Samsung MFP Security Kit Type_D V1.0

Security Target

V 1.4

Samsung Electronics Company

Document History

VERSION	DATE	DESCRIPTION OF CHANGE	SECTIONS AFFECTED	REVISED BY
0.10	2009-07-17	Initial version	ALL	SEC
0.15	2009-07-21	Updated as per Elbert-P specification	Chapter 1	SEC
0.20	2009-09-03	Change TOE Scope	ALL	SEC
0.21	2009-09-08	Update specifications	Table 1~ Table 4, Figure 1	SEC
0.50	2009-09-29	- Delete temporary memo - Change publication and publishing date	Chapter 1	SEC
0.90	2009-10-15	Update s/w version in table 4	Chapter 1	SEC
0.91	2009-10-28	Update information of PPM in table 3	Chapter 1	SEC
1.0	2010-01-07	Apply the 1st EOR - Change version, publication date, CC identification - Fix reference error for CC_Part2 - Add terms - OR-ASE-002(ASE_INT.1-3) - OR-ASE-004(ASE_SPD.1-2) - OR-ASE-005(ASE_OBJ.2-6) - OR-ASE-009(ASE_REQ.2-9) - OR-ASE-008(ASE_REQ.2-5)	ALL	SEC
1.1	2010-03-25	Change OpenSSL version to V0.9.8l	1.3	SEC
1.2	2010-10-01	Correct Grammar and Syntax Errors	ALL	SEC
1.3	2010-10-21	Correct Grammar and Syntax Errors	ALL	SEC
1.4	2013-01-10	Change version, date, and table 4	Chapter 1	Kwangwoo Lee

Contents

List of Figures

List of Tables

1 Security Target Introduction

1.1 Security Target References

Security Target Title :	Samsung MFP Security Kit Type_D V1.0 Security Target
Security Target Version :	V1.3
Publication Date :	January 10, 2013
Authors :	Samsung Electronics
Organization for Security Target Certification :	IT Security Certification Center (ITSCC) of National Intelligence Service (NIS)
ST Evaluator :	Korea System Assurance Co., Ltd.
CC Identification :	Common Evaluation Standard for Information Security System (Notification No. 2009-52 by Ministry Of Public Administration and Security (v3.1)
Keywords :	Samsung Electronics, Multi-function printer, Network Access Control

1.2 TOE References

Author	Samsung Electronics
Name	Samsung MFP Security Kit Type_D
Version	V1.0
Publishing Date	January 10, 2013

TOE Component: TOE Component is as follows:

TOE	Samsung MFP Security Kit Type_D V1.0
TOE Component	TSF_FLW_V1.50
	TSF_SAA_V1.50
	TSF_LUI_V1.50
	TSF_SFM_V1.50
	TSF_WUI_V1.50
	TSF_NAC_V1.50

1.3 TOE Overview

The TOE is embedded software on SAMSUNG Multi-function printers (MFPs). These MFPs include copy, print, scan, scan-to-email, scan-to-server, and fax features. The TOE allows the MFPs to perform fax/network separation, identification, and authentication tasks.

Table 1 shows the options that the SAMSUNG MFPs including the TOE provide.

Table 1: Models and Capabilities

	Print	Copy	Fax	Scan-to-email	Scan-to-server
SCX-5635FN/XAR	Standard	Standard	Standard	Standard	Standard

The TOE is intended to operate in a network environment that is protected from external malicious attacks (e.g., DoS), and with reliable PCs and authenticated servers. A user is able to access the TOE by using a local user interface, client machine from remote user, or a web user interface. (Refer to Figure 1: Operating Environment of the TOE.)

The local user interface is designed to be accessed by casual users and a local administrator. The users can operate copy, scan, and fax through the local user interface. In the case of a scanning job, users can operate the scanning job using the local user interface and then, transfer the scanned data to a certain destination by email addresses or server PCs. Users can also use their PCs to print out documents or to access the TOE through the internal network. The local administrator can change a PIN via LUI.

A web administrator can access TOE through the web user interface. From there, they can change the web administrator's ID and password, enable/disable the security audit service, download the security audit report and control the network access through configuration protocol/port.

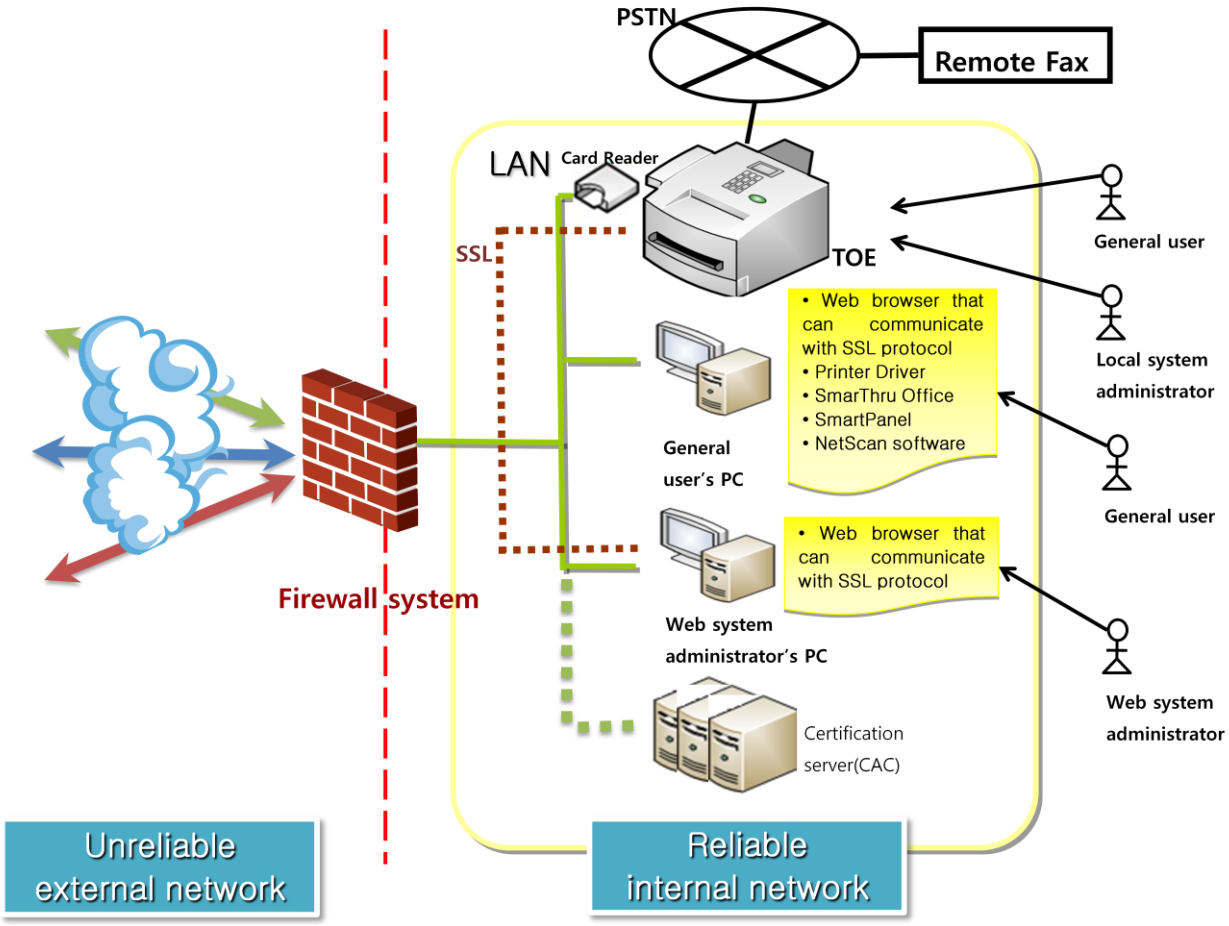

Figure 1: Operating Environment of the TOE

To operate TOE, additional non-TOE items such as hardware, firmware, and software are required.

The following table shows the non-TOE items and their specifications.

