

Samsung MFP Security Kit Type_A v1.0

Security Target

v 1.7

@

This is proprietary information of Samsung Electronics. No part of the information contained in this document may be reproduced without the prior consent of Samsung Electronics

Document History

VERSION	DATE	DESCRIPTION OF CHANGE	SECTIONS AFFECTED	REVISED BY
0.95	2008-02-25	<ul style="list-style-type: none"> - Add security audit feature. - Change Sanitize document image to image overwrite. - Change term from IOT Printer. - Define terms: Divide system administrator into web administrator and local administrator - Define terms: Divide scan function into scan-to-email, Netscan, and scan-to-server - Define terms: Divide fax function into PC fax and local fax - Add description about system architecture and structural elements - Add hardware list which TOE can be embedded. - Change term from LanFax to PC fax. - Define stored file type in hard disk drive (HDD): <ul style="list-style-type: none"> . Stored file calls every file stored in HDD. . Image file calls temporary stored files. . Preserved file calls stored files that users saved for the later use. 	All	SEC
0.96	2008-02-28	<ul style="list-style-type: none"> - Change TOE physical scope. - Change picture and description of TOE operational environment. - Add description about SSL transmitting protocol. - Add description about stored data encoding. - Change descriptions about Definition of Security Problems, Security Objectives, Security Functional Requirement, and Rationale for items. 	All	SEC
0.97	2008-03-19	<ul style="list-style-type: none"> - Change descriptions about network authentication identification 	All	SEC
0.98	2008-04-01	<ul style="list-style-type: none"> - Change Figure 5. - Change terms from network authentication and identification and to network service authentication and identification. - Change terms about SSL-enable function with "Download system audit report" and "scan-to-email" 	All	SEC
0.99	2008-04-04	<ul style="list-style-type: none"> - Change terms about SSL-enable function with "Download system audit report" - Change description about security management feature. - Define IIO for immediate image overwrite and ODIO for on-demand image overwrite. 	All	SEC
1.0	2008-04-28	<ul style="list-style-type: none"> - Delete data encoding security function. - Add revision history - Release security target documentation version 1.0 for SCX-6345N, SCX-6345NG/ SCX-6555N, SCX-6555NG/ CLX-8380ND, CLX-8380NDG. 	All	SEC
1.1	2008-05-15	<ul style="list-style-type: none"> - Add and correct fax terms such as Local fax, embedded fax, and PC-fax. - Change table 6 for security audit log item 	All	SEC

1.2	2008-05-18	- Change documentation form.	All	SEC
1.3	2008-06-06	- Change table and picture.	Picture 5	SEC
1.35	2008-06-09	- Add table 3 about retaining software version. - Change hardware specification for hard disk drive and memory)	Table 2, Table 3	SEC
1.4	2008-06-21	- Change common evaluation standard to identification. - Unify terms TOE type as software module. - Add explanation about non-TOE security function for network service authentication and identification. - Rearrange each component in terms of TOE physical scope. - Add and delete some components, and arrange components in Figure 2 and 3. - Change descriptions about threats. - Change descriptions about assumption. - Change FDP_IFF in SFR.	All	SEC
1.5	2008-07-21	- Add description about TOE operational environment in TOE Overview and change Figure 1. - Add description on non-TOE. - Add description about asset. - Add description about user's role. - Add TOE description. . Physical scope: Change component to software module. . Logical scope: Change security function - Add terminologies: local user interface, web user interface, Multifunction Peripheral, IIO, ODIO, PSTN port, DoD 5200.28-M, HIPAA, security print, stored print - Threats . Add: T.DATA_ACCESS, T.CERTIFICATION_TRIAL_FAILED . Delete: T.INFAX, T.STORED_DATA_DAMAGED . Change: from T.USER to T.CAMOUFLAGE - Assumptions . Add: A.SSL, A.TIME_STAMP . Change: A.INSTALL, A.MANAGE - Security object . Add: O. HANDLING_AUTHENTICATION_FAILURE OE.SSL, OE.TIME_STAMP . Delete: O.PROTECT_TRANSMITTED_DATA . Change: OE.INSTALL, OE.MANAGE - SFR . Delete: FCS class, FDP_IFC.1(3), FDP_IFF.1(3), FDP_UCT.1, FDP_UIT.1, FMT_MSA.2, FPT_STM.1, FTP_ITC.1, FDP_IFC.1(2), FDP_IFF.1(2) . Change: Table 10 Audit Event FDP_ACC.1, FDP_ACF.1 FDP_IFC.1, FDP_IFF.1 FMT_MOF.1, FMT_MSA.1(1)(security print), FMT_MSA.1(2) (data flow), FMT_MSA.3(1)(security print), FMT_MSA.3(2)(data flow), FMT_MTD.1,	All	SEC

		<p>FMT_SMF.1 Add table for security management</p> <ul style="list-style-type: none"> - TOE SUMMARY SPECIFICATION <ul style="list-style-type: none"> . Change related SFR to correspond with each security function. . Change description about SFR 		
1.6	2008-08-25	<ul style="list-style-type: none"> - Add "control data access" in security function. - Make table about non-TOE items. - Change figure about TOE logical scope - Change TOE physical scope - Change threats <ul style="list-style-type: none"> . Change descriptions about T.DATA_ACCESS, T.RECOVER, T.INFAX . Change T. CAMOUFLAGE to T. UNAUTHORIZED_ACCESS_ON_TOE . Add T. UNAUTHORIZED_ACCESS_ON_NETWORK_SCAN_SERVICE, T.AUDITS . Delete T.OUTFLOW_VIA_FAX - Change Assumption <ul style="list-style-type: none"> . Change description on A. NETWORK. . Add A.SERVER. . A.MANAGE, A.INSTALL . Change A.ACCESS to A.PHYSICAL_SECURITY - Change security object according to the changed Definition of Security Problems. - Delete SFR. <ul style="list-style-type: none"> . FMT_MSA.1(2), FMT_MSA.3(2) - Add SFT <ul style="list-style-type: none"> . FIA_UAU.2(1), FIA_UAU.2(2), FIA_UID.2(1), FIA_UID.2(2) - Change subject list, object, operation list, security properties of SFR <ul style="list-style-type: none"> . FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1 - Change table about SFR. 	All	SEC
1.61	2008-09-25	<ul style="list-style-type: none"> - Change figure/table about physical scope. 	All	SEC
1.7	2008-10-9	<ul style="list-style-type: none"> - Add terminology definition. <ul style="list-style-type: none"> . Fax image, Network scan service - Add security objectivity <ul style="list-style-type: none"> . O.MANAGE - Delete SFR <ul style="list-style-type: none"> . FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3 - Add SFR <ul style="list-style-type: none"> . FPT_RCV.4 	All	SEC

CONTENTS

1	Introduction	9
1.1	SECURITY TARGET REFERENCES	9
1.2	TOE REFERENCES	9
1.3	TOE OVERVIEW	9
1.4	TOE DESCRIPTION	18
1.4.1	<i>Physical Scope</i>	18
1.4.2	<i>Logical Scope</i>	20
1.5	CONVENTIONS	26
1.6	TERMS AND DEFINITIONS	27
1.7	ACRONYMS	35
1.8	ORGANIZATION	36
2	Conformance Claims	37
2.1	COMMON CRITERIA CONFORMANCE	37
2.2	CONFORMANCE OF PROTECTION PROFILE	37
2.3	CONFORMANCE OF PACKAGE	37
2.4	CONFORMANCE OF CLAIMS RATIONALE	37
3	Definition of Security Problems	38
3.1	THREATS	38
3.2	THE SECURITY POLICY OF ORGANIZATION	39
3.3	ASSUMPTION	39
4	Security Objectives	41
4.1	SECURITY OBJECTIVES FOR THE TOE	41
4.2	SECURITY OBJECTIVES FOR THE ENVIRONMENT	42
4.3	SECURITY OBJECTIVES RATIONALE	43
4.3.1	<i>Rationale for the TOE Security Objectives</i>	45
4.3.2	<i>Rationale for Security Requirements for the Environment</i>	46
5	Security Requirements	48
5.1	SECURITY FUNCTIONAL REQUIREMENT (SFR)	48
5.1.1	<i>Class FAU: Security Audit</i>	48
5.1.2	<i>Class FDP: User Data Protection</i>	50
5.1.3	<i>Class FIA: Identification and authentication</i>	53
5.1.4	<i>Class FMT: Security Management</i>	55
5.1.5	<i>Class FPT: Protection of the TSF</i>	57
5.2	SECURITY ASSURANCE REQUIREMENTS (SAR)	58
5.2.1	<i>Class ASE: Security Target evaluation</i>	58
5.2.2	<i>Class ADV: Development</i>	64
5.2.3	<i>Class AGD: Operational user guidance</i>	67
5.2.4	<i>Class ALC: Life-cycle support</i>	69
5.2.5	<i>Class ATE: Tests</i>	71
5.2.6	<i>Class AVA: Vulnerability analysis</i>	74
5.3	SECURITY REQUIREMENTS RATIONALE	75
5.3.1	<i>Rationale for the TOE Security Requirements</i>	75

