LD232c/238c
		Model 4
		(Japan) Ricoh imagio Neo W400 (Other Countries) None

2.1.1 Physical Boundary

The software is contained either on a SD memory card or a DIMM-ROM. The TOE executes on Ricoh MFP devices. At start-up, MFP firmware outside the TOE boundary checks to see if the TOE is physically installed. If it is, the TOE is loaded to RAM from the SD memory card or from the DIMM-ROM (depending on type of MFP device) by the MFP firmware and is executed on the Processing and Control Unit board. Table 1 shows the types of MFP devices that execute the HSM. Figure 1 describes the physical boundary of the TOE.

Figure 1 - Physical Boundary



2.1.2 Logical Boundary

The TOE is comprised of a buffer creation process, SF.RANDOMBUFFERS, which creates 2 buffers of random data and one buffer of nulls used for the HDD overwrite function. The TOE interfaces with a sub-module within the Common Service Module (CSM) called Image Memory Handler (IMH), a table called the Cluster Count Table (CCT) created by the IMH and resident in shared memory and the Operating System (LPUX). The TOE checks the CCT for clusters the IT Environment has determined contain residual data. If clusters are found, the TOE requests permission from IMH to begin the overwrite process. IMH does not respond directly to the TOE. IMH responds to the query from the TOE through LPUX. Once the TOE receives permission to begin the overwrite process from IHM through LPUX, the TOE creates the buffers of random data and nulls and sends the buffers through system calls to LPUX, which overwrites the clusters identified in the CCT. The rand() function of LPUX is called to generate random numbers for insertion into the buffers. MFP firmware outside the TOE boundary writes the buffers supplied by the TOE over the residual data on the hard disk drive and provides an operation panel indicator of whether or not the hard disk drive is "clean."

The TOE also performs partial self-protection, SF.Self-Protection. At each start-up, MFP firmware outside the TOE boundary checks to see if the TOE is physically installed (i.e., the DIMM or SD memory card is present). The DIMM or SD memory card must be physically removed and the MFP restarted for the TOE to be removed. The TOE interfaces are limited to the OS and to another software module within the MFP. There is no direct user interface into the TOE. Communications on these interfaces use standard UNIX socket-based methods where each communication path has a specified ID that ensures an exclusive connection, preventing use by other modules. The IT Environment, specifically LPUX, provides a separate process space in which the TOE executes that protects it from outside interference.

2.1.3 TSF Data

The TOE is dependent on the IMH to create and update the CCT table showing the existence of residual data on the HDD. While not TSF data in the strictest definition, it is information used by the TSF to make TSP decisions. The CCT table has block counters that show whether or not residual data exists on the HDD. These counters point to the HDD blocks that contain the residual data. The TOE checks the CCT table counters for the existence of residual data, if residual data is indicated the TOE obtains the HDD block addresses and then begins the random data creation process which starts the overwrite process.

2.1.3.1 Security Attributes

There are no security attributes associated with the TOE.

2.1.4 User Data

There is no user data associated with the TOE. The TOE creates buffers of random digits and nulls used by the OS to overwrite residual data on the MPF HDD.

2.1.5 Rationale for Non-Bypassability and Separation

The TOE is an application that executes on top of an underlying system that includes hardware and software required for operation. Therefore responsibility for non-bypassability and separation are split between the TOE and IT Environment.

The TOE provides a strictly controlled security function. Once installed the TOE cannot be turned off unless the software is removed. Interfaces to the TOE are limited. The TOE interfaces with the LPUX OS and the IMH module. The TOE provides strictly defined interfaces limited specifically to the functionality required from the TOE, thereby limiting the opportunity for corruption or compromise. The TOE interfaces are separated into two categories – security enforcing and security supporting. Security enforcing interfaces, of which there is only one, invoke the TSF and ensure that all enforcement functions complete successfully before allowing other actions to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (i.e., they are isolated from the TSF). The security supporting interfaces are used by the TOE to gain knowledge of the existence and location on the HDD of residual data and to seek permission for the start-up of the random data generation and overwrite process. These interfaces cannot affect the TSF once the TSF has begun.

