KECS-CR-10-59

KOMSCO JK11
인증결과보고서

인증번호 : KECS-ISIS-0272-2010

2010년 10월

IT보안인증사무국

제·개정 이력 현황

개정 번호	제·개정일	개정쪽	제·개정내용
00	2010.10.12	-	최초 작성

본 문서는 한국조폐공사의 KOMSCO JK11에 대한 인증결과 보고서이다.

인증위원

국가보안기술연구소 김춘수,

고려대학교 최진영, 서울여자대학교 박춘식,

한양대학교 송정환, 성균관대학교 김승주

인증기관

IT보안인증사무국

평가기관

한국인터넷진흥원

목 차

1. 요약

본 보고서는 KOMSCO JK11(이하 TOE)에 대한 정보보호시스템 공통평가기준(2009년 9월 1일 고시)(이하 '공통평가기준'이 한다) EAL4+ 평가결과에 대한 인증기관의 인증결과를 서술한다. 본 보고서는 평가결과의 타당성 및 적합여부를 서술한다.

TOE에 대한 평가는 한국정보보호진흥원이 수행하였으며, 2010년 9월 15일에 평가가 완료되었다. 본 보고서의 내용은 한국인터넷진흥원에서 제출한 평가결과보고서의 내용에 기초하여 작성되었다. 평가는 제품이 공통평가기준 2부와 ATE_DPT.2와 AVA_VAN.4가 추가된 EAL4 평가보증등급의 요구사항 3부를 만족함에 따라 "적합"한 것으로 평가하였다.

TOE는 KOMSCO가 개발한 개방형 카드운영체제인 자바카드로 삼성전자의 IC칩인 S3CC9GC(CC EAL4+ 보증등급으로 인증)과 S3CC9LC(CC EAL5+ 보증등급으로 인증)에 탑재된다.

TOE를 구성하는 개방형 카드운영체제는 응용프로그램에게 실행환경을 제공하는 자바카드 플랫폼 V2.2.2(JavaCard Platform)와 개방형 카드운영체제에 대한 관리기능을 제공하는 비자글로벌플랫폼 V2.1.1(Visa Global Platform, 이하 VGP), Chip OS로 구성된다.

자바카드 플랫폼은 다수의 응용프로그램들이 하나의 IC 칩에 공존하며 안전하게 상호작용 하도록 방화벽, 메모리관리, 트랜잭션 처리 등의 기능과 함께 암호키 관리 및 암호연산 기능을 제공한다. 자바카드 플랫폼의 구성요소는 JCVM 2.2.2, JCRE 2.2.2와 JCAPIs 2.2.2이다.

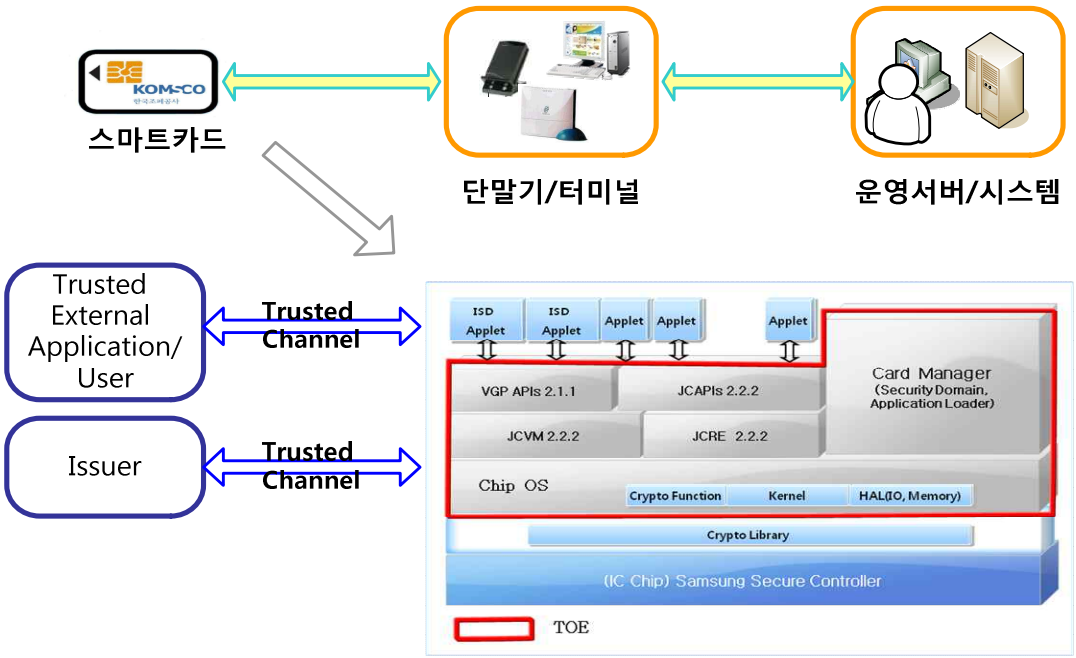
VGP는 관리자 권한인증, 응용프로그램 탑재, 설치, 삭제 등의 운영체제 관리, 운영체제 및 응용프로그램의 생명주기 관리 등의 개방형 카드운영체제에 대한 관리기능을 제공한다. VGP 구성요소는 카드매니저(Card Manager)와 VGP APIs 2.1.1이다.