5.3.2	<i>Rationale for the TOE Assurance Requirements</i>	79
5.3.3	<i>Rationale for Dependencies</i>	79
6	TOE SUMMARY SPECIFICATION	82
6.1	TOE SECURITY FUNCTIONS.....	82
6.1.1	<i>Network Authentication (TSF_NAU)</i>	82
6.1.2	<i>Data Access Control (TSF_DAC)</i>	82
6.1.3	<i>Security Audit (TSF_FAU)</i>	83
6.1.4	<i>Security Management (TSF_FMT)</i>	84
6.1.5	<i>System Authentication (TSF_SAU)</i>	86
6.1.6	<i>Image Overwrite (TSF_IOW)</i>	86
6.1.7	<i>Information Flow (TSF_FLW)</i>	88

LIST OF FIGURES

Figure 1: Operating Environment of the TOE	11
Figure 2: Physical Structure of MFP System Software	18
Figure 3: Logical Scope of the TOE.....	21
Figure 4: Information Flow Summary.....	89

LIST OF TABLES

Table 1: Models and Capabilities	10
Table 2: Details of Non-Target Items	12
Table 3: Specifications of the MFP that will use the TOE	14
Table 4: Evaluated Software/Firmware for the TOE.....	19
Table 5: Operations for each user type.....	22
Table 6: TSF data for each user type.....	23
Table 7: Acronyms	35
Table 8: Security Objectives and Definition of Security Problems.....	43
Table 9: Security Functional Requirement.....	48
Table 10: Audit Event.....	49
Table 11: Security Functions and Its Role	55
Table 12: Operation and Role of each TSF Data List	56
Table 13: Management Functions of TOE.....	57
Table 14: EAL3 5.2 Security Assurance Requirements	58
Table 15: TOE SFR Mapping to the TOE Security Objectives.....	75
Table 16: Dependencies on the TOE Security Functional Components	81
Table 17: Security Event.....	83
Table 18: Relationship between the TOE Security Function Component and SFR Security Function Component	85
Table 19: Operation and Role of each TSF Data List	85
Table 20: Component Relationship between the TOE Security Function and SFR Security Function	89

1 Introduction

1.1 Security Target References

Security Target Title	Samsung MFP Security Kit Type_A v1.0
Security Target Version	v1.7
Publication Date	November 13, 2008
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. 2008-26 by Ministry Of Public Administration and Security (v3.1)
Keywords	Samsung Electronics, Multifunction Peripheral, Image Overwrite

1.2 TOE References

Author	Samsung Electronics
Name	Samsung MFP Security Kit Type_A
Version	v1.0
Publishing Date	May 25, 2008

1.3 TOE Overview

The TOE is embedded software on SAMSUNG multifunction peripherals (MFPs). These MFPs include copy, print, scan, network scan, scan-to-email, scan-to-server, and fax features. The TOE allows the MFPs to perform image overwrite, 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	Network Scan	Fax	Scan-to-email	Scan-to-server
SCX-6345N, SCX-6345NG	Standard	Standard	Standard	Optional	Standard	Standard
SCX-6555N, SCX-6555NG	Standard	Standard	Standard	Optional	Standard	Standard
C8380ND, C8380NDG	Standard	Standard	Standard	Optional	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, server PCs or client PCs. Users can also use their PCs to print out documents or to access the TOE through the internal network. The local administrator can enable/disable IIO and ODIO, start/stop ODIO, and change a PIN via LUI.

A web administrator can access TOE through the web user interface. From there, they can add/change/delete user accounts for network scan services, change the web administrator’s ID and password, enable/disable the security audit service, and download the security audit report.

The user account information that requires asking local authentication (only for network-scan services such as network scan (NetScan), scan-to-server, or scan-to-email) can be stored in the hard disk drive of the MFP. All of the information stored on the hard disk drive is protected by the TOE. In the case of network authentication, all the account information stored on a network authentication server is assumed to be protected from external environmental space.

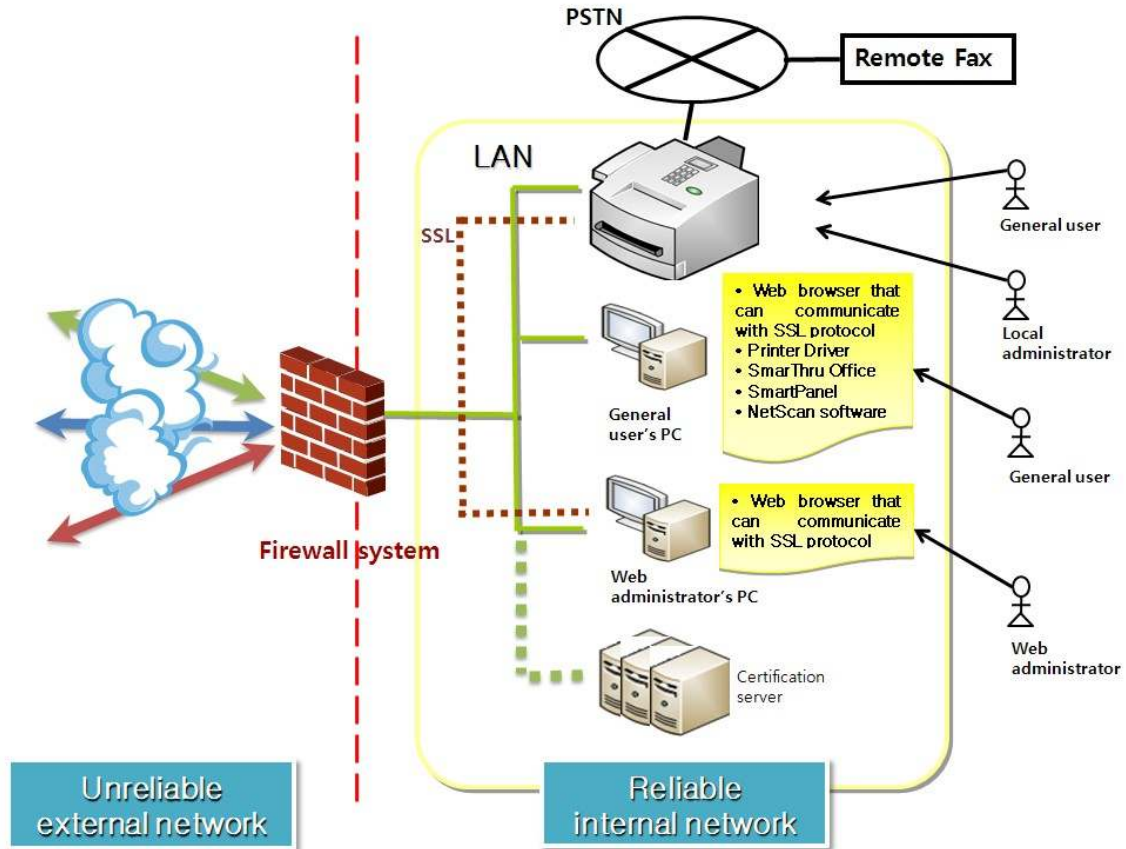


Figure 1: Operating Environment of the TOE

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

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

Table 2: Details of Non-Target Items

Types	Items	Objectives	Specification
Hardware	MFP	The TOE must be embedded in the MFP.	Refer to Table 3
	PC for web administrator	PC for web administrator to access and manage TOE.	<ul style="list-style-type: none"> • Windows 2000 <ul style="list-style-type: none"> - CPU: Pentium II 400MHz or higher - Memory: 64MB or higher - HDD: 0.6GB or higher • Windows XP <ul style="list-style-type: none"> - CPU: Pentium III 933MHz or higher - Memory: 128MB or higher - HDD: 1.5GB • Windows 2003 Server <ul style="list-style-type: none"> - CPU: Pentium III 933MHz or higher - Memory: 128MB or higher - HDD: 1.25GB or higher • Windows Vista <ul style="list-style-type: none"> - CPU: Pentium IV 3GMHz or higher - Memory: 512MB or higher - HDD: 512MB or higher • Mac OS X <ul style="list-style-type: none"> - CPU: Power PC G4/G5, Intel Processors - Memory: 128MB based on Power PC - HDD: 1GB or higher • Mac OS X 10.5 <ul style="list-style-type: none"> - CPU: 867MHz or Power PC G4/G5 - Memory: 512MB or higher - HDD: 1GB or higher • Linux <ul style="list-style-type: none"> - CPU: Pentium IV 2.4 GHZ or higher - Memory: 512MB - HDD: 1GB or higher
	PC for general user	PC for general user to print or scan or copy with TOE	
	Authentication server	Authentication server to store general user's account information and provide remote certification service before using NetScan function.	<ul style="list-style-type: none"> • Windows 2003 Server <ul style="list-style-type: none"> - CPU: Pentium III 933MHz or higher - Memory: 128MB or higher - HDD: 1.25GB or higher
	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.	

