Samsung MFP Security Kit Type_E V1.0

Security Target

Version 1.4

Samsung Electronics Company

@

Document History

VERSION	DATE	DESCRIPTION OF CHANGE	SECTIONS AFFECTED	REVISED BY
1.0	2010-05-06	- Initial version	ALL	SEC
1.1	2010-06-29	- EOR-01 revision	ALL	SEC
1.2	2010-07-13	- EOR-01 revision2	ALL	SEC
1.3	2010-08-23	- EOR-04 revision	ALL	SEC
1.4	2011-06-28	- Modify the conformance to Protection Profiles	ALL	SEC

CONTENTS

LIST OF FIGURES

5

LIST OF TABLES

1 Introduction

This document describes Samsung MFP Security Kit Type_E V1.0 for the Common Criteria EAL3+.

1.1 Security Target References

Security Target Title	Samsung MFP Security Kit Type_E V1.0 Security Target
Security Target Version	Version 1.4
Publication Date	June 28, 2011
Authors	Samsung Electronics
Certification body	IT Security Certification Center (ITSCC)
CC Identification	Common Criteria for Information Technology Security (CC Version 3.1 Revision 3)
Keywords	Samsung Electronics, Multifunction Peripheral

1.2 TOE References

Developer	Samsung Electronics
Name	Samsung MFP Security Kit Type_E V1.0
Version	V1.0
Product	SCX-8030, SCX-8040, CLX-9250, CLX-9350

1.3 TOE Overview

1.3.1 TOE Type, Usage and Security features

This TOE is an embedded software product for 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.

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. Then the TOE authorizes U.USER according to the identification & authentication result. The TOE also provides the Custom Access Control & TOE Function Access Control based on the user role assigned to User group ID by U.ADMINISTRATOR

- 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 external network by enabling/disabling or altering port numbers of various protocols. And The TOE also provides IP filtering /Mac filtering functions to control access from external 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

7

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 MFP. Audit logs are stored on the hard disk drive and can be reviewed or deleted 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.

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 MFP 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.

Figure 1 shows the expected operational environment for the usage of an MFP installed with the TOE.

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.
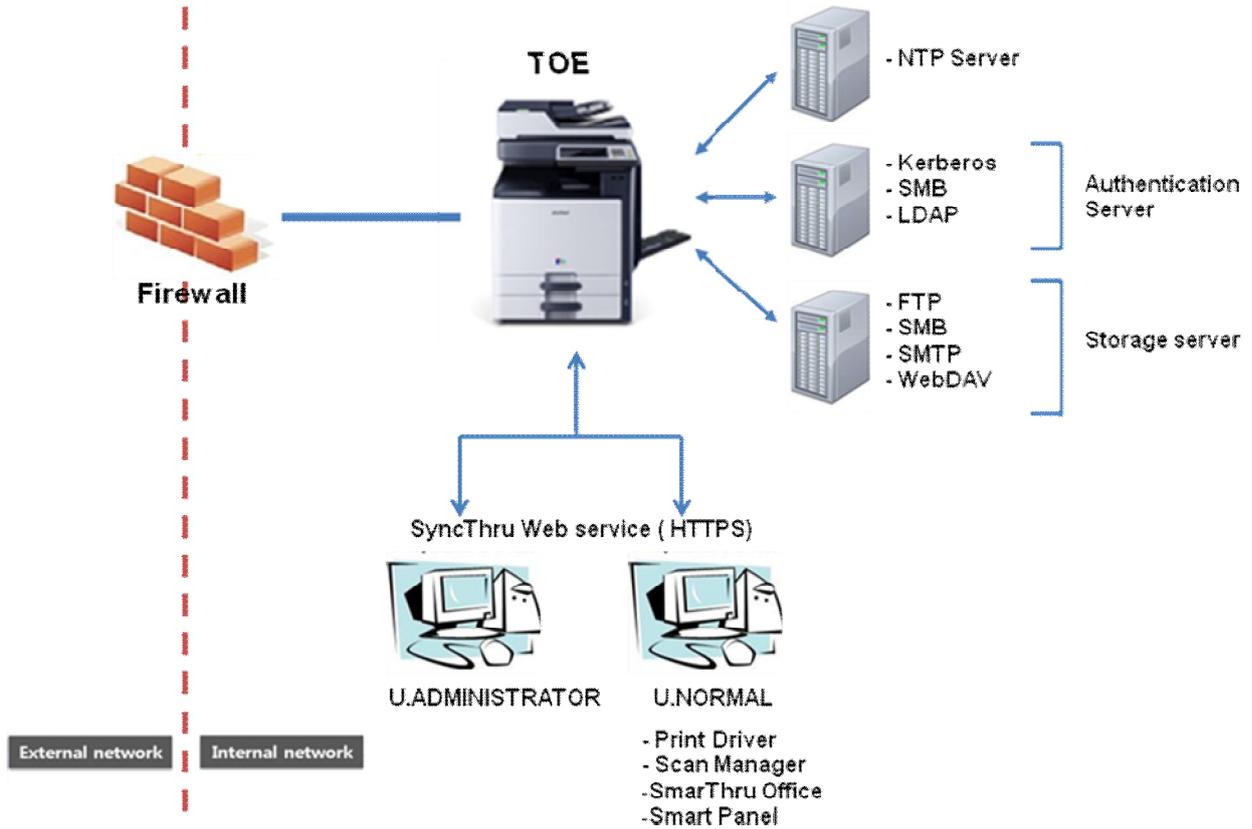
Figure 1: Operational Environment of the TOE

The TOE is intended to operate in a network environment that is protected by a firewall from external malicious attacks (e.g., DoS attack), and with reliable PCs and authenticated servers. A user is able to access the TOE by using a local user interface, U.NORMAL PC from a remote user, or a Remote User Interface (Refer to Figure 1: Operational Environment of the TOE). The local user interface (LUI) is designed to be accessed by users and a local administrator. The users can operate copy, scan, and fax functions through the LUI. In the case of a scanning job, users can operate the scanning job using the LUI and transfer the scanned data to a certain destination by email addresses, server PCs, or client PCs. Users can also use their PCs to print out documents or to access the TOE through the internal network. The administrator can enable/disable Automatic Image Overwrite, start/stop Manual Image Overwrite, and change a Password via the LUI. The administrator can access TOE through the Remote User Interface (RUI) using a web browser (refer to Table 2) supporting SSL protocol. From there, they can add/change/delete user accounts, change the web administrator's ID and password, enable/disable the security audit service, and download the security audit report. The user account information that requires asking for internal authentication by TOE (only for network-scan services such as scan manager, scan to e-mail, scan to FTP, scan to SMB, or scan to WebDAV) can be stored on the hard disk drive of the MFP. All of the information stored on the hard disk drive is protected by the TOE. In the case of external authentication by trusted authentication servers (Kerberos, LDAP, SMB server), all the account information stored on a network authentication server is assumed to be protected from external environmental space.

- NTP server

The NTP (Network Time Protocol) server synchronizes the operating system's clock, which is crucial for audit logs.

- Mail server

The TOE has features that serve as a mail delivery function, such as Scan to E-mail. The mail server stores mail data and manages the data.

- FTP server / SMB server/ WebDAV server

The FTP server, SMB server, and WebDAV serve as storage devices of received fax and scan data from the TOE. Scan-to-server is a relevant function.

- Authentication server

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

- TPM (Trusted Platform Module)

TPM provides cryptographic keys (private key, public key, secure key) to TOE for encryption/decryption of HDD storage data.

- DBMS(H2 DB 1.2.128)

H2 DB 1.2.128 is an embedded database that stores quota, audit log, configuration, and license information data. It provides several functions to the TOE as a series of functions including an audit log selecting and ordering function, audit log storage protection, and maintenance of audit log integrity.

- Web browser

A web browser allows U.ADMINISTRATOR to connect to the TOE to use security management functions (e.g., audit log review and deletion, network access control, etc.) and allows U.NORMAL to use basic functions (e.g., print information, direct print, etc.)

- SSL Library

SSL protocol uses web browsers to protect data transferred between U.USER and the TOE.

1.4.2 Non-TOE Hardware/Software/Firmware required by the TOE

1.4.2.1 Non-TOE Hardware

Table 1: Non-TOE Hardware

Item	Objective	Specifications (Minimum)
MFP Hardware	The TOE must be embedded in the MFP.	Refer to Table 4

PC for U.ADMINISTRATOR	PC for U.ADMINISTRATOR to access and manage TOE.	NIC : 10/100 Mbps * 1
		
		• Windows 2000
		  -CPU: Pentium II 400 MHz
		  -Memory: 64 MB
		  -HDD: 600 MB free disk space
		• Windows XP
		  -CPU: Pentium III 933 MHz
		  -Memory: 128 MB
		  -HDD: 1.5 GB free disk space

PC for U.NORMAL	PC for U.NORMAL to print or scan or fax with TOE	• Windows 2003 Server
		  -CPU: Pentium III 933 MHz
		  -Memory: 128 MB
		  -HDD: 1.25 GB free disk space

		• Windows 2008 Server
		  -CPU: Pentium IV 1 GHz
		  -Memory: 512 MB
		  -HDD:10 GB free disk space
		• Windows Vista
		  -CPU: Pentium IV 3 GHz
		  -Memory: 512 MB
		  -HDD: 15 GB free disk space
		• Windows 7
		  -CPU: Pentium IV 1 GHz
		  -Memory: 1 GB
		  -HDD:16 GB free disk space
		• Windows 2008 R2
		  -CPU: Pentium IV 1 GHz for x86, 1.4 GHz for x64
		  -Memory: 512 MB
		  -HDD:10 GB free disk space
		
		• Mac OS X 10.5
		  -CPU: Intel Processor / 867 MHz Power PC G4/G5
		  -Memory: 512 MB
		  -HDD: 1 GB free disk space
		• Mac OS X 10.6
		  -CPU: Intel Processor
		  -Memory: 1 GB
		  -HDD: 1 GB free disk space
		
		• Linux
		  -Operation System
		    Redhat Enterprise Linux WS 4, 5 (32/64 bit)
		    Fedora Core 2 ~ 10 (32/64 bit)
		    SuSE 10.0, 10.1 (32 bit)
		    OpenSuSE 9.2, 9.3, 10.0, 10.1 10.2, 10.3, 11.0, 11.1 (32/64 bit)
		    Mandrake 10.0, 10.1 (32/64 bit)
		    Mandriva 2005, 2006, 2007, 2008, 2009 (32/64 bit)
		    Ubuntu 6.06, 6.10, 7.04, 7.10, 8.04, 8.10 (32/64 bit)
		    SuSE Linux Enterprise Desktop 9, 10 (32/64 bit)
		    Debian 3.1, 4.0, 5.0 (32/64 bit)
		  -CPU: Pentium IV 2.4 GHz (Intel Core 2)
		  -RAM: 512 MB
		  -HDD: 1 GB free disk space

TPM	TPM provides cryptographic keys to TOE for encryption/decryption of HDD storage data	Vendor : Atmel Model names : AT97SC3204T Specification : CRYPTO TPM V1.2

1.4.2.2 Non-TOE Software

Table 2: Non-TOE Software

Item	Objective	Specification
Web browser / Web server that can serve SSL communication	Web browser that serves SSL communication among U.NORMAL's PC, U.ADMINISTRATOR's PC, and TOE.	• Web browser - Internet Explorer 7.0 ~ 8.0 - FireFox 3.0 ~ 3.6 - Safari 4.0 ~ 5.0 - Chrome 4.0 ~ 5.0

		• Web server - Jetty 6.1.9	

SSL Library	A library to protect transferred data between MFP and web browser.
	