Table 2: Details of Non-TOE Items

Types	Items	Objectives	Specification
Hardware	MFP	The TOE must be embedded in the MFP.	Refer to Table 3

Types	Items	Objectives	Specification
	PC for web system administrator	PC for Web system 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 • 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:512 MB 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 general user	PC for general user to print or scan or copy with TOE	
	Firewall system	Firewall system to protect internal assets by blocking attacks from external networks.	–
	LAN	Internal network for TOE.	–
	PSTN	PSTN for translating fax image.	–
	CAC	The card with a built-in smart chip	
	Card Reader	A device to read information from the card with a built-in smart chip	
Firmware	Operating system for PC	Operating system for general user or web administrator	1) Windows 2000/XP(32/64 bit)/2003 Server(32/64 bit)/Vista(32/64 bit)/2008(32/64 bit), 2) Various Linux OS including: - RedHat 8.0, 9.0 (32 bit) - RedHat Enterprise Linux WS 4, 5 (32/64 bit) - Fedora Core 1~7 (32/64 bit) - Mandrake 9.2 (32bit), 10.0, 10.1 (32/64 bit) - Mandriva 2005, 2006, 2007 (32/64 bit) - SuSE Linux 8.2, 9.0, 9.1 (32 bit) - SuSE Linux 9.2, 9.3, 10.0, 10.1, 10.2 (32/64 bit) - SuSE Linux Enterprise Desktop 9, 10 (32/64 bit) - Ubuntu 6.06, 6.10, 7.04 (32/64 bit) - Debian 3.1, 4.0 (32/64 bit) 3) Mac OS 10.3~10.5

Types	Items	Objectives	Specification
	OpenSSL	SSL library that serves safe communication between user's client PC or Web system administrator's PC and the TOE	0.9.8l
	RTOS	Operating system embedded in MFP.	pSOS 2.5
Software	Web browser that can serve SSL communication	Web browser that serves SSL communication between general user's PC or Web administrator's PC and the TOE	Internet Explorer, Safari, Netscape
	Printer driver	Printer driver application software for general users to install in their PC. User can configure properties and start printing jobs through this printer driver.	PCL Driver V3.10.26 (32 bit/64 bit)
	SmarThru Office	SmarThru Office is an integrated management application program. Users can install this program in their PC, then edit scanned images or send email through this program.	SmarThru office V2.01.92
	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.	SmartPanel V1.19.09

Table 3: Specifications of the MFP that will use the TOE

Specifications		SCX-5635FN/XAR
LCD		4 line Graphic LCD
System Memory		Std.128 MB (Max. 384 MB)
HDD		N/A
FAX	Compatibility	ITU-T Group 3
	Comm. System	PSTN / PABX
	Modem Speed	33.6 Kbps
Interface		Hi-Speed USB 2.0, Ethernet 10/100 base TX
Extra information		Up to 33 ppm in A4 (35 ppm in Letter)

<Security Functions>

The TOE provides fax/network separation, identification, and authentication, Network access control.

- **The separation of fax and network**

A fax image can be copied from fax memory to network card memory only when the fax image has a standard format - the standard MMR, MR, and MH image on the T.4 specification. If the fax image is not standardized, the device does not copy a fax image to network memory from fax memory.

The TOE controls over and gives restricted permission to information flow between the fax board and the network port of the main controller. The direct communication between an internal client PC and fax modem in the local area will not be processed; it is only available in TOE.

The fax forwarding function automatically forwards a received fax image to a designated number. When this function is activated, the device has to copy the received fax image from fax memory to network card memory. Before copying the image, the device inspects the fax image to make sure it is in standard format. The fax image can only be transferred to network memory via a public switched telephone network (PSTN) line if it is in standard format and sent to the SMTP/SMB/FTP server through the internal network.

- **Identification and Authentication**

The TOE requires dividing a real client into different kinds of access level, such as a Web/local/telnet system administrator, before giving permission to access system management. The system administrator position is divided into three positions: web administrator, local administrator. In the authentication process of web administrator, the web client should input an ID and a password into the web user interface. Also, the local administrator in the authentication process of the local system should input a PIN into the local user Interface.

- **Network Access Control**

The TOE can control access to TOE resource through network from outside of TOE by configuring port number, and enabling/disabling protocol. The communication methods to access the TOE resource from outside of the TOE through network are network protocol and port. Administrator can control access from outside using standard port by configuring non-standard port number as an allowable port number. The administrator can control access from outside by enabling/disabling protocol. This can be configured by only certificated administrators through authentication.

<Assets>

The TOE protects assets such as image files, system audits, and TOE configuration data.

- **Component on internal network**

  Component of the internal network is a general user's PC, web administrator's PC, and the authentication servers. Through TOE, there is the possibility of attacking internal network and devastating all internal components, and so TOE should be protected from outside threats.

- **System audit log**

  The system audit logs include system-pertinent information. Because hackers can attack the TOE with bad intentions, the system audit logs must be securely protected.

  The audit logs that are generated by system may include system data that might be abused; hence, it should be protected from all attack attempts.

- **Image file**

  An image file from a copying, printing, faxing, or scanning job may include important information that a client does not want to disclose. Therefore, it must be securely protected.

- **TOE configuration data**

  If a hacker were to acquire TOE configuration data, which includes the TOE security setup, the TOE might be compromised. System administrators must securely protect the TOE configuration data.

<Definition & Roles of User>

Users can be divided into two types: administrator and general user

The role of each user is as follows:

- **Administrator**

  Local administrator

  The local administrator role manages the Samsung MFP through a local user interface. The tasks performed by this role include confirming MFP status information and setting system configurations. Moreover, local administrators change PINs for security.

  Web administrator

  The web administrator role manages the web site (embedded in the Samsung MFP) by using the web user interface. This role performs the following:

  – Activates or deactivates security audit

- Downloads the security audit log
- Activates or deactivates protocol
- Changes the port number

- **General User**

  The general user accesses the Samsung MFP through the LUI or the user's PC. From the local user interface, users can perform copy, fax, or scan jobs. From the user's PC, the user can access the TOE from the internal network and print documents. When using SmarThru Office, the user can also scan.

1.4 TOE Description

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

1.4.1Physical Scope

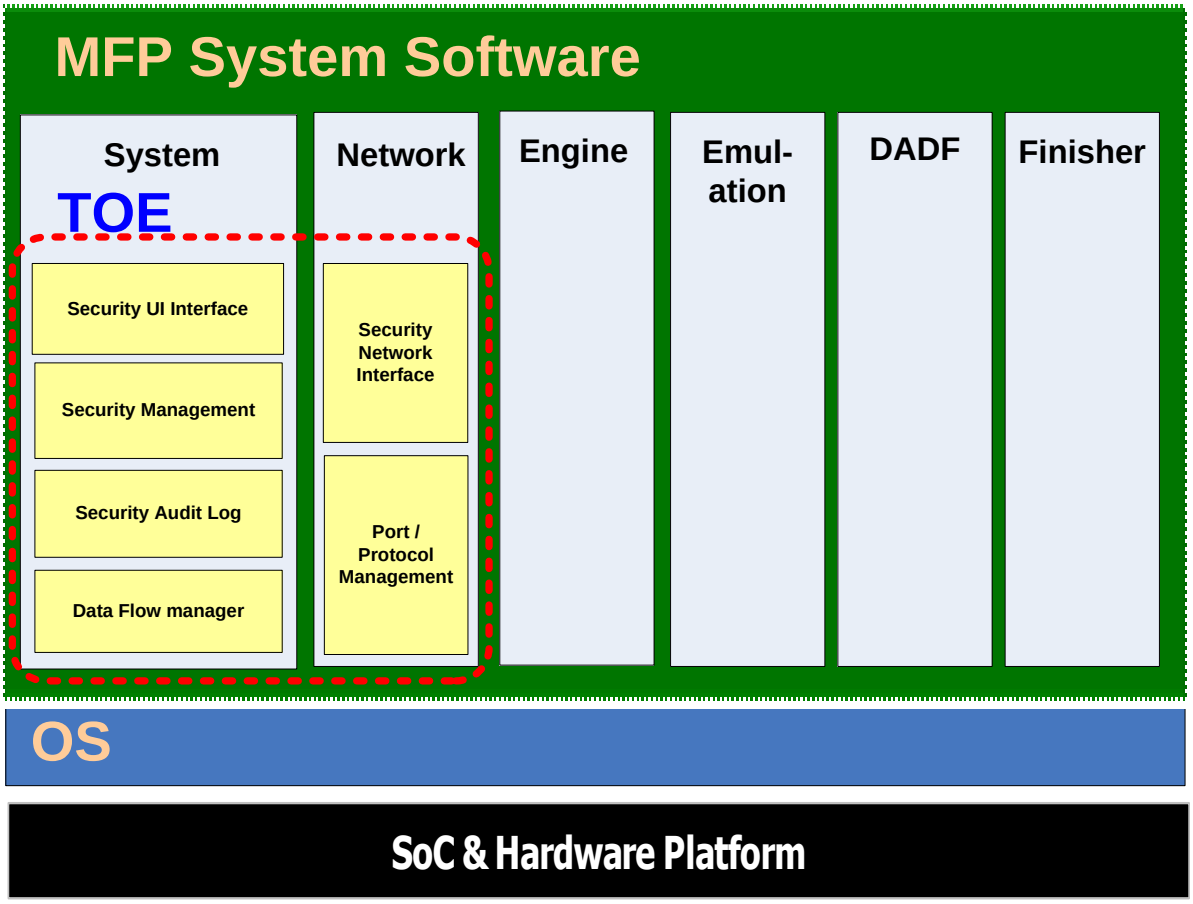

Figure 2: Physical Structure of MFP System Software

The internal structure of the MFP System Software hierarchically consists of a hardware platform, an operating system (OS) which includes a device driver, the TOE, and non-TOE software (including system software, network software, emulation software, DADF software, finisher software, and engine software).