At each start-up, MFP firmware outside the TOE boundary checks to see if the TOE is physically installed (i.e., the DIMM or SD memory card is present). The DIMM or SD memory card must be physically removed and the MFP restarted for the TOE to be removed. If the TOE is present, the IT Environment loads it into RAM for execution as a separate process.

LPUX provides a separate process domain for execution of the TOE. Memory space is allocated specifically for each process, which makes it impossible for one process to directly access the memory space of any other process. Data transfers between processes are UNIX socket-based, whereby each communication path has a specified ID that ensures an exclusive connection preventing access by other processes. Each process may only conduct data communication with other predetermined processes. All image data stored on the HDD or stored temporarily in the Image Memory is managed by a memory control module called the MCS (Memory Control Service), which ensures that the data can be accessed by specified machine functions.

The CCT table is accessed by the TOE via shared memory. The CCT is only updated by IMH (see Figure 1). The MFP does not support general purpose users. It also does not provide a mechanism for users to change the MFP firmware. Therefore, access to shared memory is restricted to predetermined processes in the MFP firmware and outside users are not able to interfere with the TOE's monitoring of the CCT table. The TOE relies on the IT Environment to not re-use a "dirty" cluster until it has been cleaned.

2.2 Evaluated Configuration

The TOE is dependent on its environment to function properly. An authorized customer engineer must turn off the following applications and functions of the MFP device:

A) Scanner Application (except Network TWAIN scanning)

B) I-Fax

C) Printer data spooling function

D) Document Box Application

E) Paperless Fax, and

F) eCabinet.

The TOE will not initialize unless the above functions are turned off.

The following data cannot be stopped or turned off; personnel responsible for managing the MFP must be aware that the hard disk drive will remain "dirty" while any of these types of data are present on the MFP.

A) User stamps,

B) Printer font set,

C) Printer form data, and

D) RTIFF emulation print data.

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption,* threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2 - Assumptions

A.Type	Description
A.ENVIRON	The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
A.INSTALL	The Ricoh Customer Engineer will install and configure the TOE according to the installation guidance.
A.NOEVIL	The personnel responsible for managing the MFP are non-hostile and follow the guidance when using the TOE.
A.PLATFORM	The Ricoh Customer Engineer will ensure that the platforms used to host the TOE conform to the hardware and software outlined in the guidance.
A.LIMITS	The personnel responsible for managing the MFP are knowledgeable about the limitations of the TOE and types of residual data that cannot be overwritten.

3.3 Threats

The threats identified in the following subsections are addressed by the TOE and the IT environment.

Table 3 - Threats

T.Type	TOE Threats
T.ANALYSE	Copy and print data resident on the MFP hard disk drive may be inadvertently accessed or maliciously accessed and analyzed by agents who gain physical access to the HDD
T.INTERFERE	The TOE could be by-passed or interfered with during operation by malicious users.

3.4 Organisational Security Policies

There are no Organisational Security Policies identified for this TOE.

CHAPTER 4

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's IT environment and the TOE's non-IT environment. The security objectives identify the responsibilities of the TOE, the TOE's IT environment, and the TOE's non-IT environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the IT environment are designated as *OE.objective*. Objectives that apply to the non-IT environment are designated with an *ON.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives:

Table 4 - Security Objectives for the TOE

O.Type	Security Objective
O.BUFFERS	The TOE will generate buffers containing random data and null data for MFP HDD over-write use.
O.SELFPROTECT	The TOE will provide partial self-protection by employing methods that ensure non-interference of its execution.

4.2 Security Objectives for the IT Environment

The TOE's IT environment must satisfy the following objectives.

