Samsung Multifunction MultiXpress M4370, M5370, M5270 Series

Security Target

Version 1.2

SAMSUNG ELECTRONICS Co., Ltd.

Document History

VERSION	DATE	DESCRIPTION OF CHANGE	SECTIONS AFFECTED	REVISED BY
1.0	2014-10-14	- Initial version	ALL	Kwangwoo Lee
1.1	2014-12-22	TOE Name Change - TOE Version Change (V5.B6.30)	ALL	Kwangwoo Lee
1.2	2014-12-30	- TOE Version Change (V5.B6.31)	ALL	Kwangwoo Lee

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

This document describes Security Target of Samsung Multifunction MultiXpress M4370, M5370, M5270 Series.

1.1 Security Target References

Security Target Title	Samsung Multifunction MultiXpress M4370, M5370, M5270 Series Security Target
Security Target Version	V1.2
Publication Date	December 30, 2014
Authors	SAMSUNG ELECTRONICS Co., Ltd.
Certification body	IT Security Certification Center (ITSCC)
CC Identification	Common Criteria for Information Technology Security (CC Version 3.1 Revision 4)
Keywords	Samsung Electronics, Multifunction, Security, IEEE Std 2600.2™-2009

1.2 TOE References

Developer	SAMSUNG ELECTRONICS Co., Ltd.
Name	Samsung Multifunction MultiXpress M4370, M5370, M5270 Series
Version	B6.31
Hardware (MFP Model)	M4370LX, M5370LX, M5270LX

1.3 TOE Overview

1.3.1 TOE Type, Usage and Security features

This TOE is MFPs (Multi-Function Peripherals) as an IT product. It controls the operation of the entire MFP, including copy, print, scan, and fax functions on the MFP controller.
This TOE can be used in a wide variety of environments such as home use by consumers, home or office use by small businesses, office use by medium or large organizations, self-service use by the public in retail copy shops, libraries, business centers, or educational institutions, and production use by commercial service providers. This TOE may contain or process valuable or sensitive assets that need to be protected from unauthorized disclosure and alteration. The utility of the device itself may be considered a valuable asset which also needs to be protected. There is also a need to ensure that the TOE cannot be misused in such a way that it causes harm to devices with which it shares network connections. This TOE is intended to conform the requirements of IEEE Std 2600.2™-2009. IEEE Std 2600.2™-2009 has defined Operational Environment B. Operational Environment B is generally characterized as a commercial information processing environment in which a moderate level of document security, network security, and security assurance are required. Typically, this environment will handle the day-to-day proprietary and nonproprietary information needed to operate an enterprise.

The TOE provides the following security features:

- Identification & Authentication
  The TOE receives U.USER's information (e.g. ID, password, domain, etc.) through either the LUI or the RUI, and performs identification & authentication functions using the acquired information. The TOE provides two types of user identification and authentication methods. If U.ADMINISTRATOR configures the local authentication, the MFP will authenticate the U.USER against an internal database. If U.ADMINISTRATOR selects the external

authentication as an authentication method, then MFP will authenticate the U.USER using an external authentication server. The TOE authorizes U.USER according to the identification & authentication result.

- Network Access Control
  The TOE provides a network access control function to control ports and protocols used in network protocol services provided by the MFP. Through this function, U.ADMINISTRATOR can control access from network by enabling/disabling or altering port numbers of various protocols. The TOE also provides IP filtering /MAC filtering functions to control access from network.

- Security Management
  The TOE provides a management function to manage security functions (e.g. security audit, image overwrite, etc.) provided by the TOE. Through this function, U.ADMINISTRATOR can enable/disable security functions, manage TSF data and the security attributes, and maintain security roles.

- Security Audit
  The TOE stores and manages internal events occurring in the TOE. Audit logs are stored on the hard disk drive and can be reviewed or exported by U.ADMINISTRATOR through the remote user interface.

- Image Overwrite
  The TOE provides an image overwrite function to securely delete temporary files and job files (e.g. printing, copying, scanning, and faxing jobs). This function is classified as two functions: automatic image overwriting and manual image overwriting. U.ADMINISTRATOR can execute the image overwriting function only through the local user interface.

- Data Encryption
  The TOE provides a data encryption function to protect data (e.g. job information, configuration information, audit logs, etc.) stored on the hard disk drive from unauthorized access.

- Fax Data Control
  The TOE provides a fax data control function to examine fax image data formats (MMR, MR, or MH of T.4 specification) received via the PSTN port and check whether received data is suitable.

- Self-testing

  The TOE provides a self-testing function to verify the TSF's correct operation and the integrity of TSF data and executable code.

- Secure Communication

  The TOE provides a trusted channel between itself and another trusted IT product to protect user data or TSF data that are transmitted or received over network.

1.4 TOE Description

This section provides detailed information for the TOE evaluator and latent customer about TOE security functions. It includes descriptions of the physical scope and logical scope of the TOE.

1.4.1 TOE Operational Environment

In general, the TOE can be used in a wide variety of environments, which means each environment may place a different value on the assets, make different assumptions about security-relevant factors, face threats of differing approaches, and be subject to different policy requirements.

The TOE is operated in an internal network protected by a firewall. U.USER is connected to the TOE and may perform jobs that are allowed.

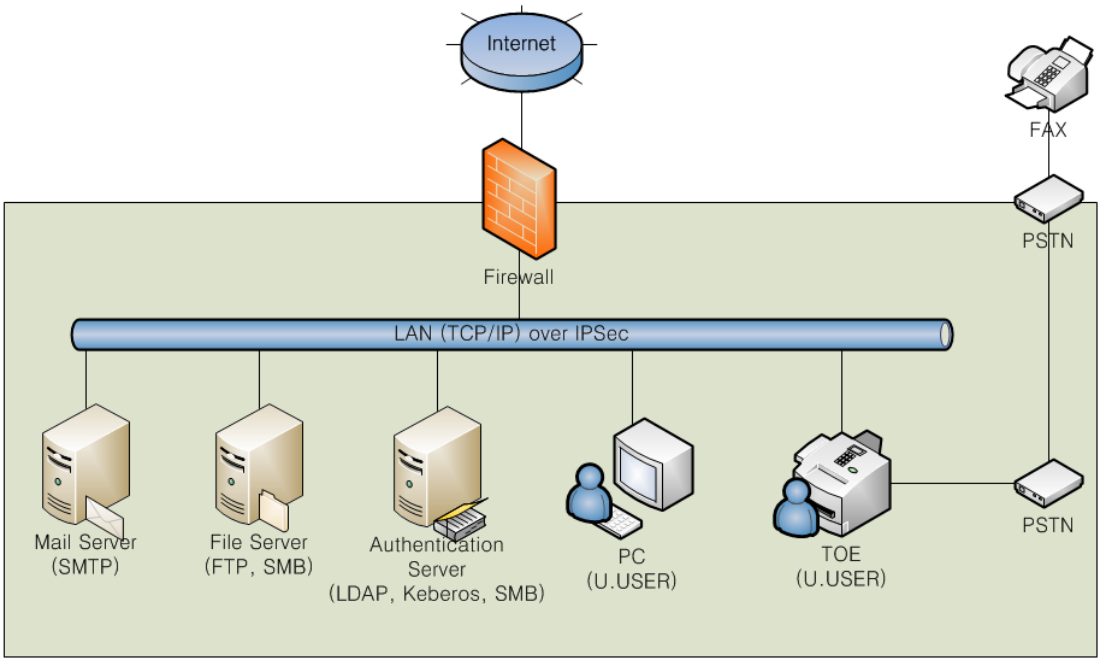


Figure 1: Operational Environment of the TOE

The TOE is intended to operate in a network environment that is protected by a firewall from external malicious attacks, and with reliable PCs and authenticated servers. U.USER is able to access the TOE by using local user interface (LUI) or remote user interface (RUI). The LUI is designed to be accessed by U.USER. The U.USER can operate copy, scan, and fax functions through the LUI. In the case of a scanning job, U.USER can operate the scanning job using the LUI and transfer the scanned data to a certain destination by email addresses and servers. U.USER can also use their PCs to print out documents or to access the TOE through the internal network. U.ADMINISTRATOR can enable/disable Automatic Image Overwrite; start/stop Manual Image Overwrite, and change a Password via the LUI. U.ADMINISTRATOR can access TOE through the RUI using a web browser through IPSec protocol. If IPSec is not configured in the TOE, all of network connection would be blocked. From there, U.ADMINISTRATOR can add/change/delete user accounts, change the

U.ADMINISTRATOR's ID and password, review the security audit service, and download the security audit report. The U.USER's account information that requires asking for internal authentication by TOE can be stored on the hard disk drive of the TOE. All of the information stored on the hard disk drive is protected by the TOE. In the case of external authentication using Kerberos, LDAP, SMB server, the external authentication servers will perform the user authentication using database of authentication server. The authentication server is assumed to be protected from external environmental space.

- Mail server

The SMTP (Simple Mail Transfer Protocol) server is used for e-mail transmission.

- File server

The FTP server and SMB server is used for storage devices of received fax and scan data from the TOE.

- Authentication server

There are several external authentication servers: Kerberos, LDAP, and SMB servers. The authentication server identifies and authenticates the U.NORMAL if external authentication mode is enabled by U.ADMINISTRATOR.

- PC

A computer for U.USER to access TOE if it is connected to the LAN and U.USER can remotely operate the TOE from the client computer. A web browser allows U.ADMINISTRATOR to connect to the TOE to use security management functions (e.g., audit log review, network access control, etc.) and allows U.NORMAL to use basic functions (e.g., print information, etc.). Note that U.USER shall set the IPSec configuration to connect the TOE. U.USER can install the printer driver to print out the documents.

1.4.1.1 General Specification for TOE

Table 1: General Specification for TOE

MFP Model	M4370LX	M5370LX	M5270LX
Color /Mono	Mono	Mono	Mono
PPM	43ppm	53ppm	52ppm
Processor	Chorus4N (Dual Core : Cortex-A9 1000MHz, ARM9 250MHz)		
RAM	DDR3 2,048MB		
ROM	NAND 128MB		
Interface	High-Speed USB 2.0 Host, High-Speed USB 2.0 Peripheral, Ethernet 10/100/1000 Base TX		
FAX	Option Kit, ITU-T G3, Super G3, 33.6 Kbps, MH/MR/MMR/JBIG		
HDD	SATA2 320 GB		
Display	10.1" 1024 x 600 WSVGA TFT Color Graphic LCD with Touch-Screen, 24-bit color		

1.4.2 Non-TOE Hardware/Software required by the TOE

1.4.2.1 Non-TOE Hardware

Table 2: Non-TOE Hardware

Item	Objective
Mail server	The SMTP (Simple Mail Transfer Protocol) server is used for e-mail transmission. In the TOE, the mail server can be used for the following services; scan to email, received fax forward and email notification.
File server	The FTP server and SMB server is used for storage devices of received fax and scan data from the TOE.
Authentication server	There are several authentication servers: Kerberos, LDAP, and SMB servers. The authentication server identifies and authenticates U.NORMAL if external authentication mode is enabled by U.ADMINISTRATOR.
PC	A computer for U.USER to access TOE if it is connected to the LAN and U.USER can remotely operate the TOE from the client computer. A web browser allows U.ADMINISTRATOR to connect to the TOE to use security management functions (e.g., audit log review, network access control, etc.) and allows U.NORMAL to use basic functions (e.g., print information, etc.). Note that U.USER shall set the IPSec configuration to connect the MFP. U.USER can install the printer driver to print out the documents. • System Requirement - Operating System : Windows® 7 32bit/64bit - CPU :Intel® Pentium® IV 1 GHz 32-bit or 64-bit processor or higher - RAM : 1 GB - Free HDD space: 16 GB

1.4.2.2 Non-TOE Software

Table 3: Non-TOE Software

Item	Objective
Web browser	Web browser that serves communication between U.ADMINISTRATOR/U.NORMAL's PC and TOE. - Internet Explorer 7.0 - Internet Explorer 8.0
Printer driver	Printer driver application software for U.USER to install in their PC. U.USER can configure properties and start printing jobs through this printer driver.
IPSec	IPSec provides secure communication between the TOE and the other trusted IT product to protect communicated data from modification or disclosure. - Confidentiality : 3DES(168bit) or AES(128bit) - Integrity: SHA-1(160bit) - Key Exchange: DH-Group MODP 1024/1536/2048/3072/4096/6144/8192

1.4.3 Physical Scope

This section describes physical scope of the TOE. The physical scope of the TOE is MFP itself. The TOE is consists of the following components; UI (Operational Panel), DADF Engine, Flatbed Engine, Fax Modem, Main Control Board, Power Unit, USB Port, Network Unit, Finisher, Optional Tray, and HDD.