	Algorithm will be determined when the MFP is connected to the web browser for the first time.
		• CLX-9250, CLX-9350 :
		  JSSE is included and supported as part of J2SE 1.5
		
		• SCX-8030, SCX-8040 :
		  JSSE is included and supported as part of Java SE 1.6	

DBMS	DBMS is an embedded database that stores Quota, audit log, configuration, and license information. It provides several functions to the TOE in a series of functions including an audit log selecting and ordering function, audit log storage protection, and maintenance of audit log integrity.	H2 DB 1.2.128	
Printer driver	Printer driver application software for U.USER to install in their PC. U.NORMAL can configure properties and start printing jobs through this printer driver.	PCL 6 Driver V3.10.79	
SmarThru Office	SmarThru Office is an integrated management application program. U.USER can install this program on their PC, then edit scanned images or send email through this program.	SmarThru office V2.06.06	
Smart Panel	Smart Panel monitors the state of the MFP connected to U.USER's PC. When an event occurs, Smart Panel notifies U.USER of the event. - Toner Remaining Status, Paper Size, and orientation information - Several error status	SmartPanel V1.23.34	
Scan Manager	Scan Manager receives scanned data from the MFP and stores it in U.USER's PC.	Scan Manager V2.00.26	
		Mono Model (SCX-8030, SCX-8040)	Color Model (CLX-9250, CLX-9350)
Engine software	Software that manages the printing hardware - Operate H/W (LSU(Laser Scanning Unit), fuser units, fan units, option tray, duplex unit, sensors, motors, etc.) to perform printing jobs - Communicate with the printer subsystem or controller	01.00.02	01.00.08
Scan software	Software that generates scanned image data in the Platen/ADF (automatic document feeder)/DADF (duplex automatic document feeder) - Generate scanned image data from the image sensor. - Enhance image data (sharpness, darkness, contrast, etc.) - Reduce/enlarge image data - Communicate with DADF to control DADF	V3.00.74.11 07-31-2010	V3.00.74.11 07-31-2010
Fax software	Software that sends image data to a remote fax	V3.00.78.16 07-18-	V3.00.78.16 07-18-

	machine or receives image data from a remote machine - Control H/W modem - Encode/decode data to Fax format (MH, MR, MMR, Jpeg) - Generate TTI (Transmission Terminal Identification) data - Generate fax data with TTI/Receive fax data	2010	2010
Image converter software	Software that handles image data - Encode/decode image data to other formats (TIFF, PDF, JPEG, BMP, etc.) - Rotate (reverse or scale) image data	N/A	V3.00.52.01
Emulator	Software that converts data to printer data format (PCL5E, PCLXL, PostScript/PDF/XPS)	-	-
	PCL5E	PCL5e 1.32 08-05-2010	PCL5Ce 1.38
	PCLXL	PCL6 1.69 08-31-2010	PCL6 1.72
	PostScript/PDF/XPS	2.68.00.49.00.54 08-11-2010	2.69.00.49.00.54
DADF software	Software that manages DADF(duplex automatic document feeder) hardware - Control H/W motors and sensors to move (or stop) documents - Communicate with Scan Board to transmit the status	01.00.04	00.90.04

1.4.2.3 Non-TOE Firmware

Table 3: Non-TOE Firmware

Item	Specification
Operating system embedded in the MFP	• Main Board: Linux 2.6.29 (Operating system for TOE) • Scan Board: pSOS • Image Converter Board: pSOS • FAX Board: pSOS • GUI Board: Linux 2.6.11 • Engine Board: pSOS • DADF Board: pSOS

1.4.2.4 General Specification for TOE

Table 4: General Specification for TOE

Categories				
Features	**Mono**		**Color**	
	SCX-8030	**SCX-8040**	**CLX-9250**	**CLX-9350**
Productivity				
CPU	SPGPv4, 800 MHz		PowerPC, 800 MHz	PowerPC, 1.0 GHz
Printing Speed (A4) (Color/Mono)	30ppm/-	40ppm/-	25ppm/25ppm	35ppm/35ppm
FCOT (Color/Mono)	< 7.5 sec / -	< 6.5 sec / -	10.5 (color) / < 9.5	<8.5 (color) / < 7.5

			(mono)	(mono)
Warm-up Time (Color/Mono)	< 25 sec / -		< 45 sec	
Duplex Printing Speed	Same as rated engine speed			
Scanning Speed (A4) (Color)	50ipm @ 300 dpi		60ipm @ 300 dpi	
Memory (Standard /Max)	768MB/1.7GB		1GB/2GB	
HDD	250GB			
Image Quality				
Engine Resolution	600 x 600 dpi x 4-bit		600 x 600 dpi x 4-bit	
Resolution Enhancement	4,800 x 600 dpi		4,800 x 600 dpi	
Gradation	256			
Scanning				
Optical Resolution	600 x 600 dpi (Color)			
Scan Resolution Enhancement	4800 x 4800 dpi (Network Scan)			
Output File Type	PDF, TIFF, JPEG, XPS			
Scan-to-Feature	Scan-to-E-mail/FTP/HDD/SMB/I-FAX/URL/LDAP/USB			
Printing				
Max. Imaging Area (mm (inch))	297 x 432 (11.7 x 17)		310 x 452 (12.2 x 18)	
Max. Effective Imaging Area (mm)	297 x 432 (11.7 x 17)		297 x 452 (11.7 x 18)	
Margin[2] (Leading Edge/L-R, mm)	3mm / 2mm		3mm / 2mm	
Emulation	Postscript 3, PCL 6, PDF 1.7+, XPS		Postscript 3, PCL 6, PDF 1.7+, XPS	
Interface	10/100/1000 BaseTX, USB 2.0 3EA			
Supported Operating Systems	Windows 2000 / XP / 2003 Server / VISTA / 7 /2008 R2, Mac OS 10.5, 10.6, Linux : - Fedora 4 ~ 12 (32/64 bit) - OpenSuSE 10.2, 10.3, 11.0, 11.1, 11.2 (32/64 bit) - SuSE 10.0, 10.1 (32 bit) - Ubuntu 5.04, 5.10, 6.04, 6.10, 7.04, 7.10, 8.04, 8.10, 9.04, 9.10 (32/64 bit) - Mandriva 2005, 2006, 2007, 2007.1, 2008, 2008.1, 2009, 2009.1 (32/64 bit) - Debian 4.0, 5.0 (32/64 bit) - Redhat Enterprise Linux WS 4, 5 (32/64 bit) - SuSE Linux Enterprise Desktop 10, 11 (32/64 bit)			
Faxing				
Resolution	203 x 98, 203 x 196, 203 x 392, 300 x 300, 400 x 400, 600 x 600 dpi			
Data Transmission Speed	33.6kbps			
Communication Mode	Super G3			
Compression Method	JBIG, MMR, MR, MH, JPEG			
Memory	HDD 250G			
Fax-to-	Fax-to-E-mail/FTP/SMB/HDD			
Media Input				

Standard Tray	520 Sheets x 2 Tray (80 gsm)		
MP Tray	100 Sheets (80 gsm)		
Max. Media Capacity	3,140 Sheets (80 gsm)		
Paper Size - Tray (Min/Max) (mm)	148 x 210 (5.8 x 8.3) / 305 x 457 (12 x 18)		
Paper Size - Bypass (Min/Max) (mm)	89 x 148 (3.5 x 5.8) / 305 x 457 (12 x 18)	89 x 148 (3.5 x 5.8) / 320 x 457 (12.625 x 18)	
Paper Size - DADF (Min/Max) (mm)	128 x 128 (5.0 x 5.0) / 297 x 432 (11.7 x 17)		
Paper Weight - Tray (Min/Max)	60 / 163 gsm	60 / 216 gsm	
Paper Weight - Bypass (Min/Max)	60 / 216 gsm	60 / 253 gsm	
Paper Weight - Simplex ADF (Min/Max)	40 / 163 gsm		
Paper Weight - Duplex ADF (Min/Max)	52 / 135 gsm		
Universal Tray	Tray 1 ~ 4		
Media Output			
Standard Output Capacity	500 (80 gsm)		650 (80gsm)
Max. Output Capacity	650 (80 gsm) (with Inner Output Tray)	650 (80 gsm) (with Right Output Tray)	
Output Orientation (Center/Right Tray)	FD/FU		
Sort			
Electronic Sorter	Standard		
Duplex			
Auto Duplex Kit	Standard		
Options			
DADF	Standard		
DCF (Dual Cassette Feeder)	2 Cassette Tray (520 x 2, 80gsm)		
Internal HCF	2,000 (80 gsm, A4, Letter)		
Cabinet Stand	Cabinet Stand		
Job Separator	150 Sheets	N/A	
Right Output Tray	N/A	150 Sheets	Standard
1,250-Sheet Standard Finisher	2 Tray (250/1,000 Sheets), 50 Sheets Stapling, 2 Position, Convenience Stapling		
3,250-Sheet Booklet Finisher	2 Tray (250/3,000 Sheets), 50 Sheets Stapling, 15 Sheets Saddle Stitching, 2 Position, Convenience Stapling, 'V' Folding		
Bridge Kit	Connect to Standard Finisher / Booklet Finisher		
Punch Kit	2/3 or 2/4 Holes		
Working Table	Small Side Tablet for Placing a Card Reader		
Keyboard Tray	Keyboard Tray supporting USB Mini-keyboard (US-Only)		
Wireless LAN Kit	802.11 a/b/g		
Fax Kit	Super G3		
Fax Multiline Kit	1 Additional		

Expansion Memory	1GB			
IP Fax Enabler Kit	T.38, SIP			
Common Criteria Security Kit	Advanced Overwrite, Encryption features			
Advanced Scan Kit	OCR, Searchable PDF, Advance Annotations			
SmarThru Workflow	Document Distribution Solution			
CounThru	Accounting Solution			
PM Kit	TBD	Transfer & Clear Kit, Tray Roller Kit, ADF Roller Kit		
Size				
H (with DCF) x W x D (mm)	1154 / 678 / 762			
Weight				
Weight (kg)	107Kg	113kg		
Environment & Regulations				
Environment Regulations	Blue Angel, Energy Star			
Solution Regulations	HIPAA, SOX, FERPA, US Patriot, Section 508, SEC 17a-4			
EME	FCC Class A (US), EU LVD (Europe), VCCI Class A (Japan), CISPR Class A (International, Korea)			
Noise (dB)	TBD	55.9 (Copying), 54.6 (Printing), 39.9 (Stand-by)		
Power (kW)	< 1,500W @ 120V ~ 220V			
Power Savings (Watts)	< 10 W			
Installation Personnel	Service man installation			
Reliability				
Unscheduled Maintenance Rate	10@AMPV 10K		20@AMPV 10K	
Max Monthly Duty	100K	150K	100K	150K
Average Monthly Printing Vol.	8K	12.5K	4K ~ 6K	9K ~ 13K
Toner Yield (Color/Mono)	-/20K	-/35K	12K/15K	20K/25K
OPC Yield (Color/Mono)	-/100K		75K/75K	
Developer Yield (Color/Mono)	-/100K		75K/75K	
Fuser Yield (Color/Mono)	-/150K		150K/150K	
Waste Bottle	75K		75K	
PM Schedule	75K (TBD)		75K	
Machine Life (Max AMPV x 2 x 60 mo)	864,000	1,350,000	720,000	1,560,000
Fault-tolerance	Industry Average			

