KECS-CR-08-37

삼성SDS SPass V1.0
인증결과보고서

인증번호 : KECS-ISIS-0120-2008

2008년 9월

IT보안인증사무국

제·개정 이력 현황

개정 번호	제·개정일	개정쪽	제·개정내용
00	2008.9.24	-	최초 작성

본 문서는 삼성에스디에스(주)의 삼성SDS S*Pass* V1.0에 대한 인증결과보고서이다.

인증위원

행정안전부 장영환, 국가보안기술연구소 윤이중,
고려대학교 차성덕, 성신여자대학교 서동수,
호서대학교 하재철, 동서대학교 이훈재

인증기관

IT보안인증사무국

평가기관

한국정보보호진흥원

목 차

1. 요약

본 보고서는 삼성SDS S*Pass* V1.0에 대한 정보보호시스템 공통평가기준(2008년 7월 16일 고시)(이하 '공통평가기준'이 한다) EAL4+ 평가결과에 대한 인증기관의 인증결과를 서술한다. 본 보고서는 평가결과의 타당성 및 적합여부를 서술한다.

삼성SDS S*Pass* V1.0에 대한 평가는 한국정보보호진흥원이 수행하였으며, 2008년 8월 29일에 평가가 완료되었다. 본 보고서의 내용은 한국정보보호진흥원에서 제출한 평가결과보고서의 내용에 기초하여 작성되었다. 평가는 제품이 공통평가기준 2부와 ADV_IMP.2, ALC_DVS.2 ATE_DPT.2와 AVA_VLA.4가 추가된 EAL4 평가보증등급의 요구사항 3부를 만족함에 따라 "적합"한 것으로 평가하였다.

TOE는 '전자여권 보호프로파일 V1.0'에서 요구하는 BAC, EAC 등 모든 보안 메커니즘을 제공하며, 추가적으로 IC칩의 진위성을 입증하기 위한 AA를 구현하고 있다.

구분	식 별 자	비 고
TOE	삼성SDS SPass V1.0	
	- 삼성SDS MULTOS SM30 R3	[MULTOS 규격]에 따라 구현된 개방형 운영체제(이하 "SM30")이라 한다.
	- SPass LDS 응용프로그램 V1.0	[전자여권 규격] 및 [EAC 규격]에 따라 구현된 전자여권 응용프로그램 이하 "전자여권 응용프로그램"이라 한다.
하 부 IC칩	S3CC9GC 또는 S3CC9GW	독일 인증기관 BSI에 의해 EAL4+ 등급으로 인증된 삼성전자 IC칩

인증기관은 평가자의 평가활동 및 시험절차를 점검하고, 기술적인 문제점 및 평가절차에 대한 지침을 제공하고, 각 평가단위 및 평가결과보고서의 내용을 검토하였다. 인증기관은 평가결과가 평가제품이 보안목표명세서에 서술된 모든 보안기능 요구사항 및 보증요구사항을 만족함을 보증함을 확인하였다. 따라서, 인증기관은 평가자의 관찰사항, 평가결과가 정확하고 타당하다고 인증하였다.

인증 효력범위 : 본 인증결과보고서에 포함된 정보는 삼성SDS S*Pass* V1.0이 대한민국 정부기관에 의한 사용 승인 또는 삼성SDS S*Pass* V1.0에 대한 품질보증을 의미하지 않는다.

2. 식별정보

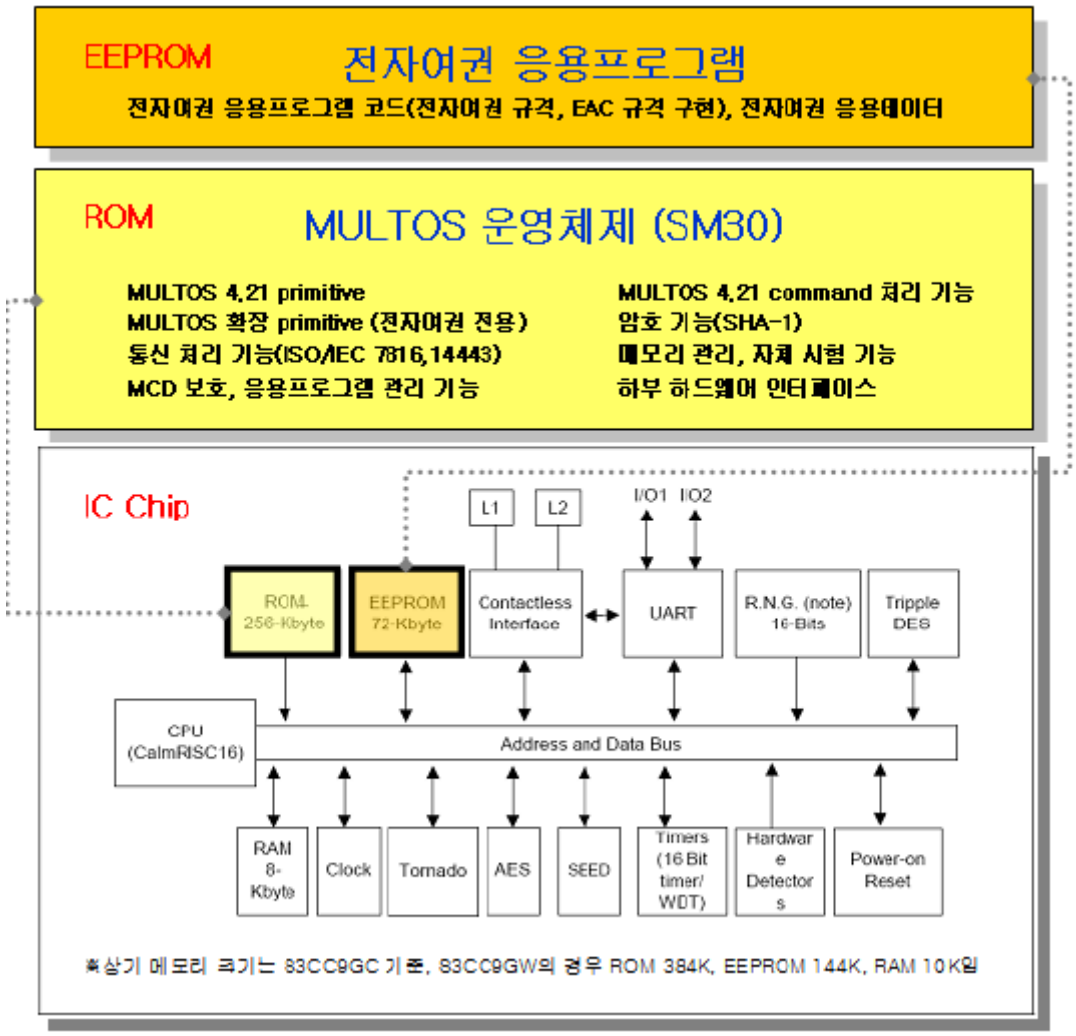
다음 [표 1]은 평가제품 식별을 위한 정보를 나타낸다.