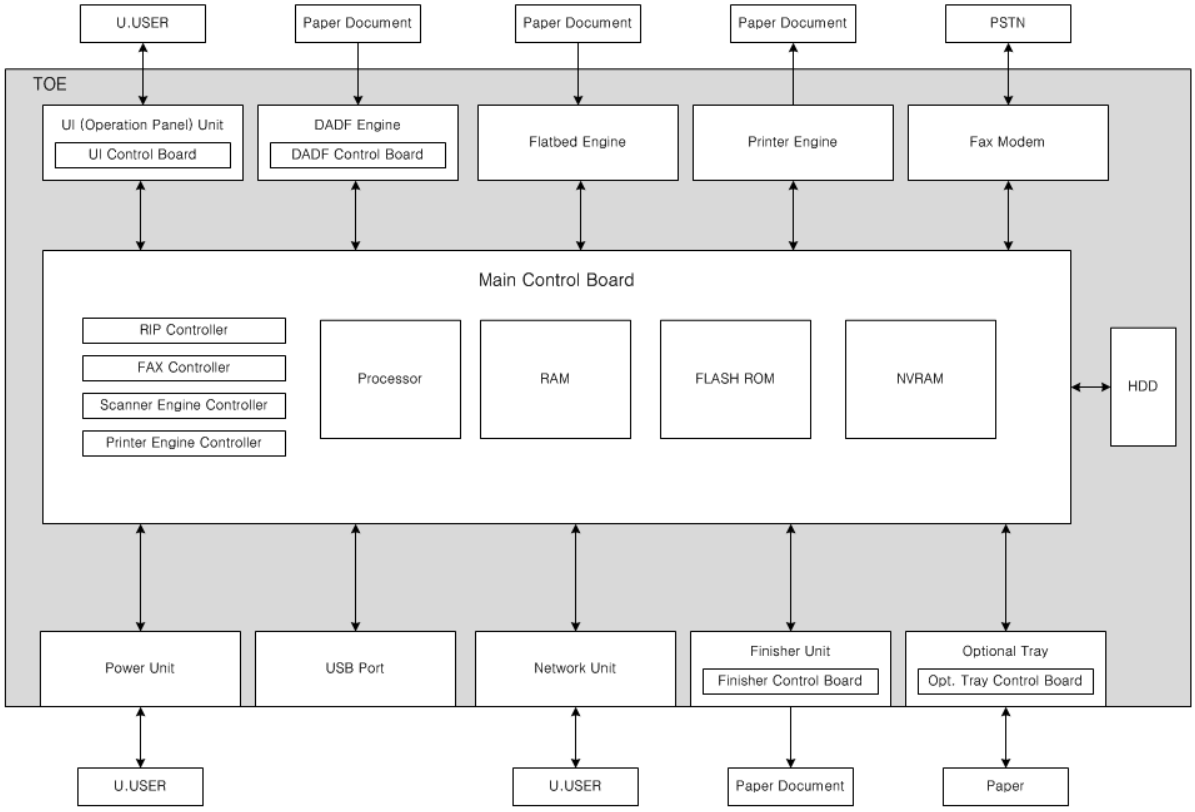


Figure 2: Physical Structure of MFP

- UI (Operation Panel)

The UI (Operational Panel) is a user interface installed on the TOE. UI is consists of UI control board, power button, LED indicators, and a TFT LCD touch screen. The UI control board manages the LUI (Local User Interface) operation and display. U.USER can operate the MFP through LCD touch screen and button. LED indicators show the current status of TOE.

- DADF Engine

A DADF (Duplexing Automatic Document Feeder) Engine controls the DADF features. It scans both sides in one pass. The advantage of the DADF is faster speed for two-sided originals.

- Flatbed Engine

A Flatbed Engine controls the flatbed scanner components. A flatbed scanner is composed of a glass platen, fixed mirror, moving optical array in CCD (Cold Cathode Fluorescent) scanning.

- Fax Modem

Fax Modem controls the function for connection to a PSTN. It sends and receives the fax data.

- Main Control Board

The Main Control Board consists of processor, RAM, Flash ROM, and NVRAM. It communicates the information with other part of TOE to control the MFP.

- Power Unit

A Power Unit provides the electric energy to operate the Engine Units and Control Boards.

- USB Port

The USB port is an external interface to communicate with universal serial bus. U.USER can directly print/scan the documents using USB port.

- Network Unit

The Network Unit is an external interface to an Ethernet.

- Finisher

A Finisher performs post-printing actions, such as stapling, hole-punching, folding, or collating.

- Optional Tray

The Optional Tray automatically takes paper.

- HDD

The HDD is a hard disk drive that is a non-volatile memory. The HDD removal is prevented by the design of the system.

The physical scope of the TOE is as follows:

1) The physical scope of the TOE consists of all hardware and firmware of the MFP.

MFP Model	M4370LX, M5370LX, M5270LX
TOE version	B6.31
System Firmware	V5.B6.31
Main Firmware	V11.01.07.31_12-29-2014
XOA Framework	V1.29.0_01-07-2014
UP	1.16.6_(20140822222122)
UI Firmware	V5.18.02.14.02_14122920
Boot Rom	V13.00.00.00.62-10-06-2014
File System	FS_V14.02.00.00.60

2) Instructions
- Samsung Multifunction MultiXpress M4370, M5370, M5270 Series User's Guide V1.2
- Samsung Multifunction MultiXpress M4370, M5370, M5270 Series Installation Guide V1.1

1.4.4 Logical Scope

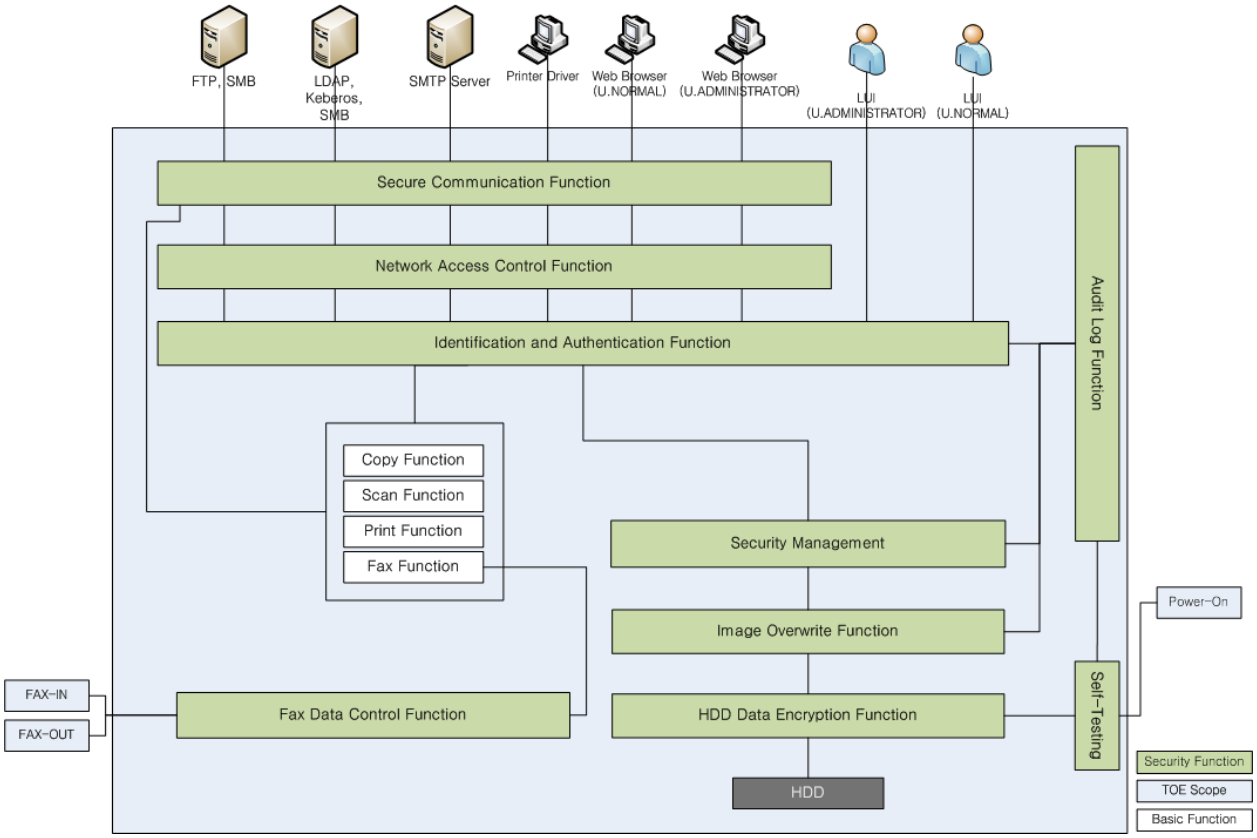


Figure 2: Logical Scope

1.4.4.1 MFP Basic Functions

Print Function: producing a hardcopy document from its electronic form

Scan Function: producing an electronic document from its hardcopy form

Copy Function: duplicating a hardcopy document

Fax Function: scanning documents in hardcopy form and transmitting them in electronic form over telephone lines and receiving documents in electronic form over telephone lines and printing them in hardcopy form

Shared-medium Interfaces: transmitting or receiving User Data or TSF Data between the MFP and external devices over communications media which, in conventional practice, is or can be simultaneously accessed by multiple users

1.4.4.2 TOE Security Functions

The following security functions are provided by the TOE:

Identification & Authentication (TSF_FIA)

The TOE provides two types of user identification and authentication methods. If U.ADMINISTRATOR configures the local authentication, the MFP will authenticate the U.USER against an internal database. If U.ADMINISTRATOR selects the external authentication as an authentication method, then MFP will authenticate the U.USER using an external authentication server.

U.USER should be identified and authenticated by entering both ID and Password to access to the TOE management functions. If U.USER fails to login specific times, the system blocks the session of the U.USER during predefined duration.

U. ADMINISTRATOR can configure Identification & Authentication Policy by using LUI or RUI.

U. ADMINISTRATOR can also give specific permission for U.USER to only use certain feature of the machine.

The TOE provides the Common Access Control & TOE Function Access Control based on the user role assigned to a user group ID by U.ADMINISTRATOR when U.NORMAL performs read/delete/modify operations on the data owned by U.NORMAL or when U.NORMAL accesses print/scan/copy/fax functions offered by the MFP.

The TOE shall terminate an interactive session after predefined time interval of user inactivity.

Network Access Control (TSF_NAC)

The MFP system has a network interface connected to a network. The MFP system can send/receive data and MFP configuration information and thus is able to configure MFP settings.

There are a couple of methods to access and communicate with the MFP from outside of the TOE through the network, and the TOE manages all incoming packets via a network interface.

1) Protocol and Port Control:

The TOE can only allow protocols and ports configured by U.ADMINISTRATOR.

U.ADMINISTRATOR can configure this information via the LUI or RUI.

2) IP and MAC address filtering:

U.ADMINISTRATOR can make filtering rules for IP addresses and MAC addresses.

After that, packets are only allowed as per the IP filtering rule registered by U.ADMINISTRATOR.

Packets via MAC addresses registered by U.ADMINISTRATOR are not allowed.