1.4.3   Physical Scope
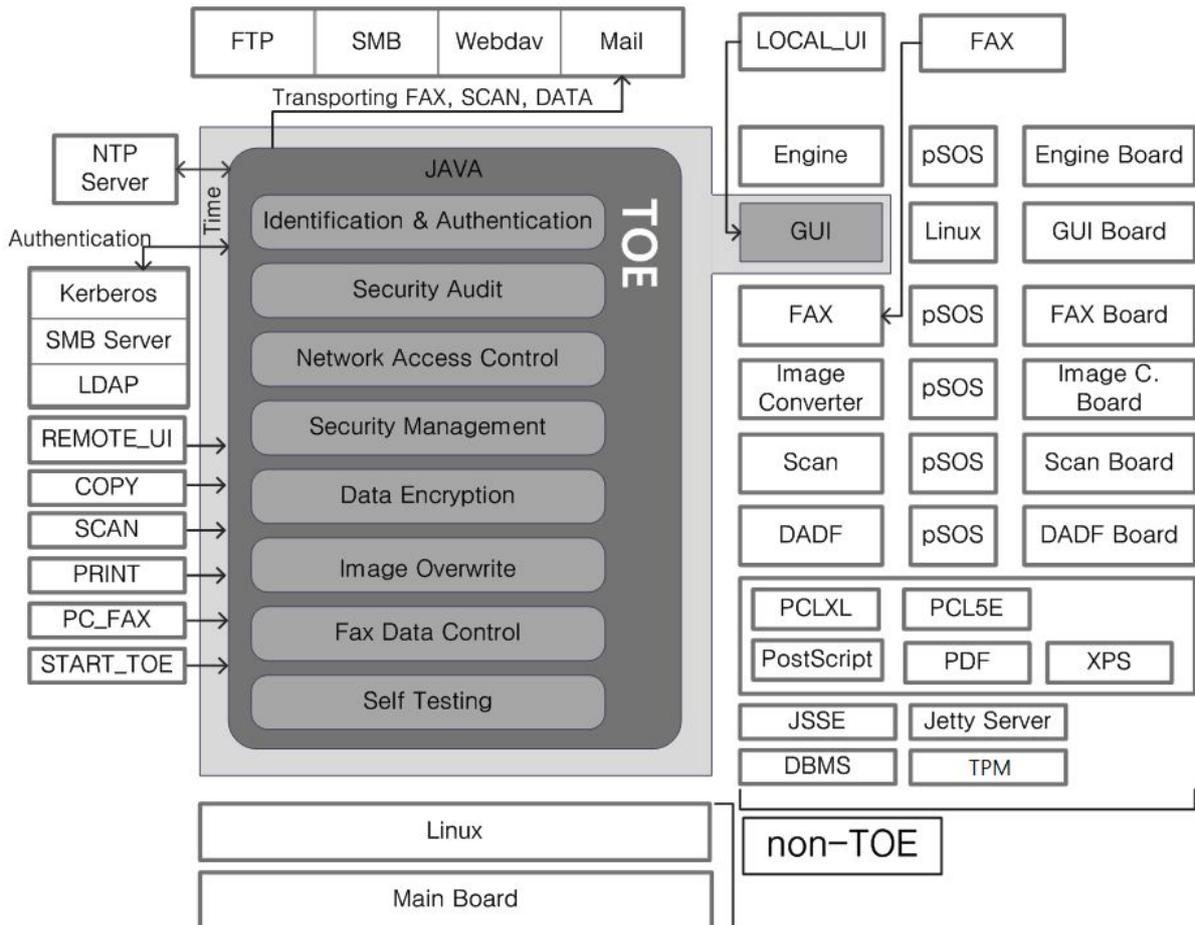
Figure 2: Physical Structure of MFP

The physical extent of the TOE is as follows:

☐☐Software
- Samsung MFP Security Kit Type_E V1.0

☐☐Instructions
- CLX-9250 9350 Series Multi-Functional Printer Administrator's Guide
- SCX-8030 8040 Series Multi-Functional Printer Administrator's Guide
- CLX-9250 9350 Series Color Multi-Functional Printer User's Guide
- SCX-8030 8040 Series Multi-Functional Printer User's Guide
- CLX-9250 9350 Series Installation Guide
- SCX-8030 8040 Series Installation Guide

The version of TSF and Software which are included in the physical scope are as follows:

Table 5: TSF Identification and Software Version

Software Version	SCX-8030	SCX-8040	CLX-9250	CLX-9350
Main Software	**V11.11.01.04ccc7**	**V11.11.01.04ccc7**	**V11.11.01.15ccc7**	**V11.11.01.15ccc7**
- Identification Authentication	TSF_FIA_V2.00	TSF_FIA_V2.00	TSF_FIA_V2.00	TSF_FIA_V2.00
- Data Encryption	TSF_NVE_V2.00	TSF_NVE_V2.00	TSF_NVE_V2.00	TSF_NVE_V2.00

- Security Management	TSF_FMT_V2.00	TSF _FMT_V2.00	TSF _FMT_V2.00	TSF _FMT_V2.00
- Security Audit	TSF_FAU_V2.00	TSF_FAU_V2.00	TSF_FAU_V2.00	TSF_FAU_V2.00
- Image Overwrite	TSF_IOW_V2.00	TSF_IOW_V2.00	TSF_IOW_V2.00	TSF_IOW_V2.00
- Fax Data Control	TSF_FLW_V2.00	TSF_FLW_V2.00	TSF_FLW_V2.00	TSF_FLW_V2.00
- Network Access Control	TSF_NAC_V2.00	TSF_NAC_V2.00	TSF_NAC_V2.00	TSF_NAC_V2.00
-Self Testing	TSF_STE_V2.00	TSF_STE_V2.00	TSF_STE_V2.00	TSF_STE_V2.00
GUI Software	**11.01.53.16**	**11.01.53.16**	**11.01.53.16**	**11.01.53.16**
- Security UI Interface	TSF_LUI_V2.00	TSF_LUI_V2.00	TSF_LUI_V2.00	TSF_LUI_V2.00

The figure above shows the physical extent of the TOE, which is JAVA and the GUI. JAVA consists of 8 sub-systems: Identification & Authentication, Network Access Control, Security Management, Security Audit, Image Overwrite, Data Encryption, Fax Data Control, and Self Testing.

The external authentication servers (i.e., LDAP, Kerberos, and SMB Server), the NTP server, and FTP server/HDD/WebDAV/Mail server are external entities, and, thus, are not included in the TOE. Additionally, Emulator (PCL5E, PCLXL, PostScript/PDF/XPS), OS (Linux, pSOS), Main Board, Engine/ Engine Board, FAX/ FAX Board, Image converter/ Image converter Board, Scan/Scan Board, DADF/DADF Board, GUI Board, DBMS, Jetty 6.1.9 and JSSE 1.0.3 are non-TOE, and, thus, are not included in the TOE as well.

1.4.4 Logical Scope
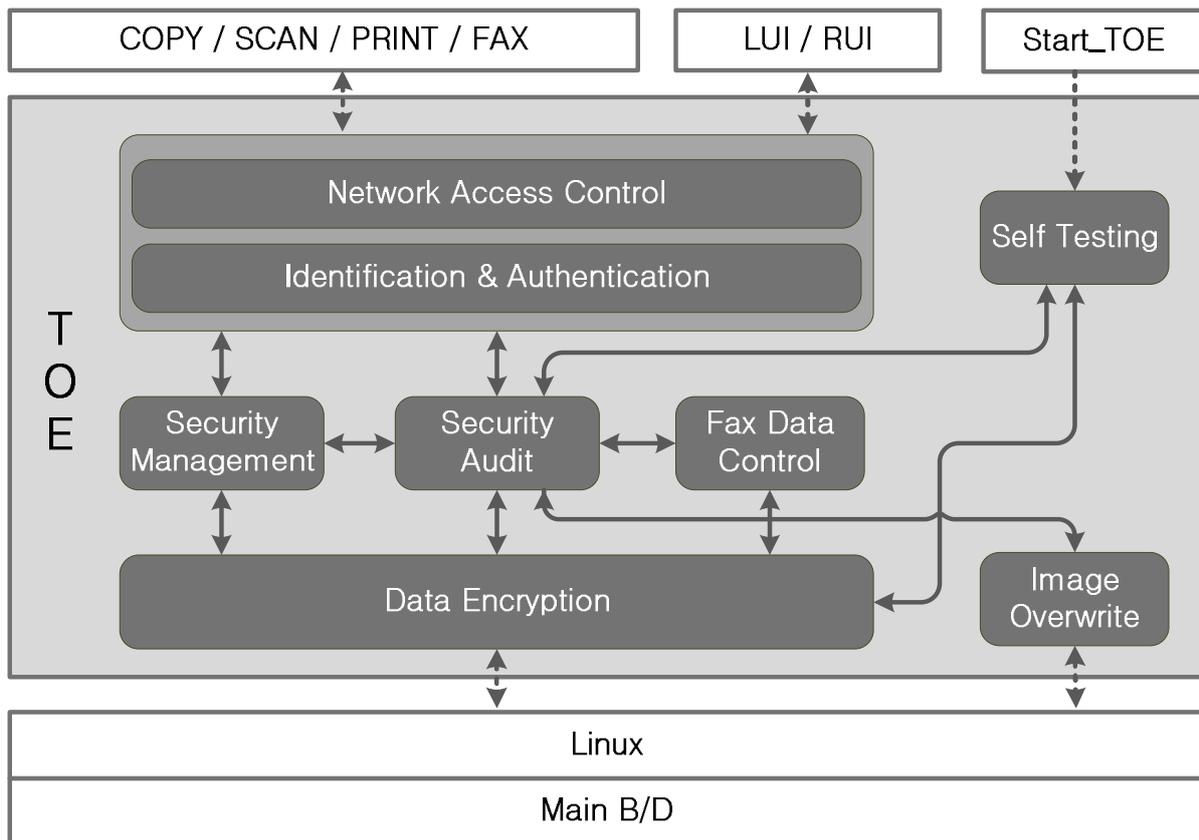
Figure 3: Logical Scope

The following security functions are provided by the TOE:

Identification & Authentication (TSF_FIA)

The TOE can restrict U.USER from accessing the machine or application.

U.USER should be identified and authenticated by entering ID, Password to access to the TOE management functions.

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 Custom 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.NORMA,L or when U.NORMAL accesses print/scan/copy/fax/document storage retrieval functions offered by the MFP.

Network Access Control (TSF_NAC)

The MFP system including the TOE has a network interface card (network card) connected to an external 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 IPv4/IPv6 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: security functions can be activated and deactivated by U.ADMINISTRATOR.

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.

Job log includes print, scan, copy, fax, and document storage and retrieval jobs.

Security event log includes authentication, log data access, and deletion and self testing.