Chip OS는 RAM, EEPROM에 대한 메모리 관리(Memory Management)기능, ISO 표준에 부합하는 I/O기능, 로우레벨의 Transaction 기능과 S/W로 구현된 암호알고리즘을 제공한다.

TOE가 탑재되는 하부 하드웨어는 중앙처리장치, 암호연산전용 프로세서, 입출력 포트, 메모리(RAM, ROM, EEPROM) 및 비접촉식 인터페이스로 구성되는 IC칩이다.

TOE는 JavaCard V2.2.2 규격에 따라 개발된 모든 자바 애플릿을 실행할 수 있다. TOE에서 실행되는 애플릿은 전자주민증 애플리케이션과 같은 공공 ID 카드 애플리케이션과 금융 애플리케이션(예: 현금/신용, 전자지갑, 전자상거래) 및 전자서명 애플리케이션(예: 디지털 서명), 교통카드 애플리케이션 등이 있다.

TOE가 운영되는 환경은 TOE가 탑재된 스마트카드와 서비스 시스템(단말기/터미널, 운영서버/시스템) 사이의 관계로 나타낼 수 있으며 다음 [그림 1]에서 확인할 수 있다.



[그림 1] TOE 운영환경

스마트카드는 스마트카드 단말기(Contact/Contactless)를 통해 서비스 시스템(터미널/단말기, 운영서버/시스템)에 필요한 정보를 상호교환한다. 즉, 스마트카드 소지자 및 발급자는 일반적으로 스마트카드 단말기와의 통신을 통해서 업무를 수행한다. 발급자는 발급시스템과 스마트카드 단말기를 이용하여, 응용프로그램 탑재, 발급 및 고장수리 등의 관리적인 업무를 수행하고, 소지자는 단말기를 이용하여 스마트카드의 기능을 사용한다. 이 때 스마트카드 단말기와 운영서버, IC 칩 및 TOE 응용프로그램은 TOE 운영환경이 된다.

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 KOMSCO JK11이 대한민국 정부기관에 의한 사용 승인 또는 KOMSCK JK11에 대한 품질보증을 의미하지 않는다.

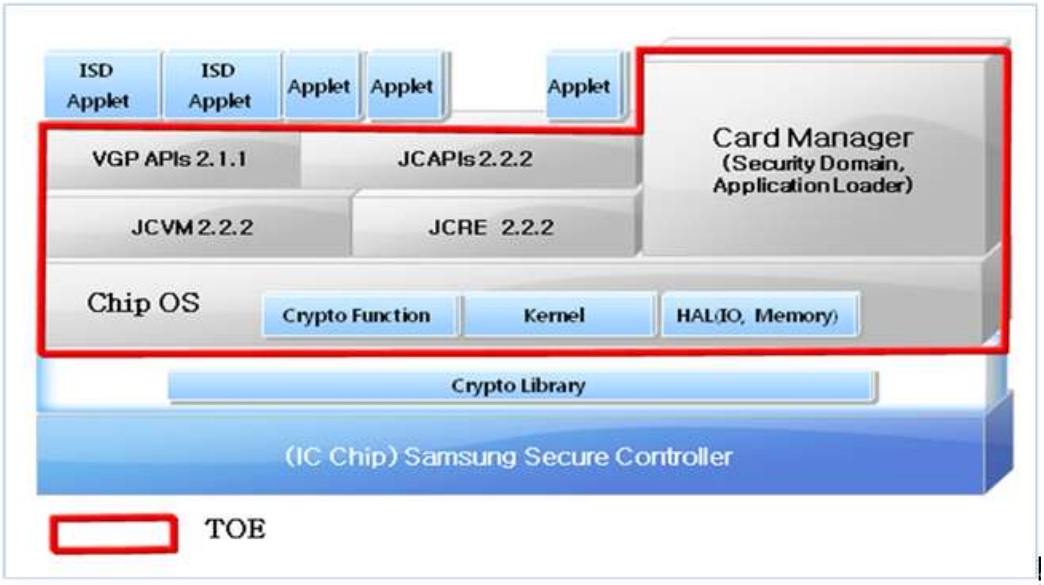
2. 식별정보

다음 [표 1]은 평가제품 식별을 위한 정보를 나타낸다.