Security Management (TSF_FMT)

The TOE accomplishes security management for the security function, TSF data, and security attribute.

Only U.ADMINISTRATOR can manage the security functions through the LUI (Local User Interface) and RUI (Remote User Interface): security functions can be start and stop by U.ADMINISTRATOR. The LUI is touch-screen based management service which is provided by TOE. RUI is web-based management service using HTTP/HTTPS protocol.

TSF data and their possible operations are specified by U.ADMINISTRATOR.

Security attributes can be operated by U.ADMINISTRATOR.

Security Audit Data (TSF_FAU)

The TOE creates an audit record security audit event including job log, security event log, and operation log. The audit data consist of the type of event, date and time of the event, success or failure, log out and access of log data.

Only U.ADMINISTRATOR is authorized to view (or export) the audit data but even U.ADMINISTRATOR shall not delete log data manually.

The TOE protects Security Audit Data stored on the hard disk drive. It prevents any unauthorized alteration to the Security Audit Data, and when each log events exceeds the maximum number, the TOE overwrites the oldest stored audit records and generates an audit record of overwriting.

Image Overwrite (TSF_IOW)

The TOE provides Image Overwrite functions that delete the stored file from the MFP's hard disk drive. The Image Overwrite function consists of Automatic Image Overwrite and Manual Image Overwrite. The TOE implements an Automatic Image Overwrite to overwrite temporary files created during the copying, printing, faxing and scanning (scan to e-mail, scan to FTP, and scan to SMB task processes). The image overwrite security function can also be invoked manually only by U.ADMINISTRATOR through the LUI. Once invoked, the Manual Image Overwrite cancels all print and scan jobs, halts the printer interface (network), overwrites the hard disk according to the procedures set by U. ADMINISTRATOR. If there are any problems during overwriting, the Manual Image Overwrite job automatically restarts to overwrite the remaining area.

Data Encryption (TSF_NVE)

The TOE provides an encryption function during the data storage procedure and a decryption function in the process of accessing stored data from hard disk drive.

The TOE generates cryptographic keys when the TOE is initialized at the first setout the secret key (256 bits) is used for encrypting and decrypting user data and TSF data that is stored on the HDD. Access to this key is not allowed to any U.USER including U.ADMINISTRATOR.

The TSF shall destroy cryptographic keys in accordance with overwriting a used cryptographic key with a newly generated cryptographic key. Before storing temporary data, document data, and system data on the HDD of the MFP, the TOE encrypts the data using AES 256 algorithm and cryptographic key.

When accessing stored data, the TOE decrypts the data using the same algorithm and key.

Therefore, the TOE protects data from unauthorized reading and falsification even if the HDD is stolen.

Fax Data Control (TSF_FLW)

If the received fax data includes malicious content, it may threaten the TOE asset. To prevent this kind of threat, the TOE inspects whether the received fax image is standardized with MMR, MR, or MH of T.4 specification or not before forwarding the received fax image to e-mail or SMB/FTP. U. ADMINISTRATOR can restrict this forwarding function. When non-standardized format data are discovered, the TOE destroys the fax image.

Self Testing (TSF_STE)

During initial start-up, the TOE performs self test. Self testing executes TSF function to verify the correct operation of the HDD encryption function. Also, the TOE verifies the integrity of the encryption key data and TSF executable code by the self testing.

Secure Communication (TSF_SCO)

The TOE also provides secure communication between the TOE and the other trusted IT product to protect communicated data from modification or disclosure by IPSec. The network which connected without IPSec shall not be allowed to communicate with MFP.

Non-TSF Function

TOE includes the local user interface based on Android platform. Although the Android platform is used to TOE's user interface, local user interface does not provide any core Android system application such as Android system setting, Search, Brower, Contacts, Gallery, and Music. Therefore, U.USER cannot access any core Android system application and its related setting interfaces.

1.5 Conventions

This section describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Four presentation choices are discussed here.

- **Refinement**
  The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. Refinement of security requirements is denoted by **bold text.**
- **Selection**
  The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.
- **Assignment**
  The assignment operation is used to assign a specific value to an unspecified parameter such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.
- **Iteration**
  Iterated functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, for example, FIA_AFL.1 (1) and FIA_AFL.1 (2).

The following is notational conventions used by the PP:

- The following prefixes in Table 4 are used to indicate different entity types**:**

Table 4: Notational Prefix Conventions

Prefix	Type of Entity
U.	User
D.	Data
F.	Function
T.	Threat
P.	Policy
A.	Assumption
O.	Objective
OE.	Environmental objective
+	Security attribute

The following is an additional convention used to denote this Security Target:

- **Application Note**
  Application note clarifies the definition of requirement. It also can be used when an additional statement except for the four presentations previously mentioned. Application notes are denoted by underlined text.

1.6 Terms and Definitions

Basically, this security target shall follow the terms and definitions specified in common criteria and the protection profile. They will not be additionally described in this document.

LUI, Local User Interface

Interface for general users or system administrators to access, use, or manage the MFP directly.

Secure printing

When a user stores files in an MFP from a remote client PC, the user must set secure printing configuration and assign a PIN to the file. Then the user can access to the file by entering the PIN through the LUI of the MFP.

Multi-Function Printer, MFP

MFP is a machine that incorporates the functionality of multiple devices (copy, print, scan, or fax) in one.

Manual Image Overwrite

The Manual Image Overwrite function overwrites all stored files, including image files and preserved files on the hard disk drive, and the function should only be manually performed by a U.ADMINISTRATOR through the LUI.

U.ADMINISTRATOR

This is an authorized user who manages the TOE. System administrator manages the TOE through LUI and RUI. The main roles are to configure system information and check MFP status for general use. The other roles for security service are enable/disable Automatic Image Overwrite / Manual Image Overwrite for security, start/stop Manual Image Overwrite, change Password. The main roles are to create/change/delete the security property, manage/change user's ID and password, review the security audit log, and download security audit logs.

Image Overwrite

This is a function to delete all stored files on the hard disk drive. There are two kinds of image overwriting: Automatic Image Overwrite and Manual Image Overwrite.

Incoming Fax

This is a fax function which is receiving a fax data through a public switched telephone network.

RUI, Remote UI, Remote User Interface

Interface for U.NORMAL or U.ADMINISTRATOR to access, use, or manage the TOE through a web service.

Image file

Temporarily stored file that is created during scan, copy, or fax job processing.

Automatic Image Overwrite

The Automatic Image Overwrite automatically carries out overwriting operations on temporary image files at the end of each job such as copy, scan, scan-to-email, scan-to-FTP, or scan-to-SMB. Or the Automatic Image Overwrite overwrites the files on the hard disk drive when a user initiates a delete operation.

FAX

This is a function that transmits data scanned in the MFP through a fax line and receives fax data directly from a fax line on the MFP.

Fax image

The data received or transmitted through a fax line

T.4

Data compression specification for fax transmissions by ITU-T (International Telecommunication Union).

MH

Abbreviation of Modified Huffman coding. This is an encoding method to compress for storing TIFF type files. It is mainly used for fax transmission.

MR

Abbreviation of Modified Relative Element Address Designate MH coding.

MMR

Abbreviation of Modified Modified Relative Element Address Designate MH coding. More advanced type than MR coding.

1.7 Acronyms

This section defines the meanings of acronyms used throughout this Security Target (ST) document.

Table 5: Acronyms

	Definition
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
ISO	International Standards Organization
IT	Information Technology
LUI	Local User Interface
MFP	Multi-Function Peripheral
OSP	Organizational Security Policy
PP	Protection Profile
PPM	Pages Per Minute
PSTN	Public Switched Telephone Network
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
RUI, Remote UI	Remote User Interface
MMR	Modified Modified READ coding
MR	Modified READ Coding
MH	Modified Huffman coding

1.8 Organization

Chapter 1 introduces the overview of Security Target, which includes references of Security Target, reference of the TOE, the TOE overview, and the TOE description.

Chapter 2 includes conformance claims on the Common Criteria, Protection Profile, package, and provides a rationale on the claims.

Chapter 3 defines security problems based on the TOE, security threats, security policies of the organization, and assumptions from the TOE or the TOE operational environment point of view.

Chapter 4 describes TOE security objectives for corresponding with recognized threats, performing the security policy of the organization, and supporting the assumptions. It also describes security objectives about the TOE operational environment.

Chapter 5 describes the extended component definition.

Chapter 6 describes security functional requirements and security assurance requirements that satisfy the security objectives.

Chapter 7 describes how the TOE satisfies the security functional requirements.

2 Conformance Claims

This chapter describes how the Security Target conforms to the Common Criteria, Protection Profile and Package.

2.1 Conformance to Common Criteria

This Security Target conforms to the following Common Criteria:

- **Common Criteria Identification**
  - Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1r4, 2012. 9, CCMB-2012-09-001
  - Common Criteria for Information Technology Security Evaluation, Part 2: SFR (Security Functional Requirement), version 3.1r4, 2012. 9, CCMB-2012-09-002
  - Common Criteria for Information Technology Security Evaluation, Part 3: SAR (Security Assurance Requirement), version 3.1r4, 2012. 9, CCMB-2012-09-003
- **Common Criteria Conformance**
  - Common Criteria for Information Technology Security Evaluation, Part 2 extended
  - Common Criteria for Information Technology Security Evaluation, Part 3 conformant

2.2 Conformance to Protection Profiles

This Security Target conforms to the following Protection Profile:

- **Protection Profile Identification**
  - Title : U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std.2600.2™-2009)
- **Protection Profile Conformance**
  - The PP to which this ST and TOE are demonstrable conformant is:
  - Title : U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std.2600.2™-2009)
  - This ST is package-conformant to and package-augmented by the following SFR packages:
    - 2600.2-PRT, conformant
    - 2600.2-SCN, conformant
    - 2600.2-CPY, conformant
    - 2600.2-FAX, conformant
    - 2600.2-SMI, conformant

2.3 Conformance to Packages

This Security Target conforms to the following Package.

- **Assurance Package: EAL2 augmented by ALC_FLR.2**
- 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
  Package version: 1.0, dated March 2009
- 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
  Package version: 1.0, dated March 2009
- 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
  Package version: 1.0, dated March 2009
- 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
  Package version: 1.0, dated March 2009
- 2600.2-SM**I**, SFR Pac**k**age for Hardcopy Device Shared-medium Interface Functions, Operational Environment B
  Package version: 1.0, dated March 2009

2.4 Conformance Claim Rationale

Protection Profile conformance method: "Demonstrable Conformance to the Security Problem Definition (APE_SPD), Security Objectives (APE_OBJ), Extended Components Definitions (APE_ECD), and the Common Security Functional Requirements (APE_REQ)"

[Note] This ST must provide adequate rationale to demonstrate that the ST is "equivalent or more restrictive" than the PP to which this ST is claiming conformance.