Operation log includes enablement of each log function (job log, security event log) except for the operation log.

The audit data consist of the type of event, date and time of the event, success or failure, log out, access and deletion of log data, and enablement and disablement of the log function.

Only U.ADMINISTRATOR is authorized to view (or delete or export) the audit data selectively.

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 deletes the oldest stored audit records (10% of each log data) and generates an audit record of deletion.

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, scan to SMB, or scan to WebDAV task processes). Also, users can delete their own files stored in the TOE. 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 procedures set by U. ADMINISTRATOR, which are DoD 5200.28-M, Australian ACSI 33, German standard (VSITR) standard, and Custom. Then the main controller reboots. 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 requests generating cryptographic keys (private key, public key, secure key) to the TPM in the operational environment of the TOE for when the TOE is initialized at the first setout. Private and public keys are used for encrypting and decrypting secure key being stored in the EEPROM, and the

secure 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 when a used cryptographic key is broken.

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)

In the TOE, the memory areas for the fax board and for the network port on the main controller board are separated. If the received fax data includes malicious content, it may threaten the TOE asset such as the TOE itself or internal 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 specification or not before forwarding the received fax image to e-mail or SMB/FTP/WebDAV. When the data is considered to be safe, the memory copy continues from the fax memory area to network memory area. The fax data in network memory is transmitted using SMTP, SMB, FTP, WebDAV servers through the internal network. When non-standardized format data are discovered, the TOE destroys the fax image. Fax security functions follow the Information Flow policy (SFP_FLW).

Self Testing (TSF_STE)

The TOE goes through self testing procedure on each initial system boot examining.

U.ADMINISTRATOR can enable the self tests for TSF function, TSF data, TSF executable code.

Self testing executes TSF function to verify the correct operation of TSF function (TSF_NVE).

And the TOE verifies the integrity of TSF data and TSF executable code by the self testing.

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 prefixes in Table 6 are used to indicate different entity types:

Table 6: 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

This section shall describe the definition of the terms used in Security Target.

Network Scan Service

This is a service that transmits scanned data to a PC on an internal network, email, or FTP server through the network. It includes scan-to-email, scan-to-FTP, scan-to-SMB, or scan-to-WebDAV.

LUI, Local User Interface

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

Fax-to-email

This is a function that transmits received fax images to email through an internal network. This function is enabled only when a mail server and address are configured.

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.

Preserved file

To store a file on the hard disk drive of TOE, two types are provided: Public and Secured. When a user stores a document as Public, all users can access and use the file. A file stored as Secured can only be accessed by the user who stored the file. When storing a file as Secured, the user must set a PIN required to access the file. Then the file can only be accessed by entering the PIN.

Multi-Function Printer, MFP

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

Human User

User who only refers to a human being

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 local administrator through the LUI. The image data is completely overwritten 1 ~ 9 times by using DoD 5200.28-M, Australian ACSI 33, VSITR (German standard) standard, and Custom setting methods.

Scan-to-server

This is a function that transmits scanned data to a remote server from the LUI. Only authorized network scan service users can use this function.

Scan-to-email

This is a function that transmits scanned data to a remote email server from the LUI. Only authorized network scan service users can use this function.

System Administrator

This is an authorized user who manages the TOE-embedded MFP. System administrator manages Samsung MFP Security Kit Type_E V1.0 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 information of scan manager service users, manage/change administrator's ID and password, enable/disable the security audit function, 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.

RUI, Remote UI, Remote User Interface

Interface for general users or system administrators to access, use, or manage the MFP through a web service.

Image file

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

Stored file

Every file stored on the hard disk drive. It includes image files and preserved files.

Public Print

The print option that prints out a user stored documents using the Public option. It is open to every user.

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, scan-to-SMB, or scan–to-WebDAV. Or the Automatic Image Overwrite overwrites the files on the hard disk drive when a user initiates a delete operation.

FAX

Job for receiving or transmitting fax images through a fax line

Fax image

The data received or transmitted through a fax line

Quota

The limited quantity of allowed jobs.

DoD 5200.28-M

DoD 5200.28-M is an image overwriting standard that Department of Defense recommends. The image data in a storage device is completely overwritten three times with overwriting '0x35' the first time, then '0xCA' the second time, and finally overwriting '0x97'.

Australlian ACSI 33

The Australian Government Information and Communications Technology Security Manual (also known as ACSI 33) has been developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government agencies on how to protect their Information Technology, and Communications systems.

The Protective Security Manual, issued by the Attorney-General's Department, provides guidance on protective security policies, principles, standards, and procedures to be followed by all Australian Government agencies for the protection of official resources.

VSITR

The German Federal office for IT Security released the VSITR standard, which overwrites the hard drive with 7 passes. For the first 6 passes, each overwrite reverses the bit pattern of the previous pass, inverting the bits in order to destabilize the remnants of data that may exist on the edges of the track of the disk to which the data is written. The final pass amplifies the effect, overwriting the entire disk with "01010101": this is widely considered to be a secure method of erasing data.

Embedded FAX

A fax job that transmits data scanned in the MFP through a fax line and receives fax data directly from a fax line on the MFP.

PC FAX

A fax function sends fax data from a client PC to an MFP first, and then transmits the fax data 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.

TPM

Trusted Platform Module offers facilities for the secure generation of cryptographic keys - often called the "TPM chip" or "TPM Security Device".

1.7   Acronyms

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

Table 7: 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

JSSE	Java Secure Socket Extension

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 3.1r3, 2009. 7, CCMB-2009-07-001
    - Common Criteria for Information Technology Security Evaluation, Part 2: SFR (Security Functional Requirement), version 3.1r3, 2009. 7, CCMB-2009-07-002
    - Common Criteria for Information Technology Security Evaluation, Part 3: SAR (Security Assurance Requirement), version 3.1r3, 2009. 7, CCMB-2009-07-003

- **Common Criteria Conformance**
    - Common Criteria for Information Technology Security Evaluation, Part 2 conformant
    - Common Criteria for Information Technology Security Evaluation, Part 3 conformant

2.2   Conformance to Protection Profiles

No Protection Profile (PP) relevant to Security Target.

2.3   Conformance to Packages

This Security Target conforms to the following Package.

- **Assurance Package: EAL3 augmented by ALC_FLR.2**

2.4   Conformance Claim Rationale

No Protection Profile (PP) relevant to Security Target. Therefore, there is no conformance claims rationale.

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 to TOE Assets

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.

The threats are as shown in Table 8 and Table 9 (Refer to chapter 6 about affected asset):

Table 8: 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
T.FAX.MAL	D.FUNC	The malicious fax data may be inflowing into the TOE by threats
T.DATA.MAL	TOE	The malicious data may be inflowing into the internal network of the TOE by threats.

Table 9: 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

Threats	Affected Asset	Description
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.

Table 10: 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.

Table 11: Assumptions for the operational environment of 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 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

Assumption	Definition
	TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.
A.TIME_STAMP.RELIABLE	The operational environment of the TOE synchronizes its time with NTP server and provides reliable time-stamps for accurate audit logs about the TOE.
A.OS.TRUST	Administrators remove unnecessary services and means of the operating system, and reinforce vulnerabilities upon operating system, and, thus, ensure the reliability and security of the TOE.
A.NETWORK.TRUST	A firewall is installed between the internal network and the external network to protect the TOE from intrusion from outside.
A.SSL.SECURE	SSL protocol protects transferred data between U.USER and the TOE.
A.DBMS.MANAGED	DBMS provides a series of functions including audit log selecting and ordering function, audit log storage protection, and maintenance of audit log integrity.
A.AUTH_SERVER.SECURE	The authentication servers (i.e. LDAP, Kerberos, and SMB Server) provide a secure remote authentication for U.NORMAL.
A.EXT_SERVER.SECURE	The FTP, SMB server, WebDAV, and mail servers that store fax and scan data transmitted from the TOE are managed securely.
A.SSL_CERT.INSTALL	Certificate for SSL communication is installed by U.ADMINISTRATOR and the TOE is managed through the secure channel.
A.KEY_GENERATION	TPM provides cryptographic keys (private key, public key, and secure key) to TOE for secure encryption/decryption of HDD storage data.

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.

Table 12: 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.
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

Objective	Definition
	persons.
O.DATA.ENCRYPTED	The TOE shall encrypt the data to be stored on the HDD so that they cannot be analyzed even if retrieved.
O.DATA.OVERWRITTEN	The TOE shall provide image overwrite to protect the used document data on the HDD from being recovered.
O. FAX_DATA.FORMAT	The TOE shall block incoming fax data if received fax data does not qualify as a fax image standard.
O.INFO.FLOW_CONTROLED	The TOE shall control inflowing information data that are not allowed from external networks.

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.

Table 13: 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.
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.

Objective	Definition
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.
OE.TIME_STAMP.RELIABLE	The environment of the TOE must synchronize its time with the NTP server and provide a reliable time stamp to mark entries in the security log.
OE.NETWORK.TRUST	A firewall system shall be installed between the internal network and external networks to protect the TOE from intrusion from outside.
OE.SSL.SECURE	SSL protocol shall protect transferred data between U.USER and the TOE.
OE.OS.TRUST	Administrators shall remove unnecessary services and means of the operating system and reinforce vulnerabilities of the operating system to ensure reliability and security of the TOE.
OE.DBMS.MANAGED	DBMS shall provide a series of functions including audit log selecting and ordering functions, audit log storage protection, and maintenance of audit log integrity.
OE.AUTH_SERVER.SECURE	The authentication servers (i.e. LDAP, Kerberos, and SMB Servers) shall provide secure remote authentication for U.NORMAL.
OE.EXT_SERVER.SECURE	FTP server, WebDAV, and mail servers that store fax and scan data transmitted from the TOE shall be managed securely.
OE.SSL_CERT.INSTALL	U.ADMINISTRATOR shall manage TOE through a secure channel after the certificate for SSL communication is installed in the TOE.
OE.KEY_GENERATION	TPM shall provide cryptographic keys (private key, public key, and secure key) to the TOE for secure encryption/decryption of HDD storage data.

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 14 shows the correspondences of security objectives, assumptions, threats, and organizational security policies. Table 15 shows that each security problem is covered by the defined security objectives.