[표 1] 평가대상제품 식별정보

평가지침	정보보호시스템 평가·인증 지침 (2009. 9. 1) 정보보호제품 평가인증 수행규정 (2010. 10. 1)
평가제품	KOMSCO JK11
보호프로파일	개방형 스마트카드 플랫폼 보호프로파일 V2.1(2010.6.10)
보안목표명세서	JK11 보안목표명세서 v1.3 (2010.8.6)
평가보고서	KOMSCO JK11 V1.0 평가결과보고서 V1.0 (2010.9.15)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 (2009. 9. 1)
평가방법론	정보보호시스템 공통평가방법론 V3.1 (2009. 9. 1)
평가신청인	한국조폐공사
개발업체	한국조폐공사
평가자	한국인터넷진흥원 보안성평가단 공공서비스보호팀 박현미, 유희준, 한정훈 (내부전문가 : 이성재, 지재덕, 현진수)
인증담당자	IT보안인증사무국

TOE의 물리적 범위는 [그림 2]와 같으며 물리적 범위에 포함된 구성요소는 [표 2]와 같다.



[그림 2] TOE 물리적 범위

[표 2] TOE 구성요소

TOE 구성요소 (형상항목)	식별자	버전	배포형태
개방형 카드운영체제(자바카드)	TOE 명 : KOMSCO JK11 TOE 버전 : R02	-	소프트웨어 (ROM에 저장)
	TOE 식별 : JK11-100C-R02(S3CC9GC) JK11-150C-R02(S3CC9LC)	-	
설명서	[JK11-MA-0005] JK11 사용자 운영 설명서	v1.3	문서
	[JK11-MA-0006] JK11 준비절차서	v1.2	문서

3. 보안정책

평가제품은 아래와 같은 보안정책을 준수하여 운영된다.

P.개방형플랫폼

TOE는 다양한 응용프로그램을 탑재하여 사용할 수 있는 개방형 플랫폼으로 개발되어야 한다.

P.역할구분

스마트카드를 제조에서부터 사용하는 단계까지 각 책임자별로 역할을 구분하여 그 역할에 따라 안전한 방법으로 TOE를 제조 및 관리해야 한다.

4. 가정사항 및 범위

4.1 가정사항

평가제품은 아래와 같은 가정사항을 준수하여 설치 및 운용되어야 한다.

A.안전한 경로

TOE와 TOE의 통신 상대인 스마트카드 단말기 간에 안전한 경로를 가진다.

A.응용프로그램

응용프로그램을 TOE에 설치 시 승인된 절차를 따라야 하며, 정당하게 설치된 응용프로그램은 악의적인 코드를 내포하고 있지 않다.

A.하부하드웨어

TOE가 운영되는 하부하드웨어는 TOE의 보안기능을 지원하기 위해 암호 연산을 제공하며, 물리적으로 안전하다.

응용 시 주의사항 : 물리적인 공격에 대해서 대응수단으르 갖추고 TOE의 안전성을 보장하기 위해 TOE가 동작하는 기반인 하드웨어(스마트카드의 IC칩)는 CC EAL4+ 보증등급으로 인증 받은 삼성전자의 스마트카드 IC칩인 S3CC9GC, CC EAL5+ 보증등급으로 인증 받은 삼성전자의 스마트카드 IC칩인 S3CC9LC이다. IC칩이 지원하는 암호연산은 소프트웨어로 구현되어 있는 암호알고리즘을 제외하고 IC칩의 암호 전용 프로세서 및 IC칩에 탑재되는 암호라이브러리에서 제공된다.

A.TOE관리

TOE를 제작에서부터 사용하는 단계는 제조자, 발급자 및 소지자로 역할이 구분되어 있으며, 각 역할에 대해 정한 규정에 따라 적절한 교육을 한다. 그리고 TOE 또는 스마트카드의 고장으로 인해 수리 및 교체할 경우 안전한 방식으로 처리된다.

A.TSF데이터

TOE가 운영되는 과정에서 TOE 외부로 유출되어 처리되는 TSF데이터는 안전하게 관리된다.

응용 시 주의사항 : TOE 외부에서 처리되는 TSF 데이터는 TOE를 초기화하는 과정에서 사용되는 Implementor Key(IK)와 Manufacturer Key(MK)이며, 이는 TOE 초기화 과정에서만 사용되므로 개발자 및 발급자(관리자) 이외의 외부로 유출되지 않고 안전하게 관리되며 TOE와 단말기간에도 안전하게 관리될 것을 가정한다.

4.2 위협 대응범위

위협원은 일반적으로 TOE 및 보호대상시스템에 불법적인 접근을 시도하거나 비정상적인 방법으로 TOE에 위해를 가하는 IT 실체 및 사용인이다. 위협원은 중간 수준의 전문지식, 자원, 동기를 가진다.

5. 제품정보

TOE는 KOMSCO가 개발한 개방형 카드운영체제인 자바카드로 삼성전자의 IC칩인 S3CC9GC(CC EAL4+ 보증등급으로 인증)과 S3CC9LC(CC EAL5+ 보증등급으로 인증)에 탑재된다.

TOE를 구성하는 개방형 카드운영체제는 응용프로그램에게 실행환경을 제공하는 자바카드 플랫폼 V2.2.2(JavaCard Platform)와 개방형 카드운영체제에 대한 관리기능을 제공하는 비자글로벌플랫폼 V2.1.1(Visa Global Platform, 이하 VGP), Chip OS로 구성된다.