Firmware	Operating system for PC	Operating system for general user or web administrator	<ul style="list-style-type: none"> • For SCX-6345N, SCX-6345NG - Windows 98/Me/2000/XP(32/64bit)/2003 Server(32/64bit), Various Linux OS including Red Hat 8~9, Fedora Core 1~4, Mandrake 9.2~10.1 and SuSE 8.2~9.2 • For SCX-6555N, SCX-6555NG - Windows 98/Me/2000/XP(32/64bit)/2003 Server(32/64bit), Various Linux OS including Red Hat 8~9, Fedora Core 1~4, Mandrake 9.2~10.1 and SuSE 8.2~9.2 Mac OS 10.3~10.4 • For CLX-8380ND, CLX-8380NDG - Windows 98/Me/2000/XP(32/64bit)/2003 Server(32/64bit), Various Linux OS including Red Hat 8~9, Fedora Core 1~4, Mandrake 9.2~10.1 and SuSE 8.2~9.2 Mac OS 8.6~9.2 / 10.3~10.4
	RTOS	Operating system embedded in MFP.	<ul style="list-style-type: none"> • For SCX-6345N, SCX-6345NG - pSOS2.5 • For SCX-6555N, SCX-6555NG - pSOS2.5 • For CLX-8380ND, CLX-8380NDG - VxWorks v5.5.1
	Operating system for server	Operating system for authentication server	MS Windows 2003 Server
Software	Web browser that can serve SSL communication	Web browser that serve SSL communication among general user's PC, web administrator's PC, and TOE.	Netscape, Explorer, Opera, Mozilla
	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 6 Driver V3.04.59
	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 V1.02.28
	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 V1.17.10
	NetScan software	NetScan software receives scanned data from the MFP and stores it in the user's PC.	NetworkScan V1.11.22

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

Specifications		SCX-6345N, SCX-6345NG	SCX-6555N, SCX-6555NG	CLX-8380ND, CLX-8380NDG
LCD		VGA (640x240)8.4" Graphic LCD (with TSP)	WVGA (800x480) 7" TFT color LCD (with TSP)	WVGA (800x480) 7" TFT color LCD (with TSP)
System Memory		256MB Max. 384MB	Std.256MB Max. 512MB	Std. 320MB (Main, 256MB + Graphic,64MB) plus 40GBor Higher hard disk drive Max. 832MB(Main, 256MB + Graphic, 64MB + Option, 512MB)
Hard disk drive		40GB IDE	80GB SATA	80GB SATA
F A X	Compatibility	ITU-T G3	ITU-T G3	ITU-T G3
	Comm. System	PSTN / PABX	PSTN / PABX	PSTN / PABX
	Modem Speed	33.6Kbps	33.6Kbps	33.6Kbps
Interface		Hi-Speed USB 2.0, Ethernet 10/100 base TX	Hi-Speed USB 2.0, USB host 1.1, Ethernet 10/100 base TX	Hi-Speed USB 2.0, USB host 1.1, Ethernet 10/100 base TX

<Security Functions>

The TOE provides image overwrite, fax/network separation, identification, and authentication.

- **Image Overwrite**

User data created during the copying, printing, network scanning, scan-to-email, or scan-to-server processes is immediately recorded on the hard disk drive.

One of the core TOE functionalities is an image overwrite function for clearly erasing image data generated during the copying, printing, network scanning, scan-to-email, and/or scan-to-server tasks. The image data is completely overwritten three times by using DoD 5200.28-M standard. There are two supported image overwrite techniques. One is Immediate Image Overwrite (IIO); the other is On Demand Image Overwrite (ODIO). The IIO automatically carries out overwriting operations on temporary image files at the end of each job or on the files on the hard disk drive when a user initiates a delete operation. The ODIO function overwrites all stored files on the hard disk drive (except some system files), and the function should only be manually performed by a local administrator.

- **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 information flow on the fax board and the network port of the central processing unit. 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.

- **Identification and Authentication**

The TOE requires dividing a real client into different kind of access level, such as a system administrator, before giving permission to access system management. The system administrator position is divided into two positions: web administrator and 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.

The TOE is available to block unacceptable uses of the transmitting function—NetScan, transmitting data after scanning, or sending an email after scanning. IDs and passwords of the network scan service users are created, changed, or deleted by the web administrator.

To retain a user's own file, the Stored Documents feature is provided. Documents can be stored using two methods: Public or Secured. When a user stores documents using the Public option, all users can access and use the documents. When a user stores documents using the Secured option, only the user who stored the document has access. A document stored using the Secured option must include a user-assigned PIN for authentication. When accessing the document, the user must enter the assigned PIN or access is denied.

<Assets>

The TOE protects assets such as image files, stored documents, 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.

- **File preservation**

A client can save a file on the hard disk drive for future work. An attacker has a chance to get the file, so it should be protected from unauthorized external access.

- **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, the TOE should be able to 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 activate or deactivate IIO/ODIO, start or stop ODIO, and 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:

- Creates, modifies, or deletes NetScan service user accounts.
- Modifies web administrator accounts and passwords.
- Activates or deactivates security audit.
- Downloads the security audit log.

- **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.

A user granted network scanning privileges can perform scan jobs through the local user interface. Network scanning services include scan-to-email, scan-to-server, and scan-to-network.

- When a user stores documents as Secured, the user who stores the document via client PC can assign PIN to the document. The PIN should not be exposed to others. When accessing the file, the user must get permission by entering the PIN through LUI and then access to the file.