Table 5 - Security Objectives of the IT Environment

OE.Type	IT Environment Security Objective
OE.OS_PROTECTION	The IT Environment will support TOE self-protection by maintaining a domain for its own execution and domains for separate application processes that protects itself and the application processes from external interference, tampering, or unauthorized disclosure through its own interfaces.
OE.OVERWRITE	The IT Environment will maintain the list of storage areas needed to be overwritten and use the random and null data buffers provided by the TOE to overwrite copy and print data on the Temporary Area of the MFP HDD thereby removing residual data.
OE.TOEON	The IT Environment will alert personnel responsible for managing the MFP that the TOE is resident in memory and active.

4.3 Security Objectives for the Non-IT Environment

The TOE's Non-IT environment must satisfy the following objectives.

Table 6 - Security Objectives for the Non-IT Environment

ON.Type	Security Objectives for the Non-IT Environment
ON.ENVIRON	The personnel responsible for managing the MFP will ensure that the TOE is installed in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.
ON.INSTALL	The Customer Engineer will install and configure the TOE according to the guidance.
ON.NOEVIL	The personnel responsible for managing the MFP are non-hostile and follow the guidance when using the TOE.
ON.PLATFORM	The Customer Engineer will ensure that the platforms used to host the TOE conform to the hardware and software outlined in the guidance.

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE.

5.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. The security functional requirements detailed in this section are explicitly stated requirements that identify security functional requirements that are not currently defined in Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.2*.

5.1.1 User Data Protection (FDP)

5.1.1.1 FDP_RDG_(EXP).1 Random Data Buffer Generation

Rationale for explicitly stated SFR: The TOE is an application that supports residual data destruction. FDP was chosen because the TOE supports User Data Protection by providing buffers containing random data and nulls used to overwrite targeted blocks of the HDD containing user residual data.

FDP_RDG_(EXP).1: The TSF shall generate successive buffers with two digit patterns and a null pattern and provide the buffers to the IT Environment for use in overwriting residual data of a size and location specified by the IT Environment.

5.1.2 Protection of the TSF (FPT)

5.1.2.1 FPT_RVM_SFT.1 Non-Bypassability of the TSP for Software TOEs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM that can be addressed by the TOE. See FPT_RVM_OS (levied on the IT Environment) for the remaining functionality.

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

5.1.1.2 FPT_SEP_SFT.1 TSF Domain Separation for Software TOEs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP that can be addressed by the TOE. See FPT_SEP_OS (levied on the IT Environment) for the remaining functionality.

FPT_SEP_SFT.1.1: The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_SFT.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2 Security Functional Requirements for the IT Environment

5.2.1 User Data Protection

5.2.1.1 FDP_DRM_(EXP).1 Data Remanence Protection

Rationale for Explicitly Stated Requirement: The CC does not include a Security Functional Requirement for the removal of data remanence. Since the overwrite may be delayed if the HDD is in use for other operations, FDP_RIP is not appropriate.

FDP_DRM_(EXP).1.1 The IT Environment shall overwrite the print and copy data stored in the Temporary Storage Area of the MFP HDD after the print or copy operation is complete.

FDP_DRM_(EXP).1.2 The IT Environment shall use an overwrite method that overwrites the target data with the buffers supplied by the TOE.

Dependencies: FDP_RDG_(EXP).1.

5.2.2 Protection of the TSF

5.2.2.1 FPT_RVM_OS.1 Non-Bypassability of the TSP

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

5.2.2.2 FPT_SEP_OS.1 TSF domain separation

FPT_SEP_OS.1.1 The IT Environment shall maintain a security domain for TSF execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP_OS.1.2 The IT Environment shall enforce separation between the security domains of subjects in the TSC.

5.2.3 Security Management

The security functional requirements detailed in this section are explicitly stated requirements that identify security functional requirements that are not currently defined in Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.2*.

5.2.3.2 FMT_ALR_(EXP) ALERT

FMT_ALR_(EXP).1.1 The IT Environment shall alert users of the TOE when the TOE is present or not present in memory.

5.2.4 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL3. These requirements are summarised in the following table.