TOE가 제공하는 IT 보안기능(TSF)을 세분화하여 요약하면 다음과 같다.

<table>
<tr><td>보안
위반분석</td><td>- 내부 데이터의 체크섬 값이나, 자원할당 오류, 인증실패 등의 사건에 대하여 보안 위반사건을 탐지하고, 카드기능 정지, 메모리 데이터 삭제 등 대응 행동을 수행
- 내부 주요시스템 구조체에 대한 체크섬 값(CRC)과 패키지 CAP 파일의 체크섬 값(SHA-1)에 대한 위반을 탐지하여 카드기능을 정지(shunt-down)
- JCVM구동 중에 자원할당 오류 등으로 발생한 security exceptions을 전용 카운터에 할당하도록 구현하여 최대값을 초과하면 카드기능을 정지
- TOE에서 지원하는 인증 프로토콜 상에서의 실패 시에 TOE를 강제적으로 리셋하고 관련 TSF 데이터의 메모리 영역을 삭제하여 자원의 재사용을 방지</td></tr>
<tr><td>암호연산</td><td>- 암호키 생성/파기, 암호화, 복호화, 전자서명 생성 및 검증의 암호연산을 수행(ARIC, SEED)
- 해쉬값 생성 및 난수의 생성을 지원(SHA-1, SHA-256, CRC32)
<table>
<tr><th>알고리즘</th><th>용도</th></tr>
<tr><td>TDES(112, 168 비트) in ECB/CBC mode</td><td>데이터 암/복호화, 데이터 서명생성 및 검증
(S3CC9GC/LC : IC칩 하드웨어에서 제공)</td></tr>
<tr><td>RSA(1024, 2048비트)</td><td>데이터 암/복호화, 서명생성 및 검증
(S3CC9GC/LC : IC 칩 하드웨어와 IC칩의 암호라이브러리에서 제공)</td></tr>
<tr><td>ECC(192, 224, 256 비트)</td><td>데이터 서명생성 및 검증
(S3CC9GC : 제공하지 않음
S3CC9LC : IC칩 하드웨어와 IC칩의 암호라이브러리에서 제공)</td></tr>
<tr><td>ECDH(192, 224, 256 비트)</td><td>키 공유 프로토콜
(S3CC9GC : 제공하지 않음
S3CC9LC : IC 칩 하드웨어와 IC 칩의 암호라이브러리에서 제공)</td></tr>
<tr><td>SEED(128 비트) in ECB/CBC mode</td><td>데이터 암/복호화
(S3CC9GC/LC : 소프트웨어로 제공)</td></tr>
<tr><td>ARIA(128, 192, 256 비트) in ECB/CBC mode</td><td>데이터 암/복호화
(S3CC9GC/LC : 소프트웨어로 제공)</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>CRC32</td><td>IC칩의 ROM에 저장된 TSF 실행코드 무결성</td></tr><tr><td>SHA-1, SHA-224/56</td><td>전자서명용 Hash 생성</td></tr></table> ※ IC칩 하드웨어에서 제공하는 알고리즘은 해당 알고리즘에 대한 하드웨어 Accelerator가 지원되며 이를 이용하는 암호함수를 구현 - RSA는 하드웨어 Crypto co-processor인 Modular multiplication accelerator를 이용하여 구현된 암호라이브러리를 활용하여 암호함수를 구현 - ECC는 S3CC9LC IC칩에 내장된 개선된 하드웨어 Crypto co-processor인 Modular multiplication accelerator를 이용하여 구현된 암호라이브러리를 활용하여 암호함수를 구현
접근통제	- JCRE를 통한 Firewall 기반 응용프로그램간 접근통제(firewall access control)를 제공. 애플릿간 방화벽 메커니즘을 통해 하나의 애플릿을 정해진 공간에 고립시킴으로써, 다른 애플릿에 의해 주요 데이터가 빠져나가는 것을 방지하며 해킹에 대한 보호를 제공
식별 및 인증	- 관리자 모드에서 초기화 인증과 사용자모드에서 SCP02 인증, DAP 인증, DM 인증을 제공 - 초기화 인증 : 승인된 관리자임을 확인하고 TOE를 초기화 - SCP02 인증 : 승인된 카드 발급자임을 확인하고 안전한 채널을 보장. 보안 채널을 통하여 메시지의 무결성을 보장하고 메시지 암호화를 통하여 비밀성을 보장하며 인증프로토콜 종료시에 사용된 관련 TSF 데이터 영역을 삭제하고 보안수준을 초기화하여 정보의 사용불가성을 보장 - DAP 인증 : TOE는 추가적인 보안이 필요한 애플릿의 경우 인가된 애플리케이션 제공자의 공개키를 이용하여 애플리케이션 제공자 인증. - DM 인증 : 발급자가 발급권한을 제2의 발급자에게 위임하고자 하는 경우 위임발급자가 해당 애플릿에 대한 정보를 발급자에 전달하고 이에 대한 Token을 받아 TOE에 제출하여 발급권한을 갖도록 함.
보안관리	- 보안기능, 보안속성, TSF 데이터, 보안역할 등과 관련된 사항을 관리. - Card Manager를 통하여 카드 발급자의 보안정책을 강제하고 카드와 응용프로그램의 생명주기관리, 데이터 전송과 데이터 액세스를 보호하는 보안채널 관리, 카드소유자 인증을 위한 PIN관리 기능을 수행하며 보안 서비스를 제공
기타 TSF 보호	- TSF 데이터 및 실행코드의 무결성을 검증하기 위한 자체시험을 수행하고, 장애가 발생한 경우 안전한 상태로의 복구기능 등을 제공 - TOE 초기화 시에 결정된 패치테이블에 대한 체크섬 값 시동 시 검증하여 불일치하면 카드기능을 정지(shuntdown)하고 시동 시 Randomness 테스트를 수행하여 오류 발생시 TOE를 강제적으로 리셋하는 자체시험을 수행 - 장애 발생시에 안전한 상태로의 복구를 위하여 먼저 주요 TSF 데이터 및 실행코드의 체크섬 값을 검증하여 보안위반 발생시에 카드기능을 정지하여 이에 대한 장애를 원천적으로 방지하고, TOE내의 자바 객체에 대하여 Atomic, Transaction 메커니즘을 제공 - 또한 애플릿 또는 패키지의 인스톨이 어떤 이유 때문에 취소되거나 중단되면, 할당된 모든 자원은 free하게 되고, 관련 메모리가 제거되도록 인스톨러는 Atomic operation 모델로 설계 - Anti-Tearing 메커니즘을 통하여 전력이 소실되었을 경우, 데이터 복구 및 저장 데이터에 대해 안전하게 보호 - 주요 TSF데이터(Keys, PIN 등)를 암호화하고 CRC 및 Hash를 이용하여 무결성 검증

