KECS-CR-06-11

삼성SDS(주) MULTOS SM10 R2
인증보고서

인증번호 : KECS-ISIS-0051-2006

2006년 9월

IT보안인증사무국

본 문서는 삼성SDS(주)의 삼성SDS MULTOS SM10 R2에 대한 인증보고서이다.

인증기관

IT보안인증사무국

평가기관

한국정보보호진흥원

목 차

1. 요약

본 보고서는 삼성SDS MULTOS SM10 R2에 대한 정보보호시스템 공통평가기준(2005년 5월 21일 고시)(이하 '공통평가기준'이 한다) EAL4+ 평가결과에 대한 인증기관의 인증결과를 서술한다. 본 보고서는 평가결과, 평가결과의 타당성 및 적합여부를 서술한다.

삼성SDS MULTOS SM10 R2에 대한 평가는 한국정보보호진흥원에서 수행되었으며, 2006년 8월 9일에 평가 완료되었다. 본 보고서의 내용은 한국정보보호진흥원에서 제출한 평가보고서의 내용에 기초하여 작성되었다. 평가는 제품이 공통평가기준 2부와 ADV_IMP.2, ALC_DVS.2 ATE_DPT.2, AVA_VLA.4가 추가된 EAL4 평가보증등급의 요구사항이 추가된 3부를 만족하여, 공통평가기준 1부 175항에 따라 "적합"한 것으로 평가하였다. 또한, 평가제품은 국가기관용 개방형 스마트카드 플랫폼 보호프로파일 V1.0 (2004. 12. 28)을 만족한다.

삼성SDS MULTOS SM10 R2는 스마트카드 IC(integrated circuit) 카드를 위한 운영체제로써, 다양한 스마트카드 어플리케이션이 스마트카드에서 안전하게 탑재되고 실행되도록 설계되었으며, 개방성과 안전성이 높은 다기능 어플리케이션 스마트카드용 운영체제이다.

삼성SDS의 MULTOS SM10 R2 제품의 TOE는 MULTOS로서 S3CC9RB와 S3CC9P9에 탑재된 MULTOS OS ROM code와 AMD(Additional MULTOS Data)이다. TOE는 동일한 어플리케이션 인터페이스(API)를 가지고 있어, 하부 하드웨어에 의존하지 않는 어플리케이션 실행이 가능하다.

또한, TOE는 스마트카드의 어플리케이션을 탑재하고, 실제 어플리케이션을 구동하기 위해서는 ATM(Automatic Teller Machine), 또는 ISO 7816 스마트카드 프로토콜을 지원하는 POS(Point-of-Sale) 단말기 등의 인터페이스 장치(IFD, Interface Device), 더미 단말기 등의 CAD(Card Acceptance Device)를 통해 사용한다.

MCD(MULTOS Carrier Device)가 IFD로부터 리셋(Reset) 신호를 받으면 ATR(Answer-to-Reset)을 IFD로 내보내고, IFD에서 MCD로 명령어가 전송되면 그 응답으로 MCD에서 IFD로 명령-응답이 이뤄지면서 스마트카드가 통신을 하게 된다.

TOE는 아래와 같은 구성요소로 이뤄져 있다.

- MULTOS 기능 모듈 - IFD와 통신을 하며, 상위 수준의 기능 수행
- MULTOS 메모리 관리자 - EEPROM 메모리를 블록으로 분리하며 메모리 변경 기능을 제공
- 안전한 쓰기 모듈 - EEPROM에 모든 데이터 쓰기 통제와 이들에 대한 atomic제공
- 암호모듈 - MEL(MULTOS Executable Language) 어플리케이션에서 사용되는 암호관련기능 제공

- AAM(Application Abstract Machine) - 어플리케이션들 간의 분리

또한, TOE는 아래와 같은 주요 보안기능을 제공한다.

- 어플리케이션에 대한 적절한 인증 기능
- 어플리케이션이 스마트카드에 탑재될 때 어플리케이션에 대한 인증과 무결성을 보장하는 능력을 제공한다. 또한 어플리케이션에 대한 삭제 요청에 대해서도 적절하게 인증됨을 보장한다.
- 암호화된 어플리케이션 탑재 및 이들이 사용가능하도록 복호화하는 기능
- 어플리케이션이 이전에 탑재된 어플리케이션 또는 MULTOS 자체와의 실행 영역분리 등을 통한 어플리케이션 보호
- 유효한 MULTOS가 탑재된 스마트카드인지에 대한 인증기능
- 인가된 어플리케이션에 대해 규정된 특성(예, 강한 암호)의 사용을 제한
- 정의된 중요기능(키 설치, 어플리케이션탑재 및 삭제 등)에 대한 시도 실패 값(Ratification Count) 관리

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

인증 효력범위 : 본 인증보고서에 포함된 정보는 삼성SDS MULTOS SM10 R2가 대한민국 정부기관에 의한 사용 승인 또는 삼성SDS MULTOS SM10 R2에 대한 품질보증을 의미하지 않는다.

