Samsung SCX-5737FW/SCX-5739FW Control Software V2.00.03.00

Security Target

Version 1.2

Samsung Electronics Company

@

Document History

VERSION	DATE	DESCRIPTION OF CHANGE	SECTIONS AFFECTED	REVISED BY
1.0	2011-07-09	- Initial version	ALL	Hyun Sook Rhee
1.1	2011-12-15	- 1st Revision	ALL	Hyun Sook Rhee
1.2	2012-01-10	- 2nd Revision	ALL	Hyun Sook Rhee
		-		

CONTENTS

1 Introduction 7
1.1 SECURITY TARGET REFERENCES 7
1.2 TOE REFERENCES 7
1.3 TOE OVERVIEW 7
1.3.1 TOE Type, Usage and Security features 7
1.3.2 General Specification for TOE 9
1.3.3 TOE Operational Environment 9
1.3.4 Non-TOE Hardware/Software/Firmware required by the TOE 11
1.4 TOE DESCRIPTION 12
1.4.1 Users 12
1.4.2 Physical Scope 14
1.4.3 Guidance 15
1.4.4 Logical Scope 15
1.4.5 Evaluated Configuration 18
1.5 CONVENTIONS 18
1.6 TERMS AND DEFINITIONS 21
1.7 ACRONYMS 24
1.8 ORGANIZATION 25

2 Conformance Claims 26
2.1 CONFORMANCE TO COMMON CRITERIA 26
2.2 CONFORMANCE TO PROTECTION PROFILES 26
2.3 CONFORMANCE TO PACKAGES 27
2.4 CONFORMANCE CLAIM RATIONALE 27
2.4.1 Security Problem Definition Related Conformance Claim Rationale 27
2.4.2 Security Objectives Related Conformance Claim Rationale 28
2.4.3 Security Functional Requirements related Conformance Claim Rationale 29
2.4.4 Security Assurance Requirements related Conformance Claim Rationale 30
2.4.5 TOE type related Conformance Claim Rationale 31

3 Security Problem Definition 32
3.1 THREATS AGENTS 32
3.1.1 Objects (Assets) 32
3.1.2 Threats to TOE Assets 35
3.2 ORGANIZATIONAL SECURITY POLICIES 36
3.3 ASSUMPTIONS 37
3.3.1 Assumptions for the TOE 37
3.3.2 Assumptions for the TOE (Additional) 37

4 Security Objectives 39
4.1 SECURITY OBJECTIVES FOR THE TOE 39
4.1.1 Security Objectives for the TOE 39
4.1.2 Security Objectives for the TOE (Additional) 39
DEFINITION 40
4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT 41
4.2.1 Security Objectives for Operational Environment 41
4.2.2 Security Objectives for Operational Environment (Additional) 41
4.3 SECURITY OBJECTIVES RATIONALE 43

5 Extended Component Definition 47
5.1 FPT_FDI_EXP RESTRICTED FORWARDING OF DATA TO EXTERNAL INTERFACES 47

6 Security Requirements 49
6.1 SECURITY FUNCTIONAL REQUIREMENTS 49
6.1.1 Class FAU: Security Audit 52
6.1.2 Class FCS: Cryptographic support 54
6.1.3 Class FDP: User data protection 57
6.1.4 Class FIA: Identification and authentication 65
6.1.5 Class FMT: Security management 68
6.1.6 Class FPT: Protection of the TSF 73
6.1.7 Class FTA: TOE access 74
6.1.8 Class FTP: Trusted path/channels 74
6.2 SECURITY ASSURANCE REQUIREMENTS 75
6.2.1 Class ASE: Security Target evaluation 76
6.2.2 Class ADV: Development 80
6.2.3 Class AGD: Guidance documents 82
6.2.4 Class ALC: Life-cycle support 83
6.2.5 Class ATE: Tests 86
6.2.6 Class AVA: Vulnerability assessment 88
6.3 SECURITY REQUIREMENTS RATIONALE 90
6.3.1 Security Functional Requirements' Rationale 90
6.3.2 Security Assurance Requirements Rationale 95
6.4 DEPENDENCY RATIONALE 97
6.4.1 SFR Dependencies 97
6.4.2 SAR Dependencies 99

7 TOE Summary Specification 100
7.1 TOE BASIC FUNCTIONS 100
7.2 TOE SECURITY FUNCTIONS 100
7.2.1 Identification & Authentication (TSF_FIA) 100
7.2.2 Network Access Control (TSF_NAC) 102
7.2.3 Security Management (TSF_FMT) 103
7.2.4 Security Audit (TSF_FAU) 105
7.2.5 Image Overwrite (TSF_IOW) 105
7.2.6 Data Encryption (TSF_NVE) 106
7.2.7 Fax Data Control (TSF_FLW) 106
7.2.8 Self Testing (TSF_STE) 107
7.2.9 Secure Communication (TSF_SCO) 108

LIST OF FIGURES

Figure 1: **Operational** Environment of the TOE 10
Figure 2: Physical Scope 14
Figure 3: Logical Scope 15
Figure 4: Information Flow Summary 107

LIST OF TABLES

Table 1: General Specification for TOE 9
Table 2 : Non-TOE Hardware/Software/Firmware 11
Table 3: Users 12
Table 4: Notational Prefix Conventions 19
Table 5: Acronyms 24
Table 6: Security Problem Definition Related Conformance Claim Rationale - Threats 27
Table 7: Security Problems Definition Related Conformance Claim Rationale - Organizational Security Policies 27
Table 8: Security Problems Definition Related Conformance Claim Rationale - Assumptions 28
Table 9: Security Objectives Related Conformance Claim Rationale – Security Objectives for the TOE 28
Table 10: Security Objectives related Conformance Claim Rationale– Security Objectives for the Operational Environment 29
Table 11: Security Functional Requirements related Conformance Claim Rationale 29
Table 12: Security Assurance Requirements related Conformance Claim Rationale 31
Table 13: User Data 32
Table 14: TSF Data 33
Table 15:Functions 33
Table 16:Attributes 34
Table 17: External Entities 34
Table 18: Threats to User Data for the TOE 35
Table 19: Threats to TSF Data for the TOE 35
Table 20: Organizational Security Policies 36
Table 21: Assumptions for the TOE 37
Table 22: Assumptions for the TOE (Additional) 37
Table 23: Security Objectives for the TOE 39
Table 24: Security Objectives for the TOE (Additional) 40
Table 25: Security Objectives for Operational Environment 41
Table 26: Security Objectives for the IT Environment 41
Table 27: Completeness of Security Objectives 43
Table 28: Sufficiency of Security Objectives 44
Table 29: Security Functional Requirements 49
Table 30: Audit data 52
Table 31: Cryptographic Operations 56
Table 32: Common Access Control SFP 58
Table 33: Service Access Control SFP 58
Table 34: TOE Function Access Control SFP 60
Table 35: Management of Security Functions Behavior 68
Table 36: Management of Security Attributes 70
Table 37: Management of TSF data 71
Table 38: Management Functions 72
Table 39: Security Assurance Requirements (EAL3 augmented by ALC_FLR.2) 75
Table 40: Completeness of security functional requirements 90
Table 41: Security Requirements Rationale 92
Table 42: Dependencies on the TOE Security Functional Components 97
Table 43 : Management of Security Functions Behavior 103
Table 44 : Management of Security Attributes 104
Table 45 : Management of TSF data 104
Table 46: Security Audit Event 105
Table 47 :Audit Event for TST 108

1 Introduction

This document describes the objectives, requirements and rationale for the Samsung SCX-5737FW/SCX-5739FW Control Software V2.00.03.00 for the Common Criteria EAL3+.

1.1 Security Target References

Security Target Title	Samsung SCX-5737FW/SCX-5739FW Control Software V2.00.03.00
Security Target Version	Version 1.2
Publication Date	Jan 10, 2012
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, Security, IEEE Std 2600.1-2009

1.2 TOE References

Developer	Samsung Electronics
Name	Samsung SCX-5737FW/SCX-5739FW Control Software V2.00.03.00
Version	SCX-5737FW (V2.00.03.00) SCX-5739FW(V2.00.03.00)
Product	SCX-5737FW SCX-5739FW

1.3 TOE Overview

1.3.1 TOE Type, Usage and Security features

This TOE is MFP (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 basic features:

- Printing—producing a hardcopy document from its electronic form
- Scanning—producing an electronic document from its hardcopy form
- Copying—duplicating a hardcopy document
- Faxing—scanning documents in hardcopy form and transmitting them in electronic form over telephone lines and receiving documents in electronic form over telephone lines and printing them in hardcopy form
- Document storage and retrieval—storing an electronic document during one document processing job for access during one or more subsequent document processing jobs, and retrieving an electronic document that was stored during a previous document processing job
- Shared-medium Interfaces—transmitting or receiving User Data or TSF Data between the HCD and external devices over communications media which, in conventional practice, is or can be simultaneously accessed by multiple users

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 WEBUI 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 Common Access Control & TOE Function Access Control based on the user role assigned to User 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. Through this function, U.ADMINISTRATOR can control access from external network by enabling/disabling or altering port numbers of various protocols. The TOE also provides IP filtering /Mac filtering functions to control access from external network. The network access control shall be provided commonly in IPv4 and IPv6.
- Security Management
  The TOE provides a management function to manage security functions (e.g. security audit, image overwrite, etc.) Through this function, U.ADMINISTRATOR can enable/disable security functions, manage TSF data and the security attributes, and maintain security roles.
- Security Audit
  The TOE stores and manages internal events occurring in the TOE. Audit logs are stored on the MSD(mass storage device) and can be reviewed or deleted or viewed by U.ADMINISTRATOR through the Web UI.
- 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 called by an image overwrite. 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 MSD from unauthorized access.
- Fax Data Control
  The TOE provides a fax data control function to examine fax image data formats (MMR, MR, or MH of T.4 specification) received via the PSTN port and check whether received data is suitable.
- Self-testing

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

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

1.3.2 General Specification for TOE

Table 1: General Specification for TOE

Specifications		SCX-5737FW	SCX-5739FW
Display		4.3'' Color Touch-Screen	4.3'' Color Touch-Screen
CPU		Samsung 600 MHz (Chrus 4)	Samsung 600 MHz (Chrus 4)
System Memory		256 MB	256 MB
MSD		4 GB Flash Memory	4 GB Flash Memory
F A X	Compatibility	ITU-T G3, ECM	ITU-T G3, ECM
	Comm. System	PSTN / PABX	PSTN / PABX
	Modem Speed	33.6 Kbps	33.6 Kbps
Interface		Hi-Speed USB 2.0, Ethernet 10/100/1000 base TX, USB host 2.0	Hi-Speed USB 2.0, Ethernet 10/100/1000 base TX, USB host 2.0
Extra information		Simplex :Up to 35 ppm in A4 (37 ppm in Letter)	Simplex :Up to 35 ppm in A4 (37 ppm in Letter)

1.3.3 TOE Operational Environment

In general, the TOE can be used in a wide variety of environments, which means each environment may place a different value on the assets, make different assumptions about security-relevant factors, face threats of differing approaches, and be subject to different policy requirements. Figure 1 shows the expected operational environment for the usage of a TOE. The TOE can be connected with other devices such as client PC of U. USER by wireless network with two types. The first type is an infrastructure mode which uses an access point to communicate with the wireless client PC. The second type is an ad hoc mode which the TOE and the wireless client PC communicates directly.