The TOE is a security software module positioned on the system software, UI software, and network software. The non-TOE software module includes the emulation software, DADF software, finisher software and engine software.

The TOE is for general users and system administrators. The following three kinds of manuals are provided with this TOE through a CD or the Web:

- The user guide/troubleshooting guide describe how to install and how to use the MFP. It also provides examples of how to deal with exceptional cases.
- The security administrator's guide describes how to use security functions that the TOE provides. It also provides examples of how to deal with exceptional cases.
- The network administrator's guide describes how to configure network functions and how to set MFP functions and security functions for administrators.

The system software includes security management, security audit log, and data flow manager. The UI software includes the security UI. The network software includes the security network interface and port/protocol management.

Table 4: Evaluated Software/Firmware for the TOE

Software Version	SCX-5635FN/XAR
System Software	V2.01.01.16_SEA31_1.57CCC
- Security Management	TSF_SFM_V1.50
- Security Audit Log	TSF_SAA_V1.50
- Data Flow Manager	TSF_FLW_V1.50
- Security UI Interface	TSF_LUI_V1.50
Network Software	V4.01.11_SEA31_1.24
- Security Network Interface	TSF_WUI_V1.50
- Port/Protocol Management	TSF_NAC_V1.50

The TOE is called the Samsung MFP Security Kit Type_D and is embedded in the MultiXpress SCX-5635FN/XAR device. It performs security functions for Samsung MFPs by using system software and network software.

The system software transforms the input data into the appropriate format. It also controls and manages the documents that are stored. Authorized administrators can manage system audit functions, security jobs, TSF data, or configuration on security items.

The network software has a web server that can be an interface between system administrators and an MFP. This software provides the functions below:

- WebUI through a web server
- Authentication for the web administrator and/or provides security management functions

- Ability for tracing the system audit log from an external network (SWS) to web administrator
- Functions for changing the port number, enabling/disabling protocol
- The web system interface

Emulation software, finisher software, DADF software, and engine software are not directly related to security functions, but these are the basic components for the TOE operation on the MFP hardware.

1.4.2Logical Scope

The logical scope of the TOE includes all of the software and firmware that are installed on the product. The TOE's logical boundary is composed of the security functions provided by the product.

The following security functions are provided by the TOE:

- Security Audit (TSF_FAU)
- Security Management (TSF_FMT)
- System Authentication (TSF_SAU)
- Information Flow (TSF_FLW)
- Network Access Control (TSF_NAC)

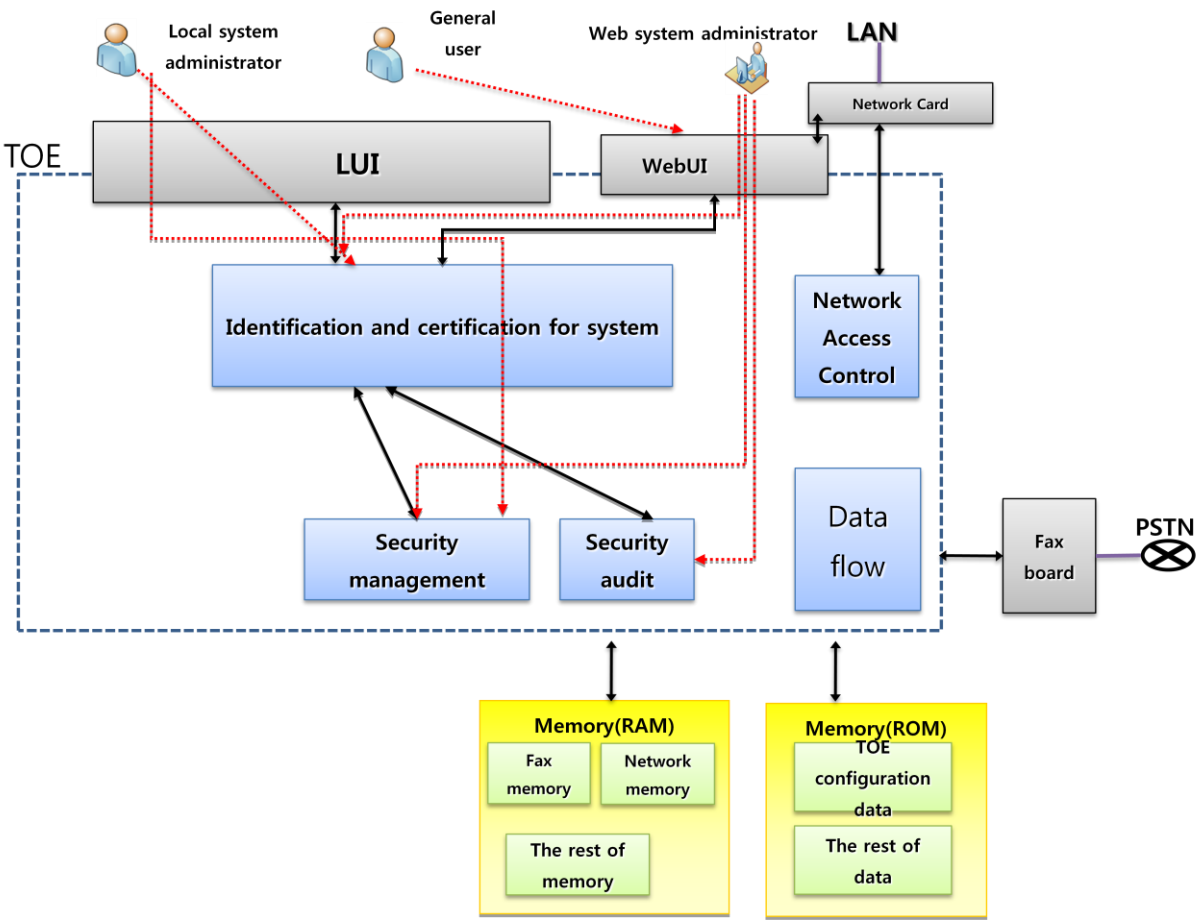

Figure 3: Logical Scope of the TOE

Security Audit (TSF_FAU)

Only authorized web administrators can download, analyze, and track the security audit log through the WebUI. The audit log provides a job owner's identification, event number, date, time, ID, description, and data to ensure credibility of the audit log. The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to users (based on network login). The audit logs are available to the TOE system administrators and can be exported for viewing and analysis. SSL must be configured in order for the system administrator to download the audit logs; the downloaded audit logs are in comma separated format so that they can be imported into an application such as Microsoft Excel™.

Security Management (TSF_FMT)

Only authorized system administrators can perform the following operations listed in Table 5:

Table 5: Operations for each user type

User Type	Operations
Local Administrator	· Change the local administrator PIN · Change or inquire the protocol and port
Web Administrator	· Change the web administrator's name and password. · Enable or disable system audit logs. · Download system audit report. · Change or inquire the protocol and port

Only authenticated system administrators can manage the following TSF data listed in Table 6:

Table 6: TSF data for each user type

User Type	TSF Data
Local Administrator	· Authentication data for local administrator · Information about protocol and port
Web Administrator	· Authentication data about web administrator. · Configuration data about system audit logs enabling or disabling. · System audit logs · Information about protocol and port

The TOE provides management functions about TSF data, security functions, and security configurations. Only authorized web or local administrators can access the management functions related to security.