Table 14: Completeness of Security Objectives

Threats/ Policies/	Security Objectives

Assumptions	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.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.DATA.ENCRYPTED	O.DATA.OVERWRITTEN	O.FAX.DATA.FORMAT	O.INFO.FLOW_CONTROLED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED	OE.AUDIT_STORAGE.PROTECTED	OE.AUDIT_ACCESS.AUTHORIZED	OE.TIME_STAMP.RELIABLE	OE.NETWORK.TRUST	OE.SSL.SECURE	OE.OS.TRUST	OE.DBMS.MANAGED	OE.AUTH_SERVER.SECURE	OE.EXT_SERVER.SECURE	OE.SSL_CERT.INSTALL	OE.KEY_GENERATION
T.DOC.DIS	✓						✓	✓					✓	✓																				
T.DOC.ALT		✓					✓	✓																										
T.FUNC.ALT			✓				✓	✓																										
T.FAX.MAL															✓																			
T.PROT.ALT				✓			✓	✓																										
T.CONF.DIS					✓		✓	✓					✓	✓																				
T.CONF.ALT						✓	✓	✓																										
T.DATA.MAL																✓																		
P.USER.AUTHORIZATION							✓	✓																										
P.SOFTWARE.VERIFICATION									✓																									
P.AUDIT.LOGGING										✓	✓	✓					✓							✓	✓									
P.INTERFACE.MANAGEMENT																		✓		✓														
A.ACCESS.MANAGED																			✓															
A.ADMIN.TRAINING																					✓													
A.ADMIN.TRUST																						✓												
A.USER.TRAINING																							✓											
A.TIME_STAMP.RELIABLE																										✓								
A.NETWORK.TRUST																											✓							
A.SSL.SECURE																												✓						
A.OS.TRUST																													✓					
A.DBMS.MANAGED																														✓				
A.AUTH_SERVER.SECURE																															✓			
A.EXT_SERVER.SECURE																																✓		
A.SSL_CERT.INSTALL																																	✓	
A.KEY_GENERATION																																		✓

Table 15: Sufficiency of Security Objectives

Threats, Policies, and Assumptions	Summary	Objectives and Rationale
T.DOC.DIS	User Document Data may be	O.DATA.ENCRYPTED protects D.DOC from

Threats, Policies, and Assumptions	Summary	Objectives and Rationale
	disclosed to unauthorized persons	unauthorized disclosure
		O.DATA.OVERWRITTEN allows the access of audit records only by authorized 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. FAX.MAL	D.FUNC may be affected by malicious fax-input data.	O. FAX.DATA.FORMAT protect D.FUNC from malicious data through a fax line
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.DATA.ENCRYPTION protects audit records from unauthorized access, deletion and modification.
		O.DATA.OVERWRITTEN protects D.DOC from unauthorized disclosure.
		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

Threats, Policies, and Assumptions	Summary	Objectives and Rationale
		responsibility of the TOE Owner to appropriately grant authorization.
T. DATA.MAL	TOE may be affected by malicious input data.	O.INFO.FLOW_CONTROLED protect Malicious data through network.
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
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.
A.TIME_STAMP.RELIABLE	The operational environment of the TOE synchronizes its time with NTP server and provides a reliable time stamp to mark entries in the security log.	OE.TIME_STAMP.RELIABLE ensures that the operational environment of the TOE synchronizes its time with NTP server and provides a reliable time stamp for recording correct security audit log entries.
A.NETWORK.TRUST	A firewall system is installed	OE.NETWORK.TRUST ensures that a firewall

Threats, Policies, and Assumptions	Summary	Objectives and Rationale
	between internal network and external network to protect the TOE from inward intrusion from outside.	system is installed between the internal network and external networks.
A.SSL.SECURE	SSL protocol protects transferred data between U.USER and the TOE.	OE.SSL.SECURE ensures that the SSL protocol protects transferred data between users and the TOE.
A.OS.TRUST	Administrators remove unnecessary services and means of operating system, and reinforce vulnerabilities upon operating system, and thus ensure reliability and security of the TOE.	OE.OS.TRUST ensures that administrators remove unnecessary services and means of the operating system, and reinforce vulnerabilities of the operating system.
A.DBMS.MANAGED	DBMS provides a series of functions including audit log selecting and ordering function, audit log storage protection, and maintenance of audit log integrity.	OE.DBMS.MANAGED ensures that the DBMS provides a series of functions including audit log selecting and ordering functions, audit log storage protection, and maintenance of audit log integrity.
A.AUTH_SERVER.SECURE	The authentication servers (i.e. LDAP, Kerberos, and SMB Server) provide a secure remote authentication for U.NORMAL.	OE.AUTH_SERVER.SECURE ensures that the authentication servers (i.e. LDAP, Kerberos, and SMB Servers) provide a secure remote authentication for U.NORMAL.
A.EXT_SERVER.SECURE	FTP server, WebDAV, and mail server which store fax and scan data transmitted from the TOE are managed securely.	OE.EXT_SERVER.SECURE ensures that FTP server, WebDAV, and mail servers that store fax and scan data transmitted from the TOE are managed securely.
A.SSL_CERT.INSTALL	Certificate for SSL communication is installed by U.ADMINISTRATOR and the TOE is managed through the secure channel.	OE.SSL_CERT.INSTALL ensures that U.ADMINISTRATOR shall manage the TOE through a secure channel after the certificate for SSL communication is installed in the TOE.
A.KEY_GENERATION	TPM provides cryptographic keys to TOE for encryption/decryption of HDD storage data.	OE. KEY_GENERATION ensures that TPM provides cryptographic keys (private key, public key, and secure key) to TOE for secure encryption/decryption of HDD storage data.

5   Extended Component Definition

There is no extended component definition in this ST.

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 16: 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 17: 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 18: 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 neither disclosure nor 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.

Functions

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

Table 19: 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.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs

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 20: 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.

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.
+DSR	Indicates data that are associated with a document storage and retrieval job.

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 21: External Entities

Designation	Definition
NTP Server	The NTP (Network Time Protocol) server synchronizes the clock of the operating system, which is crucial for audit logs.
Kerberos Server	It is the authentication server via Kerberos. The authentication servers identify and authenticate U.NORMAL if remote authentication mode is enabled
LDAP Server	It is the authentication server via LDAP. The authentication servers identify and authenticate U.NORMAL if remote authentication mode is enabled
SMB Server	It is the authentication server via SMB. The authentication servers identify and authenticate U.NORMAL if remote authentication mode is enabled
FTP Server	The MFP send received fax and scan data from the TOE to a server via FTP
WebDAV Server	The MFP send received fax and scan data from the TOE to a server via WebDAV
Mail Server	The MFP send received fax and scan data from the TOE to a server via a Mail server

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.

- **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

Table 22 summarizes the security functional requirements defined by this ST.

Table 22: Security Functional Requirements

Class	Component	
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SEL.1	Selective audit
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Cryptographic Support	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1(1)(2)	Subset access control
	FDP_ACF.1(1)(2)	Security attribute based access control
	FDP_ETC.1	Export of user data without security attributes
	FDP_IFC.1(1)(2)(3)(4)	Subset information flow control
	FDP_IFF.1(1)(2)(3)(4)	Simple security attributes
	FDP_RIP.1	Subset residual information protection
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
	FIA_USB.1	User-subject binding
Security Management	FMT_MOF.1	Management of functions in TSF
	FMT_MSA.1	Management of security attributes

Class	Component	
	FMT_MSA.3(1)(2)	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_TST.1	TSF testing
TOE Access	FTA_SSL.3	TSF-initiated termination

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:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 23;** [The Auditable Events specified in Table 23 below].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) 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 23: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [none].

Table 23: Audit data

Relevant SFR	Auditable Events	Additional Information
FDP_ACF.1(1)	Job completion	-Type of job

FIA_UAU.2	Both successful and unsuccessful use of the authentication mechanism	-
FIA_UID.2	Both successful and unsuccessful use of the identification mechanism	-
FTA_SSL.3	Termination of an interactive session by the session termination mechanism	-
FMT_MTD.1	Log data access and deletion	-
FMT_MOF.1	Modification of the setting of the audit log generation function items	-
FPT_TST.1	Execution of the TSF self tests and the results of the tests	-

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 [authorized system 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_SEL.1 Selective audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) *event type*

b) [none]

6.1.1.6 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 unauthorised deletion.

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

6.1.1.7 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.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite used cryptographic key using newly generated cryptographic key] that meets the following: [none].

6.1.2.2 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [HDD data encryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [256-bit] that meet the following: [none].

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 [Custom Access Control SFP in Table 24] on [the list of users as subjects, objects, and operations among subjects and objects covered by the Custom Access Control SFP in Table 24].

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 25] 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 TOE Function Access Control SFP in Table 25].

6.1.3.3 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 initialisation

FDP_ACF.1.1(1) The TSF shall enforce the [Custom Access Control SFP in Table 24] to objects based on the following: [the list of users as subjects and objects controlled under the Custom Access Control SFP in Table 24, and for each, the indicated security attributes in Table 24].

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 Custom Access Control SFP in Table 24 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 authorise 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 24: Custom Access Control SFP

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

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.
	+DSR	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.

6.1.3.4 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 25] to objects based on the following: [the list of users as subjects and objects controlled under the TOE Function Access Control SFP in Table 25, and for each, the indicated security attributes in Table 25].

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: [rules specified in the TOE Function Access Control SFP in Table 25 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects].

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [the user acts in the role U.ADMINISTRATOR].

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

Table 25: TOE Function Access Control SFP

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

6.1.3.5 FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the [SCN Access Control , FAX Access Control, DSR Access Control] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

6.1.3.6 FDP_IFC.1(1) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(1) The TSF shall enforce the [MAC filtering rule] on [list of subjects (External IT entities), list of information (packet), operations (allow, deny)].

6.1.3.7 FDP_IFC.1(2) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(2) The TSF shall enforce the [IP filtering rule] on [list of subjects (External IT entities), list of information (packet), operations (allow, deny)].

6.1.3.8 FDP_IFC.1(3) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(3) The TSF shall enforce the [FAX data control] on [list of subjects (External IT entities), list of information (fax data), operations (discard)].

6.1.3.9 FDP_IFC.1(4) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(4) The TSF shall enforce the [Protocol/Port information flow control] on [list of subjects (External IT entities), list of information (packet), operation (allow)].

6.1.3.10 FDP_IFF.1(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(1) The TSF shall enforce the [MAC filtering rule] based on the following types of subject and information security attributes: [list of subjects (External IT entities), list of information (packet), security attributes of subjects (MAC Address), security attributes of information (MAC Address)].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

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

   b) If U.ADMINISTRATOR registers specific MAC filtering rules, all packets via MAC address registered by U.ADMINISTRATOR are not allowed]

FDP_IFF.1.3(1) The TSF shall enforce the [none].

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.11 FDP_IFF.1(2) 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(2) The TSF shall enforce the [IP filtering rule] based on the following types of subject and information security attributes: [list of subjects (External IT entities), list of information (packet), security attributes of subjects(IP Address), security attributes of information(IP Address)].

FDP_IFF.1.2(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) All packets are allowed if there is no IP filtering rule registered by U.ADMINISTRATOR

    b) If U.ADMINISTRATOR registers specific IP filtering rules, all packets are only allowed as IP filtering rule registered by U.ADMINISTRATOR.]

FDP_IFF.1.3(2) The TSF shall enforce the [none].

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.12 FDP_IFF.1(3) 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(3) The TSF shall enforce the [FAX data control] based on the following types of subject and information security attributes: [list of subjects (External IT entities), list of information (fax data), security attributes of subjects (none), security attributes of information (fax image format)].

FDP_IFF.1.2(3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

    a) Discard the fax data if the incoming fax data is not standardized MMR, MR, or MH of T.4 specification]

FDP_IFF.1.3(3) The TSF shall enforce the [none].

FDP_IFF.1.4(3) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5(3) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.13 FDP_IFF.1(4) 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(4) The TSF shall enforce the [Protocol/Port information flow control] based on the following types of subject and information security attributes: [list of subjects (External IT entities), list of information (packet), security attributes of subjects (none), security attributes of information (Protocol type, Port number)].

FDP_IFF.1.2(4) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [
   a)   All packets are denied except for the Protocol/Port explicitly enabled by U.ADMINISTRATOR]

FDP_IFF.1.3(4) The TSF shall enforce the [none].