1.4 TOE Description

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

1.4.1 Physical Scope

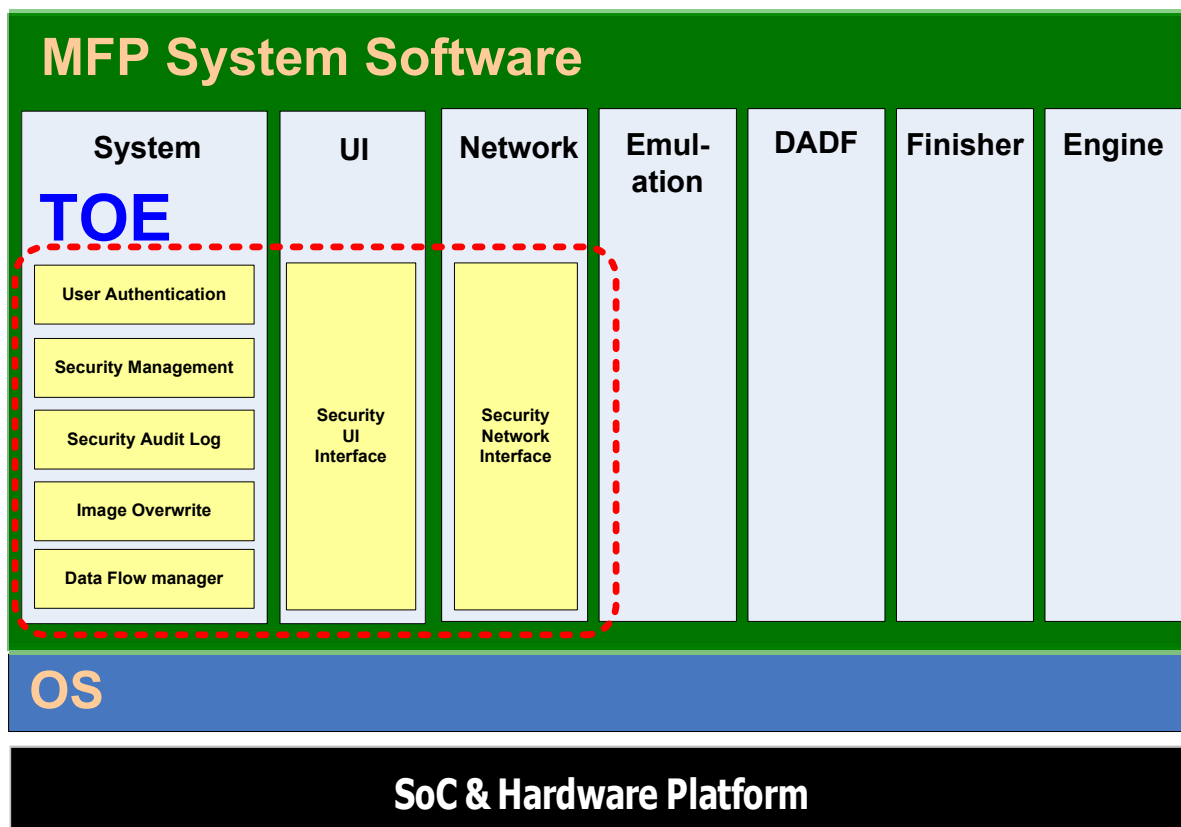


Figure 2: Physical Structure of MFP System Software

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-target software (including system software, UI 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-target 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:

- 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 user authentication, security management, security audit log, image overwrite, and data flow manager. The UI software includes security UI interface. The network software includes the security network interface.

Table 4: Evaluated Software/Firmware for the TOE

Software Version	SCX-6345N, SCX-6345NG	SCX-6555N, SCX- 6555NG	CLX-8380ND, CLX-8380NDG
System Software	V1.03.C0.78	V2.01.C1.04	V2.01.C0.72
- User Authentication	TSF_SUA_V1.0	TSF_SUA_V1.0	TSF_SUA_V1.0
- Security Management	TSF_SFM_V1.0	TSF_SFM_V1.0	TSF_SFM_V1.0
- Security Audit Log	TSF_SAA_V1.0	TSF_SAA_V1.0	TSF_SAA_V1.0
- Image Overwrite	TSF_IOW_V1.0	TSF_IOW_V1.0	TSF_IOW_V1.0
- Data Flow Manager	TFS_FLW_V1.0	TFS_FLW_V1.0	TFS_FLW_V1.0
UI Software	JF_PL_V1.01.00.60 04-03-2008	V1.00.01.26 05-15- 2008	V1.00.01.25 05-07-2008
- Security UI Interface	TSF_LUI_V1.0	TSF_LUI_V1.0	TSF_LUI_V1.0
Network Software	V2.03.04(SCX- 6345N) 04-08-2008	V4.01.04A(SCX-6x55) 05-16-08	V4.01.02A(CLX-8380) 05-16 2008
- Security Network Interface	TSF_WUI_V1.0	TSF_WUI_V1.0	TSF_WUI_V1.0

The TOE is called the Samsung MFP Security Kit Type_A and is embedded in the MultiXpress SCX-6345N, SCX-6345NG, SCX-6555N, SCX-6555NG, C8380ND, and C8380NDG devices. It performs security functions for Samsung MFPs by using system software, UI 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. Data created during printing, scanning, or copying is completely cleared right after the job is finished. This function can be performed by the Image Overwrite function. Also, when a security event occurs, 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. And this software provides the functions below:

- WebUI through a web server.
- Authentication for web administrator and/or provides security management functions.
- Network scan service to the authorized users.
- Ability for tracing the system audit log from an external network (SWS) to web administrator

The UI software provides the local user interface for local administrators or authorized user to conduct MFP functions on the TOE. It also provides security functions using authentication when a user tries to access to the TOE.

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.

1.4.2 Logical 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:

- Network Authentication (TSF_NAU)
- Data Access Control (TSF_DAC)
- Security Audit (TSF_FAU)
- Security Management (TSF_FMT)
- System Authentication (TSF_SAU)
- Image Overwrite (TSF_IOW)
- Information Flow (TSF_FLW)

Network Authentication (TSF_NAU)

The TOE prevents unauthorized use of the installed network options (network scanning, scan-to-email, and scan-to-server); the network options available are determined by the system administrator. To access a network service, the user is required to provide a user name and password, which is then validated by the designated authentication server.

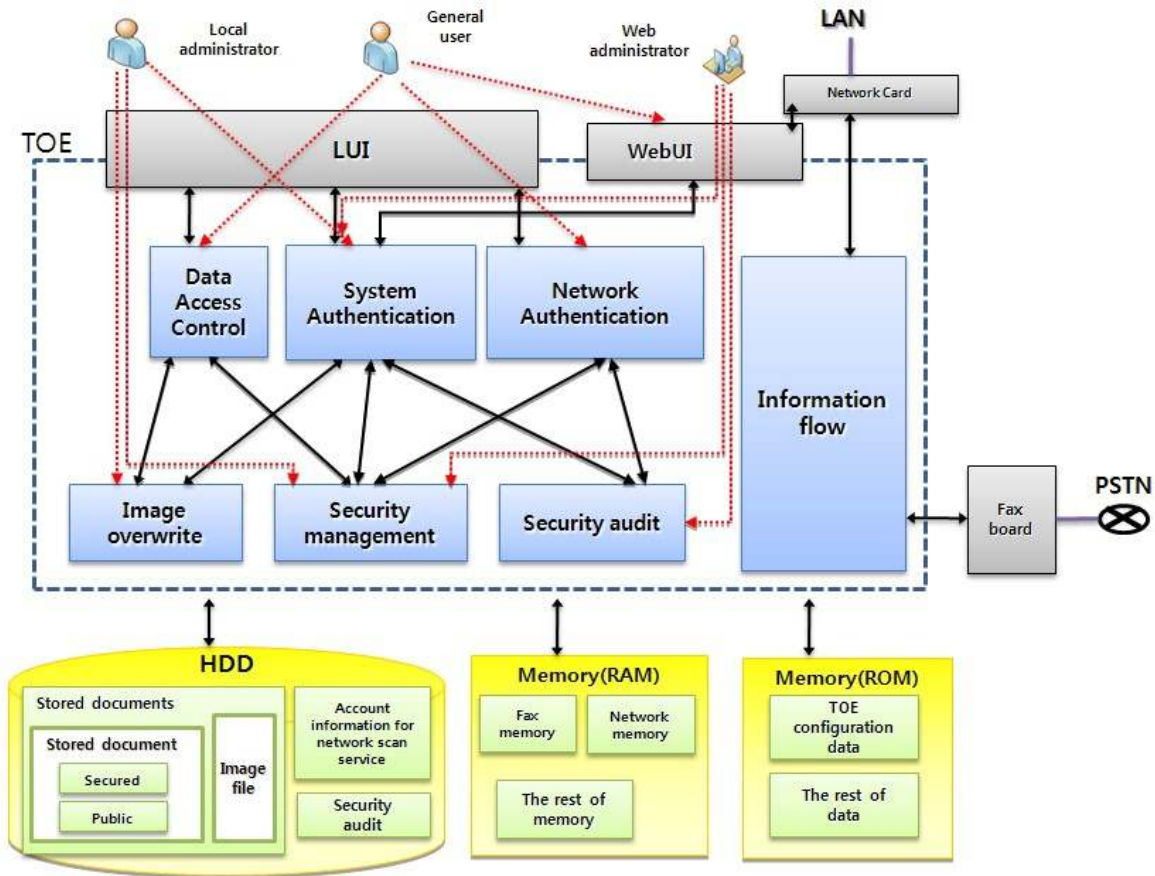


Figure 3: Logical Scope of the TOE

Data Access Control (TSF_DAC)

The TOE prevents unauthorized use of the user-created data; the user-created data is divided into two categories, Public and Secured. When a user stores a document as Public, all users can access and use the file. A file stored as Secured can only be accessed by the user who stored the file. When storing a file as Secured, the user must set a PIN required to access the file. Then the file can only be accessed by entering the PIN.

