

KECS-CR-17-64

# Samsung Multifunction M4560, M4562 Series 인증보고서

인증번호 : KECS-CISS-0828-2017

2017년 9월



IT보안인증사무국

# 1. 제품 개요

Samsung Multifunction M4560, M4562 Series (이하 'TOE' 로 명시)은 복사(copy), 프린트(print), 스캔(scan) 및 팩스(fax) 기능을 제공하는 복합기(MFP, Multi-Function Peripherals)이다.

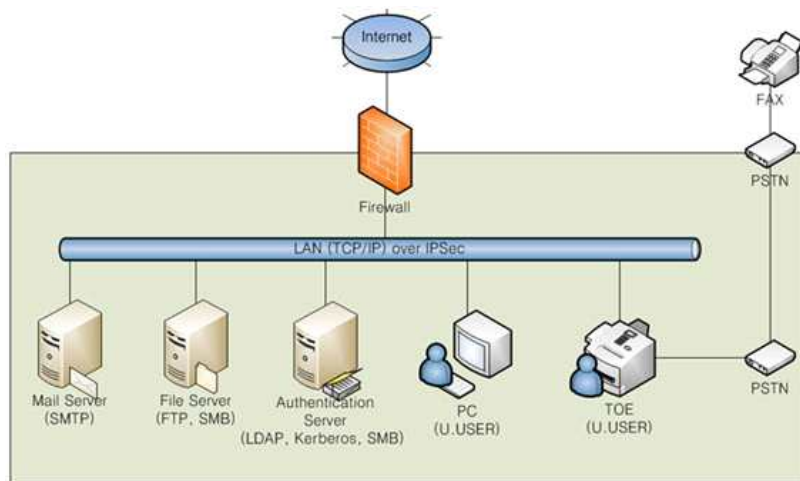
TOE는 식별 및 인증, TOE 기능 접근통제, 네트워크 접근통제, 보안관리, 감사 데이터 생성/조회/보호, 데이터 완전삭제, 데이터 암호화, 자체 시험, 팩스 데이터 통제 및 안전한 통신 등의 TOE 보안기능과 복사, 프린트, 스캔, 팩스 등의 MFP 기본기능을 제공한다.

TOE 참조 정보는 다음과 같이 식별된다.

구 분	내 용
TOE 명	Samsung Multifunction M4560, M4562 Series
TOE 버전	V1.00
TOE(펌웨어)	V5.00.01.23 (Samsung M456x series_V5.00.01.23.hds)
설명서	Samsung Multifunction M4560, M4562 Series 사용 설명서 V1.1
	Samsung Multifunction M4560, M4562 Series 설치 설명서 V1.0

[표 1] TOE 참조 정보

TOE가 동작하는 운영환경은 [그림 1]과 같다.



[그림 1] TOE 운영환경

TOE의 전용 하드웨어 모델 요구사항은 [표 1]과 같다.

MFP Model		M4560FX	M4562FX
Color/Mono		Mono	Mono
PPM		45ppm	45ppm
Processor		A3000 (1.5GHz)	
RAM		DDR3 3GB	
ROM		eMMC 4GB	
Interface		High-Speed USB 2.0 Host, High-Speed USB 2.0 Peripheral, Ethernet 10/100/1000 Base TX	
FAX		ITU-T G3, Super G3, 3sec @33.6 Kbps, MH/MR/MMR/JBIG	
HDD		SATA2 320GB	
Scanner		ADF	
		Up to A4 size	Up to Legal size
Display (LUI)	General Spec	7" 800 x 480 WVGA TFT Color Graphic LCD with Touch-Screen, 24-bit color	

[표 2] MFP 모델별 사양

TOE에 포함되는 펌웨어 및 소프트웨어 버전은 [표 3]과 같다.

MFP Model		M4560FX	M4562FX
TOE version		V1.00	
System Firmware		V5.00.01.23 (Samsung M456x series_V5.00.01.23.hds)	

[표 3] TOE 복합기 모델 및 펌웨어

**인증 효력에 관한 고지:** 상기 제품의 인증서는 IT보안인증사무국 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

## 2. 주요기능

TOE가 제공하는 보안기능은 다음과 같다.

### ■ 식별 및 인증(Identification and Authentication Function)

TOE는 로컬 인터페이스인 LUI(Local User Interface) 및 네트워크 인터페이스인 RUI(Remote User Interface)를 통해 MFP 기본기능 및 보안관리 기능에 접근하는 모든 사용자에게 대해 식별 및 인증 기능을 강제한다. TOE는 복합기 내부에 등록된 사용자 계정 정보(ID, Password)를 이용한 로컬 인증 방식(Local Authentication Method)과 TOE 운영환경에서 제공되는 외부 인증 서버(Kerberos 서버, LDAP 서버, SMB 서버)를 이용한 외부 인증 방식(External Authentication Method)의 2가지 사용자 인증 모드를 제공한다.