Accessible functions for each user type are described in Table 5. Security functions for the web administrator are setting security audit functions, downloading audit logs, and managing the account for a web administrator. Security functions for the local administrator are managing PINs for the local administrator.

TSF data includes information on local/web administrator's authentication, information on security audit configuration for web administrators, security audit log, and information on network configuration.

Only authorized web administrators can download the TOE security audit record by using the web user interface through "Save as Text File". Once the web administrator has successfully logged on to the TOE, the security audit log can be downloaded.

System Authentication (TSF_SAU)

The system administrator must be authenticated by entering a PIN prior to being granted access to the system administration functions. The web administrator types the ID and password in the web user interface and the local administrator types the PIN in the local user interface. The TOE displays an asterisk for each digit entered to hide the value entered. Identification of the local administrator at the local user interface is implicit -- administrators will identify themselves by entering their PINs.

The authentication process will be delayed at the local user interface for 3 minutes if wrong PINs are entered 3 times in succession. If wrong PINs are entered 3 times at the web interface from one particular browser session, the TOE will send an error message to this browser session.

Information Flow (TSF_FLW)

TOE has the memory to store data. The memory is divided into fax memory that fax board can only access and network memory that network port in main controller can only access. Separation between the PSTN port on the FAX board and the network port on the main controller board is established through the architectural design of the main controller software. TOE controls and restricts information flow between fax board and network port in main controller. The direct communication between client PC and fax modem in internal network is impossible; the communication can only be passed through TOE. When using fax-to-email function, the fax image received via PSTN line will be transmitted to internal network. The fax image received via PSTN line is stored first in fax memory, and then the data goes through verification process. When the fax image is proper data standardized with MMR, MR, or MH of T.4 specification, TOE copies the data to network memory. Then the fax image can be transmitted into SMTP server through network card. Every data that is transmitted to the internal network is verified by the TOE, therefore it does not threat or modify TOE component of the internal network.

Network access control (TSF_NAC)

The TOE can control access to TOE resources through the network from outside TOE by changing the port number and enabling/disabling protocol. The administrator only allows access from the port configured by changing the protocol's port number in the interface used to configure the network protocol. The administrator can also control service access from

outside of TOE by enabling/disabling protocol. It can be configured by only a certificated administrator through authentication.

1.5 Conventions

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

Refinement

The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text.**

Selection

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

Assignment

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

Iteration

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

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 for an additional statement that cannot be covered by the four presentations previously mentioned. Application notes are denoted by underlined text.

1.6 Terms and definitions

The terms in this security target basically follows the same terms used in common criteria.

Assets

Entities that the owner of the TOE presumably places value upon.

Assignment

The specification of an identified parameter in a component (of the CC) or requirement.

Attack potential

A measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation.

Authorized user

A user who may, in accordance with the SFRs, perform an operation.

Class

A grouping of CC families that share a common focus.

Component

The smallest selectable set of elements on which requirements may be based.

Dependency

A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.

Element

An indivisible statement of security need.

Evaluation assurance level (EAL)

An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

External entity

Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Family

A grouping of components that share a similar goal but may differ in emphasis or rigor.

Identity

A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Iteration

The use of the same component to express two or more distinct requirements.

Object

A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operation (on a component of the CC)

Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

Operation (on an object)

A specific type of action performed by a subject on an object.

Organizational security policy (OSP)

A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.

Refinement

The addition of details to a component.

Role

A predefined set of rules establishing the allowed interactions between a user and the TOE.

Security function policy (SFP)

A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.

Security Target (ST)

An implementation-dependent statement of security needs for a specific identified TOE.

Selection

The specification of one or more items from a list in a component.

Subject

An active entity in the TOE that performs operations on objects.

Target of evaluation (TOE)

A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality (TSF)

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

Trusted IT product

An IT product other than the TOE which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly (e. g. by being separately evaluated).

TSF Data

Data created by and for the TOE, that might affect the operation of the TOE

User

See external entity

The following are specialized terms in this security target:

Network Scan Service

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

LUI, Local User Interface

Interface for general user or system administrator to access, use, or manage directly MFP.

Local (System) administrator

System administrator to manage Samsung MFP Security Kit Type_D V1.0 through LUI. The main roles are to configure system information and to check the MFP status for general use. The other role for security service is to changing PINs.

Fax-to-email

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

Multi-Function Printer, MFP

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

Human User

User who only refers to human being

Scan-to-server

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

Scan-to-email

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

System Administrator

An authorized user who manages TOE-embedded MFP. It includes local administrator, Web administrator, and telnet administrator.

WebUI, Web User Interface

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

Web (system) administrator

System administrator to manage Samsung MFP Security Kit Type_D V1.0 through WebUI. The main roles are to manage/change web administrator's ID and password, enable/disable security audit function, download security audit logs.

Electronic Image Data

Image data created through an MFP's scanner. Image data can be printed out (copy function) or be stored on the MFP's HDD.

FAX

Job for receiving or transmitting a fax image through the fax line

Fax image

Data received or transmitted through the fax line

CAC solution

CAC solution provides the authentication function through the card (Common Access Card) with a built-in smart chip.

Embedded FAX

Fax job that transmits scanned data in the MFP through the fax line and receives fax data directly from the fax line on the MFP, and then prints the data.

HIPAA (Health Insurance Portability and Accountability Act)

Policy that creates and reviews the records about performed job in system using hardware, software, and procedural mechanism to monitor potential violation of security rules.

PC FAX

Fax function that first sends fax data from client PC to MFP, and then transmits fax data through the 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 a TIFF type file. It is mainly used for fax transmission.

MR

Abbreviation of Modified Relative Element Address Designate MH coding, which includes Modified Relative Element Address Designate MH coding.

MMR

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

General user

The user to use the MFP system through the LUI and user's client PC. The main roles are to execute copy, fax, scan, and print jobs.

Network user

The user to access the MFP supported network system through network

1.7 Acronyms

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

Table 7: Acronyms

Acronyms	Definition
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
ISO	International Standards Organization
IT	Information Technology
LUI	Local user interface
MFP	Multi-function printer
OSP	Organization Security Policy
PP	Protection Profile
PPM	Pages Per Minute
PSTN	Public Switched Telephone Network

Acronyms	Definition
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	Target Security Functionality
UI	User Interface
Web UI	Web User Interface
MMR	Modified Modified READ coding
MR	Modified READ Coding
MH	Modified Huffman coding
CAC	Common Access Card

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 describes the declaration about the Common Criteria, Protection Profile, and package.

Chapter 3 defines the security problems of the TOE and operational environment in terms of threats, organizational security policies, and assumptions.

Chapter 4 describes about TOE security objectives for countering recognized threats, enforcing the organizational security policies, and upholding the assumptions. And it describes security objectives about operating environment.

Chapter 5 describes Security Functional Requirement and Security Assurance Requirement for satisfying security objectives.

Chapter 6 describes actually implemented functions defined in SFR.

2 Conformance Claims

Conformance Claims describe how this Security Target document complies with the Common Criteria, protection profile, and package.

2.1 Common Criteria Conformance

This ST claims conformance to the CC v3.1:

- **Common Criteria Identification**

Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1r1, 2006. 9,

CCMB-2006-09-001

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, version 3.1r2, 2007. 9,

CCMB-2007-09-002

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, version 3.1r2, 2007. 9,

CCMB-2007-09-003

- **Conformance status of Common Criteria**

CC Part 2 conformant

CC Part 3 conformant

2.2 Conformance of Protection Profile

No Protection Profile (PP) relevant to Security Target.

2.3 Conformance of Package

- The evaluation assurance level targeted by the ST is EAL3.
- EAL3 conformant

2.4 Conformance Claims Rationale

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

3 Definition of Security Problems

3.1 Threats

Threat agents are IT entities or users that can adversely access the internal asset or harm the internal asset in an abnormal way. The threat agents are assumed in this ST to have low-level of expertise, resources, and motivation. The threats that described in this chapter will be resolved by security objectives in chapter 4.

T.TOE_ACCESS_ON_NETWORK
The threat agents may attempt outflow, removal, or camouflaging/forgery of user data and TSF data stored on MFP through network access by using well-known protocol and ports.

T. AUDITS
The threat agents may access the security audit log through an unauthorized approach.

T.CERTIFICATION_TRIAL_IN_A_ROW
In order to approach the TOE, the threat agents attempt to authenticate continuously and gain access level of an authorized administrator.