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.

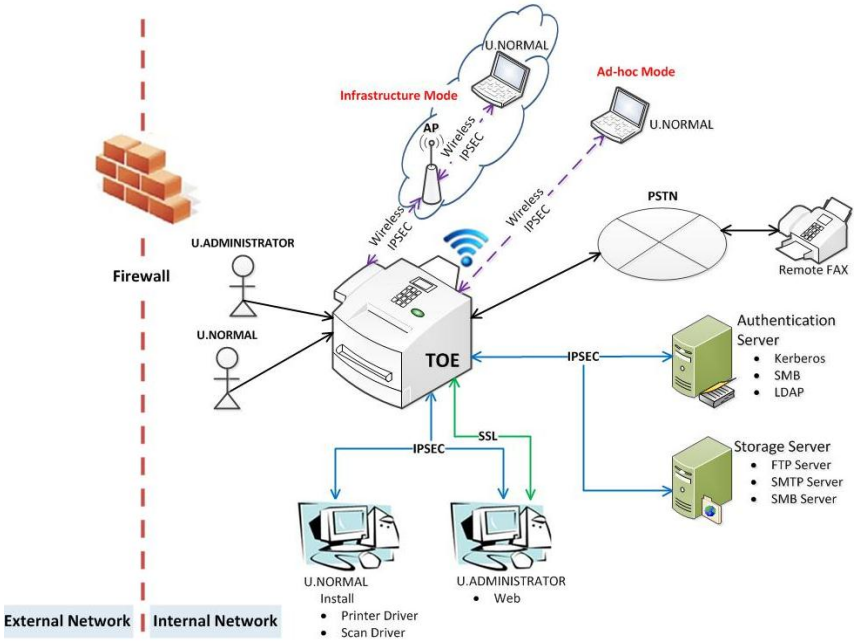

Figure 1: Operational Environment of the TOE

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 Web User Interface (Refer to Figure 1: Operational Environment of the TOE). The local user interface (LUI) is designed to be accessed by U.NORMAL and U.ADMINISTRATOR. U.NORMAL can operate copy, scan, and fax functions through the LUI. In the case of a scanning job, U.NORMAL can operate the scanning job using the LUI and transfer the scanned data to a certain destination by email addresses, local PC, server PCs, document boxes, shared folders, a portable device such as USB, and storage servers such as SMB, FTP. Users can also use their PCs to print out documents or to access the TOE through the internal network. The user's fax image can be transferred to Public Switched telephone network. U.ADMINISTRATOR can start/stop Manual Image Overwrite via the LUI, and change his password via the LUI or the WebUI. U.ADMINISTRATOR can access TOE through the Web User Interface(Web UI) using a web browser (refer to Table 1) supporting SSL protocol. From there, they can add/change/delete user accounts, enable/disable the security audit service, and view the security audit report. The information that requires asking for local user authentication by TOE shall be stored on the secure area of the MSD. All of the information stored on the MSD 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.

- Storage server

The FTP, SMB, SMTP server are storage devices for storing received fax, scanned data on the TOE. Scan-to-server and Fax-to-Email are relevant functions.

- 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.

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

Table 2 : Non-TOE Hardware/Software/Firmware

	Items	Objectives	Specification
Hardware	PC for U.ADMINISTRATOR	PC for Web U.ADMINISTRATOR to access and manage TOE.	• Windows 2000 - CPU: Pentium II 400 MHz or higher - Memory: 64 MB or higher - HDD: 0.6 GB or higher • Windows XP - CPU: Pentium III 933 MHz or higher - Memory: 128 MB or higher - HDD: 1.5 GB or higher • Windows 2003 Server - CPU: Pentium III 933 MHz or higher - Memory: 128 MB or higher - HDD: 1.25 GB or higher • Windows Vista - CPU: Pentium IV 3 GHz or higher - Memory: 512 MB or higher - HDD:15 GB or higher • Windows 7 - CPU: Pentium IV 1 GHz or higher - Memory: 1GB or higher - HDD:16 GB or higher • Mac OS X - CPU: Power PC G4/G5, Intel Processors - Memory: 128 MB Macintosh based on Power PC - HDD: 1 GB or higher • Mac OS X 10.5 - CPU: 867 MHz or Power PC G4/G5 - Memory: 512 MB or higher - HDD: 1 GB or higher • Linux - CPU: Pentium IV 2.4 GHz or higher - Memory: 512 MB - HDD: 1 GB or higher
	PC for U.NORMAL	PC for U.NORMAL to print or scan or copy with TOE	
	Firewall system	Firewall system to protect internal assets by blocking attacks from external networks.	
	PSTN	PSTN for translating fax image.	
Software	Operating system for PC	Operating system for U.NORMAL or web U.ADMINISTRATOR	• For SCX-5737FW, SCX-5739FW [Windows] - Windows 2000/XP(32/64 bit)/2003(32/64 bit)/Vista(32/64 bit)/2008/ Win 7(32,64bit) [Linux] - RedHat Enterprise Linux WS 4, 5 (32/64 bit) - Fedora Core 2~10 (32/64 bit) - SuSE Linux 9.1 (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

	Items	Objectives	Specification
			(32/64 bit) - Debian 3.1, 4.0, 5.0 (32/64 bit) [Mac] - Mac OS X 10.3~10.5
	Web browser that can serve SSL communication	Web browser that serves SSL communication between U.NORMAL's PC or Web U.ADMINISTRATOR 's PC and the TOE	Internet Explorer 6.0 or higher (~8.0)
	Printer driver	Printer driver application software for U.NORMAL to install in their PC. User can configure properties and start printing jobs through this printer driver.	Linux V3.00.52 Unified Driver Mac OS 10.3 ~ 10.6, V1.11, Print Driver Win 2000/XP/2003/Vista/2008/Win 7(32,64bit), 3.11.34.00 Printer Driver
	Smart Panel	Smart Panel monitors the state of the MFP connected to the user's PC. When an event occurs, Smart Panel notifies the user of the event.	Linux, V2.00.72, Smart Panel Mac OS 10.3 ~ 10.6, V2.04.02, Smart Panel
	Scan Driver	Scan Driver receives scanned data from the MFP and stores it in the user's PC.	Linux V3.00.27 Scanner Driver. Mac OS 10.3 ~ 10.6, V2.21.35.01 Universal Scan Driver Win 2000/XP/2003/Vista/2008/Win 7(32,64bit), V3.21.08, Universal Scan Driver

1.4 TOE Description

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

1.4.1 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 3: 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.

1.4.2 Physical Scope

The physical scope of the TOE consists of the all of the MFP hardware and Software.

The TOE consists of the System Board, Control Panel, DADF, Engine, MSD, Fax Board, NIC, USB Port.

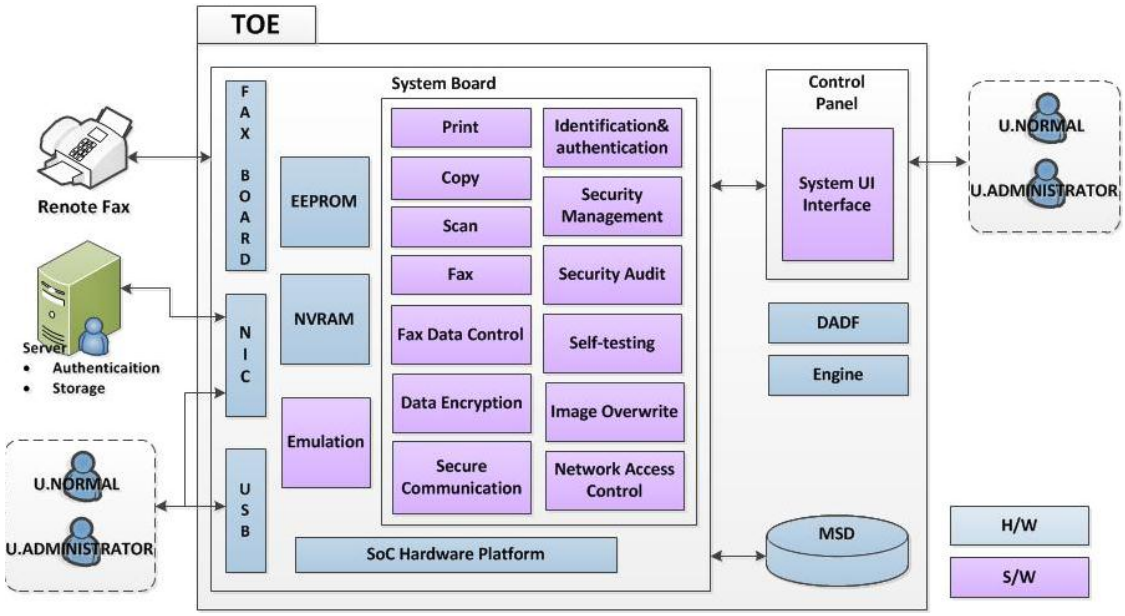

Figure 2: Physical Scope

System Board

The device system board consists of CPU and ROM, RAM and it related unit.

Control Panel

Control Panel consists of LCD panel and its controlling unit and the buttons

DADF

DADF controls the document feeding for scanning data

Engine

Engine board controls the image processing and mechanical units of printer engine

MSD (Mass Storage Device)

MSD is a form of Nonvolatile memory, which is a flash drive device for storing TOE user data, TSF data

Fax Board

Fax Board is a board working faxes and transfers TSF data into a communication link.

NIC

NIC(Network Card) is an internal card that connect TOE to a network.

USB Port

USB Port is a type of serial port for connecting peripheral devices in a system.

1.4.3 Guidance

The following is the guidance document for the TOE.