6. 설명서

평가제품이 제공하는 설명서는 아래와 같다:

- JK11 사용자 운영설명서 v1.3 (2010. 9. 6)
- JK11 준비절차서 v1.2 (2010. 8. 25)

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.

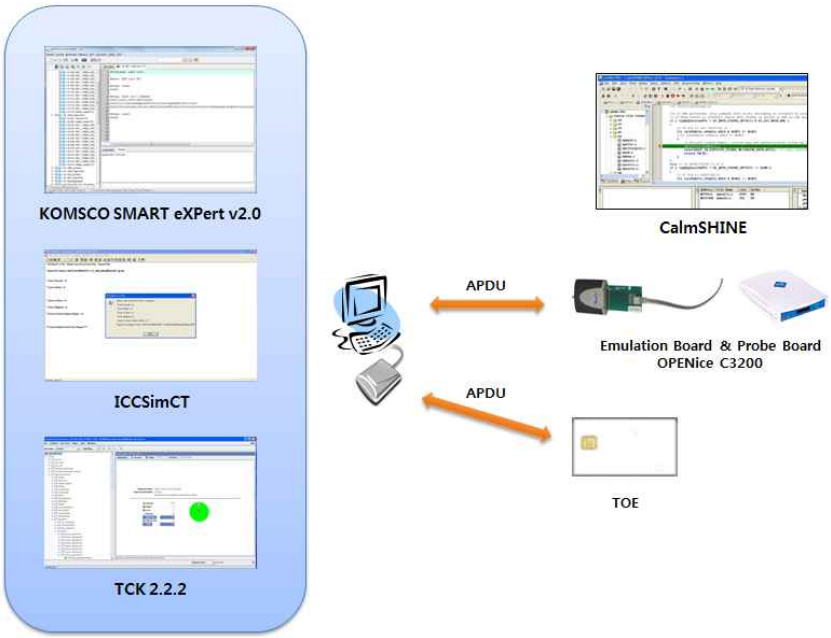
또한, 평가자는 개발자 시험에 기초하여 별도의 평가자 시험항목을 고안하여 시험한 결과, 실제결과가 예상결과와 일치함을 확인할 수 있었다.

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 [그림 3]과 같이 구성하였다.



[그림 3] TOE 시험환경

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 보안목표명세서 및 TOE를 정확하게 식별하고, TOE를 세 단계의 추상화 수준(TOE 참조, TOE 개요, TOE 설명)에서 정확하게 서술하며, 이 세 단계의 서술이 서로 일관성이 있으므로 ASE_INT.1에 대하여 통과 판정을 부여한다.

준수 선언은 보안목표명세서가 준수하는 공통평가기준에 대한 준수 선언을 정당하게 서술하고 있으므로 ASE_CCL.1에 대하여 통과 판정을 부여한다.

보안문제정의는 TOE 및 TOE의 운영 환경에서 다루어져야 하는 보안 문제를 명확히 정의하고 있으므로 ASE_SPD.1에 대하여 통과 판정을 부여한다.

보안목적은 적절하고 완전하게 보안 문제 정의를 다루고 있으며, TOE 및 TOE 운영 환경에서의 보안 문제를 명확히 분류하여 보안문제를 정의하고 있으므로 ASE_OBJ.2에 대하여 통과 판정을 부여한다.