FDP_IFF.1.4(4) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5(4) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3.14 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, temporary data, system data].

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 *U.Administrator configurable positive integer within [1 ~ 99 (default value: 3)]* unsuccessful authentication attempts occur related to [U.USER authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *exceeded*, the TSF shall [disabling of the account for 3 minutes (default value; can be set to 1-59 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, User Name, Password, Email, Fax No, and Group ID].

6.1.4.3 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 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 [*, •] to the user while the authentication is in progress**.**

6.1.4.5 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 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].

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: [U.ADMINISTRATOR associates subjects with Group ID (including role) assigned to User ID when U.USER logs in].

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: [TSF re-associates subjects with User ID in a group when U.ADMINISTRATOR changes group ID including role].

6.1.5   Class FMT: Security management

6.1.5.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behavior of, disable, and enable* the functions [list of security functions in Table 26] to [U.ADMINISTRATOR].

Table 26: Management of Security Functions Behavior

Security Function	Selection Operation		
	determine the behavior of	disable	enable
System Reboot			○
Authentication Mode	○		○
Log in Identification	○	○	○
Log in Restriction	○	○	○
Log out Policy	○	○	○
Log Configuration		○	○
Secure HTTP		○	○
IP/MAC Filtering	○	○	○
Image Overwrite	○	○	○
Data Encryption			○
Self Testing		○	○

6.1.5.2 FMT_MSA.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 The TSF shall enforce the [Custom access control SFP, TOE Function Access Control SFP, MAC filtering rule, IP filtering rule, Protocol/Port information flow control**]** to restrict

the ability to *query, modify, delete, [add]* the security attributes [list of security attributes in Table 27] to [U.ADMINISTRATOR].

Table 27: Management of Security Attributes

Security Attributes	Selection Operation			
	query	modify	delete	[add]
MAC Address	○	○	○	○
IPv4 or IPv6 Address	○	○	○	○
Protocol (to deny)	○	○		
Port	○	○		
User group ID	○	○	○	○

6.1.5.3 FMT_MSA.3(1) Static attribute initialisation

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 [FAX data control, Protocol/Port information flow control] 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 [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.4 FMT_MSA.3(2) Static attribute initialisation

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 [Custom access control SFP, TOE Function Access Control SFP, MAC filtering rule, IP filtering rule] to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.5 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 The TSF shall restrict the ability to *query, modify, delete, [add]* the [list of TSF data in Table 28] to [the authorized identified roles in Table 28]

Table 28: Management of TSF data

TSF data	Selection Operation				the authorized identified roles
	query	modify	delete	[add]	
Password of Secured Box		○	○	○	U.ADMINISTRATOR
Kerberos Server Configuration	○	○	○	○	
SMB Server Configuration	○	○	○	○	
LDAP Server Configuration	○	○	○	○	
FTP Server Configuration	○	○			
Webdav Server Configuration	○	○			
SMTP Server Configuration	○	○			
Address Box	○	○	○	○	
Log in Identification	○	○			
Log in Restriction	○	○			
Log out Policy	○	○			
User Role (Authority)	○	○	○	○	
External User Role	○	○	○	○	
User Profile (Id, Password, PIN Code, Group)	○	○	○	○	
Group Profile (Name, Role)	○	○	○	○	
Audit Log Data	○		○		
Network Protocol and Port Configuration (Raw TCP/IP Printing, LPR/LPD, HTTP, HTTPS, SLP, UPnP, mDNS, WINS, DDNS, TCP/IPv4, TCP/IPv6, IPP, SNMP, SMTP, SetIP, SNTP)	○	○			
Digital Certificate	○	○	○	○	
IPv4/6 filtering Address	○	○	○	○	
Mac filtering Address	○	○	○	○	
Image Overwrite configuration	○	○			
Encryption Key data			○	○	
Application Management	○	○	○	○	
Password(U.NORMAL)		○			U.NORMAL

6.1.5.6 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 29].

Table 29: Management Functions

Management Functions	Relevant SFR
Management of Audit data (review, delete)	FAU_GEN.1, FAU_SEL.1
Management of Custom Access Control rules	FDP_ACC.1(1), FDP_ACF.1(1)
Management of TOE Function Access Control rules	FDP_ACC.1(2), FDP_ACF.1(2)
Management of export of user data	FDP_ETC.1
Management of MAC filtering rules	FDP_IFC.1(1), FDP_IFF.1(1)
Management of IP filtering rules	FDP_IFC.1(2), FDP_IFF.1(2)
Management of Protocol/Port information flow control rules	FDP_IFC.1(4), FDP_IFF.1(4)
Management of Image overwrite function	FDP_RIP.1
Management of login restriction	FIA_AFL.1
Management of User attributes (User ID, User Name, Password, Email, Fax No, and Group ID)	FIA_ATD.1, FIA_UID.2, FIA_UAU.2
Management of security functions behavior	FMT_MOF.1
Management of security attributes	FMT_MSA.1
Management of TSF data	FMT_MTD.1
Management of security roles (User Group ID)	FMT_SMR.1
Management of TSF testing (initiation)	FTP_TST.1
Management of TSF-initiation termination (SWS session inactivity time)	FTA_SSL.3

6.1.5.7 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].

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_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 *[TSF_NVE]*

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

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *[TSF_NVE]*.

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 [1-120 minutes of U.ADMINISTRATOR and U.NORMAL inactivity (default: 5 minutes)].

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 EAL3 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 30: Security Assurance Requirements (EAL3 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

Assurance Class	Assurance components	
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures (augmentation of EAL3)
	ALC_LCD.1	Developer defined life-cycle model
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	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 summarise 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 initialisation 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.3 Functional specification with complete summary

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from SFR-enforcing actions and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.3.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.2.3 ADV_TDS.2 Architectural design

Dependencies: ADV_FSP.3 Functional specification with complete summary

Developer action elements:

ADV_TDS.2.1D	The developer shall provide the design of the TOE.
ADV_TDS.2.2D	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.2.1C	The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.2.2C	The design shall identify all subsystems of the TSF.
ADV_TDS.2.3C	The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.
ADV_TDS.2.4C	The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.2.5C	The design shall summarise the SFR-supporting and SFR-non-interfering behavior of the SFR-enforcing subsystems.
ADV_TDS.2.6C	The design shall summarise the behaviour of the SFR-supporting subsystems.
ADV_TDS.2.7C	The design shall provide a description of the interactions among all subsystems of the TSF.
ADV_TDS.2.8C	The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

Evaluator action elements:

ADV_TDS.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.2.2E	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.3 Authorisation controls

Dependencies:	ALC_CMS.1 TOE CM coverage
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model

Developer action elements:

ALC_CMC.3.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.3.2D	The developer shall provide the CM documentation.
ALC_CMC.3.3D	The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.3.1C	The TOE shall be labelled with its unique reference.
ALC_CMC.3.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.3.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.3.4C	The CM system shall provide measures such that only authorised changes are made to the configuration items.
ALC_CMC.3.5C	The CM documentation shall include a CM plan.
ALC_CMC.3.6C	The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.3.7C	The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.3.8C	The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

ALC_CMC.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.2 ALC_CMS.3 Implementation representation CM coverage

Dependencies:	No dependencies.

Developer action elements:

ALC_CMS.3.1D	The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.3.1C	The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.
ALC_CMS.3.2C	The configuration list shall uniquely identify the configuration items.
ALC_CMS.3.3C	For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.3.1E   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_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D   The developer shall produce and provide development security documentation.

Content and presentation elements:

ALC_DVS.1.1C   The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Evaluator action elements:

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

ALC_DVS.1.2E   The evaluator shall confirm that the security measures are being applied.

6.2.4.5 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.

6.2.4.6 ALC_LCD.1 Developer defined life-cycle model

Dependencies: No dependencies.

Developer action elements:

ALC_LCD.1.1D	The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.
ALC_LCD.1.2D	The developer shall provide life-cycle definition documentation.

Content and presentation elements:

ALC_LCD.1.1C	The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.
ALC_LCD.1.2C	The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E	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.2 Analysis of coverage

Dependencies:	ADV_FSP.2 Security-enforcing functional specification
	ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.2.1D   The developer shall provide an analysis of the test coverage.

Content and presentation elements:

ATE_COV.2.1C   The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C   The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

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

6.2.5.2 ATE_DPT.1 Testing: basic design

Dependencies:	ADV_ARC.1 Security architecture description
	ADV_TDS.2 Architectural design
	ATE_FUN.1 Functional testing

Developer action elements:

ATE_DPT.1.1D   The developer shall provide the analysis of the depth of testing.

Content and presentation elements:

ATE_DPT.1.1C   The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C   The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

Evaluator action elements:

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

6.2.5.3 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.

6.2.5.4 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.

Table 31: Completeness of security functional requirements

	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.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.AUDIT_STORAGE.PROTECTED	O.AUDIT_ACCESS.AUTHORIZED	O.DATA.ENCRYPTED	O.DATA.OVERWRITTEN	O.FAX_DATA.FORMAT	O.INFO.FLOW_CONTROLED
FAU_GEN.1										✔						
FAU_GEN.2										✔						

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FAU_SAR.1												✓			
FAU_SAR.2												✓			
FAU_SEL.1										✓					
FAU_STG.1											✓				
FAU_STG.4											✓				
FCS_CKM.4													✓		
FCS_COP.1													✓		
FDP_ACC.1(1)	✓	✓	✓												
FDP_ACC.1(2)							✓								
FDP_ACF.1(1)	✓	✓	✓												
FDP_ACF.1(2)							✓								
FDP_ETC.1	✓														
FDP_IFC.1(1)															✓
FDP_IFC.1(2)															✓
FDP_IFC.1(3)														✓	
FDP_IFC.1(4)															✓
FDP_IFF.1(1)															✓
FDP_IFF.1(2)															✓
FDP_IFF.1(3)														✓	
FDP_IFF.1(4)															✓
FDP_RIP.1	✓												✓		
FIA_AFL.1							✓								
FIA_ATD.1							✓								
FIA_UAU.2							✓	✓							
FIA_UAU.7							✓								
FIA_UID.2	✓	✓	✓	✓	✓	✓	✓	✓		✓					
FIA_USB.1							✓								
FMT_MOF.1								✓							
FMT_MSA.1	✓	✓	✓				✓								
FMT_MSA.3(1)															✓
FMT_MSA.3(2)	✓	✓	✓				✓								✓
FMT_MTD.1				✓	✓	✓									
FMT_SMF.1	✓	✓	✓	✓	✓	✓									
FMT_SMR.1	✓	✓	✓	✓	✓	✓	✓								
FPT_TST.1									✓						
FTA_SSL.3							✓	✓							

Table 32: Security Requirements Rationale

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS	Protection of User Data from	FDP_ACC.1(1)	Enforces protection by establishing

Objectives	Description	SFRs	Purpose
O.DOC.NO_ALT O.FUNC.NO_ALT	unauthorized disclosure or alteration		an access control policy.
		FDP_ACF.1(1)	Supports the access control policy by providing an access control function.
		FIA_UID.2	Supports access control and security roles by requiring user identification.
		FMT_MSA.1	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_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.
O.DOC.NO_DIS	Protection of User Document Data from unauthorized disclosure	FDP_ETC.1	Supports access control policy by exporting the user data without the user data's associated security attributes.
		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.2	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 roles.
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.2	Enforces authorization by requiring user authentication.
		FIA_UAU.7	Supports authorization by protecting authentication feedback.