- Network Admin Guide_v3.00.pdf
- Security Admin_v3.00.pdf
- SCX-5737FW Series User Guide REV 1.01

1.4.4 Logical Scope

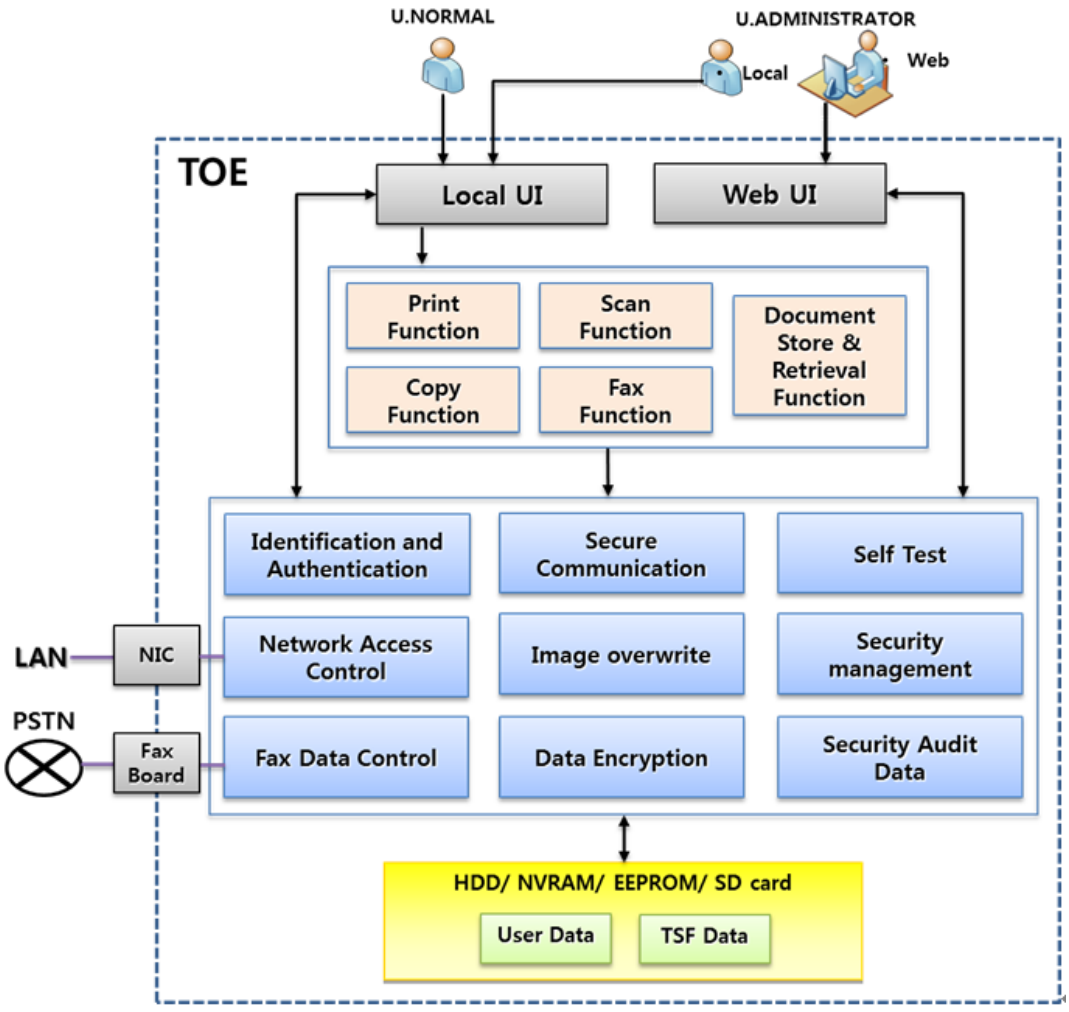

Figure 3: Logical Scope

The following basic functions are provided by the TOE:

Printing Function

The TOE can produce a hardcopy document from its electronic form such as PC print, print from document storage.

Scanning Function

The TOE can produce an electronic document from its hardcopy form such as Scan To PC, Scan To E-mail, Scan To SMB, Scan To FTP, Scan To USB, Scan To Document Box, Scan To Shared Folder, Scan To WSD.

Copying Function

The TOE can duplicate a hardcopy document.

Faxing Function

The TOE can scan documents in hardcopy form and transmit them in electronic form over telephone lines and receive documents in electronic form over telephone lines and print them in hardcopy form

Document storage and retrieval Function

The TOE can store an electronic document during one document processing job for access during one or more subsequent document processing jobs, and retrieve an electronic document that was stored during a previous document processing job. The document boxes are classified as general boxes, secure boxes. Secured box provides the confidentiality of stored data in secure box. To retrieve data from the secure box, the identical password used in adding secured box should be inserted.

The following security functions are provided by the TOE:

Identification & Authentication (TSF_FIA)

The TOE can restrict U.USER from accessing the MFP or the functions of MFP.

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

U.ADMINISTRATOR should be identified and authenticated by entering ID, Password to access to the TOE management functions. It is possible to restrict the other IP addresses except only a specific IP address which MFP can be accessed by U.ADMINISTRATOR.

U. ADMINISTRATOR can configure Identification & Authentication Policy by using LUI or Web UI. That is, U. ADMINISTRATOR can set the authentication method and the enablement of standard accounting, respectively. U. ADMINISTRATOR can also give specific permission for U.NORMAL to use certain features of the machine.

Network Access Control (TSF_NAC)

The TOE has a network interface card (network card) connected to an external network. The TOE 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 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 WEBUI.

2) IP and Mac address filtering:

U.ADMINISTRATOR can make filtering rules for IPv4/IPv6 addresses and MAC addresses.

After that, TOE restricts the IP address (or Mac address) for the incoming or outgoing packet according to the IP filtering rule (or Mac filtering rule) registered by U.ADMINISTRATOR.

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 the completion of print, scan, copy, fax jobs.

Security event log includes both successful and unsuccessful use of the authentication, log data access, a failure of the trusted channel functions and self testing.

Operation log includes changes of the time, the usage of manual image overwriting, enablement/disablement of each log function (job log, security event log) except for the operation log, enablement/disablement of IPSec, enablement/disablement of wireless, Mac filtering rule, IPv4 filtering rule, IPv6 filtering rule, enablement/disablement of protocol, the changed value of Logout policy setting, the changed value of Authentication failure setting.

The audit data consist of the category, type, description, data, user, result, destination and source 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) the audit data selectively.

The TOE protects Security Audit Data stored on the secure area of the MSD. It prevents any unauthorized alteration to the Security Audit Data**.** If the space for Security Audit Data is full then a part of the space shall be overwritten with new audit data. The target of overwriting is oldest audit data.

Image Overwrite (TSF_IOW)

The TOE implements a manual image overwrite security function to overwrite image files created during the printing, network scan, scan-to-email, or scan-to-server process. That is, the image overwrite security function can also be invoked manually by the U.ADMINISTRATOR. The files on the MSD are overwritten with 3 times. This image overwrite is implemented by DoD Standard 5200.28-M method.

Data Encryption (TSF_NVE)

The TOE encrypts image data and configuration data on the MSD. After that, the TOE stores the data on the MSD and it decrypts the stored data to use it. The TOE generates cryptographic keys when the

TOE is initialized at the first setout. The cryptographic algorithm used by the TOE is AES algorithm with 256-bit key size. Also TOE encrypts audit data on the MSD. Each product has its unique value and nobody (including the administrator) can leak the key value to the outside.

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. 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. 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 servers through the internal network. When non-standardized format data are discovered, the TOE destroys the fax image.

Self Testing (TSF_STE)

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

Self testing executes TSF function to verify the correctness and the TOE verifies the integrity of TSF data and all of TSF executable code by the self testing.

Secure Communication (TSF_SCO)

The TOE provides secure communication between the TOE and all of other trusted IT products to protect communicated data from modification or disclosure by IPSEC.

1.4.5 Evaluated Configuration

No additional Java applications are loaded into the MFP by administrators. These applications are referred to as XOA applications in end user documentation.

Network Accountings is not contained in the Evaluated Configuration.

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.**

The SFR which is completely describe on Protection Profile IEEE Std 2600.1-2009 Version 1.0 is included.

Selection

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*.

Assignment

The assignment operation is used to assign a specific value to an unspecified parameter such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.

Iteration

Iterated functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, for example, FIA_AFL.1 (1) and FIA_AFL.1 (2).

The following is notational conventions used by the PP:

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

Table 4: Notational Prefix Conventions

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

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

Application Note

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

1.6 Terms and Definitions

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

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 PC Scan, Scan To USB, Scan To Local PC, Scan To Network PC, Scan To E-mail, Scan To SMB, Scan To FTP, Scan To WSD etc.

LUI, Local User Interface

Interface for U.NORMAL or U.ADMINISTRATOR to access, use, or manage the TOE directly.

MSD (Mass Storage Device)

This is the storage of large amounts of data in a persisting and machine-readable fashion.

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 MSD 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 Peripherals, 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 on MSD, and the function should only be manually performed by a local administrator through the LUI. The image data on the MSD are overwritten with 3 times. This image overwrite is implemented by DoD Standard 5200.28-M method.

Scan-to-server

This is a function that transmits scanned data to a remote server such as SMB, FTP from the LUI. Only authorized U.NORMAL 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 U.NORMAL can use this function.

Scan-to-PC

This is a function that transmits scanned data to PC (Local PC or Network PC, selected by U.NORMAL) from the LUI. Only authorized U.NORMAL can use this function.

Scan-to-USB

This is a function that transmits scanned data to USB from the LUI. Only authorized U.NORMAL can use this function.

Scan-to-WSD

This is a function that transmits scanned data to WSD (Web Service on Device) from the LUI by using a specific protocol. Only an authorized U.NORMAL can use this function.

Scan-to-Document Box

This is a function that transmits scanned data to Document Box from the LUI. Only authorized U.NORMAL can use this function.

Scan-to-Shared Folder

This is a function that transmits scanned data to Shared Folderfrom the LUI. Only authorized U.NORMAL can use this function.

WEBUI, Web UI, Web User Interface

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

Image file

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

Stored file

Every file stored on the MSD. It includes image files and preserved files.

FAX

Job for receiving or transmitting fax images through a fax line

Fax image

The data received or transmitted through a fax line

DoD 5200.28-M

DoD 5200.28-M is an image overwriting standard that Department of Defense recommends. The image data in storage device is completely overwritten three times.

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

If a fax function sends fax data from a client PC to an MFP, then the TOE transmits the fax data through a fax line.

T.4

Data compression specification for fax transmission 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 the Modified Relative Element Address Designate MH coding. More advanced type than MR coding.

AES

Block cryptography developed by Belgium's mathematicians, J.Daemen and V.Rijmen in 2000. AES has a block size and key size of 128, 192, or 256 bits.

1.7 Acronyms

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

Table 5: Acronyms

	Definition
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
MSD	Mass Storage Device
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
WEBUI	Web User Interface
MMR	Modified Modified READ coding
MR	Modified READ Coding
MH	Modified Huffman coding

1.8 Organization

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

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

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

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

Chapter 5 describes the extended component definition.

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

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

2 Conformance Claims

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

2.1 Conformance to Common Criteria

This Security Target conforms to the following Common Criteria:

- **Common Criteria Identification**
  - Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1r3, 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 extended
  - Common Criteria for Information Technology Security Evaluation, Part 3 conformant

2.2 Conformance to Protection Profiles

This Security Target conforms to the following Protection Profile:

- **Protection Profile Identification**
  - IEEE Std 2600.1-2009 Version 1.0 (CCEVS-VR-VID10340-2009, June 12, 2009) as known as U.S. Government Protection Profile for Hardcopy Devices in Basic Robustness Environments [PP]
- **Protection Profile Conformance**
  - IEEE Std 2600.1-2009 Version 1.0 “demonstrable conformance”
    - 2600.1-PP, Protection Profile for Hardcopy Devices, Operational Environment A
    - 2600.1-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment A
    - 2600.1-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment A
    - 2600.1-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment A
    - 2600.1-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment A
    - 2600.1-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment A
    - 2600.1-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment A

2.3 Conformance to Packages

This Security Target conforms to the following Package.