Table 7 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Configuration Items and Authorization Controls

Assurance Class	Component ID	Component Title
Configuration Management	ACM_SCP.1	TOE Configuration Management Coverage
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.2	Security Enforcing High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance
Life-Cycle Support	ALC_DVS.1	Identification of Security Measures
Tests	ATE_COV.2	Analysis of Coverage
Tests	ATE_DPT.1	Testing High Level Design
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.1	Examination of Guidance
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

5.4 Strength of Function for the TOE

There is no probabilistic or permutational mechanism in the TOE.

5.5 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies.

5.5.1 TOE Security Functional Component Hierarchies and Dependencies

The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 8 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FDP_RDG_(EXP)	None	None	
FPT_RVM_SFT.1	None	None	
FPT_SEP_SFT.1	None	None	

5.5.2 IT Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified IT SFRs include the appropriate hierarchy and dependencies.

The following table lists the IT SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 9 - IT SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FDP_DRM_(EXP)	None	FDP_RDG_(EXP)	The IT Environment is dependent on the TOE to supply three buffers as input to the overwrite process.
FPT_RVM_OS	None	None	
FPT_SEP_OS	None	None	
FMT_ALR_(EXP)	None	None	

CHAPTER 6

6. TOE Summary Specification

6.1 Security Functions

6.1.1 SF.RANDOMBUFFERS

The TOE Security Function SF.RANDOMBUFFERS generates buffers containing two passes of random data and one pass of nulls that are passed to the OS and used by the OS to overwrite copy and print data located in the Temporary Storage Area of the MFP HDD. SF.RANDOMBUFFERS inspects a table resident in memory (maintained by the IT Environment) for notification that residual data exists in the Temporary Storage Area of the MFP HDD. Upon discovery of the existence of residual data, SF.RANDOMBUFFERS seeks permission to begin the overwrite process. Once permission is given SF.RANDOMBUFFERS obtains random numbers from the IT Environment and generates buffers containing two passes of random data and one pass of nulls and sends these buffers to the OS to perform the overwrite. The TOE uses the standard rand() Unix function call for generating random numbers to populate the buffers with random data, but the TOE does not claim the use of a "random number generator" as specified by FIPS 140-2. The IT Environment is responsible for writing the supplied buffers to the designated locations on the HDD.

6.1.2 SF.SELFPROTECT

At each start-up, MFP firmware outside the TOE boundary checks to see if the TOE is physically installed (i.e., the DIMM or SD memory card is present). If the TOE is present, the IT Environment loads it into RAM for execution as a separate process. In order to remove the software from the MFP, the DIMM or SD memory card must be physically removed and the MFP device restarted. The TOE uses limited interfaces and cannot be directly accessed by a user. These interfaces use standard Unix socket-based communication channels where each communication path has a specified ID that ensures an exclusive connection and prevents access by other modules.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance with any registered Protection Profile

7.2 Protection Profile Refinements

This Security Target does not claim conformance with any registered Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance with any registered Protection Profile.

7.4 Protection Profile Rationale

This section is not applicable, as this ST does not claim conformance with any registered Protection Profile.

CHAPTER 8

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 10 - Threats and Assumptions to Security Objectives Mapping

	O.BUFFERS	O.SELFPROTECT	OE.OS_PROTECTION	OE.TOEON	OE.OVERWRITE	ON.ENVIRON	ON.INSTALL	ON.NOEVIL	ON.PLATFORM
T.ANALYSE	X		X		X				
T.INTERFERE		X							
A.ENVIRON				X		X			
A.INSTALL				X			X		
A.NOEVIL				X				X	
A.PLATFORM			X	X	X				X
A.LIMITS								X	

8.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 11 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
T.ANALYSE	**O.BUFFERS** contributes to countering this threat by generating the buffers containing the random data obtained from the IT Environment and null data used by the IT Environment to overwrite the copy and print residual data on the MFP HDD, thereby mitigating the threat of data recovery from data remanence especially if the HDD is removed from its physically secure location. **OE.OVERWRITE** contributes to mitigating this threat by tracking the storage areas that need to be overwritten and using the random and null data and overwriting the copy and print residual data on the MFP HDD. **OE.OS_PROTECTION** contributes to countering this threat by ensuring that the OS can protect itself from users within its control and by providing separate application process domains. If the OS could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control. If the OS could not provide separate application process domains, the TSF could not protect itself from users or subjects outside of the TSC.
T.INTERFERE	**O.SELFPROECT** contributes to countering this threat by limiting interfaces to the TOE and not providing a user accessible interface into the TOE.