The PP conformance claim rationale is as follows:

2.4.1 Security Problem Definition Related Conformance Claim Rationale

The security problem related conformance claim rationale is as shown in Table 6, Table 7 and Table 8 below:

Table 6: Security Problem Definition Related Conformance Claim Rationale - Threats

Threat	Rationale
T.DOC.DIS	Equal to the PP: the threats in this ST are defined the same as the PP. Therefore, it satisfies the "demonstrable conformance".
T.DOC.ALT	
T.FUNC.ALT	
T.PROT.ALT	
T.CONF.DIS	
T.CONF.ALT	

Table 7: Security Problems Definition Related Conformance Claim Rationale - Organizational Security Policies

Organizational Security Policy	Rationale
P.USER.AUTHORIZATION	Equal to the PP: the security policies in this ST are defined the same as the PP. Therefore, it satisfies the "demonstrable conformance".
P.SOFTWARE.VERIFICATION	
P.AUDIT.LOGGING	
P.INTERFACE.MANAGEMENT	

Table 8: Security Problems Definition Related Conformance Claim Rationale - Assumptions

Assumption	Rationale
A.ACCESS.MANAGED	Equal to the PP: the assumptions in this ST are defined the same as the PP. Therefore, it satisfies the "demonstrable conformance".
A.USER.TRAINING	
A.ADMIN.TRAINING	
A.ADMIN.TRUST	

2.4.2 Security Objectives Related Conformance Claim Rationale

The security objectives related conformance claim rationale is as shown in Table 9 and Table 10 below:

Table 9: Security Objectives Related Conformance Claim Rationale – Security Objectives for the TOE

Security Objectives for TOE	Rationale
O.DOC.NO_DIS	Equal to the PP: the security objectives in this ST are defined the same as the PP. Therefore, it satisfies the "demonstrable conformance".
O.DOC.NO_ALT	
O.FUNC.NO_ALT	
O.PROT.NO_ALT	
O.CONF.NO_DIS	
O.CONF.NO_ALT	
O.USER.AUTHORIZED	

Security Objectives for TOE	Rationale
O.INTERFACE.MANAGED	
O.SOFTWARE.VERIFIED	
O.AUDIT.LOGGED	
O.AUDIT_STORAGE.PROTECTED	Equal to the PP: the security objectives in this ST are defined the same as the PP. If the TOE provides an internal capability to provide access to audit records, then the ST Author should add these objectives. It is described APPLICATION NOTE 5 in the PP. Therefore, it satisfies the "demonstrable conformance"
O.AUDIT_ACCESS.AUTHORIZED	

Table 10: Security Objectives related Conformance Claim Rationale – Security Objectives for the Operational Environment

Security Objectives for Operational Environment	Rationale
OE.PHYSICAL.MANAGED	Equal to the PP: the security objectives in this ST are defined the same as the PP. Therefore, it satisfies the "demonstrable conformance". .
OE.USER.AUTHORIZED	
OE.USER.TRAINED	
OE.ADMIN.TRAINED	
OE.ADMIN.TRUSTED	
OE.AUDIT.REVIEWED	
OE.AUDIT_STORAGE.PROTECTED	
OE.AUDIT_ACCESS.AUTHORIZED	
OE.INTERFACE.MANAGED	

2.4.3 Security Functional Requirements related Conformance Claim Rationale

The security functional requirements related conformance claim rationale is as shown in Table 11 below:

Table 11: Security Functional Requirements related Conformance Claim Rationale

Category	PP SFR	ST SFR	Rationale
Common Requirements from the PP	FAU_GEN.1	FAU_GEN.1	Equal to the PP: in this ST, the operations allowed in the PP on SFR were performed. It satisfies
	FAU_GEN.2	FAU_GEN.2	

Category	PP SFR	ST SFR	Rationale
	FDP_ACC.1(a)	FDP_ACC.1(1)	the “demonstrable conformance”.
	FDP_ACC.1(b)	FDP_ACC.1(2)	
	FDP_ACF.1(a)	FDP_ACF.1(1)	
	FDP_ACF.1(b)	FDP_ACF.1(2)	
	FDP_RIP.1	FDP_RIP.1	
	FIA_ATD.1	FIA_ATD.1	
	FIA_UAU.1	FIA_UAU.1	
	FIA_UID.1	FIA_UID.1	
	FIA_USB.1	FIA_USB.1	
	FMT_MSA.1(a)(b)	FMT_MSA.1(1)(2)	
	FMT_MSA.3(a)(b)	FMT_MSA.3(1)(2)	
	FMT_MTD.1	FMT_MTD.1	
	FMT_SMF.1	FMT_SMF.1	
	FMT_SMR.1	FMT_SMR.1	
	FPT_TST.1	FPT_TST.1	
	FTA_SSL.3	FTA_SSL.3	
	FPT_STM.1	FPT_STM.1	
PRT Package Requirements from the PP	FDP_ACC.1	FDP_ACC.1(3)	Equal to the PP: in this ST, the operations allowed in the PP on SFR were performed. It satisfies the “demonstrable conformance”.
	FDP_ACF.1	FDP_ACF.1(3)	
SCN Package Requirements from the PP	FDP_ACC.1	FDP_ACC.1(3)	
	FDP_ACF.1	FDP_ACF.1(3)	
CPY Package Requirements from the PP	FDP_ACC.1	FDP_ACC.1(3)	
	FDP_ACF.1	FDP_ACF.1(3)	
FAX Package Requirements from the PP	FDP_ACC.1	FDP_ACC.1(3)	
	FDP_ACF.1	FDP_ACF.1(3)	
SMI Package	FAU_GEN.1	FAU_GEN.1	

Category	PP SFR	ST SFR	Rationale
Requirements from the PP	FPT_FDI_EXP.1	FPT_FDI_EXP.1	
	FTP_ITC.1	FTP_ITC.1	
Addition	-	FAU_SAR.1	These SFRs are augmented according to PP APPLICATION NOTE 5 and 7 in order for the TOE to maintain and manage the audit logs.
	-	FAU_SAR.2	
	-	FAU_STG.1	
	-	FAU_STG.4	
	-	FIA_AFL.1	These SFR are augmented according to PP Application Note 36.
	-	FIA_UAU.7	
	-	FMT_MSA.1(3)	This SFR is augmented according to PP Application Note 78.
	-	FMT_MSA.3(3)	This SFR is augmented according to PP Application Note 78, 83, 89, 93, and 98
		FCS_CKM.1	These SFR are augmented to protect the User data and TSF data against unauthorized disclosure or alteration. These augmented SFRs do not affect the PP SFR. Rather, it is more restrictive than the PP, Therefore, it satisfies the “demonstrable conformance”
	-	FCS_CKM.4	
	-	FCS_COP.1	
	-	FMT_MSA.1(4)	These SFRs are augmented to enforce the interface by requiring network access control and management. These augmented SFRs do not affect the PP SFR. Rather, it is more restrictive than the PP, Therefore, it satisfies the “demonstrable conformance”
	-	FMT_MSA.3(4)	
		FDP_IFC.2	
		FDP_IFF.1	

2.4.4 Security Assurance Requirements related Conformance Claim Rationale

The security assurance requirements related conformance claim rationale is as shown in Table 12 below:

Table 12: Security Assurance Requirements related Conformance Claim Rationale

PP SAR	ST SAR	Rationale
Assurance Package: EAL2 augmented by ALC_FLR.2	Assurance Package: EAL2 augmented by ALC_FLR.2	Equal to the PP. Therefore, it satisfies the "demonstrable conformance".

2.4.5 TOE type related Conformance Claim Rationale

This section demonstrates that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

Table 13: TOE type related Conformance Claim Rationale

TOE Type [PP]	TOE Type	Rationale
The Hardcopy Devices (HCDs) considered in this Protection Profile are used for the purpose of converting hardcopy documents into digital form (scanning), converting digital documents into hardcopy form (printing), transmitting hardcopy documents over telephone lines (faxing), or duplicating hardcopy documents (copying). Hardcopy documents are commonly in paper form, but they can also take other forms, such as positive or negative transparencies or film.	The TOE is MFPs (Multi-Function Peripherals) as an IT product	The TOE controls the operation of the whole MFP including copy, print, scan, and fax jobs on the MFP controller. Therefore, the TOE type is consistent with the PP, and satisfies the "demonstrable conformance".

3 Security Problem Definition

This chapter defines assumptions, organizational security policies, and threats intended for the TOE and TOE operational environments to manage.

3.1 Threats agents

The threats agents are users that can adversely access the internal asset or harm the internal asset in an abnormal way. The threats have an attacker possessing a basic attack potential, standard equipment, and motive. The threats that are described in this chapter will be resolved by security objectives in chapter 4.

The following are the threat agents defined in this ST:

- Persons who are not permitted to use the TOE who may attempt to use the TOE.
- Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.
- Persons who are authorized to use the TOE who may attempt to access data in ways for which they are not authorized.
- Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

3.1.1 Threats to TOE Assets

The threats taken from the PP to which this Security Target conforms are as shown in Table 14 and Table 15 (Refer to chapter 6 about affected asset):

Table 14: Threats to User Data for the TOE

Threats	Affected Asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons

Table 15: Threats to TSF Data for the TOE

Threats	Affected Asset	Description
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

3.2 Organizational Security Policies

This chapter describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for Security Objectives that are commonly desired by TOE Owners in this operational environment but for which it is not practical to universally define the assets being protected or the threats to those assets.

This Security Target conforms to all organizational security policies mentioned in the PP. There are no additional organizational security policies in this Security Target.

Table 16: Organizational Security Policies

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.

3.3 Assumptions

The following conditions are assumed to exist in the operational environment of the TOE.

This Security Target conforms to all assumptions in the PP.

3.3.1 Assumptions for the TOE

The assumptions taken from the PP to which this Security Target conforms are as shown in the following Table 17.

Table 17: Assumptions for the TOE

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their

Assumption	**Definition**
	organization and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and to correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4 Security Objectives

The security objectives are categorized into two parts:

- The security objectives for the TOE are to meet the goal to counter all threats and enforce all organizational security policies defined in this ST.
- The security objectives for the operational environment are based on technical/ procedural measures supported by the IT environment and the non-IT environment for the TOE to provide the security functionalities correctly.

4.1 Security Objectives for the TOE

This section identifies and describes the security objectives for the TOE. This Security Target takes all the security objectives for the TOE from the PP.

4.1.1 Security Objectives for the TOE

This section describes the Security Objectives that the TOE shall fulfill. They are completely the same as the PP.

Table 18: Security Objectives for the TOE

Objective	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events and prevent its unauthorized disclosure or alteration.

4.1.2 Security Objectives for the TOE (Additional)

The security objectives for the TOE additionally defined are as follows:

Table 19: Security Objectives for the TOE (Additional)

Objective	Definition
O.AUDIT_STORAGE.PROTECTED	The TOE shall protect audit records from unauthorized access, deletion and modification.
O.AUDIT_ACCESS.AUTHORIZED	The TOE shall allow access to audit records only by authorized persons.

4.2 Security Objectives for Operational Environment

This section describes the Security Objectives that must be fulfilled by technical and procedural measures in the operational environment of the TOE. This Security Target conforms to the security objectives for the operational environment included in the PP.

4.2.1 Security Objectives for Operational Environment

The security objectives for the operational environment taken from the PP to which this Security Target conforms are as shown in the following Table 20 (they are completely the same as the PP):

Table 20: Security Objectives for Operational Environment

Objective	Definition
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion, and modification.
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order to detect potential security violations and only by authorized persons.
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.

Objective	**Definition**
OE.USER.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization and have the training and competency to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization; have the training, competency, and time to follow the manufacturer's guidance and documentation; and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.3 Security Objectives Rationale

This section demonstrates that each threat, organizational security policy, and assumption is mitigated by at least one security objective and that those security objectives counter the threats, enforce the policies, and uphold the assumptions. Table 21 shows the correspondences of security objectives, assumptions, threats, and organizational security policies. Table 22 shows that each security problem is covered by the defined security objectives.