- **Assurance Package: EAL3 augmented by ALC_FLR.2**
- 2600.1-PRT, SFR Package conformant
- 2600.1-SCN, SFR Package conformant
- 2600.1-CPY, SFR Package conformant
- 2600.1-FAX, SFR Package conformant
- 2600.1-DSR, SFR Package conformant
- 2600.1-SMI, SFR Package conformant

2.4 Conformance Claim Rationale

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

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

The PP conformance claim rationale is as follows:

2.4.1 Security Problem Definition Related Conformance Claim Rationale

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

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

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

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

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

Organizational Security Policy	Rationale
P.INTERFACE.MANAGEMENT	

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

Assumption	Rationale
A.ACCESS.MANAGED	Equal to the PP: the assumptions in this ST are defined the same as the PP. Therefore, it satisfies the "demonstrable conformance".
A.USER.TRAINING	
A.ADMIN.TRAINING	
A.ADMIN.TRUST	
A.AUTH_SERVER.SECURE	The assumptions that should be satisfied in this TOE environment are additionally defined in this ST. It satisfies the "demonstrable conformance" because it includes equivalent or more restrictive environment and assumption compare with Protection Profile.
A.EXT_SERVER.SECURE	
A.SSL_CERT.INSTALL	
A.IPSEC_EXT.OUT	
A.SSL_CLIENT.PC	
A.AP_SECURE	

2.4.2 Security Objectives Related Conformance Claim Rationale

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

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

Security Objectives for TOE	Rationale
O.DOC.NO_DIS	Equal to the PP: the security objectives in this ST are defined the same as the PP. Therefore, it satisfies the "demonstrable conformance".
O.DOC.NO_ALT	
O.FUNC.NO_ALT	
O.PROT.NO_ALT	
O.CONF.NO_DIS	
O.CONF.NO_ALT	
O.USER.AUTHORIZED	
O.INTERFACE.MANAGED	
O.SOFTWARE.VERIFIED	
O.AUDIT.LOGGED	
O.AUDIT_STORAGE.PROTECTED	The security objectives are replaced in this ST. It prevents unauthorized disclosure and alteration by protecting storage. Therefore, it enforces the equivalent or more restrictive security functionality of the TOE. It satisfies the "demonstrable conformance"
O.AUDIT_ACCESS.AUTHORIZED	
O.DATA.ENCRYPTED	The security objectives are additionally defined in this ST. Therefore, it enforces the equivalent or more restrictive security functionality of the TOE. It satisfies the "demonstrable conformance".
O.DATA.OVERWRITTEN	
O.FAX_DATA.FORMAT	
O.INFO.FLOW_CONTROLED	

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

Security Objectives for Operational Environment	Rationale
OE.PHYSICAL.MANAGED	Equal to the PP: the security objectives in this ST are defined the same as the PP. Therefore, it satisfies the "demonstrable conformance". .
OE.USER.AUTHORIZED	
OE.USER.TRAINED	
OE.ADMIN.TRAINED	
OE.ADMIN.TRUSTED	
OE.AUDIT.REVIEWED	
OE.INTERFACE.MANAGED	
OE.AUTH_SERVER.SECURE	Additionally defined in this ST and these security objectives for operational environment enhanced the security of the operational environment of the TOE. It satisfies the "demonstrable conformance" because it defines the equivalent or more restrictive environment to support TSF
OE.EXT_SERVER.SECURE	
OE.SSL_CERT.INSTALL	
OE.IPSEC_EXT.OUT	
OE.SSL_CLIENT.PC	

2.4.3 Security Functional Requirements related Conformance Claim Rationale

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

Table 11: Security Functional Requirements related Conformance Claim Rationale

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

Category	PP SFR	ST SFR	Rationale
from the PP			the PP on SFR were performed. It satisfies the "demonstrable conformance".
SCN Package Requirements from the PP	FDP_ACC.1	FDP_ACC.1(3)	
	FDP_ACF.1	FDP_ACF.1(3)	
CPY Package Requirements from the PP	FDP_ACC.1	FDP_ACC.1(3)	
	FDP_ACF.1	FDP_ACF.1(3)	
FAX Package Requirements from the PP	FDP_ACC.1	FDP_ACC.1(3)	
	FDP_ACF.1	FDP_ACF.1(3)	
DSR Package Requirements from the PP	FDP_ACC.1	FDP_ACC.1(3)	
	FDP_ACF.1	FDP_ACF.1(3)	
SMI Package Requirements from the PP	FAU_GEN.1	FAU_GEN.1	
	FPT_FDI_EXP.1	FPT_FDI_EXP.1	
	FTP_ITC.1	FTP_ITC.1	
Addition	-	FAU_SAR.1	These SFRs do not exist in PP. We added SFRs. Therefore, it satisfies the "demonstrable conformance" since we enforce the equivalent or more restrictive SFRs.
	-	FAU_SAR.2	
	-	FAU_SEL.1	
	-	FAU_STG.1	
	-	FAU_STG.4	
	-	FCS_CKM.1(1)	
	-	FCS_CKM.1(2)	
	-	FCS_CKM.4(1)	
	-	FCS_CKM.4(2)	
	-	FCS_COP.1(1)	
	-	FCS_COP.1(2)	
	-	FIA_AFL.1	
	-	FIA_UAU.7	
	-	FDP_IFC.1(1)	
	-	FDP_IFC.1(2)	
	-	FDP_IFC.1(3)	
	-	FDP_IFC.1(4)	
	-	FDP_IFC.1(5)	
	-	FDP_IFF.1(1)	
	-	FDP_IFF.1(2)	
	-	FDP_IFF.1(3)	
	-	FDP_IFF.1(4)	
	-	FDP_IFF.1(5)	
	-	FMT_MSA.1(3)	
	-	FMT_MSA.1(4)	

2.4.4 Security Assurance Requirements related Conformance Claim Rationale

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

Table 12: Security Assurance Requirements related Conformance Claim Rationale

PP SAR	ST SAR	Rationale
Assurance Package: EAL3 augmented by ALC_FLR.2	Assurance Package: EAL3 augmented by ALC_FLR.2	Equal to the PP. Therefore, it satisfies the "demonstrable conformance".

2.4.5 TOE type related Conformance Claim Rationale

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

TOE Type [PP]	TOE Type	Rationale
This TOE is MFPs (Multi-Function Peripherals) as an IT product. It controls the operation of the entire MFP, including copy, print, scan, and fax functions on the MFP controller.	This TOE is MFP (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 controls the operation including copy, print, scan, and fax jobs on the MFP controller. Therefore, the TOE type is consistent with the PP, and satisfies the "demonstrable conformance".

3 Security Problem Definition

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

3.1 Threats agents

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

The following are the threat agents defined in this ST:

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

3.1.1 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 13: 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 14: TSF Data

Designation	PP Definition	Asset Under Protection
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.	None
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.	•User, administrator, protocol (e.g., SNMP) and external server authentication data like passwords •External server authentication settings •Network configuration settings •Audit logs •Device security status information such as the enablement status of security features (such as secure protocols, Manual Image Overwriting or MSD encryption) or security protocols •Cryptographic key information and key generation algorithms •TOE Software (should be treated as TSF protected data)

Functions

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

Table 15: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
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

Attributes

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

Table 16: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.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

Operations

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

External Entities

Table 17: External Entities

Designation	Definition
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 The TOE sends received fax and scan data from the TOE to a server via SMB
FTP Server	The TOE sends received fax and scan data from the TOE to a server via FTP
Mail Server	The TOE sends received fax and scan data from the TOE to a server via a Mail server
PC	The TOE sends the scanned data from the TOE into PC via a WSD or a driver

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.
- **Shared-medium Interface**: User Data or TSF Data between the HCD and external devices over communications media which, in conventional practice, is or can be simultaneously accessed by multiple users

3.1.2 Threats to TOE Assets

The threats taken from the PP to which this Security Target conforms are as shown in Table 18 and Table 19 (Refer to chapter 5 about affected asset):

Table 18: Threats to User Data for the TOE

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

Table 19: Threats to TSF Data for the TOE

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

3.2 Organizational Security Policies

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

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

Table 20: Organizational Security Policies

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

3.3 Assumptions

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

This Security Target conforms to all assumptions in the PP.

3.3.1 Assumptions for the TOE

The assumptions taken from the PP to which this Security Target conforms are as shown in the following Table 2121

Table 21: Assumptions for the TOE

Assumption	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and to correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

3.3.2 Assumptions for the TOE (Additional)

The assumptions for the TOE additionally defined are as follows:

Table 22: Assumptions for the TOE (Additional)

Objective	Definition
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, 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.IPSEC_EXT.OUT	All of the external servers(Storage, Authentication Server) and client PC that connected with the TOE via network supports IPSEC.
A. SSL_CLIENT.PC	All of the client PCs that connected with the TOE via network supports SSL.
A.AP_SECURE	The AP is enabled and securely managed by U.ADMINISTRATOR and provides secure functions for

Objective	**Definition**
	U.NORMAL.

4 Security Objectives

The security objectives are categorized into two parts:

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

4.1 Security Objectives for the TOE

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

4.1.1 Security Objectives for the TOE

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

Table 23: Security Objectives for the TOE

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

4.1.2 Security Objectives for the TOE (Additional)

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

Table 24: Security Objectives for the TOE (Additional)

Objective	Definition
O.AUDIT_STORAGE.PROTECTED	The TOE shall protect audit records from unauthorized access, deletion and modification.
O.AUDIT_ACCESS.AUTHORIZED	The TOE shall allow access to audit records only by authorized persons.
O.DATA.ENCRYPTED	The TOE shall encrypt the data to be stored on the MSD 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 MSD 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. This Security Target conforms to the security objectives for the operational environment included in the PP.

4.2.1 Security Objectives for Operational Environment

The security objectives for the operational environment taken from the PP to which this Security Target conforms are as shown in the following Table 25 (they are completely the same as the PP):

Table 25: Security Objectives for Operational Environment

Objective	Definition
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.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.2.2 Security Objectives for Operational Environment (Additional)

The security objectives for operational environments additionally defined are as follows:

Table 26: Security Objectives for the IT Environment

Objective	Definition
OE.AUTH_SERVER.SECURE	The authentication servers (i.e. LDAP, Kerberos, and SMB

Objective	**Definition**
	Server)and OCSP server provide a secure remote authentication for U.NORMAL.
OE.EXT_SERVER.SECURE	The FTP, SMB server, and mail servers that store fax and scan data transmitted from the TOE are 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.IPSEC_EXT.OUT	All of the external servers (Storage, Authentication Server) and client PC that connected with the TOE via network supports IPSEC.
OE.SSL_CLIENT.PC	All of the client pc that connected with the TOE via network shall provide secure channel via SSL.
OE.AP_SECURE	All of the data transmitted between the TOE and outside entities is securely protected by secure mechanisms.