[표 1] 평가대상제품 식별정보

평가지침	정보보호시스템 평가·인증 지침 (2008. 7. 16) 정보보호제품 평가인증 수행규정 (2007. 12. 1)
평가제품	삼성SDS *SPass* V1.0
보호프로파일	전자여권 보호프로파일 V1.0 (KECS-PP-0084-2008, 2008.1)
보안목표명세서	삼성SDS *SPass* V1.0 보안목표명세서 V2.21
평가보고서	삼성SDS *SPass* V1.0 평가보고서, 발행버전 1.0 (2008.8.29)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V2.3 (2008. 7.16)
평가방법론	정보보호시스템 공통평가방법론 V2.3 (2008. 7.16)
평가신청인	삼성에스디에스(주)
개발업체	삼성에스디에스(주)
평가자	한국정보보호진흥원 평가기획팀 유연정 기술보증팀 이성재, 이은경 평가서비스팀 유희준
인증담당자	IT보안인증사무국

2.1 물리적 범위

전자여권은 여권책자와 여권책자 표지에 내장되는 전자여권 IC 칩 및 안테나를 의미한다. 전자여권 IC 칩은 IC 칩 운영체제, 전자여권 응용프로그램, 전자여권 응용데이터 및 IC 칩 구성요소를 포함한다. IC 칩 구성요소는 중앙처리장치, 암호연산전용 프로세서, 입출력 포트, 메모리(RAM, ROM, EEPROM)와 비접촉식 인터페이스 등으로 구성된다. TOE는 IC칩 운영체제인 SM30, 전자여권 응용프로그램, 전자여권 응용데이터로 정의하며 IC칩 구성요소는 TOE 범위에서 제외한다.



[TOE 물리적 범위]

2.2 논리적 범위

TOE의 IT보안기능	설명
암호지원 (CS)	• 암호키 관리(CS1): BAC 인증키, BAC 세션키, EAC 세션키 생성을 위한 키유도. BAC 세션키 생성용 KDF Seed 값 분배. EAC 세션키 생성용 KDF Seed 값 분배 • 암호연산 지원(CS2): BAC 또는 EAC 안전한 통신채널에 사용되는 세션키를 생성하기 위하여 SHA-1 해시 생성
데이터 보호 (DP)	• 전송데이터 무결성 및 비밀성(DP1): BAC 세션용 암호키 또는 EAC 세션용 암호키를 사용한 암호 통신. BAC 세션용 MAC키 또는 EAC 세션용 MAC키를 사용한 무결성 보호 통신. 변경 탐지 시 통신채널을 종료. 발급단계에서 TOE와 발급기관간에 전송되는 데이터 변경 탐지 시 발급기관 세션 종료 • 부분적인 잔여정보 보호(DP2): 세션 종료 시 BAC 세션키 및 EAC 세션키 삭제. 임시 메모리에 자원 회수 시 '0'으로 덮어쓰기 • 비대칭키 기반의 데이터 인증(DP3): AA를 위한 전자서명 생성
식별 및 인증 (IA)	• 개방형운영체제 인증 메커니즘(IA1): 발급기관 인증, MULTOS 응용프로그램 식별 및 인증 • 전자여권 인증 메커니즘(IA2): BAC 상호인증, EAC-TA 인증 • 비접촉식 통신(IA3): 판독시스템 식별 • 다중 인증 메커니즘(IA4): BAC 상호인증, EAC-TA 인증, 발급기관 인증, MULTOS 응용프로그램 인증 메커니즘 규칙 적용 • 인증 실패 처리(IA5): 인증 실패 시 세션 종료 및 해당 기능 비활성화 등 대응행동 수행
보안 관리 (SM)	• 개방형운영체제의 보안 관리(SM1): MCD 활성화, 응용프로그램 탑재/삭제를 위한 개방형운영체제 접근통제 기능. 개방형운영체제 접근통제 규칙의 보안속성 관리 • 전자여권의 보안 관리(SM2): 발급기관에 대한 전자여권접근통제 기능. 판독시스템과 통신 시 전자여권 접근통제 기능. 전자여권 접근통제 규칙의 보안속성 관리. BAC 통신 채널 종료 시 SSC를 '0'으로 초기화한 후 EAC 통신 채널 형성. EAC-TA 시 인증서 체인 검증. CVCA 인증서 관련 정보, AA 인증 개인키, 발급기관 발급키, 생명주기 설정값 등 업데이트
플랫폼 보호 (PP)	• 장애 시 안전한 상태 유지(PP1): 난수 생성기 검증 시 난수성이 허용된 오차를 초과하는 경우 세션을 종료함으로써 안전한 상태 유지. IC 칩이 제공하는 Detector를 사용하는 비정상 동작 시 세션 종료하고 정상 동작 범위에 돌아올 때까지 리셋 상태 유지. TSF 데이터 및 실행코드 무결성 검증 실패 시 세션 종료하여 안전한 상태 유지

	• TSF 우회 불가성 및 영역 분리(PP2): 지정된 명령어 이외에는 TSF 데이터에 대한 접근 불가. 보호 메모리와 비보호 메모리 분리하여 외부 인터페이스에서 직접적으로 보호 메모리에 접근 불가하게 영역 분리. 응용프로그램 탑재 시 블록을 설정하여 설정된 범위 내에서만 수행되도록 통제 • 자체시험을 통한 무결성 검증(PP3): TSF 실행코드의 지정된 영역 무결성 확인. 매번 명령어 수행 시 MSM 활성화 데이터의 무결성 확인. 정규 운영 동안 주기적으로 난수 생성기의 난수성을 검증하는 기능을 시험함으로써 개방형운영체제 자체 시험

3. 보안정책

평가제품은 아래와 같은 보안정책을 준수하여 운영된다.

P.국제적호환성

전자여권 발급기관은 발급된 전자여권의 보안메커니즘과 국외 입국 심사를 위한 판독시스템의 보안메커니즘 호환성을 보장해야 한다.

응용 시 주의사항 : 전자여권 규격 및 EAC 규격을 준수하여 국제적호환성을 보장하여야 한다.

P.보안메커니즘적용절차

TOE는 전자여권 발급기관의 전자여권 접근통제 정책에 위배되지 않도록 판독시스템 유형에 따른 보안메커니즘 적용순서를 보장하여야 한다.

응용 시 주의사항 : TOE는 판독시스템이 지원하는 보안메커니즘 종류에 따라 동작흐름이 달라진다. 기본 동작흐름은 EAC 규격의 2.1.1절에 서술된 표준 전자여권 판독절차(Standard ePassport Inspection Procedure)와 2.1.2 보안강화 전자여권 판독절차(Advanced ePassport Procedure)를 따른다.

P.응용프로그램탑재

전자여권 발급기관은 전자여권 IC칩에 탑재되는 응용프로그램이 TOE의 안전성에 영향을 미치지 않는지 확인한 후 탑재를 승인하여야 한다.

응용 시 주의사항 : 응용프로그램 탑재는 발급기관과 동등한 권한을 가진 기관만이 할 수 있다.

P.전자여권발급기관

전자여권 발급기관은 발급 주체가 변경되지 않았음을 확인할 수 있도록 전자여권을 안전하게 발급하여야 하며 발급 이후 전자여권 IC칩 내의 데이터가 정상적으로 동작함을 검증한 후 사용 단계로 넘겨야 한다. 발급기관은 TOE를 사용 단계로 전달하기 전에 쓰기 기능을 비활성화 시켜야 한다.

P.전자여권접근통제

전자여권 발급기관 및 TOE는 전자여권 응용 데이터를 보호하기 위하여 전자여권 접근통제 정책을 수립하여야 한다. 또한, TOE는 사용자 역할을 규정해야 한다.

응용 시 주의사항 : TOE는 전자여권 규격 및 EAC 규격에 따라 다음과 같이 접근통제 정책을 수립해야 한다.