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 with reliability of 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 system administrators can perform the following operations listed in Table 5:

Table 5: Operations for each user type

User Type	Operations
Local Administrator	<ul style="list-style-type: none"> ▪ Enable or disable IIO ▪ Enable or disable ODIO ▪ Start or stop ODIO ▪ Change the local administrator PIN
Web Administrator	<p>When using local certification in network scan service authentication,</p> <ul style="list-style-type: none"> ▪ Create/Change/Delete user account for network scan service. ▪ Configure authentication option for network scan service: (Select one among No Authentication, Require Network Authentication, and Require Local Authentication) ▪ Change the web administrator’s name and password. ▪ Enable or disable system audit logs. ▪ Download system audit report.

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	<ul style="list-style-type: none"> ▪ Authentication data for local administrator ▪ Configuration data on IIO/ODIO enabling or disabling
Web Administrator	<ul style="list-style-type: none"> ▪ Authentication data about web administrator. ▪ Configuration data about system audit logs enabling or disabling. ▪ Configuration data about network scan service authentication. ▪ System audit logs ▪ User information for network scan service

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, managing the accounts for network scan service users, and managing the account for a web administrator. Security functions for the local administrator are managing PINs for the local administrator and configuring data for IIO function.

TSF data includes information on local/web administrator’s authentication, information on IIO function configuration, information on security audit configuration for web administrators, security audit log, information on network scan service users, configurations for certifying a network scan service user, etc. There are 3 options for network scan service authentication: **No Authentication**, **Require Network Authentication**, and **Require Local Authentication**. The web administrator must select between **Require Network Authentication** and **Require Local Authentication** for network scan service.

When the **Require Local Authentication** option is selected, the TOE stores user account information on the MFP hard disk drive, then the network administrator must manage them safely. When the **Require Network Authentication** option is selected, user information can be stored on an authorized server. The users must authenticate by entering their account IDs and passwords prior to being granted access to the network resources. That is assuming that the authorized server and remote authentication service are managed safely.

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 3 wrong PINs are entered in succession. If 3 wrong PINs are entered at the web interface from one particular browser session, the TOE will send an error message to this Browser session.

Image Overwrite (TSF_IOW)

The TOE implements a hard disk drive image overwrite security function to overwrite temporary files created during the copying, printing, network scan, scan-to-email, or scan-to-server process. Immediately after the job has completed, the files on the hard disk drive are overwritten using a three pass overwrite procedure as described in DoD 5200.28-M standard. FAX jobs do not get written to the hard disk drive. The image overwrite security function can be invoked automatically (IIO) or manually by the local administrator (ODIO). IIO provides two kinds of functions: IIO and ODIO

IIO automatically overwrites temporary files created as a result of the processing or manually overwrites the temporary files created as a result of this processing on a reserved section of the hard disk drive of the main controller by the general user. The image overwrite security function can also be invoked manually by the local administrator (ODIO). Once invoked, the ODIO cancels all print and scan jobs, halts the printer interface (network), overwrites the contents of the reserved section on the hard disk drive according to DoD 5200.28-M standard, and then the main controller reboots.

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 control board 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 restrict 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

translated into 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 comes in internal network has been verified by TOE, it does not threat or modify TOE component of the internal network.

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 when an additional statement except 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 followings 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 NetScan, 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_A V1.0 through LUI. The main roles are to configure system information, check MFP status for general use. The other roles for security service are enable/disable IIO/ODIO for security, start/stop ODIO, change PIN.

Fax-to-email

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

Security printing

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

Stored file

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

Multi-Function Printer, MFP

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

Human User

User who only refers to human being

ODIO, On Demand Image Overwrite

The ODIO function overwrites all stored files including image files and preserved files on the hard disk drive, and the function should only be manually performed by a local administrator through local user interface. The image data is completely overwritten three times by using DoD 5200.28-M standard.

Scan-to-server

This is a function that transmitting 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 transmitting 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 manage TOE-embedded MFP. It includes local administrator and web administrator.

IOW , Image Overwrite

A function to delete all stored files on the hard disk drive. There are two kind of image overwriting: IIO and ODIO. The image data is completely overwritten three times by using DoD 5200.28-M standard.

WebUI, Web User Interface

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

Web System administrator

System administrator to manage Samsung MFP Security Kit Type_A V1.0 through WebUI. The main roles are to create/change/delete the information of network scan service user, manage/change web administrator's id and password, enable/disable security audit function, download security audit log.

Image file

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

Stored file

Every stored file in hard disk drive. It includes image file and preserved file.

Public Print

The file that user stored documents using the Public option. It is open to every user.

IIO, Immediate Image Overwrite

The IIO automatically carries out overwriting operations on temporary image files at the end of each job such as copy/scan/Netscan, scan-to-email, or scan-to-server. Or the IIO overwrites on the files on the hard disk drive when a user initiates a delete operation. The image data is completely overwritten three times by using DoD 5200.28-M standard.

FAX

Job for receiving or transmitting fax image through fax line

Fax image

The receiving or transmitting data through fax line

DoD 5200.28-M

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

Embedded FAX

Fax job that transmitting a scanned data in the MFP through fax line and receiving fax data directly from fax line on MFP, and then printing.

HIPAA (Health Insurance Portability and Accountability Act)

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

NetScan

Scan function that only authorized network scan service user can use. This is scan function to send scanned data in local user interface to a remote client PC.

PC FAX

Fax function that is firstly sending fax data from client PC to MFP, and then transmitting fax data through fax line.

T.4

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

MH

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

MR

Abbreviation of Modified Relative Element Address Designate MH coding.

MMR

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

1.7 Acronyms

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

Table 7: 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
IIO	Immediate Image Overwrite
ISO	International Standards Organization
IT	Information Technology
LUI	Local user interface
MFP	Multi-function Printer
ODIO	On Demand Image Overwrite
OSP	Organization Security Policy
PP	Protection Profile
PPM	Pages Per Minute
PSTN	Public Switched Telephone Network
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	Target Security Functionality
UI	User Interface
WebUI	Web User Interface
MMR	Modified modified READ coding
MR	Modified READ Coding
MH	Modified Huffman coding

1.8 Organization

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

Chapter 2 describes the declaration about the Common Criteria, Protection Profile, and package.

Chapter 3 defines security threats, security policies of the organization, and assumptions from the TOE or the TOE operating environment point of view.

Chapter 4 describes about TOE security objectives for corresponding with recognized threats, performing the security policy of the organization, and supporting the assumptions. And it describes security objectives about operating environment.

Chapter 5 describes Security Functional Requirement or 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 evaluation standard, the protective profile and package.

2.1 Common Criteria Conformance

This contains a CC v3.1 Conformance Claims that:

- **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: SFR (Security Functional Requirement), version 3.1r2, 2007. 9,

CCMB-2007-09-002

Common Criteria for Information Technology Security Evaluation, Part 3: SAR (Security Assurance Requirement), version 3.1r2, 2007. 9,

CCMB-2007-09-003

- **Conformance status of Common Criteria**

Common Criteria for Information Technology Security Evaluation, Part 2

Common Criteria for Information Technology Security Evaluation, Part 3

2.2 Conformance of Protection Profile

No Protection Profile (PP) relevant to Security Target.

2.3 Conformance of Package

- The assurance level used to evaluate on Security Target is EAL3
- Assurance package: conformance of EAL 3

2.4 Conformance of 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

Threats are IT entities or users that can adversely access to the internal asset or harm the internal asset in an abnormal way. The threats have substantial expertise, standard equipment, and motive. The threads that described in this chapter will be resolved by security objectives in chapter 4.

T.UNAUTHORIZED_ACCESS_ON_NETWORK_SCAN_SERVICE

The origin of threats snatch or outflow the TOE image file or preserved file to outside of the TOE (outside of hard disk drive) through unauthorized internal network access

T.DATA_ACCESS

The threats may attempt unauthorized removal or camouflage/forgery of a preserved file on MFP's hard disk drive.

T. AUDITS

The origin of threats may access the security audit through an unauthorized approach.

T.RECOVER

The origin of threats attempts to recover both a deleted image file and a preserved file using a commercial tool to open a preserved file and image file of the TOE.

Appiliation note: The attacking origin of threats may also attempt to access stored data physically in one of two ways. 1) The attacker may approach a discarded or unused MFP and attempt to retrieve data stored on the machine. 2) An attacker may attempt to exploit the data recovery function provided to immediately save data in the event of an emergency (e.g., a power failure).