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 27 shows the correspondences of security objectives, assumptions, threats, and organizational security policies.

Table 28 shows that each security problem is covered by the defined security objectives.

Table 27: Completeness of Security Objectives

Threats/ Policies/ Assumptions	**Security Objectives**																												
	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.INFO.FLOW_CONTROLED	O.FAX_DATAFORMAT	OE.AUDIT.REVIEWED	OE.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED	OE.AUTH_SERVER.SECURE	OE.EXT_SERVER.SECURE	OE.SSL_CERT.INSTALL	OE.IPSEC_EXT.OUT	OE.SSL_CLIENT.PC	OE.AP_SECURE
T.DOC.DIS	✓						✓	✓					✓	✓															
T.DOC.ALT		✓					✓	✓																					
T.FUNC.ALT			✓				✓	✓																					
T.PROT.ALT				✓			✓	✓																					
T.CONF.DIS					✓		✓	✓					✓	✓															
T.CONF.ALT						✓	✓	✓																					
P.USER.AUTHORIZATION							✓	✓																					
P.SOFTWARE.VERIFICATION									✓																				
P.AUDIT.LOGGING										✓	✓	✓					✓												
P.INTERFACE. MANAGEMENT															✓	✓		✓		✓									
A.ACCESS.MANAGED																			✓										
A.ADMIN.TRAINING																					✓								
A.ADMIN.TRUST																						✓							
A.USER.TRAINING																							✓						
A.AUTH_SERVER. SECURE																								✓					
A.EXT_SERVER.SECURE																									✓				
A.SSL_CERT.INSTALL																										✓			
A.IPSEC_EXT.OU																											✓		

Threats/ Policies/ Assumptions	Security Objectives																												
	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.INFO.FLOW_CONTROLED	O.FAX_DATAFORMAT	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED	OE.AUTH_SERVER.SECURE	OE.EXT_SERVER.SECURE	OE.SSL_CERT.INSTALL	OE.IPSEC_EXT.OUT	OE.SSL_CLIENT.PC	OE.AP_SECURE
T																													
A.SSL_CLIENT.PC																												✓	
A.AP_SECURE																													✓

Table 28: Sufficiency of Security Objectives

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

Threats, Policies, and Assumptions	Summary	Objectives and Rationale
	persons	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 D.CONF from unauthorized disclosure
		O.DATA.OVERWRITTEN protects D.CONFfrom 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 responsibility of the TOE Owner to appropriately grant authorization.
P.USER.AUTHORIZATION	Users will be authorized to use the TOE	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
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 establishes responsibility of, the TOE Owner to provide appropriate access to 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	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies.

Threats, Policies, and Assumptions	Summary	Objectives and Rationale
	environment	OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces
		O.INFO.FLOW_CONTROLED controls a flow of the information through network.
		O.FAX_DATAFORMAT identifies the format of the transferred fax data via network.
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.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, SMB, and OCSP Servers) provide a secure remote authentication for U.NORMAL.
A.EXT_SERVER.SECURE	FTP server and mail server which store fax and scan data transmitted from the TOE are managed securely.	OE.EXT_SERVER.SECURE ensures that FTP and SMB server 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.IPSEC_EXT.OUT	All of the external servers that communicate with the TOE support IPSEC.	OE.IPSEC_EXT.OUT ensures that all of the external servers and client PC that communicates with the TOE support IPSEC.
A.SSL_CLIENT.PC	All of the client PCs that communicates with the TOE support SSL.	OE.SSL_CLIENT.PC ensures that all of the client PCs that communicates with the TOE support SSL.
A.AP_SECURE	The AP is enabled and securely managed by U.ADMINISTRATOR and provides secure functions for U.NORMAL.	OE.AP_SECURE ensures that all of the data transmitted between the TOE and outside entities is securely protected by secure mechanisms.

5 Extended Component Definition

5.1 FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behavior:

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

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

Component leveling:

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

Management: FPT_FDI_EXP.1

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

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

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

administrative role

c) Revocation of such an allowance

Audit: FPT_FDI_EXP.1

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

There are no auditable events foreseen.

Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

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

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

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

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

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

[assignment: *list of external interfaces*].

6 Security Requirements

6.1 Security Functional Requirements

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

Table 29summarizes the security functional requirements defined by this ST.

Table 29: Security Functional Requirements

Class	Component		Defined in
Security Audit	FAU_GEN.1	Audit data generation	PP
	FAU_GEN.2	User identity association	PP
	FAU_SAR.1	Audit review	This ST additionally
	FAU_SAR.2	Restricted audit review	This ST additionally
	FAU_SEL.1	Selective audit	This ST additionally
	FAU_STG.1	Protected audit trail storage	This ST additionally
	FAU_STG.4	Prevention of audit data loss	This ST additionally
Cryptographic Support	FCS_CKM.1(1)	Cryptographic key generation	This ST additionally
	FCS_CKM.1(2)	Cryptographic key generation	This ST additionally
	FCS_CKM.4(1)	Cryptographic key destruction	This ST additionally
	FCS_CKM.4(2)	Cryptographic key destruction	This ST additionally
	FCS_COP.1(1)	Cryptographic operation	This ST additionally
	FCS_COP.1(2)	Cryptographic operation	This ST additionally
User Data Protection	FDP_ACC.1(1)	Subset access control	PP
	FDP_ACC.1(2)	Subset access control	PP
	FDP_ACC.1(3)	Subset access control	PP PRT package SCN package CPY package FAX package DSR package
	FDP_ACF.1(1)	Security attribute based access control	PP
	FDP_ACF.1(2)	Security attribute based access control	PP
	FDP_ACF.1(3)	Security attribute based access control	PP PRT package

Class	Component		Defined in
			SCN package CPY package FAX package DSR package
	FDP_IFC.1(1)	Subset information flow control	This ST additionally
	FDP_IFC.1(2)	Subset information flow control	This ST additionally
	FDP_IFC.1(3)	Subset information flow control	This ST additionally
	FDP_IFC.1(4)	Subset information flow control	This ST additionally
	FDP_IFC.1(5)	Subset information flow control	This ST additionally
	FDP_IFF.1(1)	Simple security attributes	This ST additionally
	FDP_IFF.1(2)	Simple security attributes	This ST additionally
	FDP_IFF.1(3)	Simple security attributes	This ST additionally
	FDP_IFF.1(4)	Simple security attributes	This ST additionally
	FDP_IFF.1(5)	Simple security attributes	This ST additionally
	FDP_RIP.1	Subset residual information protection	PP
Identification and Authentication	FIA_AFL.1	Authentication failure handling	This ST additionally
	FIA_ATD.1	User attribute definition	PP
	FIA_UAU.1	Timing of authentication	PP
	FIA_UAU.7	Protected authentication feedback	This ST additionally
	FIA_UID.1	Timing of identification	PP
	FIA_USB.1	User-subject binding	PP
Security Management	FMT_MOF.1	Management of functions in TSF	This ST additionally
	FMT_MSA.1(1)	Management of security attributes	PP
	FMT_MSA.1(2)	Management of security attributes	PP
	FMT_MSA.1(3)	Management of security attributes	This ST additionally
	FMT_MSA.1(4)	Management of security attributes	This ST additionally
	FMT_MSA.3(1)	Static attribute initialization	PP
	FMT_MSA.3(2)	Static attribute initialization	PP
	FMT_MTD.1	Management of TSF data	PP
	FMT_SMF.1	Specification of management functions	PP
	FMT_SMR.1	Security roles	PP

Class	Component		Defined in
Protection of the TSF	FPT_STM.1	Reliable time stamps	PP
	FPT_TST.1	TSF testing	PP
	FPT_FDI_EXP.1	Restricted forwarding of data to external interfaces	PP
TOE Access	FTA_SSL.3	TSF-initiated termination	PP
Trusted paths/channels	FTP_ITC.1	Inter-TSF trusted channel	PP

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; and

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 30;** [none].

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

Table 30: Audit data

Auditable Events	Relevant SFR	Audit Level	Additional Information
Job completion	FDP_ACF.1	Not specified	Type of job
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1	Basic	None required
Use of the management functions	FMT_SMF.1	Minimum	None required
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1	Basic	Attempted user identity, if available
Locking of an interactive session by the locking mechanism	FTA_SSL.3	Minimum	None required
Execution of the TSF self tests and the results of the tests	FPT_TST.1	Not specified	None required
Manual Image Overwrite	FDP_RIP.1	Not specified	None required
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required
Changes to the time	FPT_STM.1.	Minimum	None required

6.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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

6.1.1.3 FAU_SAR.1 Audit review

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

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

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

6.1.1.4 FAU_SAR.2 Restricted audit review

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

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

6.1.1.5 FAU_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 unauthorized deletion.

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

6.1.1.7 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.1(1) Cryptographic key generation

Hierarchical to: No other components.

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

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [random key generation method] and specified cryptographic key sizes [256-bit] that meet the following: [None].

6.1.2.2 FCS_CKM.1(2) Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with cryptographic key generation algorithm [Diffie-Hellman algorithm] during communication and specified cryptographic key sizes [768 or 1024 or 2048] that meet the following: [None].

6.1.2.3 FCS_CKM.4(1) 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.1Cryptographic key generation]

FCS_CKM.4.1(1) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [an overwrite updates a cryptographic key by overwriting previous cryptographic key with newly generated cryptographic key] that meets the following: [None].

6.1.2.4 FCS_CKM.4(2) 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.1Cryptographic key generation]

FCS_CKM.4.1(2) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite existing Pre-shared keyusing new generation cryptographic key,previous cryptographic keys will be overwritten with a newly generated key] that meets the following: [None].

6.1.2.5 FCS_COP.1(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.1Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1) The TSF shall perform [cryptographic operation of data in MSD] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [256-bit] that meet the following: [FIPS PUB 197].

