KECS-CR-15-07

# KOMSCO JK31 V1.0 on M7892
# 인증보고서

인증번호 : KECS-ISIS-0579-2015

2015년 1월

IT보안인증사무국

# 1. 제품 개요

KOMSCO JK31 V1.0 on M7892(이하 “TOE”라 한다)는 합성제품 형태로, CC EAL6+(인증번호 BSI-DSZ-CC-0782-2012) 인증 받은 인피니온社의 IC칩인 M7892 B11에 한국조폐공사가 개발한 개방형 스마트카드 운영체제를 탑재한 제품이다.

IC칩에 임베디드 되는 소프트웨어인 개방형 스마트카드 운영체제(KOMSCO JK31 V1.0)는 Java Card Platform 2.2.2, GlobalPlatform 2.1.1, Visa GlobalPlatform 2.1.1을 준수하며, 추가적으로 한국조폐공사에서 자체 개발한 Native API를 포함하고 있다.

TOE에서 사용하는 IC칩과 관련된 인증정보는 다음과 같다.

| 구 분 | 내 용 |
|---|---|
| 보호프로파일 | BSI-PP-0035-2007 |
| IC칩 식별 | Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, ECv1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) |
| 암호라이브러리 | RSA crypto library (optional) : RSA2048 v1.02.013, RSA4096 v1.02.013<br>EC library (optional) : EC v1.02.013<br>SHA-2 library (optional) : SHA-2 v1.01 |
| EAL | EAL6+ (ALC_FLR.1) |
| 인증기관 | BSI (독일) |
| 인증번호 | BSI-DSZ-CC-0782-2012 |
| 인증일자 | 2012.09.11 |
| 인증효력유지 | BSI-DSZ-CC-0782-2012-MA-01 (2013.09.05) |

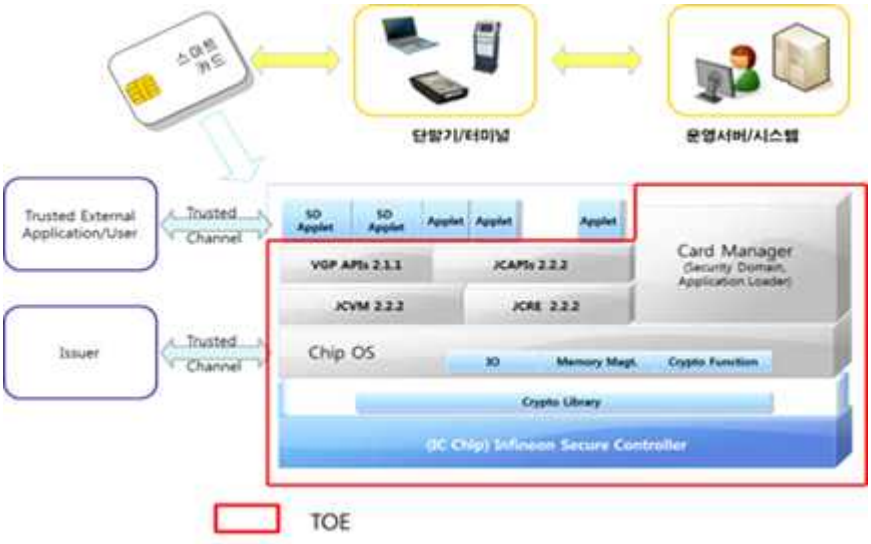
[표 1] TOE IC칩 인증정보

TOE는 개방형 스마트카드 플랫폼 보호프로파일 V2.2(KECS-PP-0097a-2008, 2010.12.20.)에 대한 입증가능한 준수를 선언하고 있다.

TOE는 다음과 같은 구성요소로 구성된다.

- IC칩 M7892 B11: 인피니온에서 제공하며, 구체적인 내용은 IC칩 인증보고서 BSI-DSZ-CC-0782-2012 및 인증효력유지 보고서 BSI-DSZ-CC-0782-2012-MA-01을 참조한다.
- 내장 소프트웨어 KOMSCO JK31 V1.0: 한국조폐공사에서 제공한다.

TOE가 설치되어 운영되는 환경은 [그림 1]과 같다.




[그림 1] TOE 운영환경

TOE는 다음 구성요소 및 관련 설명서로 구성된다.

| 구 분 | 식별자 | 버 전 | 배포 형태 |
|---|---|---|---|
| HW/SW | Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, ECv1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) | B11 | IC칩 모듈<br>(주의사항: 소프트웨어는 IC칩과 함께 인증된 암호 라이브러리를 포함하여 FLASH에 포함됨) |
| | RSA/EC Library | V1.02.013 | |
| | SHA-2 Library | V1.01 | |
| SW | KOMSCO JK31 V1.0 | V1.0 | |
| | ※ FLASH 형상 정보<br>- JK31-7805010B-R1.hex<br>- JK31-7859010B-R1.hex | | |
| 문서 | [JK31-MA-0001] 준비절차서 | V1.2 | 소프트카피 |
| | [JK31-MA-0002] 사용자 운영설명서 | V1.2 | |

[표 2] TOE 식별정보

TOE는 개방형 스마트카드 플랫폼 보호프로파일 V2.2의 생명주기 단계 중 제조단계에서 다운로드 절차를 통해 생성된다. 이후 발급자와 소지자간에 전달되는 과정은 평가범위에 포함되지 않는다. 즉, 합성 TOE를 생성하기 위한 개발 및 제도 단계의 배포 과정

과, 초기화 및 발급을 위한 합성 TOE 배포과정을 평가범위에 포함하여 다룬다.