8.1.2 Rationale Showing Assumptions to Environment Security Objectives

The following table describes the rationale for the assumption to security objectives mapping.

Table 12 - Assumptions to Security Objectives Rationale

A.TYPE	Environment Security Objective Rationale
A.ENVIRON A.INSTALL A.NOEVIL A.PLATFORM	**OE.TOEON** addresses these assumptions by stating that the IT Environment will alert personnel responsible for managing the MFP that the TOE is resident in memory and active.
A.ENVIRON	**ON.ENVIRON** addresses this assumption by restating it as an objective for the personnel responsible for managing the MFP to satisfy.
A.INSTALL	**ON.INSTALL** addresses this assumption by restating it as an

A.TYPE	Environment Security Objective Rationale
	objective for the Ricoh Customer Engineer to satisfy.
A.NOEVIL A.LIMITS	**ON.NOEVIL** addresses this assumption by restating it as an objective for the personnel responsible for managing the MFP to satisfy.
A.PLATFORM	**ON.PLATFORM** addresses this assumption by restating it as an objective for the Ricoh Customer Engineer to satisfy.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 13 - SFRs to Security Objectives Mapping

	O.BUFFERS	O.SELFPROTECT
FDP_RDG_(EXP).1	X	
FPT_RVM_SFT.1		X
FPT_SEP_SFT.1		X

The following table provides the detail of TOE security objective(s).

Table 14 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.BUFFERS	**FDP_RDG_(EXP).1** defines the type of data that is created and passed to the IT Environment for use in overwriting copy and print residual data on the MFP HDD.
O.SELFPROTECT	**FPT_SEP_SFT.1** ensures the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment. **FPT_RVM_SFT.1** ensures that the TSF makes policy decisions on all interfaces that perform operations on subjects and objects

Security Objective	SFR and Rationale
	that are within the TSC. Without this non-bypassability requirement, the TSF could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to TOE resources (including TSF data and executable code) regardless of the defined policies.

8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the IT security objectives.

The following table identifies for each SFR, the IT Environment security objective(s) that address it.

Table 15 - IT Environment Security Objectives to SFR Mapping

	OE.OVERWWRITE	OE.TOEON	OE.OS_PROTECTION
FDP_DRM_(EXP)	X		
FMT_ALR_(EXP).1		X	
FPT_RVM_OS.1			X
FPT_SEP_OS.1			X

The following table provides the rational for the SFRs of the IT Environment security objective(s).

Table 16 - Security Objectives to SFR Rationale Detail

IT Environment Security Objective	SFR and Rationale
OE.OVERWRITE	**FDP_DRM_(EXP).1** ensures that the copy and print residual data located on the Temporary Area of the MFP HDD is overwritten.
OE.TOEON	**FMT_ALR_(EXP).1** notifies the TOE users of the presence and activation of the TOE.
OE.OS_PROTECTION	**FPT_SEP_OS.1** ensures the OS provides a separate

IT Environment Security Objective	SFR and Rationale
	domain for itself and individual application processes that protects them from untrusted users. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment. **FPT_RVM_OS.1** ensures that the OS makes policy decisions on all interfaces that perform operations on subjects and objects that are within the scope of the OS control. Without this non-bypassability requirement, the OS could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to unauthorized resources regardless of the defined policies.