확장 컴포넌트가 존재하지 않으며 ASE_ECD.1-1 ~ ASE_ECD.1-13 작업단위 평가활동이 적용 가능하지 않으므로 ASE_ECD.1에 대하여 통과 판정을 부여한다.

보안요구사항이 명확하고 모호하지 않으며 잘 정의되어 있으므로 ASE_REQ.2에 대하여 통과 판정을 부여한다.

TOE 요약명세에서 모든 SFR을 다루고 있으며, TOE 요약명세가 TOE의 다른 서술적인 설명과 일관성이 있으므로 ASE_TSS.1에 대하여 통과 판정을 부여한다.

따라서, [ST]는 타당하고 내부적으로 일관성 있으며, TOE 평가를 위한 기초 자료로 사용하기에 적합하다.

그러므로 보안목표명세서 평가 클래스(ASE)에 대한 판정은 통과(Pass)이다.

• 개발

[ARC]는 TSF가 침해되거나 우회될 수 없도록 구성되었고, 보안 영역을 제공하는 TSF가 이러한 영역들을 서로 분리함을 적절히 서술하고 있으므로 ADV_ARC.1 컴포넌트에 대해 통과 판정을 부여한다.

[FSP]는 TSFI(SFR-enforcing, SFR-supporting, SFR-non interfering)에 대해 목적,

사용방법, 입력 매개변수, 오퍼레이션, 오류 메시지를 동등한 상세수준으로 명세하여서 TSFI를 정확하고 완전하게 서술하고 있으므로 ADV_FSP.4 컴포넌트에 대해 통과 판정을 부여한다.

[IMP]는 다른 평가자 분석활동에 이용하기에 적합하며, TSF의 상세한 내부 동작을 파악하기에 충분하므로 ADV_IMP.1 컴포넌트에 대해 통과 판정을 부여한다.

[TDS]는 TSF 설명을 위한 배경 및 전체 TSF 설명을 제공하며, TSF 경계를 결정하기에 충분하게 TOE에 대한 설명을 서브시스템의 관점으로 제공하고, TSF 내부에 대한 설명을 모듈의 관점으로 제공한다. 또한 SFR이 완전하고 정확하게 구현되었음을 결정하도록 SFR-수행 모듈에 대한 상세한 설명과 SFR-지원 및 SFR-비-간섭 모듈에 대한 충분한 정보를 제공한다. 이로써 TOE 설계는 구현의 표현에 대한 설명을 제공하고 있으므로, ADV_TDS.3컴포넌트에 대해 통과 판정을 부여한다.

따라서 설계 문서에 포함된 [ARC](TSF 보안 수행이 손상되거나 우회되지 않는 방법을 설명하는 TSF의 구조 속성), [FSP](TSF 인터페이스 설명), [TDS](선언된 SFR과 관련된 기능을 수행하기 위하여 TSF가 어떻게 동작하는지 구조 설명), [IMP](소스코드 수준의 설명)는 TSF가 SFR을 만족하는 방법을 이해하고, 이러한 SFR 구현이 침해 또는 우회되지 않는 방법을 이해하기에 적절하다.

그러므로 개발 클래스(ADV)에 대한 판정은 통과(Pass)이다.

- **설명서**

[OPE] 및 [PRE]는 각 사용자 역할별로 TSF가 제공하는 보안 기능성 및 인터페이스에 대하여 설명하고, TOE를 안전하게 사용하기 위한 지침 및 가이드라인을 제공하며, 모든 운영모드에 대한 안전한 절차를 다루고, TOE의 불안전한 상태 탐지 및 방지를 용이하게 하며, 오해의 소지가 있거나 비합리성이 존재하지 않으므로 AGD_OPE.1 컴포넌트에 대해 통과 판정을 부여한다.

TOE 개방형 스마트카드 플랫폼으로 이미 설치되어 운영 가능한 상태로 배포되므로 설치 절차를 적용할 필요가 없으나, 제품 수령후 TOE에 대한 무결성을 확인하기 위하여 ROM과 EEPROM Checksum값에 대한 확인절차를 준비 절차로 하였다. 그러므로 TOE의 안전한 준비를 위한 절차 및 단계로 AGD_PRE.1 컴포넌트에 대해 통과 판정을 부여한다.

따라서, [OPE] 및 [PRE]는 사용자가 TOE를 안전한 방식으로 다룰 수 있는 방법을 적절하게 서술하고 있다.

그러므로 설명서 클래스(AGD)에 대한 판정은 통과(Pass)이다.

• **생명주기 지원**

[CM]는 개발자가 TOE와 TOE 관련 형상항목을 명확히 식별하며, 이들 형상항목을 변경하는 능력이 자동화된 도구에 의해 적절하게 통제되고, 그 결과로 형상관리 시스템에서 사람의 실수 또는 태만에 의해 발생하는 오류가 감소함을 입증하므로 ALC_CMC.4에 대해 통과 판정을 부여한다.