**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.

■ Cryptographic Function
키 관리(생성/저장/폐기 등) 및 암호 연산(데이터 암호화/복호화, 서명 생성 및 검증, 해시 생성 및 검증 등), 난수 생성 및 난수성 검증 등을 수행

■ Card Manager
스마트카드에 탑재되는 애플릿 관리, 카드 발급자의 보안 정책 강제, 카드와 애플릿의 생명주기관리, 보안채널 관리, 스마트카드 식별 정보 관리, 사용자 인증을 위한 PIN 검증 등 카드 관리를 수행

■ Card Manager Command
Card Manager가 수행하는 GlobalPlatform 명령어 처리

■ Java Card Load, Install & Delete
패키지 및 애플릿 설치, 삭제 등 처리 수행

■ Hardware Abstracted Layer(HAL)
ISO 표준에 부합하는 I/O 기능, 메모리 관리 기능, 암호 기능 등 하드웨어 플랫폼 제어 수행

■ Java Card Runtime Environment(JCRE)
자바 애플릿 실행 지원을 위한 애플릿 관리, Firewall 기반 접근통제 등 제공
JCRE 초기화, 리셋, 자체시험 및 무결성 검증, 패키지 로드/설치/삭제 과정 등에서 장애 복구, 트랜잭션 무결성 보장, 응용프로그램 식별자(AID) 관리, 애플릿 선택/선택해제 관리, 자바 객체에 대한 접근통제 관리, 경계 검사, 예외 처리, 저장된 데이터 무결성 검사, TLV 포맷 데이터 분석 등 수행

■ Java Card Runtime Environment(JCRE) Memory
애플릿 및 시스템 메모리 관리

스택 할당/해지 관리, 힙 관리 및 초기화, 객체에 대한 레지스트리 관리, 자바 배열 객체 관리, 자바 객체 관리, 자바 임시 객체 관리, 자바 API 등에 의한 자바 객체 삭제 수행, 논리적 주소 및 물리적 주소 매핑 등 수행

■ Java Card Vitual Machine(JCVM)

자바 바이트코드 인터프리터 역할 수행 및 java API 실행, 보안 위반 검사 등 수행

자바 바이트코드 인터프리터, 애플릿 실행을 위한 자바 명령어 처리, 애플릿 실행을 위한 자바 API 호출, 자바 native API 호출, 보안 검사 등 수행

■ Java Card API(JCAPI)

애플릿이 수행하는 기본 기능과 암호처리 기능 등을 수행하기 위한 Java Card Platform 2.2.2에 기반한 인터페이스 제공

■ GlobalPlatform API(GPAPI)

Card Content 관리 등을 위해 GlobalPlatform 2.1.1 및 Visa GlobalPlatform 2.1.1 기반의 인터페이스 제공

■ Kernel

통신 프로토콜 처리 및 HAL과 JCRE 연계 수행

접촉식 및 비접촉식 통신 프로토콜 구현

# 3. 평가결과 요약

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

[ 인증제품 식별정보 ]

| | |
|---|---|
| **평가지침** | 정보보호시스템 평가인증지침 (2013.08.08)<br>정보보호제품 평가인증 수행규정 (2012.11.01) |
| **평가제품** | KOMSCO JK31 V1.0 on M7892 |
| **보호프로파일** | 개방형 스마트카드 플랫폼 보호프로파일 V2.2<br>(KECS-PP-0097a-2008, 2010.12.20.) |
| **보안요구사항** | 없음 |
| **보안목표명세서** | KOMSCO JK31 V1.0 on M7892 보안목표명세서 v1.2<br>([JK31-TR-0001] Security Taget-v1.2, 2014.12.19) |
| **평가보고서** | TTA-CCE-14-008 KOMSCO JK31 V1.0 on M7892 평가결과 보고서 V1.3 (2015.01.12) |
| **적합여부 평가결과** | 공통평가기준 2부 적합<br>공통평가기준 3부 적합 |
| **평가기준** | 정보보호시스템 공통평가기준 V3.1 R4 |
| **평가방법론** | 정보보호시스템 공통평가방법론 V3.1 R4 |
| **검증필 암호모듈** | 없음 |
| **평가신청인** | 한국조폐공사 |
| **개발업체** | 한국조폐공사 |
| **평가기관** | 한국정보통신기술협회 |