

KOMSCO JK31 V1.1 on M7892

인증보고서

인증번호 : KECS-ISIS-1113-2021

2021년 7월



IT보안인증사무국

1. 제품 개요

KOMSCO JK31 V1.1 on M7892(이하, TOE)는 합성제품 형태로, CC EAL6+로 인증 받은 Infineon社의 IC칩(인증번호 BSI-DSZ-CC-0782-V5-2020)에 한국조폐공사가 개발한 개방형 스마트카드 운영체제 KOMSCO JK31 V1.1을 탑재한 제품이다.

IC칩에 임베디드 되는 개방형 스마트카드 운영체제 KOMSCO JK31 V1.1은 Java Card Platform V2.2.2, GlobalPlatform 2.1.1 및 Visa GlobalPlatform 2.1.1을 준수한다.

TOE인 KOMSCO JK31 V1.1 on M7892는 다음 구성요소 및 관련 설명서로 구성된다.

구분	식별자	버전	배포형태
합성 TOE	KOMSCO JK31 V1.1 on M7892 - JK31-7805010B-R2 - JK31-7859010B-R2	R2	IC칩 모듈/ 인편 전달
TOE 구성요소: IC HW	Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013 or v2.07.003, EC v1.02.013 or v2.07.003, SHA-2 v1.01, SCL v2.02.012, Base v1.02.013 or v2.07.003, and Toolbox v1.02.013 or v2.07.003 libraries and with specific IC dedicated software (firmware) - SLE78CLFX4000PM(7805010B) - SLE78CAFX4000PM(7859010B)	B11	IC칩 모듈
TOE 구성요소: IC SW	RSA 2048 EC Base Toolbox	v2.07.003 v2.07.003 v2.07.003 v2.07.003	소프트카피
TOE 구성요소: 임베디드 SW	KOMSCO JK31 V1.1 - JK31-7805010B-R2.hex - JK31-7859010B-R2.hex	R2	Flash 코드

구분	식별자	버전	배포형태
설명서	[JK31-R2-MA-0002] 사용자 운영설명서-v1.2	v1.2	소프트카피/ PGP 이메일
	[JK31-R2-MA-0001] 준비절차서-v1.2	v1.2	

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

2. 주요기능

TOE가 제공하는 주요 보안기능은 다음과 같다.

■ Card Manager(CM)

스마트카드에 탑재되는 애플릿 관리, 카드 발급자의 보안 정책 강제, 카드와 애플릿의 생명주기 관리, 보안채널 관리, 스마트카드 식별 정보 관리, 사용자 인증을 위한 PIN 검증 등 카드 관리 기능을 제공한다.

■ Java Card Runtime Environment(JCRE)

JCRE는 TOE 내에서 동작하는 자바 카드 시스템 컴포넌트로서 자바 애플리케이션 실행 시의 자원관리, 선택된 애플릿 관리, 단말기와의 통신과 애플릿의 보안을 담당하며, JCVM을 이용하여 애플릿을 구동하는 역할을 수행한다. JCRE는 APDU 라우팅, ISO 통신 프로토콜, JCVM은 트랜잭션 처리 클래스들의 프레임워크를 포함한다.

TOE는 JCRE를 통한 Firewall 기반 응용프로그램간 접근통제(firewall access control)를 제공한다. 애플릿간 방화벽 메커니즘을 통해 하나의 애플릿을 정해진 공간에 고립시킴으로써 다른 애플릿에 의해 주요 데이터가 누출되는 것을 방지한다.

■ Java Card Virtual Machine(JCVM)

JCVM은 JCRE와 유기적인 관계를 가지며 애플릿의 실체인 CAP 파일을 실행시킨다. 바이트코드 실행, 메모리 할당 관리, 객체 관리, 실행 시 보안기능 등을 수행하며, 바이트코드 인터프리터 역할을 수행한다.

■ Java Card Application Programming Interfaces(JC APIs)

JC API는 애플리케이션을 자바 규격에 따라 개발할 수 있게 제공하는 클래스 모음으로, JCRE의 상위계층에 속하며 애플리케이션이 수행하는 기본 기능과 암호 처리 기능을 수행하기 위한 인터페이스를 제공한다. TOE는 JC APIs를 통하여 응용프로그램에 암호키 생

성/파기, 암호화, 복호화, 전자서명 생성 및 검증의 암호 연산 및 해쉬값 및 난수의 생성을 지원한다.

■ Visa Global Platform Application Programming Interfaces(VGP APIs)

VGP APIs는 Global Platform 기능을 자바 카드 인터페이스로 정의한 것으로, 카드 소지자 검증, 개인화 등과 같은 애플리케이션을 위한 보안 서비스를 제공하고, 애플리케이션에 카드 콘텐츠 관리를 위한 서비스를 제공한다.

■ Chip Operating System(Chip OS)

Chip OS는 Hardware Abstraction Layer이며, 로우 레벨의 ISO 표준에 부합하는 I/O기능, RAM, FLASH 메모리에 대한 메모리 관리 기능, 로우 레벨의 트랜잭션 기능과 대칭키 및 해시 암호 함수 기능이 구현되어 있으며 JCVM과 JCRE가 구동하기 위한 운영체제의 역할을 담당한다. TOE는 관리자 모드와 사용자 모드가 있으며, 관리자 모드에서 초기화 인증과 사용자모드에서 SCP02인증을 제공한다. 관리자 모드에서 초기화 인증을 통해 승인된 관리자임을 확인하고 TOE를 초기화한다.

Chip OS는 대칭키 및 비대칭키 암호 알고리즘 및 난수발생기를 제공한다.

3. 평가결과 요약

TOE에 대한 평가는 한국정보통신기술협회에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL5+ (ALC_DVS.2, AVA_VAN.5 추가) 평가보증등급을 만족하여, 공통평가기준 1부 330항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증지침 (2017. 8. 24.) 정보보호제품 평가인증 수행규정 (2021. 5. 17.)
평가제품	KOMSCO JK31 V1.1 on M7892
보호프로파일	개방형 스마트카드 플랫폼 보호프로파일 V2.2
보안요구사항	없음
보안목표명세서	[JK31-R2-TR-0001] KOMSCO JK31 V1.1 on M7892 보안목표명세서 v1.3, (2021.07.06)
평가보고서	TTA-CCE-19-019 KOMSCO JK31 V1.3 on M7892 평가결과보고서 V1.1 (2021.07.28)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R5
평가방법론	정보보호시스템 공통평가방법론 V3.1 R5
검증필 암호모듈	없음
평가신청인	한국조폐공사
개발업체	한국조폐공사
평가기관	한국정보통신기술협회