[CMC]은 형상목록에 TOE, TOE 구성 요소, TOE 구현의 표현, 보안결함, 평가제출물을 포함하고 있음을 입증하므로 ALC_CMS.4에 대해 통과 판정을 부여한다.

[DEL]은 TOE를 사용자에게 배포할 때 TOE 보안 유지를 위한 모든 절차를 서술하고 있으므로 ALC_DEL.1 컴포넌트에 대해 통과 판정을 부여한다.

[DVS]는 TOE의 안전한 운영이 손상되지 않도록 보장하기 위하여 TOE 설계 및 구현에 대한 비밀성 및 무결성을 제공하기 위해 개발자가 개발 환경에 적용하는 보안 통제가 적절함을 보장하므로 ALC_DVS.1 컴포넌트에 대해 통과 판정을 부여한다.

개발자가 [LCD]에 문서화된 TOE 생명주기 모델을 사용하고 있음을 확인하였으므로 ALC_LCD.1 컴포넌트에 대해 통과 판정을 부여한다.

[TAT]는 TOE 개발 시 잘 정의된 개발도구를 사용하고 있음을 서술하고 있으며, 개발자가 일관성 있고 예측 가능한 결과를 낼 수 있는 잘 정의된 개발 도구를 사용했음을 확인하였으므로 ALC_TAT.1 컴포넌트에 대해 통과 판정을 부여한다.

따라서, [CM], [DEL], [DVS], [LCD], [TAT]는 개발자가 TOE를 구현하고 유지 보수하는 동안 사용한 보안 절차가 적절한지 결정하기 위한 절차로써 개발자가 사용한 생명주기 모델, 형상관리, TOE 개발 전반에 걸쳐서 사용된 보안 대책, TOE 생명주기 전반에 걸쳐서 개발자가 사용한 도구 및 배포 활동을 적절하게 서술하고 있다.

그러므로 생명주기 지원 클래스(ALC)에 대한 판정은 통과(Pass)이다.

• **시험**

[ATE]은 개발자가 TSFI를 시험하였고, 개발자가 시험서의 시험항목과 기능명세서의 TSFI 사이의 일치성을 보여줄 수 있는 증거를 제시하였음을 입증하므로 ATE_COV.2 컴포넌트에 대해 통과 판정을 부여한다.

[ATE]는 TSF 서브시스템 및 SFR-수행 모듈이 TOE 설계 및 보안구조 설명에서 서술된 것과 같이 동작하고 상호작용함을 입증하므로 ATE_DPT.2 컴포넌트에 대해 통과 판정을 부여한다.

[ATE]은 개발자가 시험서에 서술된 시험항목을 정확히 수행하고 문서화함을 입증

하므로 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, [ATE]를 통해 TSF가 설계문서에 명세된 대로 동작하며 보안목표명세서에 명세된 TOE 보안기능요구사항에 부합하여 동작함을 확인하였다.

그러므로 시험 클래스(ATE)에 대한 판정은 통과(Pass)이다.

- **취약성 평가**

평가자는 중간의 공격성공 가능성을 지닌 공격자에 의한 잠재적인 취약성이 TOE 운영 환경에서 악용될 수 없음을 확인하였으므로 AVA_VAN.4 컴포넌트에 대해 통과 판정을 부여한다.

따라서, 개발 평가 및 예상되는 TOE 운영 시 또는 기타 방법에 의해 식별된 잠재적인 취약성이 공격자가 SFR을 위반할 수 없음을 확인하였다.

그러므로 취약성 평가 클래스(AVA)에 대한 판정은 통과(Pass)이다.

10. 권고 사항

본 TOE를 설치 및 운영하는 사용자는 아래의 사항을 반드시 준수하여야 한다.

- KOMSCO JK11은 개방형 자바카드 플랫폼으로 사용자가 개발한 애플릿을 카드에 로드하여 사용할 수 있다. 애플릿과 애플릿에서 사용되는 모든 데이터는 EEPROM에 저장되므로 중요 데이터에 대해서는 사용자가 추가 보안조치(무결성 확인, 암호화)를 취할 것을 권장한다.

- KOMSCO JK11의 발급명령어를 사용하기 위해서는 발급기관 인증이 선행되어야 하며 인증 프로토콜은 Global Platform V2.1.1 규격에 정의된 SCP02 보안메커니즘을 따라야 한다. 발급기관 인증키는 TOE 개발사와 발급기관이 협의하여 설정할 수 있으며 발급 시 발급기관에서 새로운 키로 갱신 할 수 있다.

- KOMSCO JK11의 사용자는 관리자모드 사용자와 사용자모드 사용자로 구분되며, 관리자모드 사용자는 KOMSCO JK11의 초기화와 커스터마이징을 수행하며 사용자모드 사용자는 제품의 개인화 및 어플리케이션 관리, 카드의 발급/폐기를 수행하므로 사용자의 역할에 따라 적절한 사용자 명령을 사용해야 한다.