		객체목록	객체									
			전자여권 신청인 기본정보		전자여권 신청인 바이오정보		전자여권 인증정보		EF.CVCA		EF.COM	
주체목록			읽기 권한	쓰기 권한	읽기 권한	쓰기 권한	읽기 권한	쓰기 권한	읽기 권한	쓰기 권한	읽기 권한	쓰기 권한
주체	BIS	BAC권한	허용	거부	거부	거부	허용	거부	거부	거부	허용	거부
	EIS	BAC권한	허용	거부	거부	거부	허용	거부	허용	거부	허용	거부
		EAC권한	허용	거부	허용	거부	허용	거부	허용	거부	허용	거부
	발급기관	발급권한	허용	허용	허용	허용	허용	허용	허용	허용	허용	허용

P. PKI

전자여권 발급국가는 여권전자서명체계에 따라 PA 및 EAC 보안메커니즘 PKI를 구축하고, 인증업무준칙에 따라 전자서명키를 안전하게 생성·관리하여 인증서 생성, 발급, 운영, 폐지의 인증업무를 수행해야 한다.

또한, 전자여권 발급국가는 인증서 유효기간 관리정책에 따라 인증서를 갱신하여, 검증국가 및 판독시스템으로 안전하게 배포한다. 판독시스템은 TOE에 저장된 EF.CVCA로부터 정보를 획득한 후, EAC-TA 보안메커니즘을 통하여 TOE에게 CVCA 링크인증서, DV 인증서, IS 인증서를 제공하면, TOE는 판독시스템으로부터 제공받은 인증서의 유효성을 검증하고 인증서를 갱신해야 한다.

P.RF통신 범위

전자여권 IC칩과 판독시스템의 RF 통신거리는 5cm이내여야 하며 전자여권의 IC칩 부착 면이 펼쳐지지 않은 경우에는 RF 통신채널이 형성되지 않아야 한다.

4. 가정사항 및 범위

4.1 가정사항

평가제품은 아래와 같은 가정사항을 준수하여 설치 및 운용되어야 한다.

A.인증서검증

BIS, EIS 등 판독시스템은 TOE에 기록된 전자여권 신원정보의 위변조를 검증하기 위해 PA용 인증서 체인(CSCA 인증서→DS 인증서)의 유효성을 검증한 후 SOD를 검증한다. 이를 위해, 주기적으로 DS 인증서 및 CRL을 검증해야 한다.

EIS는 IS 인증서에 대응되는 전자서명생성키를 안전하게 가지고 있어야 하며 EAC-TA 과정에서 TOE에게 CVCA 링크인증서, DV 인증서, IS 인증서를 제공하여야 한다.

A.판독시스템

판독시스템은 출입국 자에 대한 전자여권 검증정책에 따라 전자여권 규격 및 EAC 규격에 따라 PA, AA, BAC, EAC 등 보안메커니즘을 구현해야 한다.

또한, BIS 및 EIS는 BAC 세션키, EAC 세션키, 세션정보 등 TOE와 통신에 사용된 정보를 세션이 종료된 이후에 모두 안전하게 파기해야 한다.

응용 시 주의사항 : TOE는 BAC 상호인증을 성공하지 못한 판독시스템에게는 EF.SOD 접근을 요청하는 경우 거부한다.

BIS는 BAC 및 PA 보안메커니즘을 지원하므로 BAC 인증키를 이용한 BAC 상호인증이 성공하면 전자여권 신청인 기본정보 및 인증정보에 대한 읽기권한을 얻고 BAC 세션키를 이용한 BAC 안전한 통신채널을 형성함으로써 모든 송·수신데이터에 대해 비밀성 및 무결성을 보장한다. BIS는 BAC 수행 이후 PA를 수행하여 SOD를 검증하고 전자여권 신청인 기본정보 및 인증정보의 해시값 계산 및 비교를 통해 전자여권 신청인 기본정보 및 인증정보의 위변조를 검증한다. 이 때 BIS는 AA 보안메터니즘을 옵션으로 지원하는 경우 추가적으로 AA를 수행하여 TOE가 생성한 전자서명에 대한 검증을 통해 TOE의 위변조 여부를 명시적으로 탐지한다.

EIS는 BAC, EAC 및 PA 보안메커니즘을 지원하므로 전자여권 신청인 기본정보 및 인증정보에 대한 읽기권한 뿐만 아니라 전자여권 신청인 바이오정보에 대한 읽기권한을 갖는다. EIS는 BAC 상호인증 및 BAC 안전한 통신채널 형성이 성공되면 TOE의 진위성을 검증하기 위해 BAC 수행과정에서 읽은 EAC 칩인증 공개키를 이용하여 EAC-CA 과정을 수행하고 EAC 칩인증 공개키를 검증하기 위해 PA를 수행한다.

EAC-CA 수행을 성공하면 BAC 안전한 통신채널을 종료하고 EAC 세션키를 이용한 EAC 안전한 통신채널을 다시 시작하여 TOE가 판독 시스템을 인증하는 EAC-TA 과정을 수행한다. EAC-TA를 성공하면 전자여권 신청인 바이오정보 읽기권한을 획득한 것이므로 TOE로부터 전자여권 신청인 바이오정보를 제공받는다.이 때 EIS가 AA 보안메커니즘을 옵션으로 지원하는 경우 EAC-CA와 PA 수행 후 EAC-TA를 수행하기전에 AA를 수행하여 TOE의 위변조 여부를 명시적으로 탐지한다.

A.IC칩

TOE의 하부 플랫폼인 IC칩은 TOE의 보안기능을 지원하기 위해 난수 생성 및 암호연산을 제공하며 정상동작 범위를 벗어나는 경우를 탐지하고, 역공학 분석 및 Probing 등을 이용한 물리적 공격으로부터 TOE를 보호하기 위한 물리적 보호 기능을 제공한다.

응용 시 주의사항 : TOE의 안전성을 보장하기 위해 IC칩은 CCRA EAL4+(SOF-high)이상의 인증제품이어야 한다. IC칩이 지원하는 암호연산은 IC칩의 암호 전용 프로세서 또는 IC칩에 탑재되는 암호라이브러리에서 제공될 수 있다.

A.MRZ엔트로피

BAC 인증키 Seed 값은 BAC 인증키의 안전성을 보장할 수 있는 정도의 MRZ 엔트로피를 갖는다.

응용 시 주의사항 : 높은수준의 위협원으로부터 내성을 가질 수 있기 위해 현재 기술수준으로 MRZ 중 BAC 인증키 Seed 값으로 사용되는 여권번호, 생년월일, 여권 유효기간, Check Digit의 엔트로피는 80bit 이상이어야 하지만, 위험원 수준을 고려한 발급기관의 정책에 따라 정해진 MRZ 엔트로피가 TOE에 적용되므로 기능강도를 반드시 보장할 수는 없다.

4.2 위협 대응범위

전자여권은 물리적으로 통제된 장치 없이 개인이 소지하여 사용하므로, 논리적인 위협과 함께 물리적인 위협도 발생한다.

위협원은 TOE 외부에서 물리적 또는 논리적 방법을 사용하여 TOE가 보호하고자 하는 자산에 불법적인 접근을 시도하는 외부 실체이다.