6.1.2.6 FCS_COP.1(2) 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.1Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(2) The TSF shall perform [cryptographic operation listed below Table 31 outgoing to the network] in accordance with a specified cryptographic algorithm [cryptographic algorithm of data listed below Table 31] and cryptographic key sizes [cryptographic key size listed below Table 31]that meet the following: [the list of standards listed below Table 31]

Table 31: Cryptographic Operations

Algorithm	Operations	Key Size in Bits	Standards
Triple-DES	Encryption, Decryption	168	FIPS 46-3
AES	Encryption, Decryption	128	FIPS PUB 197

Algorithm	Operations	Key Size in Bits	Standards
SHA-1	Hashing	160	FIPS 180-2
Diffie-Hellman	Key agreement	768 1024 2048	PKCS #3

6.1.3 Class FDP: User data protection

6.1.3.1 FDP_ACC.1(1) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

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

6.1.3.2 FDP_ACC.1(2) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the **TOE Function Access Control SFP in Table 34**on **the list of users as subjects, objects, and the right to use the functions as operations among subjects and objects covered by the TOE Function Access Control SFP in Table 34.**

6.1.3.3 FDP_ACC.1(3) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(3) The TSF shall enforce the **Service (PRT, SCN, CPY, DSR FAX) Access Control SFP in Table 33 on the list of subjects, objects, and operations among subjects and objects covered by the Service (PRT, SCN, CPY, DSR FAX) Access Control SFP in Table 33.**

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

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

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

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

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

Table 32: Common Access Control SFP

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

Table 33: Service Access Control SFP

Access Control SFP	Object	Attribute (Object)	Operation(s)	Subject	Attribute (Subject)	Access control rule
PRT	D.DOC	+PRT	Read	U.NORMAL	User ID	Denied, except

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

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1(2) The TSF shall enforce the **TOE Function Access Control SFP** to objects based on the following: **users and** [list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP in table 34]

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *the user is explicitlyauthorized by U.ADMINISTRATOR to use a function,a user that is authorized to usethe TOE is automatically authorized to use the functions*[list offunctions in Table 34]

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

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

Table 34: 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 ID	Denied, except for the U.NORMAL explicitly authorized by U.ADMINISTRATOR to use a function
	F.SCN					
	F.CPY					
	F.FAX					
	F.DSR					

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

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1(3) The TSF shall enforce the **Service (PRT, SCN, CPY, DSR FAX) Access Control SFP in Table 33** to objects based on the following: **the list of subjects and objects controlled under the Service (PRT, SCN, CPY, DSR FAX) Access Control SFP in Table 33.**

FDP_ACF.1.2(3) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the (PRT, SCN, CPY, DSR FAX)Access Control SFP in Table 33 governing access among Users and controlled objects using controlled operations on controlled objects.**

FDP_ACF.1.3(3) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [Accounting User Rules].

FDP_ACF.1.4(3) The TSF shall explicitly deny access of subjects to objects based on the [Accounting User Rules].

6.1.3.7 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)].

6.1.3.8 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 [IPv4 filtering rule] on [list of subjects (External IT entities), list of information (packet), operations (allow, deny)].

6.1.3.9 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 [IPv6filtering rule] on [list of subjects (External IT entities), list of information (packet), operations (allow, deny)].

6.1.3.10 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 [FAXdata control] on [list of subjects (External IT entities), list of information (fax data), operations (discard**)**].

6.1.3.11 FDP_IFC.1(5) Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(5) The TSF shall enforce the [Protocol/Port information flow control] on [list of subjects (External IT entities), list of information (packet), operation (allow**)**].

6.1.3.12 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 initialization

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 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 authorize 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].

6.1.3.13 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 initialization

FDP_IFF.1.1(2) The TSF shall enforce the [IPv4filtering 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 information(IPv4 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 IPv4 filtering rule registered by U.ADMINISTRATOR
b) If U.ADMINISTRATOR registers specific IPv4 filtering rules, specific protocols and ports which are selected by U.ADMINISTRATOR are denied.]

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

FDP_IFF.1.4(2) The TSF shall explicitly authorize 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].

6.1.3.14 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 initialization

FDP_IFF.1.1(3) The TSF shall enforce the [IPv6filtering 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 information(IPv6 Address)].

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) All packets are allowed if there is no IPv6 filtering rule registered by U.ADMINISTRATOR
b) If U.ADMINISTRATOR registers specific IPv6 filtering rules, specific protocols and ports which are selected by U.ADMINISTRATOR are denied.]

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

FDP_IFF.1.4(3) The TSF shall explicitly authorize 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].

6.1.3.15 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 initialization

FDP_IFF.1.1(4) 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(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) Discard the fax data if the incoming fax data is not standardized MMR, MR, or MH of T.4 specification]

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].

6.1.3.16 FDP_IFF.1(5) Simple security attributes

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

FDP_IFF.1.1(5) 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(5) 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(5) The TSF shall enforce the [none].

FDP_IFF.1.4(5) The TSF shall explicitly authorize an information flow based on the following rules: [none].

FDP_IFF.1.5(5) The TSF shall explicitly deny an information flow based on the following rules: [none].

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

6.1.4 Class FIA: Identification and authentication

6.1.4.1 FIA_AFL.1 Authentication failure handling

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

FIA_AFL.1.1 The TSF shall detect when *[the assigned valuem [3] by U.ADMINISTRATOR]* unsuccessful authentication attempts occur related to [U.ADMINISTRATOR and U.NORAL authentication]

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met* the TSF shall [lockout the local U.ADMINISTRATOR's login for a period of 3 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, password, and role.]

6.1.4.3 FIA_UAU.1 Timing of authentication

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

FIA_UAU.1.1 The TSF shall allow [submission of network print jobs, incoming faxes, and usage of the LUI with menus that has no relation with security] on behalf of the user to be performed before the user is authenticated.

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

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

6.1.4.4 FIA_UAU.7 Protected authentication feedback

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

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

6.1.4.5 FIA_UID.1Timing of identification

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

FIA_UID.1.1 The TSF shall allow [Incoming faxes, and usage of the LUI with menus that has no relation with security] on behalf of the user to be performed before the user is identified.

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

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

6.1.4.6 FIA_USB.1 User-subject binding

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

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [U.NORMAL role, U.ADMINISTRATOR role].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [none].

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: [none].

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 35] to [U.ADMINISTRATOR].

Table 35: Management of Security Functions Behavior

Security Function	Selection Operation		
	determine the behavior of	disable	enable
System Reboot			○
Authentication Mode	○		○
Log Configuration		○	○
Secure HTTP		○	○
IP/MAC Filtering	○	○	○
Image Overwrite	○	○	○
IPSec		○	○
Secure Connection		○	○
SMTP		○	○

6.1.5.2 FMT_MSA.1(1) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

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

6.1.5.3 FMT_MSA.1(2) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(2) The TSF shall enforce the **TOE Function Access Control SFP,**[none**]** to restrict the ability to *[Execution]*the security attributes [list of security attributes in Table 34] to [U.ADMINISTRATOR].

6.1.5.4 FMT_MSA.1(3) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(3) The TSF shall enforce the [Service (PRN, SCN, CPY, DSR FAX) Access Control SFP in Table 33] to restrict the ability to *[Read]* the security attributes [list of security attributes in Table 33] to [U.ADMINISTRATOR].

6.1.5.5 FMT_MSA.1(4) Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(4) The TSF shall enforce the [MAC filtering rule, IPv4 filtering rule,IPv6 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 36] to [U.ADMINISTRATOR].

Table 36: Management of Security Attributes

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

6.1.5.6 FMT_MSA.3(1) Static attribute initialization

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

FMT_MSA.3.1(1) The TSF shall enforce the **Common Access Control SFP in Table 32,** [Service (PRN, SCN, CPY, DSR FAX) Access Control SFP in Table 33,FAXdata 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.

6.1.5.7 FMT_MSA.3(2) Static attribute initialization

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

FMT_MSA.3.1(2) The TSF shall enforce the **TOE Function Access Control Policy,** [MAC filtering rule, IPv4 filtering rule, IPv6 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.

6.1.5.8 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 37] to *U.ADMINISTRATOR*

Table 37: 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	○	○			
SMTP Server Configuration	○	○			
Log in Identification	○	○			
Audit Log Data	○		○		
Network Protocol and Port Configuration (TCP/IPv4, TCP/IPv6,Raw TCP/IP Printing, LPR,IPP, WSD, SLP, UPnP, mDNS, CIFS, SNMP, SMTP)	○	○			
Restore Default for Security Configurations and Network Configurations)	○				
Digital Certificate	○	○	○	○	
IPv4/6 filtering Address	○	○	○	○	
Mac filtering Address	○	○	○	○	
Image Overwrite configuration	○	○			

6.1.5.9 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 38].

Table 38: Management Functions

Management Functions	Relevant SFR
Management of Audit data (review, delete)	FAU_GEN.1, FAU_SEL.1
Management of Common 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 Service Access Control rules	FDP_ACC.1(3), FDP_ACF.1(3)
Management of MAC filtering rules	FDP_IFC.1(1), FDP_IFF.1(1)
Management of IP filtering rules	FDP_IFC.1(2), FDP_IFC.1(3), FDP_IFF.1(2), FDP_IFF.1(3)
Management of Protocol/Port information flow control rules	FDP_IFC.1(5), FDP_IFF.1(5)
Management of Image overwrite function	FDP_RIP.1
Management of User attributes (User ID, User Name, Password, Email, Fax No, and Group ID)	FIA_ATD.1, FIA_UID.1, FIA_UAU.1
Management of security functions behavior	FMT_MOF.1
Management of security attributes	FMT_MSA.1(1)(2)(3)(4)
Management of TSF data	FMT_MTD.1
Management of security Roles	FMT_SMR.1
Management of TSF testing (initiation)	FTP_TST.1
Management of TSF-initiation termination	FTA_SSL.3
Management of fax forward functions	FPT_FDI_EXP.1

6.1.5.10 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,** *Nobody.*

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

6.1.6 Class FPT: Protection of the TSF

6.1.6.1 FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

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

6.1.6.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.6.3 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

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

6.1.7 Class FTA: TOE access

6.1.7.1 FTA_SSL.3TSF-initiated termination

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

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [5 minutes of U.ADMINISTRATOR inactivity and 30 seconds of U.NORMAL inactivity].

6.1.8 Class FTP: Trusted path/channels

6.1.8.1 FTP_ITC.1 Inter-TSF trusted channel

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

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

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

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

6.2 Security Assurance Requirements

Security assurance requirements (SAR) defined in this document consists of assurance component in Common Criteria for Information Technology Security Evaluation, Part 3. The Evaluation Assurance Levels (EALs) is 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 39: 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
	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	Authorization 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 summarize the usage and major security features of the TOE.

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

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

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

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

Evaluator action elements:

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

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

6.2.1.4 ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

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

Evaluator action elements:

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

6.2.1.5 ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

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

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

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

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

Evaluator action elements:

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

6.2.1.6 ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

6.2.1.7 ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

6.2.2 Class ADV: Development

6.2.2.1 ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

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

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

6.2.2.2 ADV_FSP.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 summarize 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 behavior 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 behavior of the SFR-enforcing subsystems.