Objectives	Description	SFRs	Purpose
		FIA_UID.2	Enforces authorization by requiring user identification.
		FIA_USB.1	Enforces authorization by distinguishing subject security attributes associated with user roles.
		FMT_MSA.1	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	FIA_UAU.2	Enforces management of external interfaces by requiring user authentication.
		FIA_UID.2	Enforces management of external interfaces by requiring user identification.
		FMT_MOF.1	Enforces management of security functions behavior by restricting the ability to U.ADMINISTRATOR.
		FTA_SSL.3	Enforces management of external interfaces by terminating inactive sessions.
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.
		FAU_SEL.1	Supports audit policies by providing the ability to select the set of events to be audited.
		FIA_UID.2	Supports audit policies by associating a user's identity 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.	Access control of audit records only by authorized	FAU_SAR.1	Enforces the audit review function by providing authorized

Objectives	Description	SFRs	Purpose
AUTHORIZED	persons		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 all users read access to the audit records, except those users that have been granted access specifically.
O.DATA. ENCRYPTED	Encryption of the data to be stored into the HDD	FCS_CKM.4	Supports encryption of the data to be stored on the HDD by destructing cryptographic keys.
		FCS_COP.1	Supports encryption of the data to be stored on the HDD by performing a cryptographic operation.
O.DATA. OVERWRITTEN	Image overwrite to protect the used document data in the HDD	FDP_RIP.1	Enforces protection by making residual data unavailable.
O.FAX_DATA.FOR MAT	Block incoming fax data if received fax data does not qualify fax image standard.	FDP_IFC.1(3)	Enforces protection by establishing a FAX data control policy.
		FDP_IFF.1(3)	Supports FAX data control policy by providing information flow control function.
O.INFO.FLOW_CO NTROLED	Control inflowing information data that are not allowed from external network.	FDP_IFC.1(1)	Enforces protection by establishing a MAC filtering rule policy.
		FDP_IFC.1(2)	Enforces protection by establishing an IP filtering rule policy.
		FDP_IFC.1(4)	Enforces protection by establishing a Protocol/Port information flow control policy.
		FDP_IFF.1(1)	Supports the MAC filtering rule policy by providing an information flow control function.
		FDP_IFF.1(2)	Supports the IP filtering rule policy by providing an information flow control function.
		FDP_IFF.1(4)	Supports the Protocol/Port information flow control policy by providing an information flow control function.
		FMT_MSA.3(1)	Supports the access control and information flow control function by enforcing control of security attribute defaults.
		FMT_MSA.3(2)	Supports access control and information flow control function by enforcing control of security attribute defaults.

6.3.2   Security Assurance Requirements Rationale

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 3 is appropriate.

EAL 3 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

FAU_GEN.1 has a dependency relationship with FPT_STM.1. However, because the TOE records security events correctly with reliable time-stamps, FAU_GEN.1 is satisfied by OE.TIME_STAMP.RELIABLE of operational environment instead of FPT_STM.1.

FCS_CKM.4, FCS_COP.1 has a dependency relationship with FCS_CKM.1. However, because the TPM offers a key for encrypting/decrypting HDD data to the TOE, FCS_CKM.1 is satisfied by OE.KEY_GENERATION of operational environment instead of FCS_CKM.1.

FIA_AFL.1 and FIA_UAU.7 have a dependency relationship with FIA_UAU.1, but they are satisfied by FIA_UAU.2 that has a hierarchical relationship with FIA_UAU.1.

FIA_GEN.2, FIA_UAU.2 and FMT_SMR.1 have a dependency relationship with FIA_UID.1, but they are satisfied by FIA_UID.2 that has a hierarchical relationship with FIA_UID.1.

Table 33: Dependencies on the TOE Security Functional Components

No.	Functional Component ID	Dependencies	Reference
1	FAU_GEN.1	FPT_STM.1	OE.TIME_STAMP.RELIABLE
2	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Hierarchically by FIA_UID.2

3	FAU_SAR.1	FAU_GEN.1	
4	FAU_SAR.2	FAU_SAR.1	
5	FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	
6	FAU_STG.1	FAU_GEN.1	
7	FAU_STG.4	FAU_STG.1	
8	FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	OE.KEY_GENERATION
9	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	OE.KEY_GENERATION
10	FDP_ACC.1	FDP_ACF.1	
11	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	
12	FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	
13	FDP_IFC.1	FDP_IFF.1	
14	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	
15	FDP_RIP.1	-	
16	FIA_AFL.1	FIA_UAU.1	Hierarchically by FIA_UAU.2
17	FIA_ATD.1	-	
18	FIA_UAU.2	FIA_UID.1	Hierarchically by FIA_UID.2
19	FIA_UAU.7	FIA_UAU.1	Hierarchically by FIA_UAU.2
20	FIA_UID.2	-	
21	FIA_USB.1	FIA_ATD.1	
22	FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	
23	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	
24	FMT_MSA.3		
25	FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	
26	FMT_SMF.1	-	

27	FMT_SMR.1	FIA_UID.1	Hierarchically by FIA_UID.2
28	FPT_TST.1	-	
29	FTA_SSL.3	-	

6.4.2 SAR Dependencies

The dependency of each assurance package (EAL3) provided by the CC is already satisfied.

ALC_FLR.2 added to the assurance package (EAL3) 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)

7.1.1 Identification & Authentication (TSF_FIA)

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

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.

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

In the authentication process, only ambiguous feedback, like a user's password displayed as * or •, are provided to protect users from dictionary attack and leakage of user information.

U. ADMINISTRATOR can choose the authentication method for user authentication.

-Basic authentication: Activate basic authentication. U.USER is asked to login when options available only to U. ADMINISTRATOR are selected.

-Device authentication: Activate device authentication. Device authentication requests U.USER to login before using all device applications. U.USER cannot use any application without logging in.

U. ADMINISTRATOR can choose 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. ADMINISTRATOR can configure the Log in Restriction & Log out Policy.

U.ADMINISTRATOR can set the limit number of consecutive invalid authentication attempts from between 1 to 99 (default value: 3). When the number of consecutive invalid authentication attempts has exceeded the limit number set by U.ADMINISTRATOR within 3 minutes (default value: can be set to 1-59 minutes), the account will be locked for 3 minutes (default value; can be set to 1-59 minute(s)). If U.USER is idle for 5 minutes (default value: can be set to 1-120 minutes), the mutual session will be terminated automatically.

U.NORMAL password should be at least 4-characters long (default value; can be set to 4-63 characters long)

U.ADMINISTRATOR password should be at least 8-characters long and at least 1 number,1 special character, and 1 alphabetical character .

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).

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

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

-User profile: The TSF shall store user information on the machine's hard drive. U.ADMINISTRATOR can use this feature to manage the users using the machine. U.ADMINISTRATOR can also group the users and manage them as a group. U.ADMINISTRATOR can add up to 1,000 entries. The U.USER identified by user ID and password is allowed to modify his/her password. U.USER is allowed to view all of U.USER's own profile information. When it comes to the role, U.USER is allowed to see only the role to which he/she belongs.

TOE enforces the Custom Access Control & TOE Function Access Control based on the user role assigned to 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/document storage retrieval functions offered by the MFP.

-Custom Access Control rule

U.NORMAL is able to perform operations (modify & delete) on the objects (D.DOC & D.FUN) owned by his/her own when doing print/scan/fax-in/fax-out job, and U.NORMAL is able to perform operations (read) on the objects (D.DOC) owned by his/her own when doing a document storage and retrieval job. However, there is no access control restriction associated with a copy job. Additionally, the image data (.jpg, .bmp, .tiff, etc.) generated at the result of the fax/scan/document storage and retrieval job could be exported to a external server (SMB Server, FTP Server, Webdav Server, Mail Server) without security attributes associated with the user data.

-TOE Function Access Control

U.NORMAL is able to access and execute the printing/scanning/copying/faxing/document storage and retrieval functions explicitly authorized by U.ADMINISTRATOR to use the function.

User authentication is requested before accessing store print or the secure box.

This authentication needs to configure the password from the print driver, and it is used for loading a stored file using the control panel.

- Secure box

U.USER can save PC-printed, faxed, scanned, or copied documents in the box and print the saved documents later, and if U.USER wants the box to be a secured box, check the Secured Box and enter the password to be used for accessing the box.

- Store print & Confidential print

Confidential print is used for printing confidential documents. U.USER needs to enter a password to print it. Store print also only allows the U.USER who stored the file to access the file with the password by setting the secret property.

7.1.2 Network Access Control (TSF_NAC)
Relevant SFR: FDP_IFC.1(1)(2)(4), FDP_IFF.1(1)(2)(4)

The MFP system including the TOE has a network interface card (network card) connected to an external network. The MFP system can send/receive data and MFP configuration information and, thus, is able to configure MFP settings.

There are two methods to control access to the MFP from outside of the TOE through a network;

- Protocol/Port control:

1) Network protocols: Raw TCP/IP Printing, LPR/LPD, HTTP, SLP, UPnP, mDNS, WINS, SNMPv1/v2, SetIP

IPv6, HTTPS, DDNS, WSD, SNMPv3 Protocol, SNTP Protocol

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

A standard communication protocol and a port performs as a logical network channel. These services start up simultaneously as the system's network card boots. Among these services, the service that uses upper protocol utilizes a predefined "Well-known port".

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. Only U.ADMINISTRATOR can configure these functions, and these configurations are altered on each reboot of network card, and thus MFP system information and electronic image data are protected from unauthorized reading and falsification.

All packets are denied if there is no Protocol/Port information flow control rule allowed (enabled) by U.ADMINISTRATOR except for Raw TCP/IP Printing, LPR/LPD, HTTP, SLP, UPnP, mDNS, WINS, SNMPv1/v2, SetIP.

- IP and Mac Filtering:

U.ADMINISTRATOR can manage filtering rules for IPv4/IPv6 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

7.1.3   Security Management (TSF_FMT)

Relevant SFR: FMT_MOF.1, FMT_MSA.1, 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 TSF shall restrict the ability to determine the behavior of, and disable/enable the functions accessible to U.ADMINISTRATOR.