T.CERTIFICATION_TRIAL_IN_A_ROW

In order to approach the TOE, the origin of threats attempts to authenticate continuously and gain permission from a system administrator.

T.UNAUTHORIZED_ACCESS_ON_TOE

The origin of threats may attempt to gain an administrator's permission to access the network or change the TOE setting value by an unauthorized way and set up new values.

T. INFAX

The origin of threats may be caused by a received fax that has malicious code via fax line.

3.2 The Security Policy of Organization

The following section describes the TOE and the operational environment of TOE should observe the following regulations:

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 related security events, and properly go over the recorded data.

3.3 Assumption

The operational environment of the TOE should be managed by the requirements of security certification about distribution, function, and guidance for client/system administration. The following specification is an assumption of the installing operational environment of the TOE and describes the physical, resourceful, procedural, connective, and functional side.

A. PHYSICAL_SECURITY

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

A.TRUSTED_ADMINISTRATOR

The permitted system administrator in 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 maintain a 4-digit to 8-digit PIN for key maintenance and change the PIN at least once every 40 days.

A.TRUSTED_NETWORK

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

A.TRUSTED_AUTHENTICATION_SERVER

When the TOE performs client authentication for network scan services via authentication server, the authenticated server should be safely

managed and provide safe remote authentication through certificated protocol.

A.TIME_STAMP

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

A.SSL

When it comes to downloading the system audit of the TOE, in order to counterfeit/camouflage the system audit of the TOE, the device transfers audit log using safe channel SSL protocol.

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 permitted 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.IDENTIFICATION_AND_AUTHENTICATION_FOR_NETWORK_SCAN_SERVICE

The TOE should provide exact identification and authentication over a network scan client to block data scanned inside from outside the network. This service only allows the network scan service to distinguish clients.

O.CONTROL_DATA_ACCESS

The TOE should perform an authentication process to prevent unauthorized removal or camouflage/forgery of a preserved file in hard disk drive. To access stored file, a client has to enter PIN that has been configured in the file.

O. IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR

The TOE should provide identification and authentication processes for system administrators for optimized management. The TOE gives permission to decide start/stop services and allows the possibility of enabling/disabling TSF for only an authorized system administrator. A

local administrator authenticates a real client using a PIN on the local user interface and the web administrator also authenticates a real client using an ID and password on the web user interface. At that time, PINs and passwords should display as asterisks (*).

O.IMAGE_OVERWRITE

The TOE provides an Image Overwrite function to enhance the security of the MFP. The Image Immediate Overwrite function overwrites temporary document image data as described in DoD Standard 5200.28-M at the completion of each copy, print, network scan, or scan-to-email job. The appropriate sections on the hard disk drive are overwritten 3 times by methods described in the DoD 5200.28-M specification.

O. HANDLING_AUTHENTICATION_FAILURE

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

O.FAXLINE

The TOE will control access to the internal network from the MFP network card via the TOE's FAX modem (if installed). Direct communication between a user network card in an MFP and a fax modem is impossible. The communication can be made up only through the TOE.

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 on a minimum of every 40 days.

OE.TRUSTED_NETWORK

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

OE.TRUSTED_AUTHENTICATION_SERVER

When the TOE uses authentication server for network scan service user authentication , the remote authentication service through the server should be safely managed and secured.

The remote authentication services supported by the TOE are: Kerberos, LDAP, and SMB.

OE.TIME_STAMP

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

OE.SSL

When downloading the security audit log, the TOE has to send the security audit log using SSL protocol for secured data communication.

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 for the TOE	Security Objectives for the Environment
--	---------------------------------	---

4.3.1 Rationale 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.IDENTIFICATION_AND_AUTHENTICATION_FOR_NETWORK_SCAN_SERVICE

This security objective provides correct and accurate identification and authentication to the network scan service user. Therefore, the TOE protects scan data that is transmitted to the external network, and this satisfies the threat T.UNAUTHORIZED_ACCESS_ON_NETWORK_SCAN_SERVICE.

O.CONTROL_DATA_ACCESS

This security objective allows contacting the stored documents only to the authorized user. When approaching the file, users have to enter the correct PINs and then the user can get permission to contact with it. Therefore, this security objective corresponds with threat: T.DATA_ACCESS.

O.IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR

This security objective provides system administrators with the identification and authentication process to manage the TOE safely. The TOE allows only authorized system administrators to enable/disable/start/stop TSF. The web administrators must get the authentication by typing the account and password in web user interface, and the local administrators by typing the PIN number in the local user interface. Therefore this security objective supports the threat: T.UNAUTHORIZED_ACCESS_ON_TOE.

O.IMAGE_OVERWRITE

The security objective provides an image overwrite function to overwrite temporary files created during the copying, printing, network scan, scan-to-email, or scan-to-server process for preventing information leakage. The image overwrite function can also be invoked manually by the system administrator. Because the removed data never can be restored, this security objective supports the threat: T.RECOVER.

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

This security objective does not allow the direct access of fax data from fax modem to the internal network. The communication can be made up only through TOE. Therefore, the security objective supports the threat: 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.TRUSTED_AUTHENTICATION_SERVER

The TOE prevents unauthorized use of network scan services. The network scan service availability is determined by the system administrator. To access a network scan service, the user is required to provide a user name and password which are then validated by the designated authentication server. The authentication service (Kerberos, LDAP, and SMB) on authentication server will be provided securely by safe channel. Therefore, it supports assumption of A.TRUSTED_AUTHENTICATION_SERVER.

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.

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
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_IFC.1	Subset access control
	FDP_IFF.1	Security attribute based access control
	FDP_RIP.1	Subset Residual Information Protection
Identification and Authentication	FIA_AFL.1(1)	Authentication failure handling (1).
	FIA_AFL.1(2)	Authentication failure handling (2).
	FIA_UAU.2(1)	User Authentication Before Any Action (1)
	FIA_UAU.2(2)	User Authentication Before Any Action (2)
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UID.2(1)	User identification before any action (1)
	FIA_UID.2(2)	User identification before any action (2)
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
TSF Protection	FPT_RCV.4	Function recovery

5.1.1 Class 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	Decision to admit requested information flow.
FMT_MOF.1	Configuration change of security audit function, or Start/stop image overwrite.
FMT_MTD.1	Query/change of security audit function.
FPT_RCV.4	(If possible) Impossibility of reliable recovery from TSF failure.

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.

5.1.1.4 FAU_STG.1

Protected audit trail storage

- Hierarchical to: No other components.
- Dependencies: FAU_GEN.1 Audit data generation
- FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
- FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

5.1.1.5 FAU_STG.4

Prevention of audit data loss

- Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
- Dependencies: FAU_STG.1 Protected audit trail storage
- FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [no other actions] if the audit trail is full.

5.1.2 Class FDP: User Data Protection

5.1.2.1 FDP_IFC.1

Subset information flow control

- Hierarchical to: No other components
- Dependencies: FDP_IFF.1 Simple security attributes
- FDP_IFC.1.1 The TSF shall enforce the [information flow control (SFP_FLW)] on
- Subject List
 - Fax image sending/receiving process
 - Information List
 - Fax image
 - Operation List
 - Copying (Moving) fax image from fax image area to network card memory area.

5.1.2.2 FDP_IFF.1

Simple security attributes

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

- FDP_IFF.1.1 The TSF shall enforce the [information flow control (SFP_FLW)] based on the following types of subject and information security attributes: [
- The Subject List
 - Fax image sending/receiving process
 - Information List
 - Fax image
 - Security Properties
 - Subject List: No security properties
 - Information List: Standard fax image specification (MMR, MR, or MH of T.4 specification)]
- 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 the fax image from fax line is not standardized MMR, MR, or MH of T.4 specification, the fax image is not copied or moved from fax memory to network memory.
 - When the fax image that is sent to the internal network is not standardized MMR, MR, or MH of T.4 specification, the fax image is not copied or moved from fax memory to network 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_RIP.1 protection

Subset residual information

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of **a file is overwritten according to DoD 5200.28-M** upon the deallocation of the resource from the following

objects: [Stored File on the hard disk drive].

5.1.3 Class 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 or authentication of network scan service user].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [lockout the local administrator's or the network scan service user'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 (1) User authentication before any action (1)

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.2 (2) **User authentication before any action (2)**

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **general user** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **general user**.

Application note: General users are divided into network scan service users and secured print users.

5.1.3.5 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.

5.1.3.6 FIA_UID.2 (1) **User identification before any action (1)**

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.