로컬 인증 방식은 인가된 관리자가 TOE에 등록한 사용자 계정 정보를 기반으로 사용자에게 대한 식별 및 인증을 수행하며, 외부 인증 방식은 TOE 운영환경 내에 운영중인 신뢰된 인증 서버를 통해 해당 사용자에게 대한 식별 및 인증 결과를 응답받아 식별 및 인증기능을 수행한다.

또한, TOE는 사용자 식별 및 인증 과정에서 사용자의 보안속성(User ID, User Group ID, User Role)을 기반으로 사용자 문서에 대한 읽기/삭제/수정 연산을 통제하는 일반 접근 통제(Common Access Control) 및 MFP 기본기능(프린트, 스캔, 복사, 팩스)에 대한 실행 권한을 통제하는 TOE 기능 접근 통제(TOE Function Access Control)를 강제한다.

사용자의 식별 및 인증 과정에서 연속적인 인증 실패 횟수가 정의된 횟수(3회)에 도달하는 경우 해당 사용자에게 대해 일정 시간(5분)동안 인증 시도를 제한하며, 사용자가 로그인 이후 일정 시간(3분) 동안 아무런 활동을 수행하지 않을 경우 해당 사용자에게 대해 세션 종료 기능을 수행한다.

### ■ 네트워크 접근통제(Network Access Control Function)

TOE는 네트워크 인터페이스를 통해 데이터를 송·수신하기 위해 프로토콜/포트 통제, IP 주소 필터링, MAC 주소 필터링의 네트워크 접근통제 기능을 제공한다.

프로토콜/포트 통제는 인가된 관리자 설정에 따라 TOE에서 제공하는 네트워크 프로토콜을 활성화/비활성화하여 해당 네트워크 프로토콜을 통해 TOE로의 접근을 허용하거나 차단할 수 있다. TOE에서 제공하는 네트워크 프로토콜은 표준 TCP/IP 인쇄, LPR/LPD, IPP, WSD, SNMPv1/v2, SNMPv3, HTTP 프로토콜 등이 있으며, 모든 네트워크 인터페이스 및 프로토콜은 초기에 비활성화 상태로 설정되어 있다.

IP 주소 필터링과 MAC 주소 필터링에서 인가된 관리자는 IP 주소와 MAC 주소를 이용하여 필터링 규칙을 구성할 수 있다. IP 필터링 정책에서는 인가된 관리자에 의해 등록된 IP 필터링 규칙에 부합하는 경우에만 허용하며, MAC 필터링 정책에서는 인가된 관리자에 의해 등록된 MAC 필터링 규칙에 부합하는 경우 차단하는 기능을 수행한다.

## ■ 보안관리(Security Management)

TOE는 식별 및 인증 절차를 성공적으로 마친 인가된 사용자만이 로컬 인터페이스(RUI) 및 네트워크 인터페이스(LUI)를 통해 MFP 기본기능 관련 설정 및 TOE 보안 관리 기능을 수행할 수 있는 기능을 제공하며, TOE 사용자는 역할에 따라 관리자와 일반 사용자로 구분된다. 관리자는 TOE에 대한 보안관리를 수행할 수 있는 권한이 부여되며, 일반 사용자는 TOE 보안관리 권한은 부여되지 않고 인가된 관리자에 의해 부여된 역할에 따라 MFP 기본기능(프린트, 복사, 스캔, 팩스)을 사용 및 자신의 패스워드 변경을 수행하도록 허용된다. TOE의 인가된 관리자에게 제공되는 보안관리 기능은 다음과 같다.

- 제품설정 : 시스템, 프린터, 복사, 빠른/ID 복사, 팩스, 스캔 및 전송, 전자메일 알림
- 네트워크 설정 : 일반, 인터페이스, IP 라우팅, 네트워크 프로토콜
- 시스템 보안 : 시스템 관리자, 기능 관리, 정보 은닉, 재 부팅, 고급 보안
- 네트워크 보안 : 디지털 인증서, 보안 연결, SNMPv3, IP 보안, IP/MAC 필터링, 외부 인증 서버 등
- 사용자 접근 제어 : 인증, 권한, 계정, 사용자 프로필
- 시스템 로그 : 로그 설정, 로그 정보

## ■ 보안감사(Audit Log Function)

TOE는 운영 과정에서 발생하는 감사대상 사건에 대해 작업 로그(job log), 보안 이벤트 로그(security event log), 운영 로그(operation log)로 구분하여 감사 데이터를 생성하여 하드디스크에 저장하며, 인가된 관리자만이 네트워크 인터페이스(RUI)를 통해 모든 감사 데이터를 조회할 수 있는 기능을 제공한다.

TOE는 감사저장소에 저장된 감사 데이터에 대해 비인가된 삭제 또는 변경으로부터 보호하는 기능을 제공하고, 감사 저장소가 포화 임계치를 도달하는 경우 가장 오래된 감사 데이터를 삭제하여 감사 데이터의 손실을 방지한다.