2. 식별정보

다음 [표 1]은 평가제품 식별을 위한 정보를 나타낸다.

[표 1] 평가제품 식별정보

평가지침	정보보호시스템 평가·인증 지침 (2005. 5. 21) 정보보호시스템 평가·인증업무 수행 규정 (2005. 9. 22)
평가제품	삼성SDS MULTOS SM10 R2
보호프로파일	국가기관용 개방형 스마트카드 플랫폼 보호프로파일 V1.0 (2004. 12. 28)
보안목표명세서	SM10 보안목표명세서 V1.2 (2006. 3. 15), 삼성SDS(주)
평가보고서	삼성SDS MULTOS SM10 R2 평가보고서, 발행버전 1.0 (2006. 8. 9)
적합여부 평가결과	공통평가기준 2부 적합 추가된 3부 적합(ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_VLA.4가 추가된 EAL4 적합)
평가기준	정보보호시스템 공통평가기준 V2.3 (2005. 8)
평가방법론	정보보호시스템 공통평가방법론 V2.3 (2005. 8)
평가신청인	삼성SDS(주)
개발업체	삼성SDS(주)
평가자	한국정보보호진흥원 보안성평가단 평가1팀 윤여웅, 이성재, 손경호
인증담당자	IT보안인증사무국

삼성SDS MULTOS SM10 R2는 다양한 스마트카드 어플리케이션이 스마트카드에서 안전하게 탑재되고 실행되도록 설계되었으며, 개방성과 안전성이 높은 다기능 어플리케이션 스마트카드용 운영체제이며 IC 칩에 마스킹된다.

하부 하드웨어 사양은 아래 [표 2]와 같다.

[표 2] 삼성SDS MULTOS SM10 R2가 탑재되는 IC칩 H/W 사양

CPU	16-bit CalmRISC 16 core
ROM	ROM : 160Kbytes(S3CC9P9), 320Kbytes(S3CC9RB) - User area : 144K bytes, 304K bytes - Crypto Library : 16K bytes
EEPROM	64Kbytes(S3CC9RB), 32Kbytes(S3CC9P9)
RAM	6K bytes
Crypto-Coprocessor	- Module exponential accelerator - SHA-1 accelerator
DES/3-DES	Built-in hardware DES/3-DES
기타 H/W	- MPU(Memory Protection Unit) - 16bit RNG(Random Number Generator) - Timer : 16bit Timer and 20bit Watchdog Timer - Clock : 2.5MHz, 5MHz, 10MHz

3. 보안정책

평가제품은 아래와 같은 보안정책을 준수하여 운영된다:

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

암호 TOE는 국가정보원장이 승인한 암호 알고리즘 및 모듈을 사용하여야 한다.

개방형플랫폼 TOE는 다양한 어플리케이션을 탑재하여 사용할 수 있는 개방형 플랫폼으로 개발되어야 한다.

4. 가정사항 및 범위

4.1 가정사항

평가제품은 아래와 같은 가정사항을 준수하여 설치 및 운용되어야 한다.

A.공격자수준	공격자는 높은 수준의 전문지식, 자원, 동기를 가지며, 공격자가 악용 가능한 취약성을 발견할 가능성은 높음이다.
A.안전한경로	TOE와 TOE의 통신 상대인 스마트카드 단말기간에 안전한 경로를 가진다.
A.어플리케이션	어플리케이션을 TOE에 설치 시 승인된 절차를 따라야 하며, 정당하게 설치된 어플리케이션은 악의적인 코드를 내포하고 있지 않다.
A.하부하드웨어	TOE가 운영되는 하부하드웨어는 물리적으로 안전하다.
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 TSF 데이터는 안전하게 관리된다.