5.1.3.7 FIA_UID.2 (2) **User identification before any action (2)**

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies

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

Application note: Secured print users among general users perform with authentication by entering the corresponding PIN with a stored file, without any identification function.

5.1.4 Class 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
Enable security audit function	Disable, Enable	Web administrator
Download security audit log.	Determine the behavior of	Web administrator
Configure the network scan service authentication.	Determine the behavior of	Web administrator
Create/modify/delete user's account for network scan service on local user interface.	Determine the behavior of	Web administrator
Modify web administrator's id and password.	Determine the behavior of	Web administrator
Modify PIN of local administrator.	Determine the behavior of	Local administrator
Image overwrite	Disable, Enable, Determine the behavior of, Modify the behavior of	Local 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].

Application note: Downloading the security audit records can be performed only when SSL is configured, only through a safe channel provided by operating environment, and only by the system administrator.

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
Configurations on the network scan service authentication.	Query, Modify	Web administrator
User certificate information of network scan service.	Query, Modify, Delete	Web administrator
Record security audit log.	Download	Web administrator
Authentication information for local administrator.	Modify	Local administrator
Configurations on IIO enabling/disabling of local administrator.	Query, Modify	Local administrator

5.1.4.3 FMT_SMF.1 Functions

Specification of Management

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.
FMT_MOF.1	Manage the group to communicate with TSF function.
FMT_MTD.1	Manage the group to communicate with TSF 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.

5.1.5 Class FPT: Protection of the TSF

5.1.5.1 FPT_RCV.4

Function recovery

- Hierarchical to: No other components.
- Dependencies: No dependencies.
- FPT_RCV.4.1 The TSF shall ensure that [
- Function List
 - Image Overwrite including ODIO and IIO
 - Failure Scenario
 - Power off (blackout) during image overwriting job
-] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

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. The SARs are not iterated or refined from Common Criteria for Information Technology Security Evaluation Part 3.

Table 14: EAL3 5.2 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
	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

5.2.1 Class 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.

5.2.2 Class 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.

5.2.3 Class 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.

5.2.4 Class 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 coverage

Implementation representation CM

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.

5.2.5 Class 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:
description

ADV_ARC.1 Security architecture

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.

5.2.6 Class AVA: Vulnerability analysis

5.2.6.1 AVA_VAN.2

Vulnerability analysis

Dependencies:
description

ADV_ARC.1 Security architecture

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.

5.3.1 Rationale 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. AUDITS	O. MANAGE	O.IDENTIFICATION_AND_AUTHENTICATION_FOR_NETWORK_SCAN_SERVICE	O.CONTROL_DATA_ACCESS	O.IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR	O.IMAGE_OVERWRITE	O.HANDLING_AUTHENTICATION_FAILURE	O.FAXLINE
FAU_GEN.1	X							
FAU_SAR.1	X							
FAU_SAR.2	X							
FAU_STG.1	X							
FAU_STG.4	X							
FDP_IFC.1								X
FDP_IFF.1								X
FDP_RIP.1						X		

FIA_AFL.1(1)			X		X		X	
FIA_AFL.1(2)					X		X	
FIA_UAU.2(1)					X			
FIA_UAU.2(2)			X	X				
FIA_UAU.7			X	X	X			
FIA_UID.2(1)					X			
FIA_UID.2(2)			X					
FMT_MOF.1		X						
FMT_MTD.1		X						
FMT_SMF.1		X						
FMT_SMR.1		X						
FPT_RCV.4						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.

FAU_STG.1 (Protected audit trail storage)

This component is required to ensure the ability to protect the security audit log in storage from unauthorized users. Therefore, it satisfies security object O.AUDITS.

FAU_STG.4 (Prevention of audit data loss)

This component is required to ensure the ability to overwrite the security audit log when storage is full of log data, and also to prevent unauthorized changes to the audit log. Therefore, it satisfies security object O.AUDITS.

FDP_IFC.1 (Subset access control)

This component defines information flow control that doesn't allow the direct access of a received fax image from a fax modem to the internal network. Therefore, it satisfies security object O.FAXLINE.

FDP_IFF.1 (Security attribute based access control)

This component defines the information flow control that prevents the direct access of a received fax image from a fax modem to the internal network, accomplished by the security properties and rules. Therefore, it satisfies security object O.FAXLINE.

FDP_RIP.1 (Subset Residual Information Protection)

It is ensured that in case of deleting the stored file from the hard disk drive, this component completely deletes the stored file by using the methods defined in the DoD5200.28-M policy. Therefore, it satisfies security object O.IMAGE_OVERWRITE.

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 3 wrong PINs are entered in succession. Therefore, it satisfies security object O.IDENTIFICATION_AND_AUTHENTICATION_FOR_NETWORK_SCAN_SERVICE, O.IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR, and O.HANDLING_AUTHENTICATION_FAILURE.

FIA_AFL.1 (2) (Authentication failure handling)

This component provides a proper error message through the web interface, and ensures detection of the wrong trial of authentication. Therefore, it satisfies security object O.IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR, and O.HANDLING_AUTHENTICATION_FAILURE.

FIA_UAU.2 (1) (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.2 (2) (User Authentication before Any Action)

This component ensures that the network scan service user or security print user must get authentication before accessing the TOE functionality. Therefore, it satisfies security object O.

IDENTIFICATION_AND_AUTHENTICATION_FOR_NETWORK_SCAN_SERVICE and O. CONTROL_DATA_ACCESS.

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_FOR_NETWORK_SCAN_SERVICE, O. CONTROL_DATA_ACCESS, and O. IDENTIFICATION_AND_AUTHENTICATION_ON_ADMINISTRATOR

FIA_UID.2 (1) (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.

FIA_UID.2 (2) (User identification before any action)

This component ensures the identification of network scan service users before granting access to the TOE functionality. Therefore, it satisfies security object O.

IDENTIFICATION_AND_AUTHENTICATION_FOR_NETWORK_SCAN_SERVICE.

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.

FPT_RCV.4 (Function recovery)

This component ensures that TSF is recovered to a stable and safe state from pre-defined errors. Therefore, it satisfies security object O.IMAGE_OVERWRITE.

5.3.2 Rationale for the TOE Assurance Requirements

This Samsung MFP Security Kit Type_A 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.

5.3.3 Rationale 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 has a subordinate relationship with FMT_MSA.3. But because the security properties of fax image used in SFP_FLW are not an object for management, FMT_MSA.3 is not required. Therefore, the subordinate relationship is not satisfied.

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	FAU_STG.1	FAU_GEN.1	1
5	FAU_STG.4	FAU_STG.1	4
6	FDP_IFC.1	FDP_IFF.1	7
7	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	6, #
8	FDP_RIP.1	-	-
9	FIA_AFL.1(1)	FIA_UAU.1	11, 12 (Hierarchically by FIA_UAU.2(1),(2))
10	FIA_AFL.1(2)	FIA_UAU.1	11 (Hierarchically by FIA_UAU.2(1))
11	FIA_UAU.2(1)	FIA_UID.1	14 (Hierarchically by FIA_UID.2(1))
12	FIA_UAU.2(2)	FIA_UID.1	15 (Hierarchically by FIA_UID.2(2))
13	FIA_UAU.7	FIA_UAU.1	11, 12 (Hierarchically by FIA_UAU.2(1),(2))
14	FIA_UID.2(1)	-	-
15	FIA_UID.2(2)	-	-
16	FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	18, 19
17	FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	18, 19
18	FMT_SMF.1	-	-
19	FMT_SMR.1	FIA_UID.1	14 (Hierarchically by FIA_UID.2(1))
20	FPT_RCV.4	-	-

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.

- Network Authentication (TSF_NAU)
- Data Access Control (TSF_DAC)
- Security audit (TSF_FAU)
- Security management (TSF_FMT)
- System Authentication (TSF_SAU)
- Image overwrite (TSF_IOW)
- Information flow (TSF_FLW)

6.1.1 Network Authentication (TSF_NAU)

The TOE can prevent unauthorized use of the installed network options - network scan, scan-to-email, and scan-to-server. To access network scan service, a client is required to enter an ID and password which are then validated by the designated authentication server. Only web administrators can create, change or delete the user accounts. The authentication process is delayed for 3 minutes when 3 wrong passwords are entered in succession. The TOE continuously maintains authorized user's account during job performed. During authentication process, TOE provide only Domain name or user account and password which is displayed by asterisk(*) for attackers to prevent getting user information.