Table 34 : Management of Security Functions Behavior

Security Function	Selection Operation		
	determine the behavior of	disable	enable
System Reboot			○
Authentication Mode	○		○
Log in Identification	○	○	○
Log in Restriction	○	○	○
Log out Policy	○	○	○
Log Configuration		○	○
Secure HTTP		○	○
IP/MAC Filtering	○	○	○
Image Overwrite	○	○	○
Data Encryption			○
Self Testing		○	○

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

Table 35 : Management of Security Attributes

Security Attributes	Selection Operation			
	query	modify	delete	[add]
MAC Address	○	○	○	○
IPv4 or IPv6 Address	○	○	○	○
Protocol (to deny)	○	○		
Port	○	○		
User group ID	○	○	○	○

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

Table 36 : Management of TSF data

TSF data	Selection Operation				the authorized identified roles
	query	modify	delete	[add]	
Password of Secured Box		○	○	○	U.ADMINISTRATOR
Kerberos Server Configuration	○	○	○	○	
SMB Server Configuration	○	○	○	○	
LDAP Server Configuration	○	○	○	○	
FTP Server Configuration	○	○			
Webdav Server Configuration	○	○			
SMTP Server Configuration	○	○			
Address Box	○	○	○	○	
Log in Identification	○	○			
Log in Restriction	○	○			
Log out Policy	○	○			
User Role (Authority)	○	○	○	○	
External User Role	○	○	○	○	
User Profile (Id, Password, PIN Code, Group)	○	○	○	○	
Group Profile (Name, Role)	○	○	○	○	
Audit Log Data	○		○		
Network Protocol and Port Configuration (Raw TCP/IP Printing, LPR/LPD, HTTP, HTTPS, SLP, UPnP, mDNS, WINS, DDNS, TCP/IPv4, TCP/IPv6, IPP, SNMP, SMTP, SetIP, SNTP)	○	○			
Digital Certificate	○	○	○	○	
IPv4/6 filtering Address	○	○	○	○	
Mac filtering Address	○	○	○	○	
Image Overwrite configuration	○	○			
Encryption Key data			○	○	
Application Management	○	○	○	○	
Password(U.NORMAL)		○			U.NORMAL

There are two types of Users:　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, Document Box) of the TOE and to modify his/her own password.

U.NORMAL 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, but in case that U.ADMINISTRATOR gives the permission of admin role to U.NORMAL, then the U.NORMAL is also allowed to access the security management.

7.1.4   Security Audit (TSF_FAU)

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

The TSF provides an internal capability to generate an 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, success or failure, log out, access and delete, 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 TSF can select the set of events to be audited from the set of all auditable events based on the event type.

The TSF protects the stored audit records in the audit trail from unauthorized deletion. Only U.ADMINISTRATOR can delete audit log data. Additionally, the TSF provides a capability to export audit log data from the TOE.

The TOE can store up to 15,000 for all log events.

(The maximum number for each log event: job log: 10,000; security log: 5,000; operation log: 5,000) When each log events exceeds the maximum number, the TOE deletes the oldest stored audit records (10% of each log data) and generates an audit record of deletion.

After that, a new audit log is generated.

Table 37: Security Audit Event

Relevant SFR	Auditable Events	Additional Information
FDP_ACF.1(1)	Job completion	-Type of job
FIA_UAU.2	Both successful and unsuccessful use of the authentication mechanism	-
FIA_UID.2	Both successful and unsuccessful use of the identification mechanism	-
FTA_SSL.3	Termination of an interactive session by the session termination mechanism	-
FMT_MTD.1	Log data access and deletion	-
FMT_MOF.1	Modification of the setting of the audit log generation function items	-
FPT_TST.1	Execution of the TSF self tests and the results of the tests	-

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, scan-to-SMB, or scan-to-WebDAV task processes). Also, users can delete their own files stored in the TOE. 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 procedures set by U.ADMINISTRATOR, which are DoD 5200.28-M, Australian ACSI 33, and German standard (VSITR) standard, and Custom, and then the main controller reboots. If there are any problems during overwriting, the Manual Image Overwrite job automatically restarts to overwrite the remaining area.

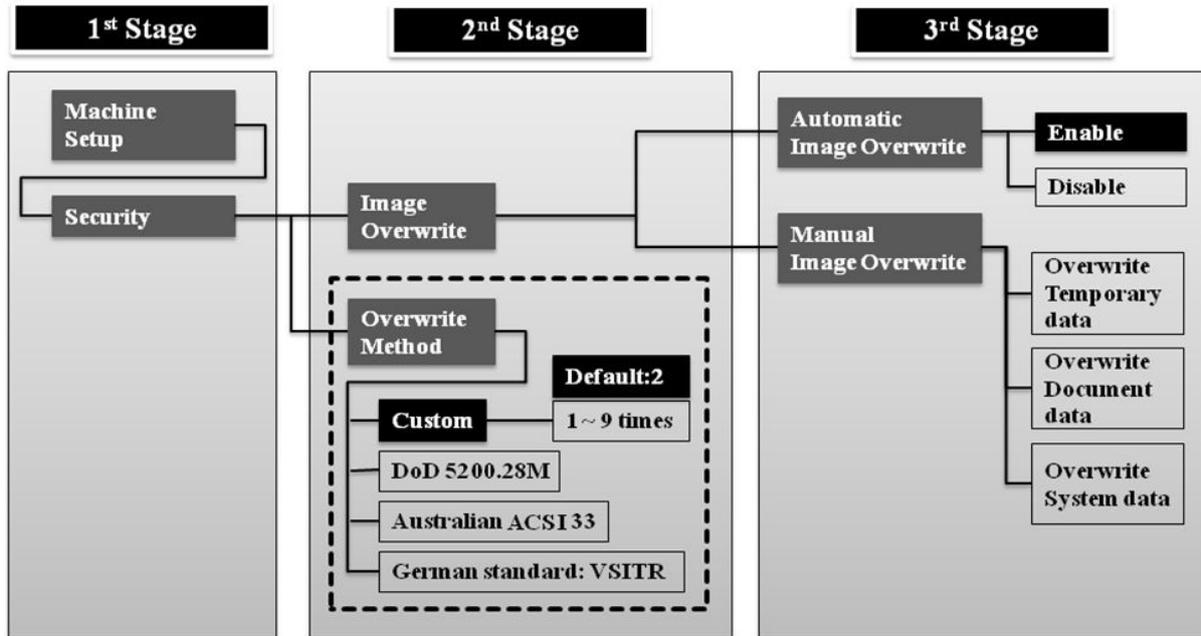The options for U.ADMINISTRATOR to configure the Image Overwrite are as follows:.

Figure 4: The process of Image Overwrite

Manual Image Overwrite will remove all data in the partitions selected. The user shall select more than one area to be overwritten from options below:

Table 38: The options for Image Overwrite

options	Data stored	Partition
Overwrite Temporary data	Temp data, Job data including delayed jobs, Pending jobs	HDD_DOC_SPOOL DOC_DOC_SWAP DOC_DOC_PRINT
Overwrite Document data	Box data, Secure Jobs	HDD_DOC
Overwrite System data	User profile, Address book, Device settings, complete job queue	HDD_SYS

U.ADMINISTRATOR shall select the algorithm to overwrite the area

● Custom: 1~9 times (default: 3)

● DoD 5200.28M (3 times)

● Australian ACSI 33 (5 times)

● German standard: VSITR (7 times)

Automatic Image Overwrite will remove temporary area used for job operation after job completion. U.ADMINISTRATOR shall select enable/disable.

7.1.6 Data Encryption (TSF_NVE)

Relevant SFR: 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 requests generating cryptographic keys (private key, public key, secure key) to TPM in the operational environment of the TOE for when the TOE is initialized at the first setout. Private and public keys are used for encrypting and decrypting the secure key stored in the EEPROM, and 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 when the used cryptographic key is broken.

- 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: FDP_IFC.1(3), FDP_IFF.1(3)

In the TOE, the memory areas for the fax board and for the network port on the main controller board are separated. If the received fax data includes malicious content, it may threaten the TOE asset such as the TOE itself or internal 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 or not before forwarding the received fax image to e-mail or SMB/FTP/WebDAV. When the data is considered to be safe, the memory copy continues from the fax memory area to the network memory area. The fax data in network memory is transmitted using SMTP, SMB, FTP, WebDAV servers through the internal network. When non-standardized format data are discovered, the TOE destroys the fax image. Fax security functions follow the Information Flow policy (SFP_FLW).

The information flow policy (SFP_FLW) is as follows:

Direct access to a received fax image from the fax modem to the user PC through the internal network is not possible. Communication can be made only through the TOE.

The fax image received from the fax line is inspected first. When the data is determined to be safe, the memory copy continues from the fax memory area to the network memory area.

When a fax board is not installed, the information flow does not exist and does not need the protection.

• 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.
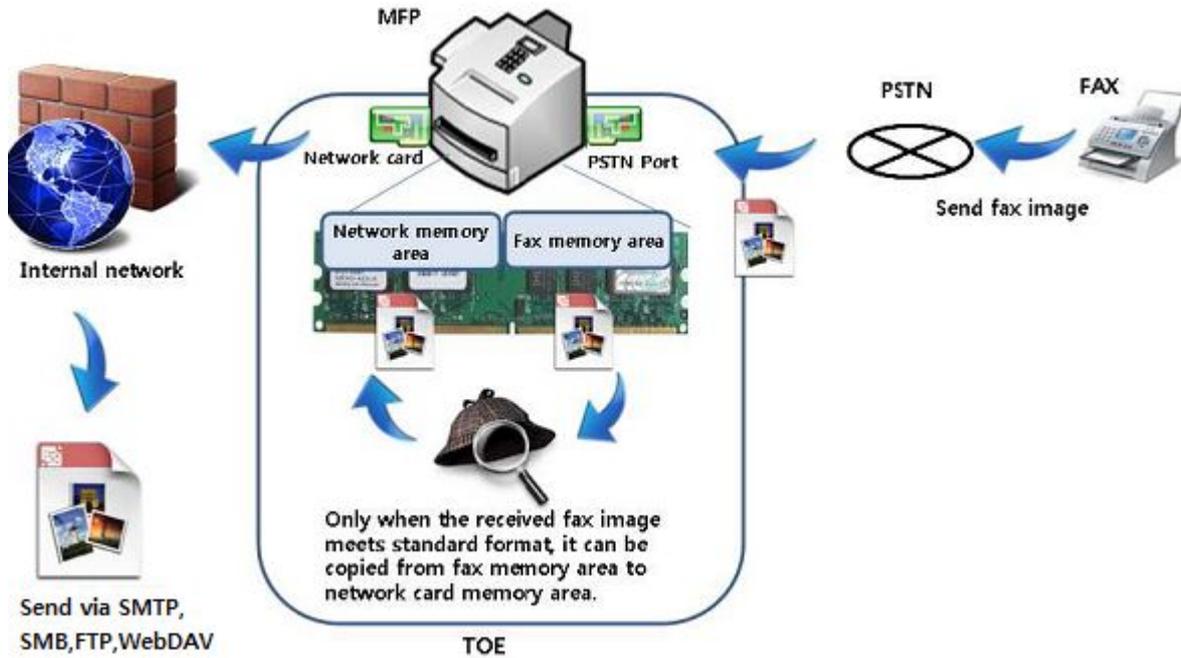

Figure 5: Information Flow Summary

7.1.8   Self Testing (TSF_STE)

Relevant SFR: FPT_TST.1

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

U.ADMINISTRATOR can enable the self tests for TSF function, TSF data, or TSF code.

Self testing executes the TSF function to verify the correct operation of the TSF function (TSF_NVE).

The TOE extracts the encryption Key data and compares saved encryption key data with SHA256 hash data of encryption Key data to verify the integrity of TSF data (Encryption Key data).

Additionally, the TOE executes the SHA256 hash algorithm with executable codes for the TSF function. 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 as below.

U.ADMINISTRATOR is authorized to view the audit log.

Table 39 :Audit Event for TST

Relevant SFR	Auditable Events	Additional Information

FPT_TST.1	Both successful and unsuccessful use of TSF Function Verification result of the integrity of TST data and executable code	-Success and failure -Date and time of the event