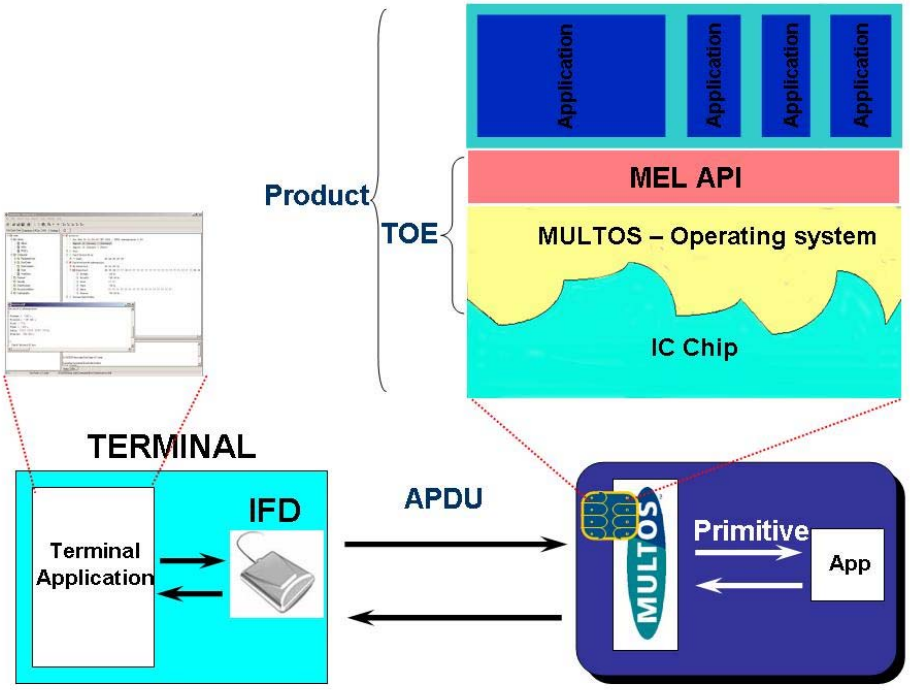
4.2 위협 대응범위

평가제품은 보호 대상인 TOE 자신의 자산 침해 시도 등의 보안위협에 대한 대처 방법을 제공한다. 평가제품은 보안기능을 무력화하거나 우회하는 직접적인 물리적 공격에 대한 대처방법을 제공하고 있다. 평가제품은 높은 수준의 전문지식, 자원 동기를 가진 위협원에 의해 발생하는 논리적/물리적 공격에 대한 대처방법을 제공한다.

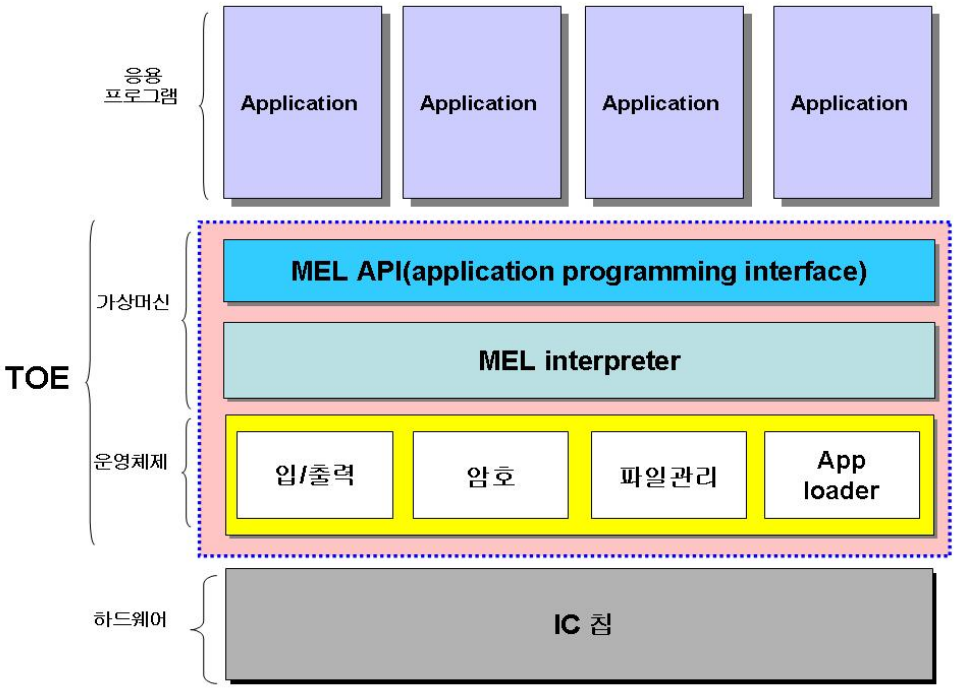
모든 보안목적 및 보안정책은 식별된 보안위협에 대한 대처방법을 제공할 수 있도록 서술되어 있다.