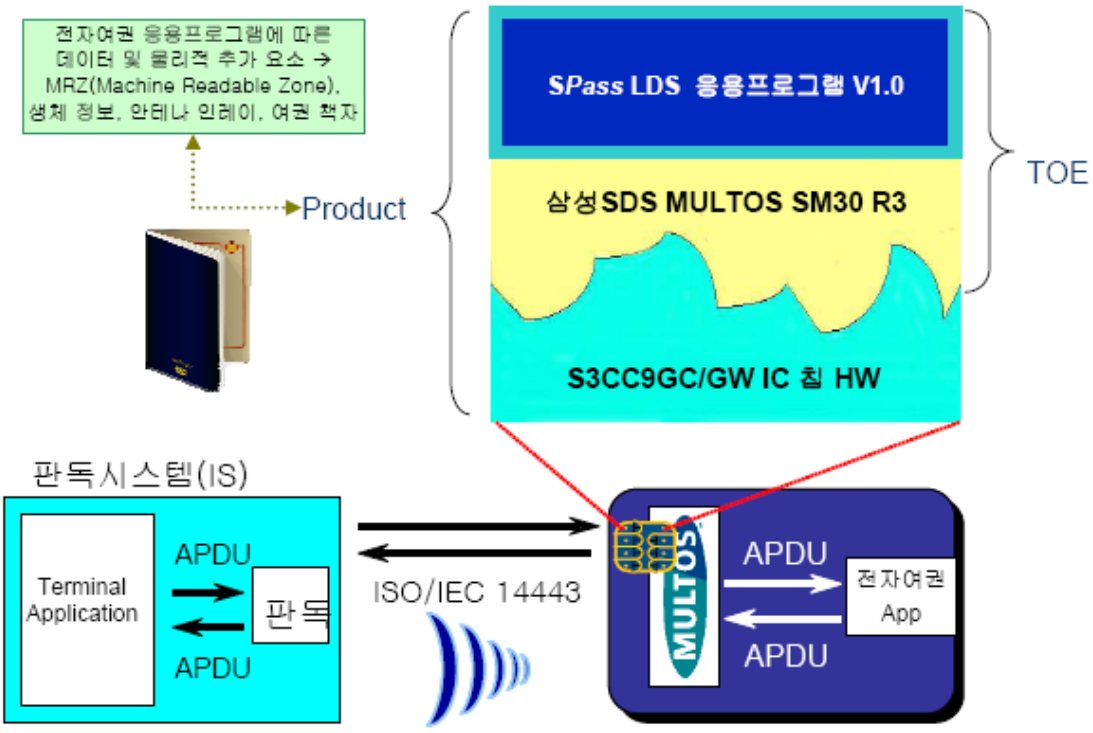
본 인증결과보고서에서는 가정사항 A.IC칩에 따라 TOE를 보호하기 위해 IC칩이 물리적 보호 기능을 제공하므로 높은 수준의 위협원에 의한 IC칩 자체의 물리적 위협은 고려하지 않지만, 그럼에도 불구하고 논리적 방법을 통한 높은 수준의 공격 가능성이 높음을 무시할 수 있다.

따라서 TOE에 대한 위협원은 높은 수준의 전문지식, 자원, 동기를 가지고, 공격자가 악용 가능한 취약성을 발견할 가능성은 높음이다.

5. 제품정보

삼성SDS SPass V1.0 (이하 “TOE”라 한다)은 ‘전자여권 보호프로파일 V1.0’에서 요구하는 보안요구사항에 따라 [전자여권 규격] 및 [EAC 규격]에 따른 보안기능을 구현하고 있으며, IC칩 개방형 운영체제인 MULTOS와 MULTOS에 탑재되는 전자여권 응용프로그램으로 구성된다. 개방형 운영체제인 MULTOS는 [MULTOS 규격]에 따라 하드웨어와 통신, 메모리 관리, 응용프로그램 탑재/삭제 관리 등을 수행하여 전자여권 응용프로그램을 위한 안전한 실행환경을 제공한다.

하부 IC칩인 S3CC9GC 및 S3CC9GW는 접촉식 및 비접촉식 통신을 모두 지원하도록 구현되어 있으나, TOE가 탑재된 전자여권에서 사용되는 경우 IC칩이 동작하도록 활성화하는 단계에서 접촉식 통신을 위한 하드웨어 컨트롤러를 비활성화하여 비접촉식 통신만을 지원하도록 한다.
SM30은 IC칩 위에 임베디드되고, 전자여권 응용프로그램은 SM30과 별개로 구현되어 SM30 위에 탑재된다.



[TOE 개요]

TOE는 전자여권 '전자여권 보호프로파일 V1.0'에서 요구하는 BAC, EAC 등 모든 보안 메커니즘을 제공하며, 추가적으로 IC칩의 진위성을 입증하기 위한 AA를 구현하고 있다.

TOE가 제공하는 IT 보안기능은 다음과 같다.

암호지원 (CS)	• 암호키 관리(CS1): BAC 인증키, BAC 세션키, EAC 세션키 생성을 위한 키유도. BAC 세션키 생성용 KDF Seed 값 분배. EAC 세션키 생성용 KDF Seed 값 분배 • 암호연산 지원(CS2): BAC 또는 EAC 안전한 통신채널에 사용되는 세션키를 생성하기 위하여 SHA-1 해시 생성
데이터 보호 (DP)	• 전송데이터 무결성 및 비밀성(DP1): BAC 세션용 암호키 또는 EAC 세션용 암호키를 사용한 암호 통신. BAC 세션용 MAC키 또는 EAC 세션용 MAC키를 사용한 무결성 보호 통신. 변경 탐지 시 통신채널을 종료. 발급단계에서 TOE와 발급기관간에 전송되는 데이터 변경 탐지 시 발급기관 세션 종료 • 부분적인 잔여정보 보호(DP2): 세션 종료 시 BAC 세션키 및 EAC 세션키 삭제. 임시 메모리에 자원 회수 시 '0'으로 덮어쓰기 • 비대칭키 기반의 데이터 인증(DP3): AA를 위한 전자서명 생성
식별 및 인증 (IA)	• 개방형운영체제 인증 메커니즘(IA1): 발급기관 인증, MULTOS 응용프로그램 식별 및 인증 • 전자여권 인증 메커니즘(IA2): BAC 상호인증, EAC-TA 인증 • 비접촉식 통신(IA3): 판독시스템 식별 • 다중 인증 메커니즘(IA4): BAC 상호인증, EAC-TA 인증, 발급기관 인증, MULTOS 응용프로그램 인증 메커니즘 규칙 적용 • 인증 실패 처리(IA5): 인증 실패 시 세션 종료 및 해당 기능 비활성화 등 대응행동 수행
보안 관리 (SM)	• 개방형운영체제의 보안 관리(SM1): MCD 활성화, 응용프로그램 탑재/삭제를 위한 개방형운영체제 접근통제 기능. 개방형운영체제 접근통제 규칙의 보안속성 관리 • 전자여권의 보안 관리(SM2): 발급기관에 대한 전자여권 접근통제 기능. 판독시스템과 통신 시 전자여권 접근통

	제 기능. 전자여권 접근통제 규칙의 보안속성 관리. BAC 통신 채널 종료 시 SSC를 '0'으로 초기화한 후 EAC 통신 채널 형성. EAC-TA 시 인증서 체인 검증. CVCA 인증서 관련 정보, AA 인증 개인키, 발급기관 발급키, 생명주기 설정값 등 업데이트
플랫폼 보호 (PP)	• 장애 시 안전한 상태 유지(PP1): 난수 생성기 검증 시 난수성이 허용된 오차를 초과하는 경우 세션을 종료함으로써 안전한 상태 유지. IC 칩이 제공하는 Detector를 사용하는 비정상 동작 시 세션 종료하고 정상 동작 범위에 돌아올 때까지 리셋 상태 유지. TSF 데이터 및 실행코드 무결성 검증 실패 시 세션 종료하여 안전한 상태 유지 • TSF 우회 불가성 및 영역 분리(PP2): 지정된 명령어 이외에는 TSF 데이터에 대한 접근 불가. 보호 메모리와 비보호 메모리 분리하여 외부 인터페이스에서 직접적으로 보호 메모리에 접근 불가하게 영역 분리. 응용프로그램 탑재 시 블록을 설정하여 설정된 범위 내에서만 수행되도록 통제 • 자체시험을 통한 무결성 검증(PP3): TSF 실행코드의 지정된 영역 무결성 확인. 매번 명령어 수행 시 MSM 활성화 데이터의 무결성 확인. 정규 운영 동안 주기적으로 난수 생성기의 난수성을 검증하는 기능을 시험함으로써 개방형운영체제 자체 시험

