KECS-CR-13-25

SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/S3CT9K9 인증보고서

인증번호 : KECS-ISIS-0456-2013

2013년 7월

IT보안인증사무국

1. 제품 개요

SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/S3CT9K9(이하 "TOE"라 한다)은 합성제품 형태로, CC EAL5+(인증번호 ANSSI-CC-2012/70) 인증 받은 삼성전자사의 IC칩인 S3CT9KW/S3CT9KC/S3CT9K9 revision 2에 삼성에스디에스(주)가 개발한 폐쇄형 IC칩 운영체제, 전자여권 응용프로그램 및 전자여권 응용 데이터인 SPass NX V1.0 R3을 탑재한 전자여권 IC칩이다.

TOE에서 사용하는 IC칩과 관련된 인증정보는 다음과 같다.

구 분	내 용
보호프로파일	BSI-PP-0035-2007
IC칩 식별	Samsung S3CT9KW/S3CT9KC/S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional Secure RSA/ECC V2.2 Library including specific IC Dedicated Software
암호라이브러리	Secure RSA/ECC Library V2.2, TRNG Library V2.0
EAL	EAL5+ (ALC_DVS.2, AVA_VAN.5)
인증기관	ANSSI (프랑스)
인증번호	ANSSI-CC-2012/70
인증일자	2012.10.12

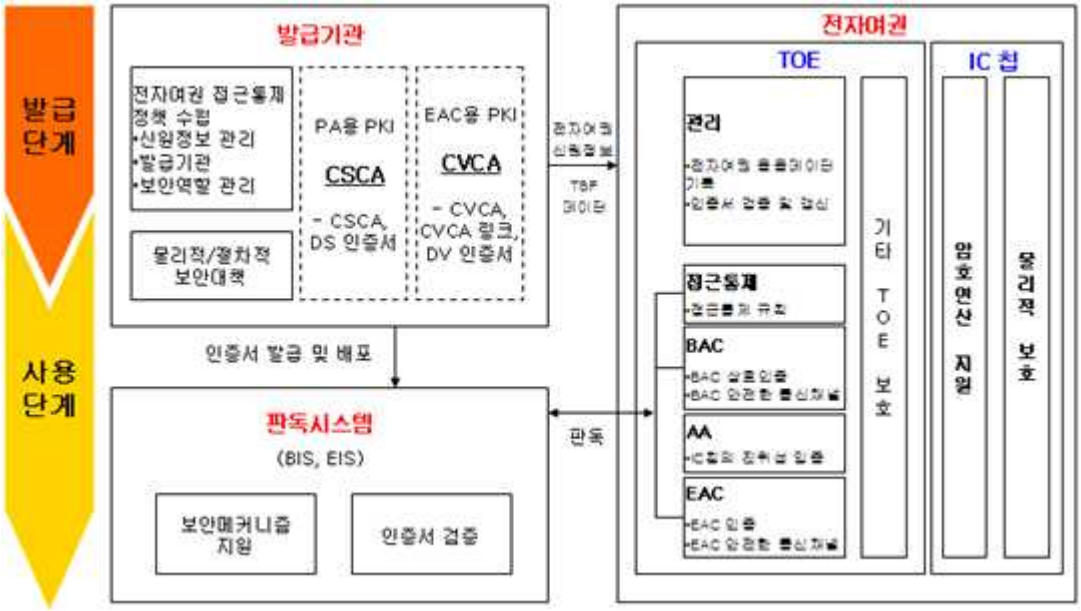
[표 1] TOE IC칩 인증정보

TOE는 전자여권 보호프로파일 V2.1(KECS-PP-0163a-2009, 2010.6.10.)에 대한 입증가능한 준수를 선언하고 있으며, 국제민간항공기구(ICAO) 및 BSI에서 규정하는 국제표준에 따른 BAC, AA, EAC 기능을 제공한다.

TOE는 다음과 같은 구성요소로 구성된다.

- IC칩 S3CT9KW/S3CT9KC/S3CT9K9 Revision 2: 삼성전자에서 제공하며, 구체적인 내용은 IC칩 인증보고서 ANSSI-CC-2012/70을 참조한다.
- 내장 소프트웨어 SPass NX V1.0 R3: 삼성에스디에스(주)에서 제공한다.

TOE가 설치되어 운영되는 환경은 [그림 1]과 같다.



[그림 1] 운영환경

TOE는 다음 구성요소 및 관련 설명서로 구성된다.