Table 21: Completeness of Security Objectives

Threats/ Policies/ Assumptions	Objective																			
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECT	O.AUDIT_ACCESS.AUTHORIZE	OE.AUDIT_STORAGE.PROTEC	OE.AUDIT_ACCESS.AUTHORIZ	OE.AUDIT.REVIEWED	OE.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	O.INTERFACE.MANAGED	OE.USER.TRAINED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED
T.DOC.DIS	✓						✓	✓												
T.DOC.ALT		✓					✓	✓												
T.FUNC.ALT			✓				✓	✓												
T.PROT.ALT				✓			✓	✓												
T.CONF.DIS					✓		✓	✓												
T.CONF.ALT						✓	✓	✓												
P.USER.AUTHORIZATION							✓	✓												
P.SOFTWARE.VERIFICATION									✓											
P.AUDIT.LOGGING										✓	✓	✓	✓	✓	✓					
P.INTERFACE.MANAGEMENT																✓		✓		
A.ACCESS.MANAGED																	✓			
A.USER.TRAINING																		✓		
A.ADMIN.TRAINING																			✓	
A.ADMIN.TRUST																				✓

Table 22: Sufficiency of Security Objectives

Threats, Policies, and Assumptions	Summary	Objectives and Rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.DOC.ALT	User Document Data may be altered by unauthorized persons	O.DOC.NO_ALT protects D.DOC from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.FUNC.ALT	User Function Data may be altered by unauthorized persons	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons	O.PROT.NO_ALT protects D.PROT from unauthorized alteration
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons	O.CONF.NO_ALT protects D.CONF from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
P.USER.AUTHORIZATION	Users will be authorized to use the TOE	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization

Threats, Policies, and Assumptions	Summary	Objectives and Rationale
P.SOFTWARE.VERIFICATION	Procedures will exist to self-verify executable code in the TSF	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF.
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events, and prevents unauthorized disclosure or alteration
		O.AUDIT_STORAGE.PROTEDTED protects audit records from unauthorized access, deletion, and modification.
		O.AUDIT_ACCESS.AUTHORIZED allows the access of audit records only by authorized persons,
		OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion and modification,
		OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of the TOE Owner to provide appropriate access to exported audit records.
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed.
P.INTERFACAE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies.
		OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE.
A.ADMIN.TRAINING	Administrators are aware of and trained to follow security policies and procedures	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes	OE.ADMIN.TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	TOE Users are aware of and trained to follow security policies and procedures	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate user training.

5 Extended Component Definition

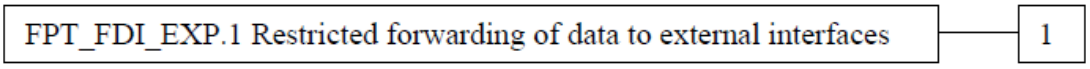
5.1 FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:



FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

The following actions could be considered for the management functions in FMT:

a) Definition of the role(s) that are allowed to perform the management activities

b) Management of the conditions under which direct forwarding can be allowed by an administrative role

c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the ST:

There are no auditable events foreseen.

Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the

data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or the FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this led the authors to define a new family with just one member.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [assignment: *list of external interfaces*] from being forwarded without further processing by the TSF to [assignment: *list of external interfaces*].

6 Security Requirements

This Security Target defines the subjects (user), objects, operations, security attributes, external entities, and other conditions used in the security requirements as follows:

Users

Users are entities that are external to the TOE and interact with the TOE. There may be two types of Users: Normal and Administrator.

Table 23: Users

Designation		Definition
U.USER		Any authorized User
	U.NORMAL	A User who is authorized to perform User Document Data processing functions of the TOE
	U.ADMINISTRATOR	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Objects (Assets)

Objects are passive entities in the TOE, that contain or receive information, and upon which Subjects perform Operations. In this ST, Objects are equivalent to TOE Assets. There are three types of Objects: User Data, TSF Data, and Functions.

User Data

User Data are data created by and for Users and do not affect the operation of the TOE Security Functionality (TSF). This type of data is composed of two objects: User Document Data and User Function Data.

Table 24: User Data

Designation	Definition
D.DOC	User Document Data consist of the information contained in a user's document. This includes the original document itself (in either hardcopy or electronic form), image data, or residually-stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

TSF Data

TSF Data are data created by and for the TOE and that might affect the operation of the TOE. This type of data is composed of two objects: TSF Protected Data and TSF Confidential Data.

Table 25: TSF Data

Designation	Definition
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE but for which disclosure is acceptable.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

A list of the TSF data used in this TOE is given in Table 26.

Table 26: TSF Data

TSF Data	D.CONF	D.PROT
Kerberos Server Configuration	✓	
SMB Server Configuration	✓	
LDAP Server Configuration	✓	
FTP Server Configuration	✓	
SMTP Server Configuration	✓	
Address Books		✓
Log- in Identification Configuration (Password Expiration Period, Password Policy)	✓	
Log in Restriction Configuration (Minutes, No. of attempt, Lock period)	✓	
Log out Policy (Logout Time)	✓	
User Role (Authority)		✓
External User Role		✓
User Profile (ID, Group)		✓
User Profile (Password)	✓	
Group Profile (Name, Role)		✓
Audit Log Data	✓	

Network Protocol and Port Configuration		✓
Digital Certificate	✓	
IP Filtering Address	✓	
MAC Filtering Address	✓	
Image Overwrite Configuration	✓	
Encryption Key Data	✓	
Scan/Fax/SMB/E-mail destination lists	✓	
Job status log		✓
Credentials for accessing external devices (LDAP, SMB, Kerberos, FTP, E-mail)	✓	

Functions

Functions perform processing, storage, and transmission of data that may be present in the MFP products.

Table 27: Functions

	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

Attributes

When a function is performing processing, storage, or transmission of data, the identity of the function is associated with that particular data as a security attribute. This attribute in the TOE model makes it possible to distinguish differences in Security Functional Requirements that depend on the function being performed.

Table 28: Attributes

Designation	Definition
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

Operations

Operations are a specific type of action performed by a Subject on an Object. In this ST, five types of operations are considered: those that result in disclosure of information (Read), those that result in alteration of information (Create, Modify, Delete), and those that invoke a function (Execute).

External Entities

Table 29: External Entities

Designation	Definition
Authentication Server	The authentication servers (Kerberos, LDAP and SMB servers) identify and authenticate U.NORMAL if remote authentication mode is enabled
Storage Server	The TOE sends received fax and scan data to the storage servers (FTP,SMB)

Channels

Channels are the mechanisms through which data can be transferred into and out of the TOE.

- **Private Medium Interface**: mechanisms for exchanging information that use (1) wired or wireless electronic methods over a communications medium which, in conventional practice, is not accessed by multiple simultaneous Users; or, (2) Operator Panel and displays that are part of the TOE. It is an input-output channel.
- **Shared Media Interface**: Mechanism for transmitting or receiving data that uses wired or wireless network or non-network electronic methods over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users.
- **Original Document Handler**: mechanisms for transferring User Document Data into the TOE in hardcopy form. It is an input channel.
- **Hardcopy Output Handler**: mechanisms for transferring User Document Data out of the TOE in hardcopy form. It is an output channel.

6.1 Security Functional Requirements

The security functional requirements defined in this Security Target conform to the PP. Additional security functional requirements in this ST not defined in the PP are based on the functional requirements in Part 2 of the Common Criteria.

Table 30 summarizes the security functional requirements defined by this ST.

Table 30: Security Functional Requirements

Class	Component		Defined in
Security Audit	FAU_GEN.1	Audit data generation	PP
	FAU_GEN.2	User identity association	PP
	FAU_SAR.1	Audit review	This ST additionally
	FAU_SAR.2	Restricted audit review	This ST additionally
	FAU_STG.1	Protected audit trail storage	This ST additionally
	FAU_STG.4	Prevention of audit data loss	This ST additionally
Cryptographic Support	FCS_CKM.1	Cryptographic key generation	This ST additionally
	FCS_CKM.4	Cryptographic key destruction	This ST additionally
	FCS_COP.1	Cryptographic operation	This ST additionally
User Data Protection	FDP_ACC.1(1)(2)(3)	Subset access control	PP PRT package SCN package CPY package FAX package
	FDP_ACF.1(1)(2)(3)	Security attribute based access control	PP PRT package SCN package CPY package FAX package
	FDP_IFC.2	Complete information flow control	This ST additionally
	FDP_IFF.1	Simple security attributes	This ST additionally
	FDP_RIP.1	Subset residual information protection	PP
Identification and Authentication	FIA_AFL.1	Authentication failure handling	This ST additionally
	FIA_ATD.1	User attribute definition	PP
	FIA_UAU.1	Timing of authentication	PP
	FIA_UAU.7	Protected authentication feedback	This ST additionally

Class	Component		Defined in
	FIA_UID.1	Timing of identification	PP
	FIA_USB.1	User-subject binding	PP
Security Management	FMT_MSA.1(1)(2)	Management of security attributes	PP
	FMT_MSA.1(3)(4)	Management of security attributes	This ST additionally
	FMT_MSA.3(1)(2)	Static attribute initialization	PP
	FMT_MSA.3(3)(4)	Static attribute initialization	This ST additionally
	FMT_MTD.1	Management of TSF data	PP
	FMT_SMF.1	Specification of management functions	PP
	FMT_SMR.1	Security roles	PP
Protection of the TSF	FPT_STM.1	Reliable time stamps	PP
	FPT_TST.1	TSF testing	PP
	FPT_FDI_EXP.1	Restricted forwarding of data to external interfaces	PP SMI package
TOE Access	FTA_SSL.3	TSF-initiated termination	PP
Trusted paths/channels	FTP_ITC.1	Inter-TSF trusted channel	PP SMI package

6.1.1 Class FAU: Security Audit

6.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the *not specified* level of audit; and
- **All Auditable Events as each is defined for its Audit Level (if one is specified) for the**

Relevant SFR in Table 31; [The Auditable Events specified in Table 31 below].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 31: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [none].

Table 31: Audit data

Auditable Events	Relevant SFR	Audit Level	Additional Information
Job completion	FDP_ACF.1(1)(2)	Not specified	Type of job
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU. 1	Basic	None required
Both successful and unsuccessful use of the identification mechanism	FIA_UID. 1	Basic	Attempted user identity, if available
Termination of an interactive session by the session termination mechanism	FTA_SSL.3	Minimum	None required
Use of the management functions	FMT_SMF.1	Minimum	None required
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required
Log data access	FMT_MTD.1	Not specified	None required
Manual Image Overwrite	FDP_RIP.1	Not specified	None required
Execution of the TSF self tests and the results of the tests	FPT_TST.1	Not specified	None required
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required
Change to the time	FPT_STM.1	Minimum	None required

6.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [U.ADMINISTRATOR] with the capability to read [all of audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

6.1.1.6 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [none] if the audit trail is full.

6.1.2 Class FCS: Cryptographic support

6.1.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [random key generation method] and specified cryptographic key sizes [256-bit] that meet the following: [None].

6.1.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or
FCS_CKM.1Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [an overwrite updates a cryptographic key by overwriting previous cryptographic key with newly generated cryptographic key] that meets the following: [None].

6.1.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or
FCS_CKM.1Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [encryption/decryption of HDD] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [256-bit] that meet the following: [FIPS PUB 197].

6.1.3 Class FDP: User data protection

6.1.3.1 FDP_ACC.1(1) Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the **Common Access Control SFP in Table 32** on **the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 32**.

6.1.3.2 FDP_ACC.1(2) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the **TOE Function Access Control SFP in Table 33** on **users as subjects, TOE functions as objects, and the right to use the functions as operations.**

6.1.3.3 FDP_ACC.1(3) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(3) The TSF shall enforce the **Service (PRT, SCN, CPY, FAX) Access Control SFP in Table 34** on **the list of users as subjects, TOE Functions as objects, and the right to use the functions as operations among subjects and objects covered by the Service (PRT, SCN, CPY, FAX) Access Control SFP in Table 34**.

6.1.3.4 FDP_ACF.1(1) Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1(1) The TSF shall enforce the **Common Access Control SFP in Table 32** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 32, and for each, the indicated security attributes in Table 32**.

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the Common Access Control SFP in Table 32 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects**.

FDP_ACF.1.3(1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].

Table 32: Common Access Control SFP

Access Control SFP	Object	Attribute (Object)	Operation(s)	Subject	Security Attribute	Access control rule
Common Access Control	D.DOC	+PRT +SCN +FAXIN +FAXOUT	Delete	U.NORMAL	User ID	Denied, except for his/her own documents
	D.FUNC	+PRT +SCN +FAXIN +FAXOUT	Modify, Delete	U.NORMAL	User ID	Denied, except for his/her own function data

6.1.3.5 FDP_ACF.1(2) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(2) The TSF shall enforce the **TOE Function Access Control SFP in Table 33** to objects based on the following: **user and** [the list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP in Table 33].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *the user is explicitly authorized by U.ADMINISTRATOR to use a function*

FDP_ACF.1.3(2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **the user acts in the role U.ADMINISTRATOR**: [none].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the [none].