【 TOE IT 보안기능 】

6. 설명서

평가제품이 제공하는 설명서는 아래와 같다:

- 삼성SDS S*Pass* V1.0 관리자설명서 V1.28
- 삼성SDS S*Pass* V1.0 사용자설명서(판독시스템) V1.11
- 삼성SDS S*Pass* V1.0 사용자설명서(MULTOS 응용프로그램 개발자) V1.20

7. 제품시험

7.1 개발자 시험

- **시험방법**

개발자는 제품의 보안기능을 고려하여 시험항목을 도출하였다. 각 시험항목은 시험서에 서술되어 있다. 시험서에 서술된 각 시험항목은 아래의 세부 항목을 포함하고 있다:

- 시험번호/시험자 : 시험항목 식별자 및 시험에 참여한 개발자
- 시험목적 : 시험 대상 보안기능 및 보안모듈을 포함하여 시험의 목적을 서술
- 시험환경 : 시험을 수행하기 위한 세부 시험환경
- 세부 시험절차 : 보안기능을 시험하기 위한 세부 절차
- 예상결과 : 시험절차를 수행하였을 때 나타날 것으로 예상되는 시험결과
- 실제결과 : 시험절차를 실제로 수행하였을 때 나타나는 시험결과
- 예상결과와 실제결과의 비교 : 예상결과 및 실제결과를 비교한 결과

평가자는 시험서의 시험환경, 시험절차, 시험범위 분석, 상세설계 시험 등 시험의 타당성을 평가하였다. 평가자는 개발자의 시험 및 시험결과가 평가환경에 적합함을 검증하였다.

- **시험환경**

시험서에 서술된 시험환경은 시험을 위한 구성, 평가대상제품, 내부망 및 외부망 등 세부 환경을 포함하고 있다. 또한, 각 시험항목을 시험하기 위해 필요한 시험도구 등 세부적인 시험환경을 서술하고 있다.

- **시험범위 분석/상세설계 시험**

세부 평가결과는 ATE_COV 및 ATE_DPT 평가결과에 서술되어 있다.

- **시험결과**

시험서는 각 시험항목의 예상결과 및 실제결과를 서술하고 있다. 실제결과는 실제 제품의 동작화면 뿐만 아니라 감사기록을 통해서도 확인할 수 있다.

7.2 평가자 시험

평가자는 개발자 시험과 동일한 평가환경 및 평가도구를 사용하여 평가제품을 설치하고 개발자가 제공한 시험항목 전체를 시험하였다. 평가자는 모든 시험항목에서 실제결과가 예상결과와 일치함을 확인하였다.

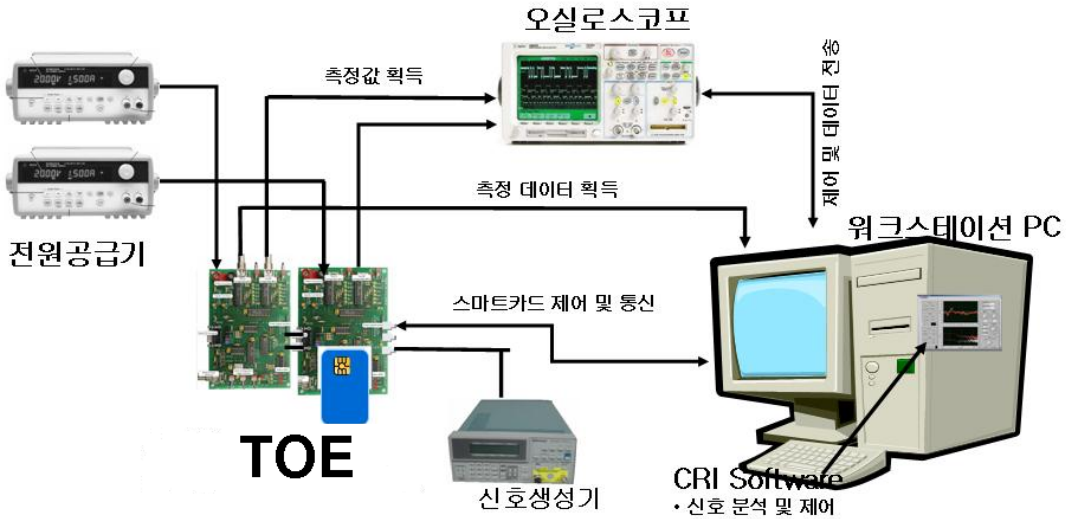
또한, 평가자는 개발자 시험에 기초하여 별도의 평가자 시험항목을 고안하여 시험한 결과, 실제결과가 예상결과와 일치함을 확인할 수 있었다.

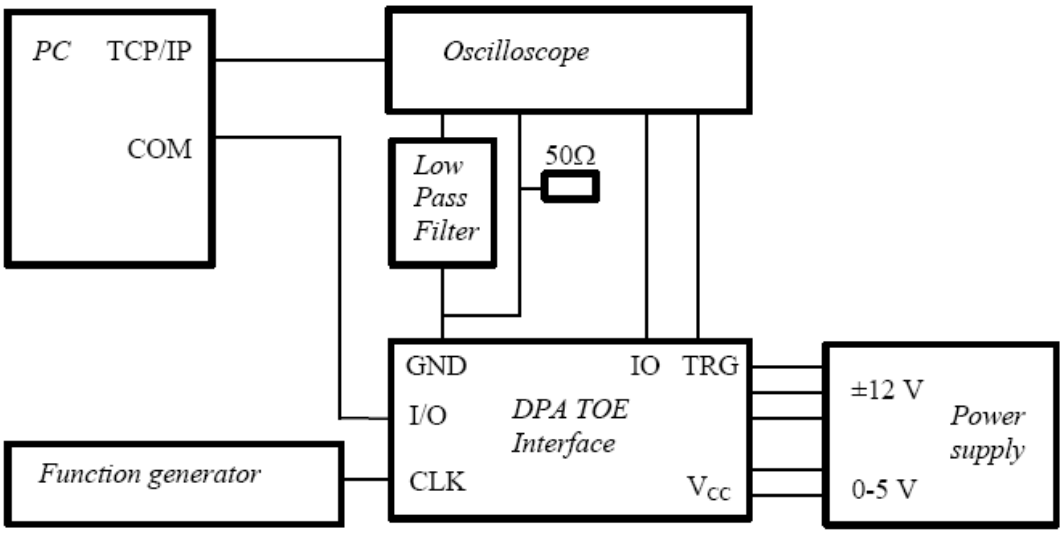
평가자는 취약성 시험을 수행한 결과, 평가환경에서 어떠한 취약성도 악용 가능하지 않다는 점을 확인하였다.

평가자의 시험결과는 평가제품이 설계문서에 서술된 대로 정상적으로 동작됨을 보증하였다.

8. 평가환경

평가자는 시험을 위해서 보안목표명세서에서 명시된 환경구성과 일관성 있게 시험환경은 다음]과 같이 구성하였다.