ADV_TDS.2.5C The design shall summarize the SFR-supporting and SFR-non-interfering behavior of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarize the behavior 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 behavior 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 Authorization 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 labeled 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 authorized 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 40: 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										✓						
FAU_SAR.1												✓				
FAU_SAR.2												✓				
FAU_SEL.1										✓						
FAU_STG.1											✓					
FAU_STG.4											✓					
FCS_CKM.1(1)													✓			
FCS_CKM.1(2)	✓															
FCS_CKM.4(1)													✓			
FCS_CKM.4(2)	✓															
FCS_COP.1(1)													✓			
FCS_COP.1(2)	✓															
FDP_ACC.1(1)	✓	✓	✓													
FDP_ACC.1(2)							✓									

	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
FDP_ACC.1(3)	✓															
FDP_ACF.1(1)	✓	✓	✓													
FDP_ACF.1(2)							✓									
FDP_ACF.1(3)	✓															
FDP_IFC.1(1)																✓
FDP_IFC.1(2)																✓
FDP_IFC.1(3)																✓
FDP_IFC.1(4)															✓	
FDP_IFC.1(5)																✓
FDP_IFF.1(1)																✓
FDP_IFF.1(2)																✓
FDP_IFF.1(3)																✓
FDP_IFF.1(4)															✓	
FDP_IFF.1(5)																✓
FDP_RIP.1	✓													✓		
FIA_AFL.1							✓									
FIA_ATD.1							✓									
FIA_UAU.1							✓	✓								
FIA_UAU.7							✓									
FIA_UID.1	✓	✓	✓	✓	✓	✓	✓	✓		✓						
FIA_USB.1							✓									
FMT_MOF.1				✓	✓	✓										
FMT_MSA.1(1)	✓	✓	✓													
FMT_MSA.1(2)							✓									
FMT_MSA.1(3)	✓															
FMT_MSA.1(4)																✓
FMT_MSA.3(1)	✓	✓	✓													
FMT_MSA.3(2)							✓									✓
FMT_MTD.1				✓	✓	✓										

	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
FMT_SMF.1	✓	✓	✓	✓	✓	✓										
FMT_SMR.1	✓	✓	✓	✓	✓	✓	✓									
FPT_FDI_EXP.1								✓								
FPT_STM.1										✓						
FPT_TST.1									✓							
FTA_SSL.3							✓	✓								
FTP_ITC.1	✓	✓	✓	✓	✓	✓										

Table 41: Security Requirements Rationale

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS O.DOC.NO_ALT O.FUNC.NO_ALT	Protection of User Data from unauthorized disclosure or alteration	FDP_ACC.1(1)	Enforces protection by establishing an access control policy.
		FDP_ACF.1(1)	Supports the access control policy by providing an access control function.
		FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MSA.1(1)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(1)	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.
		FTP_ITC.1	Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.
O.DOC.NO_DIS	Protection of User	FCS_CKM.1(2)	Supports encryption of the data to

Objectives	Description	SFRs	Purpose
	Document Data from unauthorized disclosure		protect the data transmitted via network by generating cryptographic keys.
		FCS_CKM.4(2)	Supports encryption of the data to protect the data transmitted via network by destructing cryptographic keys.
		FCS_COP.1(2)	Supports encryption of the data to protect the data transmitted via network by performing a cryptographic operation.
		FDP_RIP.1	Enforces protection by making residual data unavailable.
		FDP_ACC.1(3)	Enforces protection by establishing an access control policy.
		FDP_ACF.1(3)	Supports access control policy by providing access control function.
O.PROT.NO_ALT O.CONF.NO_DIS O.CONF.NO_ALT	Protection of TSF Data from Unauthorized disclosure or alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MOF.1	Restricts the ability to determine the behavior of disable and enable the functions
		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.
		FTP_ITC.1	Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.
O.USER. AUTHORIZED	Authorization of Normal Users and Administrators to use the TOE	FDP_ACC.1(2)	Enforces authorization by establishing an access control policy.
		FDP_ACF.1(2)	Supports the access control policy by providing an access control function.
		FIA_AFL.1	Supports authentication by handling authentication failure.
		FIA_ATD.1	Supports authorization by associating security attributes with users.
		FIA_UAU.1	Enforces authorization by requiring user authentication.
		FIA_UAU.7	Supports authorization by protecting authentication feedback.
		FIA_UID.1	Enforces authorization by requiring user identification.
		FIA_USB.1	Enforces authorization by distinguishing subject security attributes associated with user roles.
		FMT_MSA.1(2)	Supports access control function by

Objectives	Description	SFRs	Purpose
			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.1	Enforces management of external interfaces by requiring user authentication.
		FIA_UID.1	Enforces management of external interfaces by requiring user identification.
		FTA_SSL.3	Enforces management of external interfaces by terminating inactive sessions.
		FPT_FDI_EXP.1	Enforces management of external interfaces by requiring(as needed) administrator control of data transmission from external Interfaces t Shared-medium Interfaces.
O.SOFTWARE. VERIFIED	Verification of software integrity	FPT_TST.1	Enforces verification of software by requiring self-tests.
O.AUDIT.LOGGED	Logging and authorized access to audit events	FAU_GEN.1	Enforces audit policies by requiring logging of relevant events.
		FAU_GEN.2	Enforces audit policies by requiring logging of information associated with audited events.
		FAU_SEL.1	Supports audit policies by providing the ability to select the set of events to be audited.
		FIA_UID.1	Supports audit policies by associating a user's identity with events.
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.
O.AUDIT_STORAG E.PROTECTED	Protected audit trail storage and prevention of audit data loss	FAU_STG.1	Enforces protection of audit trail storage by preventing unauthorized modification, access, deletion to the stored audit records in the audit trail.
		FAU_STG.4	Enforces prevention of audit data loss by overwriting the oldest stored audit records.
O.AUDIT_ACCESS. AUTHORIZED	Access control of audit records only by authorized persons	FAU_SAR.1	Enforces the audit review function by providing authorized U.ADMINISTRATOR with the ability to read all of audit information from the audit records.
		FAU_SAR.2	Enforces restriction of the audit review function by prohibiting all

Objectives	Description	SFRs	Purpose
			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 MSD	FCS_CKM.1(1)	Supports encryption of the data to be stored on the MSD by generating cryptographic keys.
		FCS_CKM.4(1)	Supports encryption of the data to be stored on the MSD by destructing cryptographic keys.
		FCS_COP.1(1)	Supports encryption of the data to be stored on the MSD by performing a cryptographic operation.
O.DATA. OVERWRITTEN	Image overwrite to protect the used document data in the MSD	FDP_RIP.1	Enforces protection by making residual data unavailable.
O.FAX_DATA.FORMAT	Block incoming fax data if received fax data does not qualify fax image standard.	FDP_IFC.1(4)	Enforces protection by establishing a FAX data control policy.
		FDP_IFF.1(4)	Supports FAX data control policy by providing information flow control function.
O.INFO.FLOW_CONTROLED	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) FDP_IFC.1(3)	Enforces protection by establishing an IP filtering rule policy.
		FDP_IFC.1(5)	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) FDP_IFF.1(3)	Supports the IP filtering rule policy by providing an information flow control function.
		FDP_IFF.1(5)	Supports the Protocol/Port information flow control policy by providing an information flow control function.
		FMT_MSA.1(4)	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.

6.3.2 Security Assurance Requirements Rationale

Security assurance requirements of this security target conform to IEEE Std 2600.1-2009 Version 1.0 (CCEVS-VR-VID10340-2009, June 12, 2009) as known as U.S. Government Protection Profile for Hardcopy Devices in Basic Robustness Environments [PP].

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

Table 42: Dependencies on the TOE Security Functional Components

No.	Functional Component ID	Dependencies	Reference
1	FAU_GEN.1	FPT_STM.1	48
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	1, 35
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	1, 44
6	FAU_STG.1	FAU_GEN.1	1
7	FAU_STG.4	FAU_STG.1	6
8	FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	10, 12
9	FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	11,13
10	FCS_CKM.4(1)	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	8
11	FCS_CKM.4(2)	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	9, 51
12	FCS_COP.1(1)	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	8, 10
13	FCS_COP.1(2)	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	9, 11, 51
14	FDP_ACC.1(1)	FDP_ACF.1	17
15	FDP_ACC.1(2)	FDP_ACF.1	18

No.	Functional Component ID	Dependencies	Reference
16	FDP_ACC.1(3)	FDP_ACF.1	19
17	FDP_ACF.1(1)	FDP_ACC.1 FMT_MSA.3	14, 42
18	FDP_ACF.1(2)	FDP_ACC.1 FMT_MSA.3	15, 43
19	FDP_ACF.1(3)	FDP_ACC.1 FMT_MSA.3	16, 43
20	FDP_IFC.1(1)	FDP_IFF.1	25
21	FDP_IFC.1(2)	FDP_IFF.1	26
22	FDP_IFC.1(3)	FDP_IFF.1	27
23	FDP_IFC.1(4)	FDP_IFF.1	28
24	FDP_IFC.1(5)	FDP_IFF.1	29
25	FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	20, 43
26	FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	21, 43
27	FDP_IFF.1(3)	FDP_IFC.1 FMT_MSA.3	22, 43
28	FDP_IFF.1(4)	FDP_IFC.1 FMT_MSA.3	23, 42
29	FDP_IFF.1(5)	FDP_IFC.1 FMT_MSA.3	24, 42
30	FDP_RIP.1	-	
31	FIA_AFL.1	FIA_UAU.1	33
32	FIA_ATD.1	-	
33	FIA_UAU.1	FIA_UID.1	35
34	FIA_UAU.7	FIA_UAU.1	33
35	FIA_UID.1	-	
36	FIA_USB.1	FIA_ATD.1	32
37	FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	45, 46

No.	Functional Component ID	Dependencies	Reference
38	FMT_MSA.1(1)	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	14, 46, 47
39	FMT_MSA.1(2)	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	15, 46, 47
40	FMT_MSA.1(3)	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	16, 46, 47
41	FMT_MSA.1(4)	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	21,22, 23, 24, 25, 46, 47
42	FMT_MSA.3(1)	FMT_MSA.1 FMT_SMR.1	38, 40, 41, 46
43	FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1	39, 41, 46
44	FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	45, 46
45	FMT_SMF.1	-	
46	FMT_SMR.1	FIA_UID.1	35
47	FPT_FDI_EXP.1	FMT_SMR.1 FMT_SMF.1	45, 46
48	FPT_STM.1	-	
49	FPT_TST.1	-	
50	FTA_SSL.3	-	
51	FTP_ITC.1	-	

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 Basic Functions

The TOE provides the following basic features:

− Printing—producing a hardcopy document from its electronic form

− Scanning—producing an electronic document from its hardcopy form

− Copying—duplicating a hardcopy document

− Faxing—scanning documents in hardcopy form and transmitting them in electronic form over telephone lines and receiving documents in electronic form over telephone lines and printing them in hardcopy form

− Document storage and retrieval—storing an electronic document during one document processing job for access during one or more subsequent document processing jobs, and retrieving an electronic document that was stored during a previous document processing job

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

7.2 TOE Security Functions

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

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

7.2.1 Identification & Authentication (TSF_FIA)

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

1. Authentication

The TOE can restrict U.NORMAL from accessing the machine or application. U. ADMINISTRATOR can also give specific permission for U.NORMAL to only use certain features of the machine. To identify U.NORMAL and U.ADMINISTRATOR, TOE should provide an authentication method. To access the TOE's functions, U.NORMAL or U.ADMINISTRATOR sends his ID and Password to the TOE. The TOE identifies U.NORMAL or U.ADMINISTRATOR with checking the validity of their ID and password.

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

The TOE provides the following authentication methods. The authentication method which is applied by the TOE can be chosen by only the authenticated U. ADMINISTRATOR.