Table 33: TOE Function Access Control SFP

Access Control SFP	Object	Attribute (Object)	Operation(s)	Subject	Security Attribute	Access control rule
TOE Function Access Control	F.PRT	Permission	Execution	U.NORMAL	User ID, User Role, User group ID	Denied, except for the U.NORMAL explicitly authorized by U.ADMINISTRATOR to use a function
	F.SCN					
	F.CPY					
	F.FAX					

6.1.3.6 FDP_ACF.1(3) Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1(3) The TSF shall enforce the **Service (PRT, SCN, CPY, FAX) Access Control SFP in Table 34** to objects based on the following: **the list of subjects and objects controlled under the Service (PRT, SCN, CPY, FAX) Access Control SFP in Table 34, and for each, the indicated security attributes in Table 34..**

FDP_ACF.1.2(3) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the Service (PRT, SCN, CPY, FAX) Access Control SFP in Table 34 governing access among Users and controlled objects using controlled operations on controlled objects.**

FDP_ACF.1.3(3) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [None].

FDP_ACF.1.4(3) The TSF shall explicitly deny access of subjects to objects based on the [None].

Table 34: Service (PRT, SCN, CPY, FAX) Access Control SFP

Access Control SFP	Object	Attribute (Object)	Operation(s)	Subject	Security Attribute	Access control rule
PRT Access Control	D.DOC	+PRT	Read	U.NORMAL	User ID	Denied, except for his/her own documents
SCN Access Control	D.DOC	+SCN	Read	U.NORMAL	User ID	Denied, except for his/her own documents
FAX Access Control	D.DOC	+FAXIN +FAXOUT	Read	U.NORMAL	User ID	Denied, except for his/her own documents
CPY Access Control	D.DOC	+CPY	Read	Not specify any access control restriction		

Application Note :

Operation(s)	Attribute (Object)	Description
Read	+PRT	Refers (as a minimum) to the release of pending hardcopy output to a Hardcopy Output Handler. It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.
	+SCN	Refers (as a minimum) to the transmission of User Document Data through an Interface to a destination of the user's choice. It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.
	+ CPY	Refers to the release of pending hardcopy output to a Hardcopy Output Handler. It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.
	+FAXIN +FAXOUT	Refers (as a minimum) to the release of pending hardcopy output to a Hardcopy Output Handler for receiving faxes (+FAXIN) and to the transmission of User Document Data through an Interface for sending or receiving faxes (+FAXOUT or +FAXIN). It may also be used to refer to previewing documents on a display device, if such a feature is present in a conforming TOE.

6.1.3.7 FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [NAC Policy SFP] on [subjects: External IT entities, information: network packet] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.1.3.8 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [NAC Policy SFP] based on the following types of subject and information security attributes: [security attribute of subject (External IT entities): IP/MAC Address, security attribute of information (network packet): Service Port Number].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) The source IP/MAC address should not match the IP/MAC filtering rule (blocking list) registered by U.ADMINISTRATOR
b) The service port number of information should match the service port number registered by U.ADMINISTRATOR]

FDP_IFF.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.9 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 *deallocation of the resource from* the following objects: **D.DOC, [D.FUNC]**.

6.1.4 Class FIA: Identification and authentication

6.1.4.1 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 *[3]* unsuccessful authentication attempts occur related to [U.ADMINISTRATOR and U.NORMAL authentication]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed* the TSF shall [lockout the U.ADMINISTRATOR and U.NORMAL's login for a period of 5 minutes].

6.1.4.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components
Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User ID, Group ID, and User Role].

6.1.4.3 FIA_UAU.1 User authentication before any action

Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [incoming faxes, and usage of the menus that has no relation with security in browser (Device Information, Supplies Information, Options and Capabilities, Usage Counters, Address Book, Maintenance Information, and Job Status)] on behalf of the user to be performed before the user is authenticated.

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

Application Note: U.ADMINISTRATOR authentication is performed internally by the TOE. However, U.NORMAL authentication is performed internally by the TOE or externally by authentication servers (SMB, Kerberos, LDAP server) in the operational environment of the TOE.

6.1.4.4 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [obscured feedback] to the user while the authentication is in progress**.**

6.1.4.5 FIA_UID.1 Timing of identification

Hierarchical to: No other components
Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [Incoming faxes, and usage of the menus that has no relation with security (Device Information, Supplies Information, Options and Capabilities, Usage Counters, Address Book, Maintenance Information, and Job Status)] on behalf of the user to be performed before the user is identified.

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

Application Note: U.ADMINISTRATOR identification is performed internally by the TOE. However, U.NORMAL identification is performed internally by the TOE or externally by identification servers (SMB, Kerberos, LDAP server) in the operational environment of the TOE.

6.1.4.6 FIA_USB.1 User-subject binding

Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [User ID, Group ID, and User Role].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [subjects will be assigned the security attributes of the U.USER that they are acting on behalf of the users].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [the security attributes do not change during a session].

6.1.5 Class FMT: Security management

6.1.5.1 FMT_MSA.1(1) Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(1) The TSF shall enforce the **Common access control SFP in Table 32**, [none**]** to restrict the ability to *query, delete, [create]* the security attributes [list of security attributes in Table 32] to [U.ADMINISTRATOR].

6.1.5.2 FMT_MSA.1(2) Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(2) The TSF shall enforce the **TOE Function Access Control SFP in Table 33**, [none] to restrict the ability to *query, modify, delete, [create]* the security attributes [list of security attributes in Table 33] to [U.ADMINISTRATOR].

6.1.5.3 FMT_MSA.1(3) Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(3) The TSF shall enforce the [Service (PRN, SCN, CPY, FAX) Access Control SFP in Table 34] to restrict the ability to *query, delete, [create]* the security attributes [list of security attributes in Table 34] to [U.ADMINISTRATOR].

6.1.5.4 FMT_MSA.1(4) Management of security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(4) The TSF shall enforce the [NAC Policy**]** to restrict the ability to *query, modify, delete, [add]* the security attributes [list of security attributes in Table 35] to [U.ADMINISTRATOR].

Table 35: Management of Security Attributes

Security Attributes	Selection Operation			
	query	modify	delete	[add]
MAC Address	○	○	○	○
IP Address	○	○	○	○
Protocol	○	○		
Port	○	○		

6.1.5.5 FMT_MSA.3(1) Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1(1) The TSF shall enforce the **Common Access Control SFP in Table 32**, [none] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.6 FMT_MSA.3(2) Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the **TOE Function Access Control SFP in Table 33**, [none] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.7 FMT_MSA.3(3) Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(3) The TSF shall enforce the [Service (PRN, SCN, CPY, FAX) Access Control SFP in Table 34] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(3) The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.8 FMT_MSA.3(4) Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(4) The TSF shall enforce the [NAC Policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(4) The TSF shall allow the [none] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.9 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query, modify, delete, [add]* the [list of TSF data in Table 36] to [the authorized identified roles in Table 36]

Table 36: Management of TSF data

TSF data	Selection Operation				the authorized identified roles
	query	modify	delete	[add]	
Kerberos Server Configuration	○	○	○	○	U.ADMINISTRATOR
SMB Server Configuration	○	○	○	○	
LDAP Server Configuration	○	○	○	○	
FTP Server Configuration	○	○			
SMTP Server Configuration	○	○			
Address Book	○	○	○	○	
Log in Identification	○	○			
Log in Restriction	○				
Log out Policy	○	○			
User Role (Authority)	○	○	○	○	
External User Role	○	○	○	○	
User Profile (Id, Password, Group)	○	○	○	○	
Group Profile (Name, Role)	○	○	○	○	
Audit Log Data	○				
Network Protocol and Port Configuration	○	○			
Digital Certificate	○	○	○	○	
IP filtering Address	○	○	○	○	
MAC filtering Address	○	○	○	○	
Image Overwrite configuration	○	○			
Application Management	○	○	○	○	
Password(U.NORMAL)		○			U.NORMAL
Network Protocol and Port Configuration	○				

6.1.5.10 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 management functions: [the list of Management Functions in Table 37].

Table 37: Management Functions

Management Functions
Management of Audit data (review)
Management of Common Access Control rules
Management of TOE Function Access Control rules
Management of Service Access Control rules
Management of MAC filtering rules
Management of IP filtering rules

Management Functions
Management of Protocol/Port information flow control rules
Management of Image overwrite function
Management of User attributes (User ID, User Name, Password, Email, Fax No, and Group ID)
Management of security roles (User Group ID)
Management of TSF testing (initiation)
Management of fax forward functions

6.1.5.11 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 U.ADMINISTRATOR, U.NORMAL, *[none]*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles, except for the role "Nobody" to which no user shall be associated.

6.1.6 Class FPT: Protection of the TSF

6.1.6.1 FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **any external Interface** from being forwarded without further processing by the TSF to **any Shared-medium Interface**.

6.1.6.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note: TOE can only use internal time-stamps.

6.1.6.3 FPT_TST.1 TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up* to demonstrate the correct operation of *[HDD Encryption Function]***.**

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *[Encryption Key data]*.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *[stored TSF executable code].*.

6.1.7 Class FTA: TOE access

6.1.7.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [3 minutes of U.ADMINISTRATOR and U.NORMAL inactivity].

6.1.8 Class FTP: Trusted path/channels

6.1.8.1 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF, another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface**.

6.2 Security Assurance Requirements

Security assurance requirements (SAR) defined in this document consists of assurance component in Common Criteria for Information Technology Security Evaluation, Part 3. The Evaluation Assurance Levels (EALs) is EAL2 augmented by ALC_FLR.2. Following table shows the summary of assurance components. The SARs are not iterated or refined from Common Criteria for Information Technology Security Evaluation Part 3.

Table 38: Security Assurance Requirements (EAL2 augmented by ALC_FLR.2)

Assurance Class	Assurance components	
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures

Assurance Class	Assurance components	
	ALC_FLR.2	Flaw reporting procedures (augmentation of EAL3)
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.2.1 Class ASE: Security Target evaluation

6.2.1.1 ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.1.2 ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or non-conformance to these elements can be demonstrated.

Evaluator action elements:

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

6.2.1.3 ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview, and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

6.2.1.4 ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives' rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.1.5 ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements' rationale.

Content and presentation elements:

ASE_REQ.2.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C	All operations shall be performed correctly.
ASE_REQ.2.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C	The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C	The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C	The security requirements rationale shall explain why the SARs were chosen.
ASE_REQ.2.9C	The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.1.6 ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

ASE_SPD.1.1D	The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C	The security problem definition shall describe the threats.
ASE_SPD.1.2C	All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C	The security problem definition shall describe the OSPs.
ASE_SPD.1.4C	The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.1.7 ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.2 Class ADV: Development

6.2.2.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2.2 ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describethe SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.2.3 ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarise the SFR-enforcing behaviour of the SFR enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

Evaluator action elements:

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3 Class AGD: Guidance documents

6.2.3.1 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.4 Class ALC: Life-cycle support

6.2.4.1 ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system. Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labelled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.2 ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.3 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.4 ALC_FLR.2 Flaw reporting procedures

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.2.1D The developer shall document and provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.5 Class ATE: Tests

6.2.5.1 ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.5.2 ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results, and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.5.3 ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Class AVA: Vulnerability assessment

6.2.6.1 AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures.

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.3 Security Requirements Rationale

This section demonstrates that the security requirements are satisfied with the security objectives for the TOE.

6.3.1 Security Functional Requirements' Rationale

The security functional requirements' rationale shall demonstrate the following:

- Each security objective is addressed based on at least one security functional requirement.
- Each security functional requirement addresses at least one security objective.