【 TOE 침투시험 환경구성 】

9. 평가결과

평가는 최신 공통평가기준, 공통평가방법론을 적용하였다. 평가는 평가제품이 공통평가기준 2부, EAL4+ 평가보증등급의 요구사항 3부에 적합하다고 평가하였다. 자세한 평가결과는 평가보고서에 서술되어 있다.

• 보안목표명세서

보안목표명세서 소개는 완벽하고 보안목표명세서의 다른 부분과 일관성이 있으며 보안목표명세서를 정확하게 식별하고 있으므로 ASE_INT.1에 대하여 **통과** 판정을 부여한다.

TOE 설명은 TOE 목적 및 TOE의 기능성을 이해할 수 있도록 설명하고 있으며, 조리 있고 완벽하며 내부적으로 일관성이 있다. 또한 보안목표명세서의 다른 부분과 일관성 있게 서술되어 있으므로 ASE_DES.1에 대하여 **통과** 판정을 부여한다.

보안환경은 TOE와 TOE 보안환경에서 유도된 명확하고 일관된 보안상의 문제를 가정사항, 위협, 조직의 보안정책으로 정의하여 제공하고 있으며, 완전하고 일관성 있게 서술되어 있으므로 ASE_ENV.1에 대하여 **통과** 판정을 부여한다.

보안목적은 식별된 위협을 만족시키며 식별된 조직의 보안정책을 달성하고, 서술된 가정사항을 만족시키고 있으므로 ASE_OBJ.1에 대하여 **통과** 판정을 부여한다.

IT 보안요구사항은 완전하고 일관성 있게 서술되어 있으며, 보안목적을 달성하기 위해 TOE의 개발에 알맞은 기반을 제공하고 있으므로 ASE_REQ.1에 대하여 **통과** 판정을 부여한다.

별도로 명시한 IT 보안요구사항은 공통평가기준을 참조하지 않고 별도로 명시한 모든 TOE 보안요구사항을 식별하고 별도로 명시한 이유를 정당화하며 명확하고 모호하지 않게 표현되어 있으므로 ASE_SRE.1에 대하여 **통과** 판정을 부여한다.

TOE 요약명세는 보안기능과 보증 수단을 정확하고 일관성 있게 정의하고, 서술된 TOE 보안요구사항을 만족하고 있으므로 ASE_TSS.1에 대하여 **통과** 판정을 부여한다.

보안목표명세서는 수용한 보호프로파일을 정확히 실체화하고 있으므로 ASE_PPC.1에 대하여 **통과** 판정을 부여한다.

따라서, “삼성SDS S*Pass* V1.0 보안목표명세서 V2.21”는 위협에 대응하고 보안정책을 수행하는 보안기능을 완전하게 서술하고 있으며, 보안기능이 위협에 대응하고 보안정책을 수행하기에 적절함을 판단하기에 충분하며, ST는 내부적으로 일관성이 있다. 또한 SFRs을 보안기능으로 정확하게 실체화하였다.

• **형상관리**

형상관리 문서는 개발자가 TOE와 TOE에 관련된 형상항목을 명확히 식별하며, 형상항목을 변경하는 능력이 적절하게 통제됨을 입증하므로 ACM_CAP.4에 대해 **통과** 판정을 부여한다.

형상관리 문서는 개발자가 최소한 TOE 구현의 표현, ST의 보증 컴포넌트에서 요구하는 평가증거물, 보안 결함에 대하여 형상관리를 수행함을 입증하므로 ACM_SCP.2에 대해 **통과** 판정을 부여한다.

형상관리 문서는 구현 표현의 변경사항들이 자동화 도구를 사용하여 통제되고 있음을 입증하므로 ACM_AUT.1에 대해 **통과** 판정을 부여한다.

따라서, 형상관리문서는 소비자가 제품이 평가된 TOE임을 식별할 수 있도록 해주며, 형상항목이 유일하게 식별됨을 보장하고, 개발자가 TOE 변경을 통제 및 추적하기 위해 사용한 절차가 적절함을 보장한다.

• **배포 및 운영**

배포 문서는 TOE를 사용자 측에 배포할 때 TOE의 보안을 유지하고 TOE의 변경 및 대체를 탐지하기 위한 모든 절차를 서술하고 있으므로 ADO_DEL.2 컴포넌트에 대해 **통과** 판정을 부여한다.

TOE의 안전한 설치, 생성 시동을 위한 절차 및 단계가 문서화되어 있으며, 그 결과 TOE는 안전하게 구성됨을 확인하였으므로 ADO_IGS.1 컴포넌트에 대해 **통과** 판정을 부여한다.

따라서, 배포 및 운영 문서는 개발자가 의도한 방식과 동일하게 TOE가 설치, 생성, 시동되며, TOE가 변경되지 않고 배포됨을 보장하기에 적절하다.

• **개발**

기능명세는 TOE 보안기능을 적절히 서술하고 있으며, TOE 보안기능이 보안목표명세서의 보안기능요구사항을 만족시키기에 충분함을 설명하고 있다. 또한, TOE 외부 인터페이스를 적절하게 서술하고 있으므로 ADV_FSP.2 컴포넌트에 대해 **통과** 판정을 부여한다.

보안정책모델은 보안정책의 규칙과 특징을 기술하는데 명확하고 일관성이 있으며, 기능명세에 기술된 보안기능과 대응하도록 기술하고 있으므로 ADV_SPM.1 컴포넌트에 대해 **통과** 판정을 부여한다.

기본설계는 TSF를 주요 구성 요소인 서브시스템으로 서술하고 있으며, 서브시스템의 인터페이스를 적절하게 서술하고 있다. 또한 기능명세를 서브시스템으로 정확하게 실현하고 있으므로 ADV_HLD.2 컴포넌트에 대해 **통과** 판정을 부여한다.

상세설계는 TOE 보안기능의 내부 동작을 모듈과 모듈간의 상호관계 및 종속관계에 관하여 서술하고 있다. 상세설계는 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, 기본설계를 정확하고 효과적으로 정교화하고 있으므로 ADV_LLD.1 컴포넌트에 대해 **통과** 판정을 부여한다.

구현의 표현은 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, 상세설계를 정확하게 실현하고 있으므로 ADV_IMP.2 컴포넌트에 대해 **통과** 판정을 부여한다.

표현의 일치성은 개발자가 보안목표명세서의 요구사항을 기능명세, 기본설계, 상세설계, 구현의 표현으로 정확하게 완벽하게 구현했음을 보여주고 있으므로 ADV_RCR.1 컴포넌트에 대해 **통과** 판정을 부여한다.

따라서, TOE 외부 인터페이스를 설명하는 기능명세, TOE 구조를 내부 서브시스템으로 설명하는 기본설계, TOE 구조를 내부 모듈로 설명하는 상세설계, 소스코드 수준의 설명인 구현의 표현, 이러한 TOE 표현방법의 일관성을 보장하기 위해 서로 대응시키는 표현의 일치성으로 구성된 개발문서는 TOE 보안기능을 제공하는 방법을 이해하기에 적절하다.

• 설명서

관리자 설명서는 TOE를 안전한 방식으로 관리하는 방법을 서술하고 있으므로 AGD_ADM.1 컴포넌트에 대해 **통과** 판정을 부여한다.

따라서, 설명서는 TOE를 사용하는 방법을 적절하게 서술하고 있다.

• 생명주기 지원

개발자의 개발환경에 대한 보안통제는 TOE를 안전하게 운영하기 위해 필요한 TOE 설계 및 구현의 비밀성 및 무결성을 제공하기에 적절함을 확인하였으므로 ALC_DVS.2 컴포넌트에 대해 **통과** 판정을 부여한다.