## ■ 완전삭제(Image Overwrite Function)

TOE는 하드디스크(HDD)에 저장된 사용자 데이터에 대하여 이미지 덮어쓰기를 통해 완전삭제 기능을 수행한다. 완전삭제 기능은 사용자가 MFP 기본기능(프린트, 복사, 스캔, 팩스) 실행 과정에서 생성되는 임시 파일(temporary files)에 대해 작업이 완료되거나 취소되었을 경우 자동으로 덮어쓰기를 수행하는 자동완전삭제(Automatic Image Overwrite) 기능과 인가된 관리자가 로컬 인터페이스(LUI)를 통해 완전삭제 기능을 호출하여 HDD에 저장된 데이터에 대해 덮어쓰기를 실행할 수 있는 수동완전삭제(Manual Image Overwrite) 기능의 2가지 방식이 제공된다.

완전삭제 기능은 인가된 관리자가 설정한 완전삭제 알고리즘에 따라 완전삭제를 수행하며, TOE는 다음과 같은 5가지 방식의 완전삭제 알고리즘을 제공한다.

- DoD 5220.28-M : 3회 덮어쓰기
- DoD 5220.22-M(ECE) : 7회 덮어쓰기
- Australian ASCI 33 : 5회 덮어쓰기
- German standard(VSITR) : 7회 덮어쓰기
- Custom : 관리자 설정에 따라 1~9회 덮어쓰기(기본값 2회)

■ 데이터 암호화(HDD Data Encryption Function)

TOE는 HDD로 데이터(임시 파일, 문서 데이터, 시스템 데이터)를 저장되는 과정에서 해당 파티션에 대해 암호화(AES256) 기능을 제공하고, HDD에 저장된 데이터를 접근하는 과정에서 복호화(AES256) 기능을 수행한다. TOE는 최초 구동 시 암호키로 사용되는 비밀키(256 bits)를 생성하며, 생성된 비밀키는 사용자가 접근 불가능하도록 암호화하여 안전하게 보관한다. 한번 생성된 비밀키는 별도의 파기 명령이 존재하지 않지만, TOE 부팅 시 비밀키에 대한 해쉬값을 비교하여 일치하지 않는 경우 새로운 비밀키를 생성하고 기존에 저장된 비밀키를 덮어쓰기하여 새로운 비밀키로 교체한다.

■ 팩스 데이터 통제(Fax Data Control Function)

팩스 데이터를 통한 악의적인 공격을 방어하기 위해 TOE는 수신된 모든 팩스 데이터가 팩스 이미지 표준 형식(MMR, MR, 또는 MH of T.4)에 부합되는지 검사를 수행하고, 팩스 이미지 표준 형식에 위배되는 팩스 이미지가 발견되는 경우 파기하는 기능을 제공한다. 정상적으로 수신된 팩스 데이터는 인가된 관리자에 의해 인쇄물로 출력되거나 외부 파일 서버로(Fax to Email, Fax to FTP, Fax to SMB)로 전송할 수 있다. 팩스 인터페이스는 미리 정의된 팩스 프로토콜에 대해서만 응답하고, 이 외 다른 프로토콜에 대해서는 응답하지 않도록 구현되어 있다.

■ 자체 시험(Self-Testing)

TOE는 초기 시동 과정에서 일련의 자체시험을 수행한다. 자체시험 수행 시 HDD 암호화 기능이 정확하게 운영되는지 검증하고, TSF 데이터(HDD 암호화 키) 및 TSF 실행코드에 대해 SHA-256 알고리즘을 이용하여 해쉬값 비교를 통해 무결성 훼손 여부를 검사한다.

■ 안전한 통신(Secure Communication Function)

TOE는 네트워크 인터페이스를 통해 TOE와 연결된 모든 사용자 및 신뢰된 외부 IT 실체간의 안전한 통신을 위해 IPSec 프로토콜을 사용한다. 사용자 및 신뢰된 외부 IT 실체는 TOE와의 IPSec 통신 시 인가된 관리자가 설정한 Shared Key를 사용하며, 통신 세션의 모든 패킷은 암호화되어 전송된다. IPSec은 TOE 부팅 과정에서 구동되며, IPSec을 사용하는 경우에만 TOE와 네트워크 통신이 허용된다.

### 3. 평가결과 요약

TOE에 대한 평가는 한국아이티평가원에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL2+(ALC\_FLR.2) 평가보증등급을 만족하여, 공통평가기준 1부 330항에 따라 “적합” 한 것으로 평가하였다.

[ 인증제품 식별정보 ]

평가지침	정보보호시스템 평가인증지침 (2016. 6. 27) 정보보호제품 평가인증 수행규정 (2017. 6. 26)
평가제품	Samsung Multifunction M4560, M4562 Series
보호프로파일	U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std.2600.2™-2009)
보안요구사항	없음
보안목표명세서	Samsung Multifunction M4560, M4562 Series Security Target V1.2
평가보고서	Samsung Multifunction M4560, M4562 Series 평가결과보고서 V1.00
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R5
평가방법론	정보보호시스템 공통평가방법론 V3.1 R5
검증필 암호모듈	없음
평가신청인	에스프린팅솔루션주식회사
개발업체	에스프린팅솔루션주식회사
평가기관	(주) 한국아이티평가원