T.UNAUTHORIZED_ACCESS_ON_TOE
The threat agents may attempt to access the management functions of the TOE in an unauthorized way or change the TOE setting value by an unauthorized way and set up new values.

T. INFAX
Threat agents may access the TOE or a component in the internal network via fax line to add malicious code.

3.2 Organizational Security Policies

This section describes the organizational security policies that the TOE or operational environment should follow.

P.HIPAA_OPT

In order to keep track of related security actions according to HIPAA policy, the TOE should precisely leave the job history on record and safely maintain their security-relevant events, and properly go over the recorded data.

P.SAFE_MANAGEMENT

The TOE should provide a safe management tool on the Web or local user interface so that only an authorized administrator can manage the TOE in a secure manner.

3.3 Assumption

The operational environment of the TOE should be managed according to the security assurance requirements about distribution, function, and guidance for user/system administrator. The following specification is an assumption of the environment where the TOE will be installed, which describes the physical, personnel, procedural, connective, and functional aspects.

A. PHYSICAL_SECURITY

The TOE is protected from unauthorized physical counterfeit/camouflage in the office environment.

A.TRUSTED_ADMINISTRATOR

The authorized system administrator of the TOE has no malice, has received education about the TOE administrative functions, and should perform proper actions according to the proposed manual provided with the TOE. The local administrator should change the PIN at least once every 40 days.

A.TRUSTED_NETWORK

The network connected to the TOE should install a firewall system between the internal and external network to block attacks from outside.

A.TIME_STAMP

The environment of the TOE provides reliable time-stamps for accurate audit logs about the TOE.

A.SSL

SSL protocol is used to serve safe communication between the user's client PC or web system administrator's PC and TOE through a web interface. Therefore, it provides confidentiality and integrity of data transferred between TOE and the web system administrator.

A. IDENTIFICATION_AND_AUTHENTICATION_ON_CAC

This security objective provides safe identification and authentication to prevent access of the MFP by unauthorized users.

4 Security Objectives

The security objectives are categorized into two parts: the objectives for the TOE and for the operational environment. The purpose of the former is to meet the goal to resolve the definition of security problems/threats. The latter is to meet the goal to support technical/procedural ways that provide the functionality of security.

4.1 Security Objectives for the TOE

This section identifies and describes the security objectives of the TOE.

O. AUDITS

In order to trace an action of relevance to security, the TOE should provide the audit logs to only the authorized system administrator. The audit log should be protected from unauthorized change, elimination, and failure of recording in accordance with HIPAA policy.

O. MANAGE

The TOE should provide efficient and effective management service to an authorized system administrator.

O.NETWORK_ACCESS_CONTROL

The TOE should not allow access on unauthorized network protocol services and ports to prevent outflow, removal or camouflaging/forgery of user data and TSF data stored on the MFP through network access by using protocol service and port numbers that are allowed explicitly.

O.IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR

The TOE should provide identification and authentication processes for system administrators to prevent access to the TOE by unauthorized users. This only allows the access of security management functions to authorized administrators.

O. HANDLING_AUTHENTICATION_FAILURE

To block attacks, the TOE must take a proper action once 3 invalid login attempts have been detected.

O.FAXLINE

The TOE should not allow the access of non-standard fax data from the fax modem.

4.2 Security Objectives for the Environment

The security objectives for the operating environment are to support technical and procedural ways for the TOE to provide SFR (security functional requirements).

OE.PHYSICAL_SECURITY

The TOE will be located in an office environment where it will be monitored by the office personnel for unauthorized physical connections, manipulation or interference.

OE.TRUSTED_ADMIN

The system administrator of the TOE is assumed not to disclose their authentication credentials. The system administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. The local administrator manages a 4~8 digit PIN for security and changes the PIN at least once every 40 days.

OE.TRUSTED_NETWORK

The TOE environment must protect user data from disclosure, or modification, by establishing a firewall system between external and internal network systems.

OE.TIME_STAMP

The operational environment must provide a reliable time stamp to mark entries in the security log.

OE. SSL

In case that web system administrator's PC communicates with TOE by using a web interface, data should be transferred by SSL protocol to guarantee confidentiality and integrity.

OE. IDENTIFICATION_AND_AUTHENTICATION_ON_CAC

The TOE should provide identification and authentication through CAC to prevent access of the MFP's services (Print/Copy/Network Scan/Fax) by unauthorized users.

4.3 Security Objectives Rationale

This section demonstrates that all security objectives for the TOE are traced back to aspects of the assumptions to be met, identified threats to be countered or organizational security policies.

Table 8: Security Objectives and Definition of Security Problems

Security Objectives	Security Objectives for the TOE						Security Objectives for the Environment					
Definition of Security Problems	O. MANAGE	O.AUDITS	O. IDENTIFICATION_AND_AUTHENTICATION_ON _ADMINISTRATOR	O. HANDLING_AUTHENTICATION_FAILURE	O. NETWORK_ACCESS_CONTROL	O. FAXLINE	OE. PHYSICAL_SECURITY	OE. TRUSTED_ADMIN	OE. TRUSTED_NETWORK	OE. TIME_STAMP	OE. SSL	OE. IDENTIFICATION_AND_AUTHENTICATION_ON _CAC
T.AUDITS		X										
T.CERTIFICATION_TRIAL_IN_A_ROW				X								
T. INFAX						X						
T.UNAUTHORIZED_ACCESS_ON_TOE	X		X									
T.TOE_ACCESS_ON_NETWORK					X							
P.HIPAA_OPT		X										
P.SAFE_MANAGEMENT	X											
A.PHYSICAL_SECURITY							X					
A.TRUSTED_ADMIN	X							X				
A.TRUSTED_NETWORK									X			
A.TIMESTAMP										X		

A.SSL											X	
A.IDENTIFICATION_AND _AUTHENTICATION_ON_CAC												X

4.3.1Rationale for the TOE Security Objectives

O.AUDITS
This security objective correctly and safely records and maintains every event related with security to trace responsibility on security-related actions, and also reviews only by system administrators. Therefore, O.AUDITS corresponds with threat T.AUDITS and satisfies the organization security policy P.HIPAA_OPT.

O. MANAGE
This security objective provides the resources to install, configure, and operate the TOE only to the system administrators. This security objective satisfies the T.UNAUTHORIZED_ACCESS_ON_TOE, and support A.TRUSTED_ADMINISTRATOR because the TOE is managed only by the system administrator in a safe management environment.

O.NETWORK_ACCESS_CONTROL
This security objective prevents the access of MFP from unauthorized network protocol service and port. Therefore, the TOE satisfies the T.TOE_ACCESS_ON_NETWORK.

O.IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR
The security objective provides identification and authentication processes for system administrators that access the security management function in TOE and only allows the access of the security management function to authorized administrator. Therefore, the TOE satisfies the T.UNAUTHORIZED_ACCESS_ON_TOE.

O.HANDLING_AUTHENTICATION_FAILURE
This component defends against an attack by taking proper measures if 3 wrong PIN numbers were entered in succession. Therefore, this security objective supports the threat: T.CERTIFICATION_TRIAL_IN_A_ROW.

O. FAXLINE
The security objective prevents the access of nonstandard fax data from fax modem. Therefore, the TOE satisfies the T.INFAX.

4.3.2 Rationale for Security Requirements for the Environment

OE.PHYSICAL_SECURITY

The IT environment provides the TOE with appropriate physical security that is placed in a manned office environment secured from unauthorized physical access, falsification, or interference. Therefore, it supports assumption of A.PHYSICAL_SECURITY.

OE.TRUSTED_ADMINISTRATOR

The system administrator of the TOE will not disclose their authentication credentials. The administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. Therefore, it supports assumption of A.TRUSTED_ADMINISTRATOR.

OE.TRUSTED_NETWORK

The objective about this operating environment ensures that attack network resources from outside is blocked by installing monitoring system between internal and external network. Therefore, it supports assumption of A.TRUSTED_NETWORK.

OE.TIME_STAMP

The TOE provides a reliable time stamp for recording correct security audit log entries. Therefore, it supports assumption of A. TIME_STAMP.

OE.SSL

When downloading security audit log, the TOE provides SSL protocol for secured data communication. Therefore, it supports assumption of A.SSL.

OE. IDENTIFICATION_AND_AUTHENTICATION_ON_CAC

The TOE provides identification and authentication through CAC to prevent access of the MFP's services by unauthorized users.