Bold typeface items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 39: Completeness of Security Objectives

Security Functional Requirement	TOE Security Function											
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.INTERFACE.MANAGED
FAU_GEN.1									**P**			
FAU_GEN.2									**P**			
FAU_SAR.1											**P**	
FAU_SAR.2											**P**	
FAU_STG.1										**P**		
FAU_STG.4										**P**		
FCS_CKM.1	S	S	S	S	S	S						
FCS_CKM.4	S	S	S	S	S	S						
FCS_COP.1	**P**	**P**	**P**	**P**	**P**	**P**						
FDP_ACC.1(1)	**P**	**P**	**P**									
FDP_ACC.1(2)							**P**					
FDP_ACC.1(3)	**P**	**P**	**P**									
FDP_ACF.1(1)	S	S	S									
FDP_ACF.1(2)							S					
FDP_ACF.1(3)	S	S	S									
FDP_IFC.2												**P**
FDP_IFF.1												S
FDP_RIP.1	**P**											
FIA_AFL.1							S					
FIA_ATD.1							S					
FIA_UAU.1							**P**					**P**
FIA_UAU.7							S					
FIA_UID.1	S	S	S	S	S	S	**P**		S			**P**
FIA_USB.1							**P**					
FMT_MSA.1(1)	S	S	S									
FMT_MSA.1(2)							S					
FMT_MSA.1(3)	S	S	S									
FMT_MSA.1(4)												S
FMT_MSA.3(1)	S	S	S									
FMT_MSA.3(2)							S					
FMT_MSA.3(3)	S	S	S									
FMT_MSA.3(4)												S
FMT_MTD.1				**P**	**P**	**P**						
FMT_SMF.1	S	S	S	S	S	S						
FMT_SMR.1	S	S	S	S	S	S	S					
FPT_FDI_EXP.1												**P**
FPT_STM.1									S			
FPT_TST.1								**P**				
FTA_SSL.3							**P**					**P**
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**						

Table 40: Security Requirements Rationale

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS O.DOC.NO_ALT O.FUNC.NO_ALT	Protection of User Data from unauthorized disclosure or alteration	FDP_ACC.1(1)(3)	Enforces protection by establishing an access control policy.
		FDP_ACF.1(1)(3)	Supports the access control policy by providing an access control function.
		FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MSA.1(1)(3)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(1)(3)	Supports access control and information flow control function by enforcing control of security attribute defaults.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
		FCS_CKM.1	Supports cryptographic operation by requiring the key generation for HDD encryption..
		FCS_CKM.4	Supports cryptographic operation by requiring the key destruction for HDD encryption..
		FCS_COP.1	Enforces protection by requiring the cryptographic operation for HDD encryption.
		FTP_ITC.1	Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	FDP_RIP.1	Enforces protection by making residual data unavailable.
O.PROT.NO_ALT O.CONF.NO_DIS O.CONF.NO_ALT	Protection of TSF Data from Unauthorized disclosure or alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MTD.1	Enforces protection by restricting access.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security

Objectives	Description	SFRs	Purpose
			roles.
		FCS_CKM.1	Supports cryptographic operation by requiring the key generation for HDD encryption..
		FCS_CKM.4	Supports cryptographic operation by requiring the key destruction for HDD encryption..
		FCS_COP.1	Enforces protection by requiring the cryptographic operation for HDD encryption.
		FTP_ITC.1	Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces
O.USER. AUTHORIZED	Authorization of Normal Users and Administrators to use the TOE	FDP_ACC.1(2)	Enforces authorization by establishing an access control policy.
		FDP_ACF.1(2)	Supports the access control policy by providing an access control function.
		FIA_AFL.1	Supports authentication by handling authentication failure.
		FIA_ATD.1	Supports authorization by associating security attributes with users.
		FIA_UAU.1	Enforces authorization by requiring user authentication.
		FIA_UAU.7	Supports authorization by protecting authentication feedback.
		FIA_UID.1	Enforces authorization by requiring user identification.
		FIA_USB.1	Enforces authorization by distinguishing subject security attributes associated with user roles.
		FMT_MSA.1(2)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(2)	Supports access control and information flow control function by enforcing control of security attribute defaults.
		FMT_SMR.1	Supports authorization by requiring security roles.
		FTA_SSL.3	Enforces authorization by terminating inactive sessions.
O.INTERFACE. MANAGED	Management of external interfaces	FDP_IFC.2	Enforces management by establishing a network access control policy.
		FDP_IFF.1	Supports the network access control policy by providing an information flow control

Objectives	Description	SFRs	Purpose
			function.
		FIA_UAU.1	Enforces management of external interfaces by requiring user authentication.
		FIA_UID.1	Enforces management of external interfaces by requiring user identification.
		FMT_MSA.1(4)	Supports information flow control function by enforcing control of security attribute.
		FMT_MSA.3(4)	Supports information flow control function by enforcing control of security attribute defaults.
		FTA_SSL.3	Enforces management of external interfaces by terminating inactive sessions.
		FPT_FDI_EXP.1	Enforces management of external interfaces by requiring (as needed) administrator control of data transmission from external Interfaces to Shared-medium Interfaces.
O.SOFTWARE. VERIFIED	Verification of software integrity	FPT_TST.1	Enforces verification of software by requiring self-tests.
O.AUDIT.LOGGED	Logging and authorized access to audit events	FAU_GEN.1	Enforces audit policies by requiring logging of relevant events.
		FAU_GEN.2	Enforces audit policies by requiring logging of information associated with audited events.
		FIA_UID.1	Supports audit policies by associating a user's identity with events.
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.
O.AUDIT_STORAGE.PROTECTED	Protected audit trail storage and prevention of audit data loss	FAU_STG.1	Enforces protection of audit trail storage by preventing unauthorized modifications to the stored audit records in the audit trail.
		FAU_STG.4	Enforces prevention of audit data loss by overwriting the oldest stored audit records.
O.AUDIT_ACCESS. AUTHORIZED	Access control of audit records only by authorized persons	FAU_SAR.1	Enforces the audit review function by providing authorized U.ADMINISTRATOR with the ability to read all of audit information from the audit records.
		FAU_SAR.2	Enforces restriction of the audit review function by prohibiting

Objectives	Description	SFRs	Purpose
			all users read access to the audit records, except those users that have been granted access specifically.

6.3.2 Security Assurance Requirements Rationale

Security assurance requirements of this security target conform to IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600™ - 2008 Operational Environment B (IEEE Std. 2600.2-2009) Version 1.0.

This Security Target has been developed for Hardcopy Devices used in restrictive commercial information processing environments that require a relatively high level of document security, operational accountability, and information assurance. The TOE environment will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any non-volatile storage without disassembling the TOE, except for removable non-volatile storage devices, where protection of User and TSF Data are provided when such devices are removed from the TOE environment. Agents have limited or no means of infiltrating the TOE with code to effect a change, and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.

EAL 2 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

6.4 Dependency Rationale

6.4.1 SFR Dependencies

Table 41: Dependencies on the TOE Security Functional Components

No.	TOE Security Functional Requirements	Claimed Dependencies	Dependencies Satisfied in ST (No.)
1	FAU_GEN.1	FPT_STM.1	37
2	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	1, 23
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_STG.1	FAU_GEN.1	1
6	FAU_STG.4	FAU_STG.1	5

7	FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	8, 9
8	FCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	7
9	FCS_COP.1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	7, 8
10	FDP_ACC.1(1)	FDP_ACF.1(1)	13
11	FDP_ACC.1(2)	FDP_ACF.1(2)	14
12	FDP_ACC.1(3)	FDP_ACF.1(3)	15
13	FDP_ACF.1(1)	FDP_ACC.1(1), FMT_MSA.3(1)	10, 29
14	FDP_ACF.1(2)	FDP_ACC.1(2), FMT_MSA.3(2)	11, 30
15	FDP_ACF.1(3)	FDP_ACC.1 (3), FMT_MSA.3(3)	11, 31
16	FDP_IFC.2	FDP_IFF.1	17
17	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3(4)	16, 32
18	FDP_RIP.1	-	-
19	FIA_AFL.1	FIA_UAU.1	21
20	FIA_ATD.1	-	-
21	FIA_UAU.1	FIA_UID.1	23
22	FIA_UAU.7	FIA_UAU.1	21
23	FIA_UID.1	FIA_UAU.1	21
24	FIA_USB.1	FIA_ATD.1	20
25	FMT_MSA.1(1)	[FDP_ACC.1(1) or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	10, 34, 35
26	FMT_MSA.1(2)	[FDP_ACC.1(2) or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	11, 34, 35
27	FMT_MSA.1(3)	[FDP_ACC.1(3) or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	12, 34, 35

28	FMT_MSA.1(4)	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	16, 34, 35
29	FMT_MSA.3(1)	FMT_MSA.1(1) FMT_SMR.1	25, 34
30	FMT_MSA.3(2)	FMT_MSA.1(2) FMT_SMR.1	26, 34
31	FMT_MSA.3(3)	FMT_MSA.1(3) FMT_SMR.1	27, 34
32	FMT_MSA.3(4)	FMT_MSA.1(4) FMT_SMR.1	28, 34
33	FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	34, 35
34	FMT_SMF.1	-	-
35	FMT_SMR.1	FIA_UID.1	23
36	FPT_FDI_EXP.1	FMT_SMF.1, FMT_SMR.1	34, 35
37	FPT_STM.1	-	-
38	FPT_TST.1	-	-
39	FTA_SSL.3	-	-
40	FTP_ITC.1	-	-

6.4.2 SAR Dependencies

The dependency of each assurance package (EAL2) provided by the CC is already satisfied.

ALC_FLR.2 added to the assurance package (EAL2) has no dependency relationship with others, so it is satisfied.

7 TOE Summary Specification

7.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 6.1

- Identification & Authentication (TSF_FIA)
- Network Access Control (TSF_NAC)
- Security Management (TSF_FMT)
- Security Audit (TSF_FAU)
- Image Overwrite (TSF_IOW)
- Data Encryption (TSF_NVE)
- Fax Data Control (TSF_FLW)
- Self Testing (TSF_STE)
- Secure Communication (TSF_SCO)

7.1.1 Identification & Authentication (TSF_FIA)

Relevant SFR: FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_USB.1, FTA_SSL.3, FDP_ACC.1(1)(2)(3), FDP_ACF.1(1)(2)(3)

U. ADMINISTRATOR can select the authentication method among basic authentication, application authentication, and device authentication. If the device authentication selected, it requests U.USER to login before using all device applications. In this case, U.USER cannot use any application without logging in.

U. ADMINISTRATOR can select the login identification method.

- Local authentication is performed internally by the TOE (for U.USER).

- Remote authentication is performed externally by authentication servers (SMB, Kerberos, LDAP server) in the operational environment of the TOE (only for U.NORMAL).

U.USER should be identified and authenticated by entering as ID and Password to access the TOE's functions.

The TOE restricted the number of consecutive invalid authentication attempts as 3 times. When the number of consecutive invalid authentication attempts has exceeded the limit number within 3 minutes, the account will be locked for 5 minutes. If U.USER is idle for 3 minutes, the mutual session will be terminated automatically.

The TOE can restrict U.USER from accessing the machine or application. U. ADMINISTRATOR can also give specific permission for U.USER to only use certain features of the machine based on User ID, Group ID.

The TOE does not display the entered U.USER's login password while the authentication is in progress. The TOE displays a sequence of '*' or '•' characters whose length is the same as that of the entered.

If U.USER is identified and authenticated, the use of the TOE by the U.USER is allowed as the identified User Role. The User Role assigned to the User ID and User group ID at login will be maintained during a session.

U.ADMINISTRATOR can make periodical password expiration compulsory. If password expiration period is enabled, the default period value is 90 days and can be set to 1-180 day(s).

TOE enforces the Common Access Control SFP, TOE Function Access Control SFP, and Service (PRT, SCN, CPY, FAX) Access Control SFP based on the User ID, User Role and User Group ID when U.NORMAL performs read/delete/modify operations on the data (D.DOC, D.FUNC) owned by U.NORMAL or when U.NORMAL accesses print/scan/copy/fax functions offered by the MFP.