개발자가 문서화된 TOE 생명주기 모델을 사용하고 있음을 확인하였으므로 ALC_LCD.1 컴포넌트에 대해 **통과** 판정을 부여한다.

개발자가 일관성 있고 예측할 수 있는 결과를 낼 수 있는 잘 정의된 개발 도구를 사용했음을 확인하였으므로 ALC_TAT.1 컴포넌트에 대해 **통과** 판정을 부여한다.

따라서, 생명주기 지원은 TOE 개발 전 과정에 사용된 보안절차 및 도구와 TOE를 개발하고 유지보수하는 동안 개발자가 사용하는 절차를 적절하게 서술하고 있다.

• **시험**

시험은 TOE 보안기능이 기능명세에 대하여 체계적으로 시험되었음을 확립하기에 충분하였으므로 ATE_COV.2 컴포넌트에 대해 **통과** 판정을 부여한다.

개발자가 기본설계 및 상세설계에 대한 TOE 보안기능 시험을 수행하였음을 확인하였으므로 ATE_DPT.2 컴포넌트에 대해 **통과** 판정을 부여한다.

개발자의 기능 시험서는 보안기능이 명세된 대로 수행함을 입증하기에 충분하므로 ATE_FUN.1 컴포넌트에 대해 **통과** 판정을 부여한다.

평가자는 TSF 일부에 대한 독립적인 시험을 수행하여 TOE가 명세된 대로 동작함을 확인하였고, 개발자 시험에 대한 전수시험을 통하여 개발자가 수행한 시험에 대한 신뢰를 얻었으므로 ATE_IND.2 컴포넌트에 대해 **통과** 판정을 부여한다.

따라서, 시험서를 통해 TOE 보안기능 보안목표명세서에 명시된 TOE 보안기능요구사항을 만족하고 설계 문서에 기술된대로 동작함을 확인하였다.

• **취약성 평가**

오용 분석에서 설명서가 오해되지 않고 불합리하지 않으며 상충되지 않음을 확인하였으며, 모든 운영모드에 대한 안전한 절차가 다루어졌으며, 설명서를 사용하면 TOE의 불안전한 상태를 방지 및 탐지할 수 있음을 확인하였으므로 AVA_MSU.2 컴포넌트에 대해 **통과** 판정을 부여한다.

기능강도 선언은 보안목표명세서의 모든 확률 및 순열 메커니즘에 대하여 선언되었으며, 개발자의 기능강도 선언에 대한 분석은 정확함을 확인하였으므로 AVA_SOF.1 컴포넌트에 대해 **통과** 판정을 부여한다.

취약성 분석서에는 TOE에 대해서 명백하게 알려진 취약성과 이에 대한 대응책을 기능 구현 또는 지침서나 설명서에 운용환경을 명시하는 등 대응책을 적절하게 서술하고 있으며, 평가자가 독립적인 취약성 분석을 수행하여 취약성 분석의 정확성을 확인하였고 취약성 분석에서 TOE는 의도된 환경 내에서 높은 수준의 공격 수준을 가진 공격자에 의해 악용 가능한 취약성을 가지지 않음을 확인하였으므로 AVA_VLA.4 컴포넌트에 대해 **통과** 판정을 부여한다.

따라서, 개발자 및 평가자의 취약성 분석 및 평가자의 침투시험에 기반하여 의도한 환경 내에서 TOE에 악용 가능한 결함 및 약점이 존재하지 않음을 확인하였다.

10. 권고 사항

평가 받은 TOE 운영환경에서만 TOE의 안전성을 보장할 수 있으므로 다음의 가정사항을 반드시 준수하여 TOE를 운영하여야 한다.

① TOE는 전자여권을 구성하는 소프트웨어 부분만을 포함하므로, 전자여권 IC칩의 복제 및 Grandmater chess 공격 시도, 사진 대체, MRZ 데이터 변경 등을 탐지하기 위해 전자여권의 물리적 보안 기술이 마련되어야 한다.

② 출입국심사관은 전자여권에 인쇄된 신원정보면과 전자여권 소지자의 신분을 확인하는 절차를 갖추어야 한다.

③ TOE는 개방형 운영체제로써 발급 및 사용 단계에서 전자여권 응용프로그램 이외의 응용프로그램 탑재가 가능하므로, 전자여권 발급기관은 전자여권 IC칩에 탑재되는 응용프로그램이 TOE의 안전성에 영향을 미치지 않는지 확인한 후 탑재를 승인해야 한다.

④ 판독시스템은 TOE에 기록된 전자여권 신원정보의 위변조를 검증하기 위해 PA용 인증서 체인(CSCA 인증서→DS 인증서)의 유효성을 검증한 후 SOD를 검증한다. 이를 위해, 주기적으로 DS 인증서 및 CRL을 검증해야 한다. EAC를 지원하는 판독시스템은 IS 인증서에 대응되는 전자서명생성키를 안전하게 가지고 있어야 하며 EAC-TA 과정에서 TOE에게 CVCA 링크인증서, DV 인증서, IS 인증서를 제공하여야 한다.

⑤ 판독시스템은 전자여권 발급기관의 전자여권 접근통제 정책에 위배되지 않도록 판독시스템 유형에 따른 보안메커니즘을 구현하고, 적용순서를 보장하여야 한다. 또한, TOE와 통신에 사용된 정보를 세션이 종료된 이후에 모두 안전하게 파기해야 한다.

⑥ 전자여권 발급기관은 발급 주체가 변경되지 않았음을 확인할 수 있도록 전자여권을 안전하게 발급하여야 하며 전자여권의 정상동작 및 호환성을 검증한 후 사용 단계로 넘겨야 한다. 발급기관은 TOE를 사용 단계로 전달하기 전에 쓰기 기능을 비활성화시켜야 한다.

⑦ 전자여권 발급기관은 BAC 인증키의 안전성을 보장할 수 있는 정도의 MRZ 엔트로피를 보장해야 한다.

⑧ 전자여권 발급국가는 여권전자서명체계에 따라 PA용 PKI 및 EAC용 PKI를 구축하여 인증업무준칙에 따라 전자서명키를 안전하게 생성・관리하고 인증서 생성・발급・운영・폐지 등 인증업무를 수행한다. 또한, 전자여권 발급국가는 인증서 유효기간 관리정책에 따라 인증서를 갱신하여 검증국가 및 판독시스템으로 안전하게 배포한다.

⑨ 전자여권 IC 칩과 판독시스템의 RF 통신거리는 5cm이내여야 하며 전자여권의 IC 칩 부착 면이 펼쳐지지 않은 경우에는 RF 통신채널이 형성되지 않도록 보장

되어야 한다.

11. 약어 및 용어 정의

아래의 약어 및 용어가 본 보고서에서 사용되었다.