Therefore, it supports assumption of A.IDENTIFICATION_AND_AUTHENTICATION_ON_CAC.

5 Security Requirements

5.1 Security Functional Requirement (SFR)

Table 9: Security Functional Requirement

Class	Security Functional components	
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
User Data Protection	FDP_IFC.2(1)	Complete information flow control (1)
	FDP_IFF.1(1)	Simple security attributes(1)
	FDP_IFC.2(2)	Complete information flow control(2)
	FDP_IFF.1(2)	Simple security attributes (2)
Identification and Authentication	FIA_AFL.1(1)	Authentication failure handling (1).
	FIA_AFL.1(2)	Authentication failure handling (2).
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles

5.1.1Class FAU: Security Audit

5.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) [The events specified in Table 10 below].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [No audit action].

Table 10: Audit Event

SFR	Audit Event
FDP_IFF.1(1)	Decision to admit requested information flow.
FMT_MOF.1	Configuration change of security audit function
FMT_MTD.1	Query/change of security audit function.

5.1.1.2 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 [Web administrator] with the capability to read [all 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.

5.1.1.3 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.

5.1.2Class FDP: User data protection

5.1.2.1 FDP_IFC.2(1) Complete information flow control (1)

Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1	The TSF shall enforce the [fax flow control policy] on [• Subject List - Fax image user • Information List - Fax image] and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

5.1.2.2 FDP_IFF.1(1) Simple security attributes (1)

Hierarchical to:	No other components
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
FDP_IFF.1.1	The TSF shall enforce the [fax flow control policy] based on the following types of subject and information security attributes: [• The Subject List – Fax user • Information List

- Fax image

- Security Properties
  - Subject List: No security properties
  - Information List: Standard fax image specifications]

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

- When security properties of information received from a fax line is Standard fax image specification (MMR, MR, or MH of T.4 specification), information flow is permitted from fax memory to network memory.
- When security properties of information that is sent to the internal network is standardized MMR, MR, or MH of T.4 specification, information flow is permitted from network memory to fax memory.]

FDP_IFF.1.3 The TSF shall enforce [none].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [no additional information flow rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [no denial of information flow rules].

5.1.2.3 FDP_IFC.2(2) Complete information flow control (2)

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [Network access control policy] on

[

- Subject List

- Network user

- Information List

- All information in the MFP to flow to and from

any subject

]

and all operations that cause that information to flow to and from subjects covered by the SFP.

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

5.1.2.4 FDP_IFF.1(2) Simple security attributes (2)

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [network access control policy] based on the following types of subject and information security attributes: [

- The Subject List
  - Network user
- Information List
  - All information in the MFP to flow to and from any subject
- Security Properties
  - Subject List: No security properties
  - Information List: protocol or port information]

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

- When security properties of information are included in the protocol list that the authorized administrator set, information flow from outside to the MFP is permitted.
- When security properties of information are the same port information that the authorized administrator set, information flow from outside to the MFP is permitted.

]

FDP_IFF.1.3 The TSF shall enforce [none].

FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: [no additional information flow rules].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [no denial of information flow rules].

5.1.3Class FIA: Identification and authentication

5.1.3.1 FIA_AFL.1 (1) Authentication failure handling (1)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when *[3]* unsuccessful authentication attempts occur related to [authentication of the local administrator].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been *met,* the TSF shall [lockout the local administrator's login for a period of 3 minutes on the local user interface].

5.1.3.2 FIA_AFL.1 (2) Authentication failure handling (2)

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when *[3]* unsuccessful authentication attempt occurs related to [authentication at the web administrator interface from one particular Browser session].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [send an error message to this Browser session].

5.1.3.3 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each **System administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **System administrator**.

Application note: System administrator includes local administrator and web administrator.

5.1.3.4 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

5.1.3.5 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each **System administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that **System Administrator**.

Application note: Local administrator performs with authentication by PIN, without any identification function.

5.1.4Class FMT: Security Management

5.1.4.1 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, enable, modify the behavior of* the functions [on the table 11] to [the authorized identified roles on the table 11].

Table 11: Security Functions and Its Role

Security Function	Action	Role
security audit function	Disable, Enable	Web administrator

Download security audit log	Determine the behavior of	Web administrator
Protocol management function	Disable, Enable	Web Administrator

5.1.4.2 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 *delete, modify, query, [download]* the [user's role corresponding with TSF data listed on the Table 12 below and operation].

Table 12: Operation and Role of each TSF Data List

TSF Data	Operation	Role
Authentication information of web administrator	Modify	Web administrator
Configurations on the security audit enabling/disabling.	Query, Modify	Web administrator
Record security audit log.	Download	Web administrator
Management information of Protocol	Query, Modify	administrator
Configurations on the port number	Query, Modify	administrator
Authentication information for local administrator.	Modify	Local administrator

5.1.4.3 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 specification of management functions on Table 13 below]

Table 13: Management Functions of TOE

Specification of security functions	Management functions of TOE
FAU_SAR.1	Maintain the user group who can read the security audit records. (add, modify, delete)
FIA_UAU.2	a) Manage authentication data by system administrator. b) Manage authentication data related with secured data.
FIA_UID.2	Manage the user's identification.
FDP_IFF.1(2)	Manage rules for information flow of control
FAU_GEN.1	Manage security audit function
FAU_SAR.1	Manage security audit data

5.1.4.4 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 [system administrator].

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

5.2 Security Assurance Requirements (SAR)

Security assurance requirements (SAR) defined in this document consists of assurance component in Common Evaluation Standard part 3. The Evaluation Assurance Levels (EALs) is EAL3. Table 14 shows the summary of assurance components.

Table 14: EAL3 Security Assurance Requirements

Assurance Class	Assurance components	
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extendable components definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements

Assurance Class	Assurance components	
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorization controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	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

5.2.1Class ASE: Security Target evaluation

5.2.1.1 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.

5.2.1.2 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 nonconformance 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.

5.2.1.3 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.

5.2.1.4 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 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.

5.2.1.5 ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Objectives

ASE_ECD.1 Extended components definition

Content and presentation elements:

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

ASE_REQ.2.2D The developer shall provide 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 of the requirements for content and presentation of evidence.

5.2.1.6 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.

5.2.1.7 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.

5.2.2Class ADV: Development

5.2.2.1 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.

5.2.2.2 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 security enforcing effects 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.

5.2.2.3 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 behavior described in the TOE design is mapped to the TSFIs that invoke it.

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.

5.2.3Class AGD: Operational user guidance

5.2.3.1 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.

5.2.3.2 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.

5.2.4Class ALC: Life-cycle support

5.2.4.1 ALC_CMC.3 Authorization controls

Dependencies: ALC_CMS.1 TOE CM (Content Management) 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.

5.2.4.2 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.

5.2.4.3 ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document 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..

5.2.4.4 ALC_DVS.1 Identification of security measures

Dependencies: No dependencies.

Developer action elements:

ALC_DVS.1.1D The developer shall produce 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.

5.2.4.5 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.

5.2.5Class ATE: Tests

5.2.5.1 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.

5.2.5.2 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.

5.2.5.3 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 output 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.

5.2.5.4 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.

5.2.6Class AVA: Vulnerability analysis

5.2.6.1 AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.1 Basic 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.

5.3 Security Requirements Rationale

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

All TOE security requirements can be traced back to one or more TOE security objectives, and all TOE security objectives are supported by at least one security requirement.

5.3.1Rationale for the TOE Security Requirements

This section demonstrates that the security objectives of the TOE are satisfied by the security requirements. Table 15 provides rationale that the security requirements are corresponding with security objectives.

Table 15: TOE SFR Mapping to the TOE Security Objectives

	TOE Security Objectives					
	O. MANAGE	O. AUDITS	O.IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR	O.HANDLING_AUTHENTICATION_FAILURE	O.NETWORK_ACCESS_CONTROL	O. FAXLINE
FAU_GEN.1		X				
FAU_SAR.1		X				
FAU_SAR.2		X				
FDP_IFC.2(1)						X
FDP_IFF.1(1)						X
FDP_IFC.2(2)					X	
FDP_IFF.1(2)					X	
FIA_AFL.1(1)				X		
FIA_AFL.1(2)				X		
FIA_UAU.2			X			
FIA_UAU.7			X			
FIA_UID.2			X			
FMT_MOF.1	X					
FMT_MTD.1	X					
FMT_SMF.1	X					
FMT_SMR.1	X					

FAU_GEN.1 (Audit Data Generation)
This component is provided to define the object of security audit related with authorized users or jobs, and also to ensure the ability of generation audit records. It satisfies security object O.AUDITS.