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

6.1.2 Data Access Control (TSF_DAC)

The TOE controls data access to the stored document which users stored as security property. In the Stored Documents feature, the documents can be stored using two methods: Public or Secured. When a user stores documents as Public, all users can access and use the files. Files stored as Secured only allow the user who stored the file to access the file with a PIN. When storing a Secured file, the user must enter a PIN to secure the file. When accessing the file, the user must enter the PIN again.

Relevant SFR: FIA_UAU.2(2), FIA_UAU.7

6.1.3 Security Audit (TSF_FAU)

The TOE track events/actions (e.g., print/scan/fax job submission) for 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 viewing 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
3	ODIO started	Device name, Serial number of the device
4	ODIO complete	Device name, Serial number of the device, Completion status
5	Print Job	Job name, User name, Completion status, IIO job status, SyncThru user’s account
6	Network scan job	Job name, User name, Completion status, IIO job status, SyncThru user’s account, total number of the destination address, Destination address
7	Server fax job NOTE: This item is not for the TOE Evaluation.	Job name, User name, Completion status, IIO job status, SyncThru user’s account, Total number of the fax number to receive , Fax number to receive, Destination address
8	IFAX	The TOE does not support this function. NOTE: This item is not for the TOE Evaluation.
9	Scan-to-email job	Job name, User name, Completion status, IIO 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, IIO job status, SyncThru user’s account
13	Embedded fax job	Job Type (Sending fax, Receiving fax), Job name, User name, Completion status, IIO 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, IIO 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 about security audit function, image overwriting start/completion, inquiry/change about security audit configuration, and recovery from failure of image overwriting job. 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 viewing 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, FAU_STG.1, FAU_STG.4,

6.1.4 Security 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, configure how to get certification for network scan service, create/change/delete the accounts of network scan service user, change the account of a web administrator, etc. Local administrators can manage the following functions: change PIN of local administrator, enable/disable/start/stop the image overwriting function, etc. General users can perform the following functions: configure security printing on the stored documents on the hard disk drive.

TSF data that stated in Table 19: Authentication information of local administrator, Authentication information of web administrator, Enable or disable IIO setting value for local administrator, Enable or disable security audit setting value for web administrator, user account information of network scan service, configuration information for network scan service user. Web administrators must select among **No Authentication**, **Require Network Authentication** or **Require Local Authentication** for network scan service. When using **Require Local Authentication** option, the TOE stores user account information on the hard disk drive of the MFP, then the network administrator can manage them safely. Only web administrators can create/change/delete the account information. When using **Require Network Authentication** option, user information can be stored on an authentication server. The users must be authenticated by entering their account ID and password prior to being granted access to network scan service. That is assuming that the authentication server and remote authentication service are managed safely.

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

Security Function	Action	Role
Enable security audit function	Disable, Enable	Web administrator
Download security audit log	Determine the behavior of	Web administrator
Configure how to get certification for network scan service	Determine the behavior of	Web administrator
Create/change/delete the account of network scan service users at local authentication.	Determine the behavior of	Web administrator
Change the account of web administrator	Determine the behavior of	Web administrator
Change local administrator's PIN number	Determine the behavior of	Local administrator
Image Overwrite	Disable,Enable,Determine the behavior of, Modify the behavior of	Local administrator

Table 19: 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
Configurations on the network scan service authentication.	Query, Modify	Web administrator
User certificate information of network scan service.	Query, Modify, Delete	Web administrator

Record security audit log.	Download	Web administrator
Authentication information for local administrator.	Modify	Local administrator
Configurations on IIO enabling/disabling of local administrator.	Query, Modify	Local administrator

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

6.1.5 System 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 3 wrong passwords are entered in succession in a local user interface. If 3 wrong passwords were entered 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(1), FIA_UAU.7, FIA_UID.2(1)

6.1.6 Image Overwrite (TSF_IOW)

The TOE provides Image Overwrite functions that delete the stored file from the hard disk drive. The Image Overwrite function consists of IIO and ODIO. The TOE implements an image overwrite security function (IIO) to overwrite temporary files created during the copying, printing, network scan, scan-to-email, or scan-to-server processes. Also, users can delete their own files stored in the TOE.

The image overwrite security function can also be invoked manually only by the system administrator (ODIO). Once invoked, the ODIO cancels all print and scan jobs, halts the printer interface (network), overwrites the contents of the reserved section 3 times on the hard disk, and then the main controller reboots. If there are any problems during overwriting, the ODIO job automatically restarts to overwrite the remaining area.

Relevant SFR: FDP_RIP.1, FPT_RCV.4

6.1.7 Information 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 copying, 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 using SMTP servers through the internal network. When malignant codes are discovered, the TOE destroys the fax image. Fax security functions follow the Information Flow policy (SFP_FLW).

The information flow policy (SFP_FLW) is as follows:

Direct access to a received fax image from the fax modem to the user PC through the internal network is not possible. Communication can be made only through 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.1, FDP_IFF.1

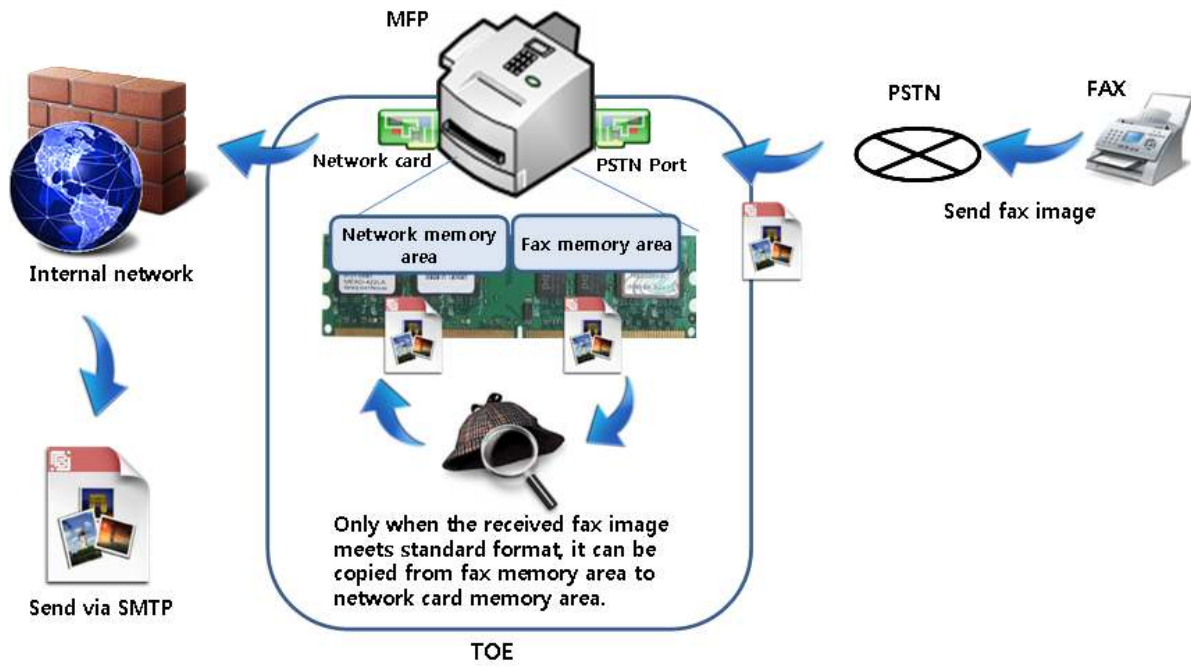


Figure 4: Information Flow Summary

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

	TOE Security Function						
	Network Authentication	Data Access Control	Security Audit	Security Management	System Authentication	Image overwrite	Information flow
FAU_GEN.1			X				
FAU_SAR.1			X				
FAU_SAR.2			X				
FAU_STG.1			X				
FAU_STG.4			X				
FDP_IFC.1							X
FDP_IFF.1							X

FDP_RIP.1						X	
FIA_AFL.1(1)	X				X		
FIA_AFL.1(2)					X		
FIA_UAU.2(1)					X		
FIA_UAU.2(2)	X	X					
FIA_UAU.7	X	X			X		
FIA_UID.2(1)					X		
FIA_UID.2(2)	X						
FMT_MOF.1				X			
FMT_MTD.1				X			
FMT_SMF.1				X			
FMT_SMR.1				X			
FPT_RCV.4						X	