구 분	식별자	버 전	배포 형태
HW/SW	Samsung S3CT9KW/S3CT9KC/ S3CT9K9 16-bit RISC Microcontroller for Smart Card, Revision 2 with optional secure RSA/ECC V2.2 Library including specific IC Dedicated Software	Revision 2	IC칩 모듈 (주의사항: 소프트웨어는 ROM 및 EEPROM에 포함되며, 전자여권 책자 및 인레이는 포함되지 않음)
	Secure RSA/ECC Library	V2.2	
	TRNG Library	V2.0	
SW	SPass NX	V1.0 R3	
문서	SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/ S3CT9K9 User Guidance Initialization	V1.00	소프트카피
	SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/ S3CT9K9 User Guidance Personalization	V1.00	
	SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/ S3CT9K9 User Guidance Inspection	V1.00	

[표 2] TOE 식별정보

TOE는 전자여권 PP에 따라 전자여권 IC칩 및 TOE 생명주기 2단계의 ⑤에서 완료된다. TOE 완료 후 전자여권 제조자(즉, 인레이 및 e-Cover 제조자)는 TOE를 전자여권 책자에 내장한다. 안테나 적용 및 인레이 제작 과정은 TOE에 포함되지 않는다.

발급기관은 안전하게 배포된 발급키 셋을 사용해서만 전자여권에 접근할 수 있다. 발급

키 셋 및 설명서는 소프트웨어 개발자로부터 발급기관으로 PGP 또는 직접 전달을 통해서 안전하게 배포된다.

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

2. 주요 기능

TOE가 제공하는 일반적인 보안 특성은 다음과 같다.

■ 초기화 인증
초기화 인증키를 사용하여 초기화 세션키를 생성하고, 초기화를 수행하는 제조사에 대한 인증 메커니즘을 수행함

■ 발급기관 인증
발급 인증키를 사용하여 발급 세션키를 생성하고, 전자여권 발급을 수행하는 발급기관에 대한 인증 메커니즘을 수행함

■ BAC(Basic Access Control)
TOE에 저장된 전자여권 신청인 기본정보에 대한 접근을 통제하고 읽기 권한을 가진 판독시스템으로 전송할 때 안전한 통신채널을 형성하여 전자여권 신청인 기본정보의 비밀성과 무결성을 제공함. BAC는 BAC 상호인증, BAC 키분배, BAC 안전한 통신채널을 포함함

■ AA(Active Authentication)
TOE의 진위성을 판독시스템에게 입증하기 위하여 전자서명 기반의 인증 프로토콜을 구현한 것으로, TOE는 판독시스템이 전송한 난수에 AA 개인키로 전자서명을 생성하여 판독시스템에 전송하면 판독시스템은 전자서명을 AA 공개키로 검증함으로서 TOE를 인증함

■ EAC(Extended Access Control)
TOE에 저장된 전자여권 신청인 바이오정보에 대한 접근을 통제하고 읽기 권한을 가진 판독시스템으로 전송할 때 안전한 통신채널을 형성하여 전자여권 신청인 바이오정보의 비밀성과 무결성을 제공하는 것임. EAC는 EAC-CA, EAC 안전한 통신채널, EAC-TA를 포함함

PA, AA, BAC, EAC 보안메커니즘의 기본 동작흐름은 EAC 규격의 2.1.1절에 서술된

표준 전자여권 판독절차와 2.1.2절 보안강화 전자여권 판독절차를 따른다.

TOE의 전자여권 보안메커니즘 판독 절차는 다음과 같다.

1) BAC 판독시스템

- BAC → PA → AA

2) EAC 판독시스템

- BAC → EAC-CA → PA → AA → EAC-TA

3. 평가결과 요약

TOE에 대한 평가는 한국정보통신기술협회에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL5+(ADV_IMP.2, ALC_DVS.2, AVA_VAN.5) 평가보증등급을 만족하여, 공통평가기준 1부 305항에 따라 "적합"한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증지침 (2009. 9. 1) 정보보호제품 평가인증 수행규정 (2012. 11. 1)
평가제품	SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/S3CT9K9
보호프로파일	전자여권 보호프로파일 V2.1 (KECS-PP-0163a-2009, 2010.6.10)
보안요구사항	없음
보안목표명세서	SPass NX V1.0 R3 on S3CT9KW/S3CT9KC/S3CT9K9 보안목표명세서 V1.02 (2013.04.10)
평가보고서	SPass NX V1.0 R3 on S3CT9KW/ S3CT9KC/S3CT9K9 평가결과보고서 V1.5 (2013.07.04)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R4
평가방법론	정보보호시스템 공통평가방법론 V3.1 R4
평가신청인	삼성에스디에스(주)
개발업체	삼성에스디에스(주)
평가기관	한국정보통신기술협회