FAU_SAR.1 (Audit Review)
This component is required to ensure the ability to review the security audit log. Therefore, it satisfies security object O.AUDITS.

FAU_SAR.2 (Restricted audit Review)
It is ensured that only authorized web administrators can access to and read the security audit log of this component. Therefore, it satisfies security object O.AUDITS.

FDP_IFC.2(1) (Complete information flow control)
This component is required to ensure the ability to enforce the fax flow control policy on Fax image user, Fax image and all operations. Therefore, it satisfies security object O.FAXLINE.

FDP_IFF.1(1) (Simple security attributes)
This component is required to ensure the ability to define roles for fax flow control policy and enforce the fax flow control policy based on roles defined. Therefore, it satisfies security object O.FAXLINE.

FDP_IFC.2(2) (Complete information flow control)
This component is required to ensure the ability to enforce the network access control policy on network users and all operations that cause that information to flow from network user to MFP. Therefore, it satisfies security object O.NETWORK_ACCESS_CONTROL.

FDP_IFF.1(2) (Simple security attributes)
This component is required to ensure the ability to define roles for fax flow control policy and enforce the fax flow control policy based on roles defined. Therefore, it satisfies security object O.NETWORK_ACCESS_CONTROL.

FIA_AFL.1 (1) (Authentication failure handling)
This component ensures defense against attacks from a wrong trial of authentication. The authentication process will be delayed at the local user interface for 3 minutes if wrong PINs are entered 3 times in succession. Therefore, it satisfies security object O.HANDLING_AUTHENTICATION_FAILURE.

FIA_AFL.1 (2) (Authentication failure handling)

This component is required to ensure the ability to detect when an unsuccessful authentication attempt occurs and send an error message to this browser session when the three unsuccessful authentication attempts criteria has been met. Therefore, it satisfies security object O.HANDLING_AUTHENTICATION_FAILURE.

FIA_UAU.2 (User Authentication Before Any Action)
This component ensures that the system administrator must get authentication before accessing the TOE functionality. Therefore, it satisfies security object O.IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR.

FIA_UAU.7 (Protected Authentication Feedback)
This component ensures that fake characters (e.g. asterisk [*]) are displayed for each digit entered to hide the value entered. Therefore, it satisfies security object O. IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR

FIA_UID.2 (User identification before any action)
This component ensures the identification of system administrators before granting access to the TOE. Therefore, it satisfies security object O. IDENTIFICATION_AND_ AUTHENTICATION_ON_ADMINISTRATOR.

FMT_MOF.1 (Management of Security Functions Behavior)
This component ensures that only authorized system administrators can limitedly access the TSF management function. Therefore, it satisfies security object O. MANAGE.

FMT_MTD.1 (Management of TSF data)
This component defines that only authorized system administrators can change, query, delete, or download the TSF data. Therefore, it satisfies security object O. MANAGE.

FMT_SMF.1 (Specification of Management Functions)
This component ensures that the security management function in the TOE is available. Therefore, it satisfies security object O. MANAGE.

FMT_SMR.1 (Security roles)
This component ensures that the TOE plays a reliable system administrator’s role to manage the TOE and TSF. Therefore, it satisfies security object O. MANAGE.

5.3.2Rationale for the TOE Assurance Requirements

This Samsung MFP Security Kit Type_D V1.0 satisfies the assurance requirements of EAL3

EAL3 is an assurance package that requires well-organized test and inspection.

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.

To understand security actions, EAL3 provides assurance using the specifications of function or interface, guidance, and structural explanation of the TOE structure by analyzing SFR included in a complete ST. This analysis is supported by independent testing of TSF, the proof of developer's test based on the functional specification or the TOE design, independent confirmation of test result samples by the developer, vulnerability analyses to ensure the tolerance to the attack based on the functionality specification, the TOE design, security structure, or guidance. EAL3 also provides assurance by controlling the development environment, managing the TOE version control, and proofing a safe releasing process.

5.3.3Rationale for Dependencies

5.3.3.1 SFR Dependencies

FIA_UAU.2 and FMT_SMR.1 have a subordinate relationship with FIA_UID.1, but they are satisfied by FIA_UID.2 that is a hierarchical relationship with FIA_UID.1.

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

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

FDP_IFF.1(1) and FDP_IFF.1(2) have a subordinate relationship with FDP_IFC.1, but they are satisfied by FDP_IFC.2(1), FDP_IFC.2(2) that is a hierarchical relationship with FDP_IFC.1.

FDP_IFF.1(1) has a subordinate relationship with FMT_MSA.3, but because the security properties of FDP_IFF.1(2)'s subject (None) and the security properties of information (fax image standard) are not objects for management, FMT_MSA.3 is not required.

FDP_IFF.1(2) has a subordinate relationship with FMT_MSA.3, but because the security properties of FDP_IFF.1(1)'s subject (None) and the security properties of information (protocol and port) are not objects for management, FMT_MSA.3 is not required.

Table 16: Dependencies on the TOE Security Functional Components

Number	Functional Component ID	Dependencies	Reference Number
1	FAU_GEN.1	FPT_STM.1	*
2	FAU_SAR.1	FAU_GEN.1	1
3	FAU_SAR.2	FAU_SAR.1	2
4	FDP_IFC.2(1)	FDP_IFF.1(1)	5
5	FDP_IFF.1(1)	FDP_IFC.1, FMT_MSA.3	4, # (Hierarchically by FDP_IFC.2(1))
6	FDP_IFC.2(2)	FDP_IFF.1(2)	7
7	FDP_IFF.1(2)	FDP_IFC.1, FMT_MSA.3	6, # (Hierarchically by FDP_IFC.2(2))
8	FIA_AFL.1(1)	FIA_UAU.1	10 (Hierarchically by FIA_UAU.2)
9	FIA_AFL.1(2)	FIA_UAU.1	10 (Hierarchically by FIA_UAU.2)
10	FIA_UAU.2	FIA_UID.1	12 (Hierarchically by FIA_UID.2)
11	FIA_UAU.7	FIA_UAU.1	10 (Hierarchically by FIA_UAU.2)
12	FIA_UID.2	-	-
13	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	15, 16
14	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	15, 16
15	FMT_SMF.1	-	-

Number	Functional Component ID	Dependencies	Reference Number
16	FMT_SMR.1	FIA_UID.1	12 (Hierarchically by FIA_UID.2)

5.3.3.2 SAR Dependencies

SAR dependencies provided in the Common Evaluation Standard for Information Security System have been already met.

6 TOE SUMMARY SPECIFICATION

This section presents an overview of the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

6.1 TOE Security Functions

This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.2.

- Security Audit (TSF_FAU)
- Security Management (TSF_FMT)
- System Authentication (TSF_SAU)
- Information Flow (TSF_FLW)
- Network Access Control (TSF_NAC)

6.1.1Security Audit (TSF_FAU)

The TOE tracks events/actions (e.g., print/scan/fax job submission) to login users. The audit logs are created for each event in fixed size. Each audit log provides the user's identification, event number, date, time, ID, description, and data. The audit logs are available to web administrators and can be exported for review and analysis by using the web user interface.

Table 17: Security Event

Audit log consists of the following fixed-size input data. Input Number (An integer number from 1 to the number of log data) Event Date (mm/dd/yyyy) Event Time (hh:mm:ss) – Event ID (Specific number – Refer to the following table)		
Event ID	**Event Explanation**	**Input Data**
1	System startup	Device name, Serial number of the device
2	System shutdown	Device name, Serial number of the device
5	Print Job	Job name, User name, Completion status, Automatic Image Overwrite job status, SyncThru user's account
6	Network scan job	Job name, User name, Completion status, Automatic Image Overwrite job status, SyncThru

		user's account, total number of the destination address, Destination address
9	Scan-to-email job	Job name, User name, Completion status, Automatic Image Overwrite job status, SyncThru user's account, Total number of SMTP receiver , SMTP receiver
10	Audit Log Disabled	Device name, Serial number of the device
11	Audit Log Enabled	Device name, Serial number of the device
12	Copy job	Job name, User name, Completion status, Automatic Image Overwrite job status, SyncThru user's account
13	Embedded fax job	Job Type (Sending fax, Receiving fax), Job name, User name, Completion status, Automatic Image Overwrite job status, SyncThru user's account, Total number of the fax number to receive , Fax number to receive, Destination address
14	PC-Fax job	Job name, User name, Completion status, Automatic Image Overwrite job status, SyncThru user's account, Total number of the fax number to receive , Fax number to receive, Destination address

The audit log traces decisions that allow requested data flow, changes in security audit function and inquiry/change of security audit configuration. Because the audit records are only available to the authorized web administrators, unauthorized users cannot change or delete them. Audit records can be downloaded by using the Web interface for review and analysis. When storage is full of log data, the latest records overwrite the oldest audit records.