CC	공통평가기준(Common Criteria)
EAL	평가보증등급(Evaluation Assurance Level)
PP	보호프로파일(Protection Profile)
SOF	기능강도(Strength of Function)
ST	보안목표명세서(Security Target)
TOE	평가대상(Target of Evaluation)
TSC	TSF 통제범위(TSF Scope of Control)
TSF	TOE 보안기능(TOE Security Functions)
TSP	TOE 보안정책(TOE Security Policy)

발급기관 (Personalization Agent)	전자여권 신원정보 등을 접수 및 교부기관으로부터 받아 이에 대해 전자서명하여 SOD를 생성하고 이들을 전자여권 IC 칩에 기록한 후 전자여권 TSF 데이터를 생성하여 전자여권 IC 칩의 보호메모리영역에 저장하는 기관이며 PA-PKI 및/또는 EAC-PKI 를 운영하는 기관
보안객체 (SOD : Document Security Object)	발급기관이 전자여권 발급 단계에서 기록한 전자여권 신원정보 및 전자여권 인증정보에 발급기관의 전자서명생성키로 서명한 것으로 "RFC 3369 Cryptographic Message Syntax, 2002.8"의 Signed Data Type으로 구현되며 DER 방식으로 인코딩된 객체
여권 전자서명	전자적 방법으로 처리된 여권의 발급 및 기재 수록사항의 확인등을 위해 발급기관이 여권전자서명체계에서 발급한 전자서명 생성키로 전자여권에 서명한 고유 정보
전자여권 (ePassport)	국제민간항공기구(ICAO)와 국제표준화기구(ISO)에서 규정하는 국제표준에 따라 여권 신청인의 신원정보 및 기타 정보가 저장된 비접촉식 IC 칩(Contactless IC Chip)을 내장한 여권
전자여권 사용자 데이터	전자여권 신원정보, 전자여권 인증정보를 포함
전자여권 신원정보	전자여권 신청인 기본정보와 전자여권 신청인 바이오정보를 포함
전자여권 신청인 기본정보	전자여권 신원정보면에 인쇄되어 육안으로 식별할 수 있

	는 정보와 기타 신원정보가 LDS 구조로 전자여권 IC 칩에 저장된 정보
전자여권 신청인 바이오정보 (Sensitive Data)	전자여권 신청인의 지문 및/또는 홍채 정보가 LDS 구조로 전자여권 IC 칩에 저장된 정보
전자여권 응용데이터	전자여권 사용자 데이터, 전자여권 TSF 데이터를 포함
전자여권 응용프로그램 (MRTD Application)	전자여권 규격의 LDS에 따라 프로그래밍되고, BAC, PA, EAC 등 보안 메커니즘을 제공하는 전자여권 IC 칩 탑재용 프로그램
판독 (Inspection)	출입국 관리기관이 전자여권 소지자가 제시한 전자여권 IC 칩을 조사하여 전자여권 IC 칩의 진위 검증을 통해 전자여권 소지자의 신분을 확인하는 절차
판독시스템 (IS : Inspection System)	전자여권 판독을 지원하기 위해 광학적 MRZ 가독 기능 및 보안메커니즘(PA, BAC, EAC, AA 등)을 구현한 정보시스템으로 전자여권 IC 칩과의 RF 통신을 하는 단말기와 이 단말기를 통해 전자여권 IC 칩으로 명령어를 전송하고 이에 대한 응답을 처리하는 시스템으로 구성
Application Protocol Data Unit (APDU)	스마트카드와 단말간의 Application의 package화된 데이터를 교환하기 위한 데이터 포맷으로 APDU는 명령 APDU와 응답 APDU로 구분됨. 카드와 단말간의 통신 프로토콜에 따른 하위 계층의 TPDU가 존재하며 APDU는 통신 프로토콜에 맞게 적절한 TPDU로 전환되어 전달됨
AA (Active Authentication)	전자여권 IC 칩이 판독시스템으로부터 전송된 난수에 서명함으로써 판독시스템에게 자신의 진위성을 입증하고, 판독시스템은 서명값을 검증함으로써 전자여권 IC 칩의 진위성을 검증하는 보안 메커니즘
BAC (Basic Access Control)	전자여권 IC 칩과 판독시스템의 상호인증을 위한 대칭키 기반 실체인증 프로토콜과 전자여권 IC 칩과 판독시스템의 안전한 통신채널 형성에 필요한 세션키 생성을 위한 대칭키 기반 키분배 프로토콜을 구현한 보안메커니즘
BAC 상호인증	ISO 9798-2 대칭키 기반 실체인증 프로토콜에 따라 전자여권 IC 칩과 판독시스템을 상호인증하는 것
BAC 판독시스템 (BIS : BAC Inspection System)	BAC, PA, AA 보안메커니즘을 구현한 판독시스템
DFA (Differential Fault Analysis)	암호연산과정에서 전압, 클럭등의 강제적인 변형을 통해 오동작을 유발하고 이로부터 암호키를 유추하는 방법
DPA (Differential Power Analysis)	암호연산과정에서 소모되는 전력량을 대량으로 수집하여 통계적인 분석을 통해 암호키를 유추하는 방법
EAC (Extended Access Control)	전자여권 IC 칩에 저장된 전자여권 신청인 바이오정보에 대한 접근통제를 위해 EAC를 지원하는 판독시스템(EIS)만이 전자여권 신청인 바이오정보를 읽을 수 있도록 칩인증

	을 위한 EAC-CA과정과 판독시스템 인증을 위한 EAC-TA 과정으로 구성된 보안메커니즘
EAC 판독시스템 (EIS : EAC Inspection System)	BAC, PA 및 EAC 보안메커니즘을 구현하고 AA를 옵션으로 구현한 판독시스템
EAC-CA (EAC-Chip Authentication)	전자여권 IC 칩의 EAC 칩인증 공개키 및 개인키와 EIS의 임시 공개키 및 개인키에 대한 키확인을 통해 EAC를 지원하는 판독시스템이 전자여권 IC 칩을 인증할 수 있도록 Ephemeral-Static DH 키분배 프로토콜(PKCS#3, ANSI X.42 등)을 구현한 보안메커니즘
EAC-TA (EAC-Terminal Authentication)	EIS가 EAC-CA 과정에서 사용한 임시 공개키에 자신의 전자서명생성키로 전자서명하여 전송한 값을 전자여권 IC 칩이 IS 인증서를 이용하여 전자서명을 검증함으로써 전자여권 IC 칩이 EIS를 인증하는 전자서명 기반 Challenge-Response 인증 프로토콜을 구현한 보안메커니즘
EMA (Electromagnetic Analysis)	암호연산과정에서 방출되는 잔자파를 수집하고 해석하여 암호키를 유추하는 방법
LDS (Logical Data Structure)	전자여권 사용자 데이터를 전자여권 IC 칩에 저장하기 위해서 전자여권 규격에서 정의한 논리적 자료 구조
PA (Passive Authentication)	DS 인증서를 가진 판독시스템이 SOD에 서명된 전자서명을 검증하고 전자여권 접근통제 정책의 읽기권한에 따라 해당 전자여권 사용자 데이터의 해시값을 검증하여 전자여권에 기록된 신원정보가 위변조되지 않았음을 증명하는 보안메커니즘
SCP02(Secure Channel Protocol 02) 상호인증	GlobalPlatform 2.1.1 Card Specification에서 정의하고 있는 대칭키 기반 실체인증 프로토콜
SPA (Simple Power Analysis)	암호연산과정에서 소모되는 전력량을 수집하고 해석하여 암호키를 유추하는 방법

12. 참고문헌

인증기관은 아래의 문서를 사용하여 본 인증결과보고서를 작성하였다:

[1] 정보보호시스템 공통평가기준 (2008. 7)
[2] 정보보호시스템 공통평가방법론 V2.3
[3] 정보보호시스템 평가·인증 지침 (2008. 7. 16)
[4] 정보보호시스템 평가·인증업무 수행 규정 (2007. 12. 1)
[5] 삼성SDS S*Pass* V1.0 보안목표명세서 V2.21 (2008. 8. 24)
[6] 삼성SDS S*Pass* V1.0 평가결과보고서, 발행버전 1.0 (2008. 8. 29)