8.2.3 Security Assurance Requirements Rationale

8.2.3.1 TOE Security Assurance Requirements Rationale

The TOE meets the assurance requirements for EAL3. The following table provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 17 - Assurance Measures

Component ID	Rationale
ACM_CAP.3	The Configuration Management Plan for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B provides the following information: Use of the automated tool for revision control Use of documented procedures for product builds Use of documented procedures for product test Use of documented procedures for release to manufacturing Use of documented procedures for distribution to customers List of configuration items and evidence that the automated tool maintains them. .
ACM_SCP.1	The Configuration Management Plan for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B provides the following information: The documentation contains lists of the items tracked by the automated revision tool. These items include the TOE

Component ID	Rationale
	implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.
ADO_DEL.1	The Delivery and Setup Procedure for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.
ADO_IGS.1	The Delivery and Setup Procedure for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B and Production Procedure for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B describe the procedures necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	The Security Functional Specification for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B describes the purpose and method of use of all external TSF interfaces and completely represents the TSF.
ADV_HLD.2	The High-level Design for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B contains a representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems, and describe the security functions. All subsystem interfaces are identified and the externally visible ones are noted. The purpose and method of use of all interfaces to the TSF subsystems are described.
ADV_RCR.1	The correspondence between the TOE security functions and the high-level design subsystems is described in the Correspondence Analysis for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B.
AGD_ADM.1	Guidance to personnel responsible for managing the MFP is effectively supported by the DataOverwriteSecurity Unit Type A DataOverwriteSecurity Unit Type B Operating Instructions.
AGD_USR.1	Guidance to non- administrative users is effectively supported by the DataOverwriteSecurity Unit Type A DataOverwriteSecurity Unit Type B Operating Instructions.

Component ID	Rationale
ALC_DVS.1	The Development Security Plan for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B describes the security measures employed to protect the confidentiality and integrity of the TOE design and implementation and provide evidence that measures are used.
ATE_COV.2	The Security Test Documentation for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B describes the mapping between the functional specification and the test procedures.
ATE_DPT.1	The Security Test Documentation for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B describes the mapping between the high level design and the test procedures.
ATE_FUN.1	The Security Test Documentation for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B describes the functional and penetration test performed and their results.
ATE_IND.2	The Security Test Documentation for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B describes the functional and penetration test performed and their results.
AVA_MSU.1	The DataOverwriteSecurity Unit Type A DataOverwriteSecurity Unit Type B Operating Instructions is reviewed by the CCTL.
AVA_SOF.1	No probabilistic or permutational mechanisms are used by the TOE, so no evidence in support of this assurance requirement is provided.
AVA_VLA.1	The Vulnerability Assessment for imagio Security Module Type A, imagio Security Card Type A, DataOverwriteSecurity Unit Type A, and DataOverwriteSecurity Unit Type B describes the vulnerability analysis performed and the results of the analysis.

8.2.3.2 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3 from part 3 of the Common Criteria.

8.3 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 18 - SFRs to TOE Security Functions Mapping

	SF.RANDOMBUFFERS	SF.SELFPROTECT
FDP_RDG_(EXP).1	X	
FPT_RVM_SFT.1		X
FPT_SEP_SFT.1		X

Table 19 - SFR to SF Rationale

SFR	SF and Rationale
FDP_RDG_(EXP).1	**SF.RANDOMBUFFERS** – Random Data Buffer Generation . SF.RANDOMBUFFERS supports FDP_RDG_(EXP) by ensuring that two passes of unique random data and a single pass of null data is created and sent to the IT Environment to be used to overwrite copy and print residual data located in the Temporary Area of the MFP HDD.
FPT_RVM_SFT.1	**SF.SELFPROTECT** – Self Protection. SF.SELFPROTECT supports FPT_RVM_SFT.1 by ensuring that the TOE is always resident and active in memory.

SFR	SF and Rationale
FPT_SEP.SFT.1	**SF.SELFPROTECT** – Self Protection. SF.SELFPROTECT supports FPT_SEP.SFT.1 by limiting interfaces into the TOE and not having user accessible interfaces into the TOE.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.