- Local authentication: Activate local authentication. An authentication is managed by using the user information registered in TOE.
- Network authentication: Activate network authentication. An authentication is conducted to the remote authentication server such as LDAP, Kerberos, SMB. User information is not registered in TOE.
- Standard Accounting: Activate Standard Accounting. An authentication requests U.NORMAL to login before using all device applications. U.NORMAL cannot use any application without logging in. It also manages use of specific applications such as fax, copy, print, scan-to-email, scan-to-server.

The Restriction of authentication methods is as follows.

(1) When the number of consecutive invalid authentication attempts which is tried by U. ADMINISTRATOR has exceeded the 3 times within 3 minutes, the account will be locked for 3 minutes.

(2) If U.ADMINISTRATOR is idle for 3 minutes, the mutual session will be terminated automatically.

(3) U.NORMAL's password cannot be longer than4-characters long. The U.ADMINISTRATOR's password which is entered in Local UI and GUI shall be 8 or more characters (8~15) which the password contains at least 1 alphabet, at least 1 number, and at least 1 special character (#, $, +, etc.). It is not required that the U.ADMINISTRATOR's password which is entered in Local UI is identical to the password which is entered in GUI.

2. Role Management

The TOE supports the role management of U.USER by U. ADMINISTRATOR.

- Role Management: U.ADMINISTRATOR can give permissions to U.NORMAL to only use certain features of the machine and can give different rights to different U.NORMAL by using role management.
- User Account List: The TSF shall store user information on the machine's MSD. U.ADMINISTRATOR can use this feature to manage the users using the machine. U.ADMINISTRATOR can add up to 500 entries. U.USER is allowed to view all of U.NORMAL's own Account information.

3. PIN number Authentication

The TOE provides PIN number authentication. PIN number authentication is requested before accessing store print, confidential print or the secure box. This authentication needs to configure the PIN number from the print driver, and it is used for loading a stored file using the control panel on LUI.

(1) Secure box

U.NORMAL can save PC-printed, faxed, scanned documents in the box and print the saved documents later. If U.NORMAL wants the box to be a secured box, U.NORMAL checks the Secured Box and sets PIN number to be used for accessing the box.

(2) Store print & Confidential print

Confidential print is a print feature that only U.NORMAL who directly enters PIN number in LUI can obtain his printed documents from TOE. To do this, U.USER needs to set PIN number on a driver to be used for printing the confidential documents. Store print also allows only U.USER who stored a file to access the file with the PIN number by setting securely and previously.

4. Common Access Control & TOE Function Access Control

TOE enforces the Common Access Control & TOE Function Access Control based on the user account assigned to User ID by U.ADMINISTRATOR when U.NORMAL accesses print/scan/copy/fax/document storage retrieval functions offered by the MFP.

- Common Access Control

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 an external server (SMB Server, FTP 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.

7.2.2 Network Access Control (TSF_NAC)

Relevant SFR: FDP_IFC.1(1)(2)(3)(5), FDP_IFF.1(1)(2)(3)(5), FMT_MSA.1(4)

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

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

- Protocol/Port control:

1) Network protocols: TCP/IPv4, TCP/IPv6,Raw TCP/IP Printing, LPR,IPP, WSD, SLP, UPnP, mDNS, CIFS, SNMP, SMTP Protocol
2) Port number: Logical channel in the range of 1 to 65535

   A standard communication protocol and a port perform 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

TOE. Only U.ADMINISTRATOR can configure these functions, and these configurations are altered on each reboot of network card, and thus TOE 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 TCP/IPv4, TCP/IPv6,Raw TCP/IP Printing, LPR,IPP, WSD, SLP, UPnP, mDNS, CIFS, SNMP, SMTP protocols.

- 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

Only packets using IPv4/IPv6 addresses which are not exhibited withIPv4/IPv6 filtering rule by U.ADMINISTRATOR are allowed to communicate between TOE and outside objects.

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

7.2.3 Security Management (TSF_FMT)

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

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

The TSF shall restrict the ability to determine the behavior of, and disable/enable the functions accessible to U.ADMINISTRATOR.

Table 43 : Management of Security Functions Behavior

Security Function	Selection Operation		
	determine the behavior of	disable	enable
System Reboot			○
Authentication Mode	○		○
Log Configuration		○	○
Secure HTTP		○	○
IP/MAC Filtering	○	○	○
Image Overwrite	○	○	○
IPSec		○	○
Secure Connection		○	○
SMTP		○	○

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

Table 44 : Management of Security Attributes

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

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

Table 45 : 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	◯	◯			
SMTP Server Configuration	◯	◯			
Log in Identification	◯	◯			
Audit Log Data	◯		◯		
Network Protocol and Port Configuration (TCP/IPv4, TCP/IPv6,Raw TCP/IP Printing, LPR,IPP, WSD, SLP, UPnP, mDNS, CIFS, SNMP, SMTP)	◯	◯			
Restore Default for Security Configurations and Network Configurations)	◯				
Digital Certificate	◯	◯	◯	◯	
IPv4/6 filtering Address	◯	◯	◯	◯	
Mac filtering Address	◯	◯	◯	◯	
Image Overwrite configuration	◯	◯			

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.

7.2.4 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, FPT_STM.1

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, description, data, user, result, destination and source of jobs, success or failure, log out, access and deletion of log data, and enablement and disablement of the log function).

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. The TOE can store up to 7,000 for all log events.

(The maximum number for each log event: job log: 5,000; security log: 1,000; operation log: 1,000) When each log events exceeds the maximum number, the TOE overwrites the oldest stored audit records.

The records defined audit event is associated with identity of user who caused the event.

The TOE provides time stamp of clock function which is issued the defined audit event occurred.

The clock setting only can be changed by U.ADMINISTRATOR

Table 46: Security Audit Event

Relevant SFR	Auditable Events	Additional Information
FDP_ACF.1	Job completion	Type of job
FIA_UAU.1	Both successful and unsuccessful use of the authentication mechanism	None required
FIA_UID.1	Both successful and unsuccessful use of the identification mechanism	Attempted user identity, if available
FTA_SSL.3	Locking of an interactive session by the locking mechanism	None required
FMT_SMF.1	Use of the management functions	None required
FPT_TST.1	Execution of the TSF self tests and the results of the tests	None required
FDP_RIP.1	Manual Image Overwrite	None required
FTP_ITC.1	Failure of the trusted channel functions	None required
FPT_STM.1.	Changes to the time	None required

7.2.5 Image Overwrite (TSF_IOW)

Relevant SFR: FDP_RIP.1

The TOE provides Manual Image Overwrite functions that delete the stored file from the hard MSD. The TOE implements an image overwrite security function to overwrite temporary files created

during the copying, printing, scan-to-email, or scan-to-server processes or the intentionally stored files in the TOE.

The manual image overwrite function can also be invoked manually only by U.ADMINISTRATOR. Once invoked, the Manual Image Overwrite cancels all Print and Scan jobs, halts the printer interface (network), overwrites the contents of the reserved section 3 times on the MSD, and then the main controller reboots. If there are any problems during overwriting, the Manual Image Overwrite job automatically restarts after the problem is resolved to overwrite the remaining area.

7.2.6 Data Encryption (TSF_NVE)

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

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

The TOE generates cryptographic keys (private key, public key, secure key) 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 MSD.

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 MSD, the TOE encrypts the data using the AES 256 algorithm and cryptographic key.

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

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

7.2.7 Fax Data Control (TSF_FLW)

Relevant SFR: FDP_IFC.1(4), FDP_IFF.1(4), FPT_FDI_EXP.1

In the TOE, the memory areas for the fax board and for the network port on the main controller board are separated. 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. 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 servers through the internal network. When non-standardized format data are discovered, the TOE destroys the fax image.

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.

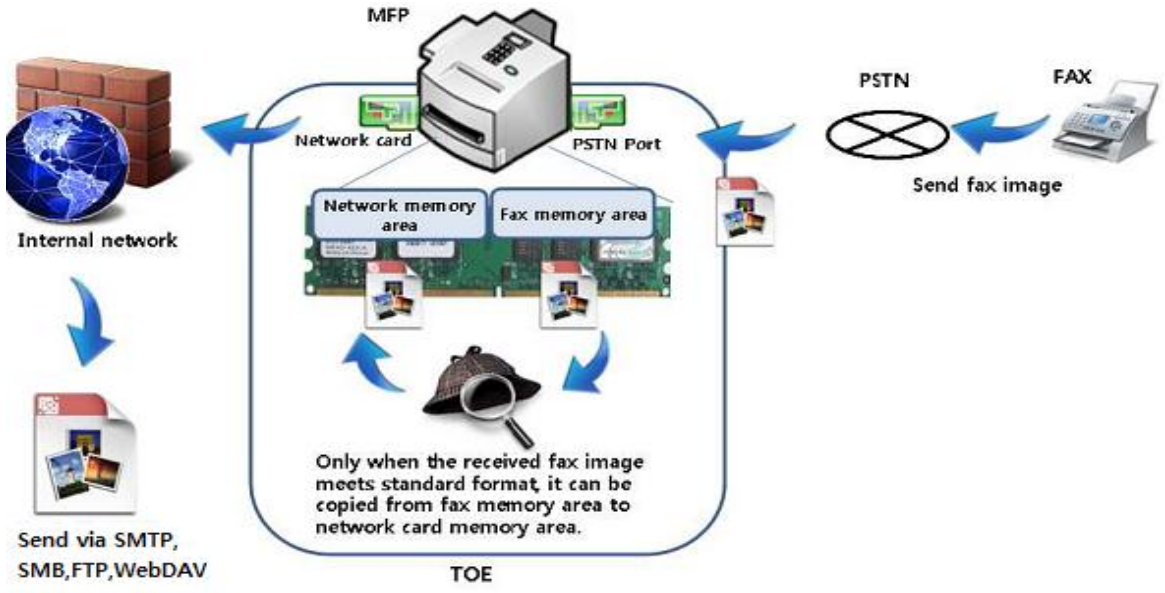

Figure 4: Information Flow Summary

7.2.8 Self Testing (TSF_STE)

Relevant SFR: FPT_TST.1

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

Self testing executes the TSF code and data integrity check to verify the correctness of TSF code and Data.

The TOE executes the CRC encoding as well as the AES encryption with executable codes of TOE. 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.

The TOE saves the TSF data to the encryption section. To verify TSF data integrity the TOE checks the sample string encryption. The TOE extracts the encryption Key data and decrypts the sample code with that Key and compare to the saved original sample string. If the sample string is same with previous the TOE defined the TSF data is not to corrupted..

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 47 :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

7.2.9 Secure Communication (TSF_SCO)

Relevant SFR: FCS_CKM.1(2), FCS_CKM.4(2), FCS_COP.1(2), FPT_ITC.1

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

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

IPSEC support ESP to provide confidentiality, origin authentication, integrity and IKE for key exchange. IPSEC supports 3DES, AES for encryption, SHA-1 for integrity and DH-Group: 1, 2, 5, 14, 15, 16, 17, 18 for key agreement.

Only data by using IPSEC via network can be access the TOE.