- Common Access Control SFP

U.NORMAL is able to perform modify & delete operations on the objects (D.FUNC) owned by his/her own when doing print/scan/fax-in/fax-out job, and U.NORMAL is able to perform delete operation on the objects (D.DOC) owned by his/her own. In other words, U.NORAL is denied to perform the operations on the object except for his/her own documents.

- TOE Function Access Control SFP

Base on security attribute (User ID, User Role, User Group ID), U.NORMAL is able to execute the printing/scanning/copying/faxing functions explicitly authorized by U.ADMINISTRATOR to use the function.

- Service (PRT, SCN, CPY, FAX) Access Control SFP

U.NORMAL is able to perform read operation on the objects (D.DOC) owned by his/her own when doing print/scan/fax-in/fax-out job. In other words, U.NORAL is denied to perform the operation on the object except for his/her own documents. However, there is no access control restriction associated with a copy job.

7.1.2 Network Access Control (TSF_NAC)

Relevant SFR: FDP_IFC.2, FDP_IFF.1, FMT_MSA.1(4), FMT_MSA.3(4)

The TOE has a network interface to communicate through the network. The TOE can send/receive data and configuration information.

The TOE enforces the network access control policy on external IT entities for the network packet and all operation that cause that information to flow to and from external IT entities.

The TOE provides two network access control policies.

- Protocol/Port control:

1) Network protocols: Raw TCP/IP Printing, LPR/LPD, HTTP, WINS, SNMPv1/v2, HTTPS, DDNS, WSD, SNMPv3 Protocol

2) Service port number: Logical channel in the range of 1 to 65535

The TOE only allows access from authorized ports, connection using authorized protocol services by configuring the port number, and enabling/disabling network services accessing the MFP system. The default values of protocol/port are “disabled”. Therefore, all packets will be denied until U.ADMINISTRATOR’s changes. Only U.ADMINISTRATOR can query and modify these functions.

- IP and MAC Filtering:

U.ADMINISTRATOR can manage (query, modify, delete and add) filtering rules for IP address and MAC address.

U.ADMINISTRATOR can register specific IP/MAC filtering rules.

All packets are allowed if there is no IP and MAC filtering rule registered by U.ADMINISTRATOR.

1) IP filtering

All packets are only allowed as IP filtering rule registered by U.ADMINISTRATOR

U.ADMINISTRATOR can register priority to perform a filtering and services to accept.

(Services to accept: Raw TCP/IP Printing, LPR/LPD, HTTP, IPP, SNMP / Priority: 1~9)

2) MAC filtering

All packets via MAC addresses registered by U.ADMINISTRATOR are not allowed

In summary, all packets are denied if one of the below conditions are not satisfied;

a) The source IP /MAC address should not match the IP/MAC filtering rule (blocking list) registered by U.ADMINISTRATOR
b) The service port number of information should match the service port number registered by U.ADMINISTRATOR]

7.1.3 Security Management (TSF_FMT)

Relevant SFR: FMT_MSA.1(1)(2)(3)(4), FMT_MSA.3(1)(2)(3)(4), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

The TOE accomplishes security management for the security function, TSF data, and security attribute. Only U.ADMINISTRATOR can manage the security functions after identification and authentication.

The TOE shall restrict the ability to query, modify, delete, and add the security attributes accessible to U.ADMINISTRATOR.

Table 42 : Management of Security Attributes

Security Attributes	Selection Operation			
	query	modify	delete	[add]
MAC Address	○	○	○	○
IP Address	○	○	○	○

Protocol (to deny)	○	○		
Port	○	○		
User Role, User ID, User group ID	○	○	○	○

The TOE shall restrict the ability to query, modify, delete, and add the TSF data to the authorized identified roles.

Table 43: Management of TSF data

TSF data	Selection Operation				the authorized identified roles
	query	modify	delete	[add]	
Kerberos Server Configuration	○	○	○	○	U.ADMINISTRATOR
SMB Server Configuration	○	○	○	○	
LDAP Server Configuration	○	○	○	○	
FTP Server Configuration	○	○			
SMTP Server Configuration	○	○			
Address Book	○	○	○	○	
Log in Identification	○	○			
Log in Restriction	○				
Log out Policy	○	○			
User Role (Authority)	○	○	○	○	
External User Role	○	○	○	○	
User Profile (Id, Password, Group)	○	○	○	○	
Group Profile (Name, Role)	○	○	○	○	
Audit Log Data	○				
Network Protocol and Port Configuration	○	○			
Digital Certificate	○	○	○	○	
IP filtering Address	○	○	○	○	
MAC filtering Address	○	○	○	○	
Image Overwrite configuration	○	○			
Application Management	○	○	○	○	
Password(U.NORMAL)		○			U.NORMAL
Network Protocol and Port Configuration	○				

The TOE shall be capable of performing the following management functions:

Table 44: Management Functions

Management Functions
Management of Audit data (review)
Management of Common Access Control rules
Management of TOE Function Access Control rules
Management of Service Access Control rules
Management of MAC filtering rules
Management of IP filtering rules
Management of Protocol/Port information flow control rules
Management of Image overwrite function
Management of User attributes (User ID, User Name, Password, Email, Fax No, and Group ID)

Management Functions
Management of security roles (User Group ID)
Management of TSF testing (initiation)
Management of fax forward functions

There are two types of Users in the TOE; U.NORMAL and U.ADMINISTRATOR:

U.ADMINISTRATOR has been specifically granted the authority to perform security management of the TOE and U.NORMAL is authorized to perform User Document Data processing functions (Copy, Scan, Fax, Print) of the TOE and to modify his/her own password.

U.USER has five roles: ADMIN, GENERAL USER, GUEST, LIMITED RESOURCE USER, RESTRICTED INFOR USER.

Each role type has different rights predefined. U.NORMAL has no permission to access the security management of the TOE as a general rule.

The TOE supports the role management and user profile to manage U.USER.

-Role Management: U.ADMINISTRATOR can give permissions to U.NORMAL to only use certain features of the machine and can give different rights to different U.NORMAL by using role management.

-User profile: The TOE shall store U.USER's information on the TOE. U.ADMINISTRATOR can use this feature to manage the U.USER's authorization. The U.NORMAL is allowed to modify his/her password.

7.1.4 Security Audit (TSF_FAU)

Relevant SFR: FAU_GEN.1 FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4, FPT_STM.1

The TOE provides an internal capability to generate a audit record of the security audit event (job log, security event log, operation log) and audit data includes the following information (type of event, date and time of the event, subject identity, success or failure, log out, access, enabled and disabled).

U.ADMINISTRATOR only has the capability to manage this function and to read all of the audit data (job log, security event log, operation log) from the audit records.

The TOE protects the stored audit records in the audit trail from unauthorized deletion. Additionally, the TOE provides a capability to export audit log data from the TOE.

If the audit trail is full, the TOE overwrites the oldest stored audit records. After that, a new audit log is generated.

Time & Date values used in security audit only can be changed by U.ADMINISTRATOR manually. TOE use only internal time-stamps.

Table 45: Security Audit Event

Auditable Events	Relevant SFR	Audit Level	Additional Information
Job completion	FDP_ACF.1(1)(2)	Not specified	Type of job

Both successful and unsuccessful use of the authentication mechanism	FIA_UAU. 1	Basic	None required
Both successful and unsuccessful use of the identification mechanism	FIA_UID. 1	Basic	Attempted user identity, if available
Termination of an interactive session by the session termination mechanism	FTA_SSL.3	Minimum	None required
Use of the management functions	FMT_SMF.1	Minimum	None required
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required
Log data access	FMT_MTD.1	Not specified	None required
Manual Image Overwrite	FDP_RIP.1	Not specified	None required
Execution of the TSF self tests and the results of the tests	FPT_TST.1	Not specified	None required
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required
Change to the time	FPT_STM.1	Minimum	None required

7.1.5 Image Overwrite (TSF_IOW)

Relevant SFR: FDP_RIP.1

The TOE provides Image Overwrite functions that delete the stored file from the hard disk drive. The Image Overwrite function consists of Automatic Image Overwrite and Manual Image Overwrite. The TOE implements an Automatic Image Overwrite to overwrite temporary files created during the copying, printing, faxing and scanning (scan-to-email, scan-to-FTP, or scan-to-SMB task processes). The image overwrite security function can also be invoked manually only by U.ADMINISTRATOR (Manual Image Overwrite) through the LUI. Once invoked, the Manual Image Overwrite cancels all print and scan jobs, halts the printer interface (network), overwrites the contents of the reserved section on the hard disk according to the overwrite method set by U.ADMINISTRATOR, which are DoD 5220.28-M, Australian ACSI 33, DoD5220.22-M (ECE), German standard (VSITR) standard, and Custom. If there are any problems during overwriting, the Manual Image Overwrite job automatically restarts to overwrite. Automatic Image Overwrite will remove temporary area used for job operation after job completion. U.ADMINISTRATOR shall manage the Automatic Image Overwrite feature whether it enable or disable.

7.1.6 HDD Data Encryption (TSF_NVE)

Relevant SFR: FCS_CKM.1, FCS_CKM.4, FCS_COP.1

The TOE provides an encryption function during the data storage procedure and decryption function in the process of accessing stored data from the hard disk drive.

The TOE generates cryptographic keys when the TOE is initialized at the first setout. The secure key (256 bits) is used for encrypting and decrypting user data and TSF data stored in the HDD.

The access to this key is not allowed to any U.USER including U.ADMINISTRATOR.

The TSF destroys cryptographic keys in accordance with overwriting a used cryptographic key with a newly generated cryptographic key.

- Encryption and Decryption:

Before storing temporary data, document data, and system data on the HDD of the MFP, the TOE encrypts the data using the AES 256 algorithm and cryptographic key.

When accessing stored data, the TOE decrypts the data using the same algorithm and key.

Therefore, the TOE protects data from unauthorized reading even if the HDD is stolen.

7.1.7 Fax Data Control (TSF_FLW)

Relevant SFR: FPT_FDI_EXP.1

If the received fax data includes malicious content, it may threaten the TOE asset such as the TOE itself or network components. To prevent this kind of threat, the TOE inspects whether the received fax image is standardized with MMR, MR, or MH of T.4 specifications. When non-standardized format data are discovered, the TOE destroys the fax image.

• The fax modem controller in the TOE is physically separated from the MFP controller, and fax function is logically separated from MFP functions.

• The fax interface only answers to the predefined fax protocol and never answers to any other protocol.

• The fax modem controller provides only a standardized fax image format of MMR, MR, or MH of T.4 specification. Therefore, the TOE does not answer to non-standardized format data.

The TOE restricts forwarding of data to external interfaces. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

7.1.8 Self Testing (TSF_STE)

Relevant SFR: FPT_TST.1

The TOE performs a suite of self tests during initial start-up.

Self testing executes the TSF function to verify the correct operation of all of the HDD Encryption Function.

The TOE extracts the HDD encryption key data and calculates the hash value of HDD encryption key using SHA 256. Then, the TOE compares the calculated hash value with pre-stored hash value of encryption key data to verify the integrity of encryption key data.

Additionally, the TOE executes the SHA256 hash algorithm with executable codes for all of the TSF functions. It also compares the resulting hash data with saved data to verify the integrity.

If the compared result is the same, integrity verification is successful.

When the TOE executes the self testing, the TOE generates audit log data for self testing.

U.ADMINISTRATOR is authorized to view the audit log.

7.1.9 Secure Communication (TSF_SCO)

Relevant SFR: FTP_ITC.1

The TOE also provides secure communication between the TOE and the other trusted IT product by IPSec.

IPSec provides securing Internet Protocol communications by authenticating and encrypting each IP packet of a communication session.

IPSec supports ESP to provide confidentiality, origin authentication, integrity and IKE for key exchange. IPSec supports 3DES, AES for encryption, SHA-1 for integrity and DH-Group for key agreement.

The IPSec will be initialized in the process of booting on MFP. The network using IPSec will be only allowed to communicate with MFP.