Relevant SFR : FAU_GEN.1, FAU_SAR.1, FAU_SAR.2

6.1.2Security Management (TSF_FMT)

The TOE accomplishes security management for security function, TSF data, and security attribute. Only authorized web/local administrators can manage the security functions.

The available security functions for each user's role are displayed in Table 18. Web administrators can manage the following functions: enable or disable security audit function, download security audit log, change the account of a web administrator, etc. Local administrators can manage the following function: change PIN of local administrator.

TSF data that is stated in Table 19: Authentication information of local administrator, authentication information of web administrator, enable or disable security audit setting value for web administrator.

Only authorized web administrators can download the TOE security audit record by using the web user interface through "Save as Text File". Once the web administrator has successfully logged on to the TOE, the security audit log can be downloaded.

Table 18: The TOE Security Function, Relation action and Role

Security Function	Action	Role
Enable security audit function	Disable, Enable	Web administrator
Download security audit log	Determine the behavior of	Web administrator
Protocol management	Disable, Enable	Web administrator

Table 19: Operation and Role of each TSF Data List

TSF 데이터	오퍼레이션	역할
Authentication information of web administrator	Modify	Web administrator
Configurations on the security audit enabling/disabling.	Query, Modify	Web administrator
Record security audit log.	Download	Web administrator
Protocol management	Query, Modify	Administrator
Configurations on the port number	Query, Modify	Administrator
Authentication information for local administrator.	Modify	Local administrator

Relevant SFR: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.1.3System Authentication (TSF_SAU)

The local administrator must be authenticated by entering a PIN prior to being granted access to the TOE management functions. The TOE displays an asterisk (*) for each digit entered to hide the value entered. The local administrator can type the PIN in a local user interface without any other identification. The PIN number can be managed only by the local administrator. The web administrator must type an ID and password in the web user interface. Therefore, each web administrator can be identified with each other. The TOE displays an asterisk (*) for each digit entered, and just provides ambiguous feedback with success or fail information. This prevents users from acquiring any information during the trial. The authentication process will be delayed for 3 minutes if wrong passwords are entered 3 times in succession in a local user interface. if wrong passwords were entered 3 times in succession in the web user interface, the web browser displays an error message.

Relevant SFR: FIA_AFL.1(1), FIA_AFL.1(2), FIA_UAU.2, FIA_UAU.7, FIA_UID.2

6.1.4Information Flow (TSF_FLW)

In the TOE, the memory areas for the fax board and for the network port on the main controller board are separated. If the received fax data includes malicious virus content, it may threaten the TOE asset such as the TOE itself or internal network components. To prevent this kind of threat, the TOE, before “fax forward to email” or “fax forward to server(SMB/FTP)”, inspects whether the received fax image is standardized with MMR, MR, or MH of T.4 specification or not. 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 to SMTP server through the internal network. When malignant codes are discovered, the TOE destroys the fax image. Fax security functions follow the fax flow control policy.

The fax flow control policy 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 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.

- Fax modem controller in the TOE is physically separated with MFP controller, and fax function is logically separated with MFP functions.
- Fax interface only answers to the predefined fax protocol, and never answers to any other protocol.

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 malicious code or vicious executable files.

Relevant SFR: FDP_IFC.2(1), FDP_IFF.1(1)

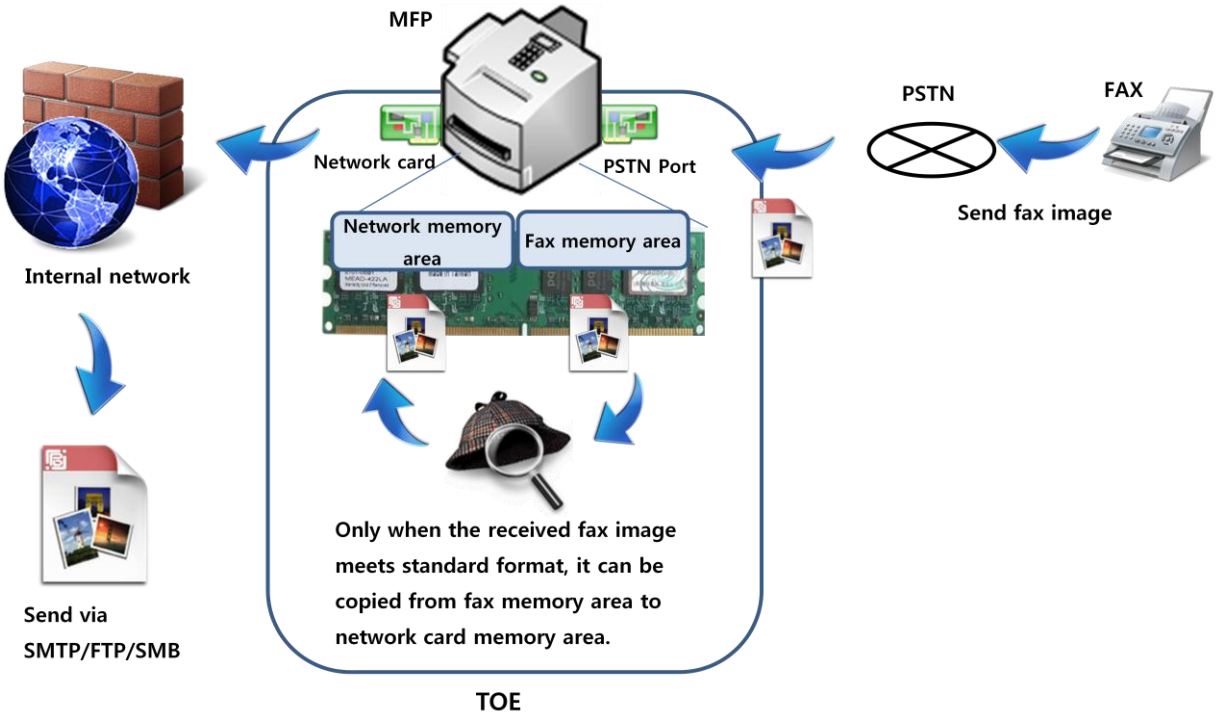

Figure 4: Information Flow Summary

6.1.5Network Access Control (TSF_NAC)

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

There are a couple of methods to access and communicate with the MFP from outside of the TOE through the network; a standard communication protocol and a port that performs as a logical network channel. These services start up simultaneously as a system's network card boots, and the port number is defined as a logical channel in the range of 1 to 65535. Among these services, the service that uses upper protocol utilizes a predefined "well-known port".

The TOE only allows access from authorized ports and connection using authorized protocol services by configuring port number, and enabling/disabling network services accessing to MFP system. Only the web system administrator authorized through login can configure these functions, and these configurations are altered on each reboot of the network card, and, thus, the MFP system information and electronic image data are protected from unauthorized reading and falsification.

Relevant SFR: FDP_IFC.2(2), FDP_IFF.1(2), FMT_SMF.1, FMT_SMR.1

Table 20: Component Relationship between the TOE Security Function and SFR Security Function

	TOE Security Function				
	Security Audit	Security Management	System Authentication	Network Access Control	Information flow
FAU_GEN.1	X				X
FAU_SAR.1	X				
FAU_SAR.2	X				
FDP_IFC.2(1)					X
FDP_IFF.1(1)					X
FDP_IFC.2(2)				X	
FDP_IFF.1(2)				X	
FIA_AFL.1(1)			X		
FIA_AFL.1(2)			X		
FIA_UAU.2			X		
FIA_UAU.7			X		
FIA_UID.2			X		
FMT_MOF.1		X			

	TOE Security Function				
	Security Audit	Security Management	System Authentication	Network Access Control	Information flow
FMT_MTD.1		X			
FMT_SMF.1		X			
FMT_SMR.1		X			