- KOMSCO JK11은 S/W 방식으로 SEED 및 ARIA 알고리즘을 제공하며 사용자 모드 사용자인 어플리케이션 개발자는 SEED 및 ARIA 함수를 사용하여 활용할 수 있다.

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)

스마트카드 단말기 (Smartcard Terminal)	스마트카드의 판독기/기록기 기능과 키패드, 디스플레이, 보안모듈 등을 탑재한 장치
인가된 발급자 (Authorized Issuer)	TOE 보안정책에 따라 기능을 안전하게 운영 및 관리하는 인가된 사용자
인가된 사용자 (Authorized User)	SFR(보안기능요구사항)에 따라서 기능을 실행할 수 있는 사용자
Applet(애플릿)	애플릿은 자바카드 기술에 근거한 사용자 어플리케이션의 이름으로 카드 외부에서부터 실행을 위해서 선택될 수 있는 기본 코드임. 각 애플릿은 자신의 AID로 식별됨
EEPROM (Electrically Erasable Programmable Read-Only Memory)	전원 없이도 장기간 안정적으로 기억하는 비휘발성 기억장치. 소거 및 프로그램 가능 읽기 전용 기억 장치(EPROM)의 변형으로 일단 기록된 데이터를 전기적으로 소거하여 재기록할 수 있음. 따라서 프로그램을 재기록하는 것이 필요한 응용에 편리하게 사용할 수 있음. 칩을 구성하는 소자의 전하를 전기적으로 변화시킴으로써 데이터를 기록, 소거함. 전기적으로 판독이나 기록을 할 수 있어서 시스템 내에 내장된 상태로 프로그램을 다시 할 수 있음
IC 칩 (Integrated Circuit Chip)	스마트카드의 기능을 처리하기 위한 중요한 반도체이며, 마스크 ROM(mask ROM), EEPROM, RAM과 I/O 포트 등 네 개의 기능 단위를 포함하는 처리장치

JCAPI (JavaCard Application Programming Interface)	자바 프레임워크와 확장 자바 패키지에 정의된 기능에 대한 인터페이스로서 자바카드의 어플리케이션을 구성하는데에 사용됨. JavaCard Application Programming Interface는 Java Programming language의 서브셋임
package	Package는 클래스(Classes)와 인터페이스(interfaces)를 포함하는 자바 프로그래밍 언어의 이름으로 사용자 라이브러리와 하나 이상의 애플릿을 정의. 패키지는 export 파일과 CAP 파일로 나뉘어 짐.
RAM (Random Access Memory)	램(RAM)은 컴퓨터 프로세서가 빠르게 접근할 수 있도록 하기 위하여, 운영체제, 응용프로그램 그리고 현재 사용중인 데이터를 유지하고 있는 저장소임. 램은 하드디스크, 플로피 디스크, CD-ROM 등 다른 그 어떤 컴퓨터 저장장치보다 빠르게 읽고 쓰기를 할 수 있음. 그러나 램에 저장되어 있는 데이터는 오직 컴퓨터가 작동하는 동안에만 유지되며, 컴퓨터의 전원이 꺼지면 램에 있는 데이터는 사라짐. 컴퓨터의 전원이 다시 켜지면 하드디스크에 있던 운영체제나 다른 파일들이 다시 램에 적재됨
ROM (Read-Only Memory)	반도체 기억 장치의 한 가지로 그 내용을 읽을 수는 있어도 바꿀 수는 없는 것. 읽고 쓰기가 모두 가능한 램(RAM)에 비교됨. 이는 컴퓨터의 전원이 끊어져도 저장되어 있는 내용이 변함없이 유지되므로 보통 컴퓨터에 기본적인 운영체제 기능이나 언어의 해석 장치(interpreter)를 내장시키기 위해 이용됨
APDU	ISO 7816에 의해 정의된 카드 단말기와 스마트카드 사이의 표준 통신메시지 프로토콜
SCP02	GlobalPlatform Card Specification, Version 2.1.1에 정의되어 있는 보안통신 프로토콜과 보안 서비스의 집합으로서 발급기관 인증을 위해 사용
CVM (Cardholder Verification Method)	카드 발행자임을 확인하는 방법
DAP	Load File Data Block이 인증됨을 검증하기 위해 Security Domain에의해 사용되는 메커니증
DM (Delegated Management)	승인된 어플리케이션 제공자가 수행하는 미리 승인된 카드 내용 변경

12. 참고문헌

인증기관은 아래의 문서를 사용하여 본 인증결과보고서를 작성하였다:

[1] 정보보호시스템 공통평가기준 (2009. 9)
[2] 정보보호시스템 공통평가방법론 V3.1
[3] 정보보호시스템 평가·인증 지침 (2009. 9. 1)
[4] 정보보호시스템 평가·인증업무 수행 규정 (2010. 10. 1)
[5] JK11 보안목표명세서 v1.3 (2010. 8. 6)
[6] KOMSCO JK11 평가결과보고서 V1.0 (2010. 9. 15)