5. 제품정보

평가제품은 안전한 어플리케이션 탑재 등의 보안기능을 지원하며 운영환경은 [그림 1]과 같으며, 기본구조는 다음 [그림 2]와 같다.



[그림 1] 삼성SDS MULTOS SM10 R2 운영환경



[그림 2] 삼성SDS MULTOS SM10 R2 기본구조

평가제품은 아래와 같은 주요 서브시스템으로 구성된다.

- **응용 추상기계 서브시스템**

응용 추상기계 서브시스템(SS_AM)은 어플리케이션과 코드렛(Codelet, ROM에 탑재된 어플리케이션)을 안전하게 해석하고 실행하는 역할을 한다. 만약 어플리케이션이 암호 등의 프리미티브(Primitive, 어떤 연산을 위한 기본적인 단위)를 실행하고자 한다면, 어플리케이션이 프리미티브를 실행할 수 있는지를 확인하다.

- **명령어관리 서브시스템**

명령어관리 서브시스템(SS_CH)은 MULTOS 명령어를 처리하며, 각각의 명령어를 위한 인터페이스 기능을 제공하며, 이 인터페이스를 통해, 메모리관리 등의 다른 서브시스템으로 명령어를 전달한다. 또한 카드가 활성화되기 전의 명령어인 CHECK DATA, SET MSM Controls Data 명령어를 직접 처리한다.

- **메모리관리 서브시스템**

메모리관리 서브시스템(SS_MM)은 어플리케이션과 코드렛 메모리를 관리하는 역할을 하며, 어플리케이션 탑재, 생성, 삭제 관리와 각 어플리케이션에 관련된 메모리 관리 및 어플리케이션 간 접근통제를 수행한다.

- **암호기능 서브시스템**

암호기능 서브시스템(SS_CF)은 MULTOS 키와 MEL 응용에 의해 요구되는 암호연산을 수행하며, MSM Controls data, 어플리케이션 생성 등 암호연산과 관련된 기능을 제공한다.

6. 설명서

평가제품이 제공하는 설명서는 아래와 같다:

- 삼성SDS MULTOS SM10 R2 관리자설명서 V1.5, 2006년 6월 13일
- 삼성SDS MULTOS SM10 R2 사용자설명서 V1.5, 2006년 6월 13일
- 삼성SDS MULTOS SM10 R2 배포 및 운용문서 V1.2, 2006년 6월 22일

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. 평가가는 개발자의 시험 및 시험결과가 평가환경에 적합함을 검증하였다.

- **시험환경**

시험서에 서술된 시험환경은 시험을 위한 구성, 평가제품, TOE가 탑재된 스마트카드 또는 프로브 보드 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.

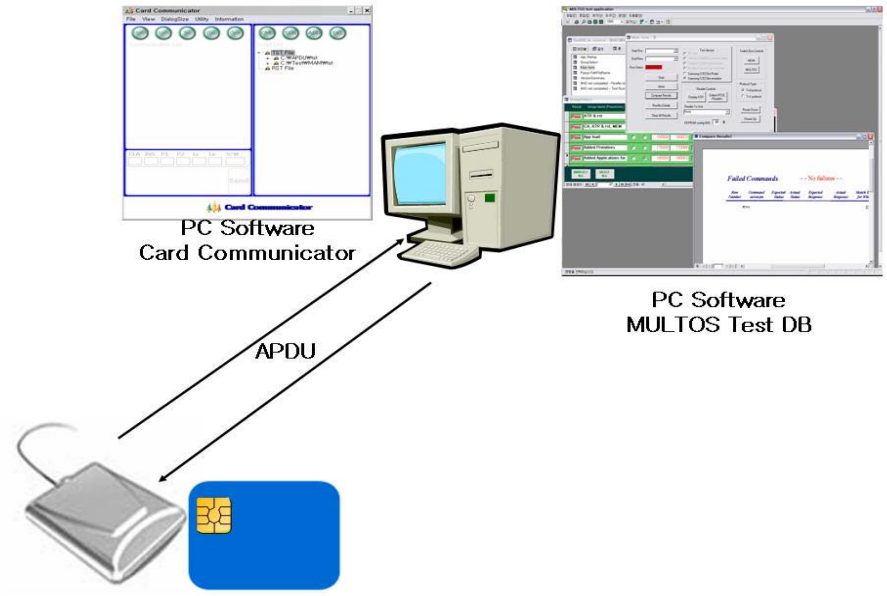
또한, 평가자는 개발자 시험에 기초하여 별도의 평가자 시험항목을 고안하여 시험한 결과, 실제결과가 예상결과와 일치함을 확인할 수 있었다.

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

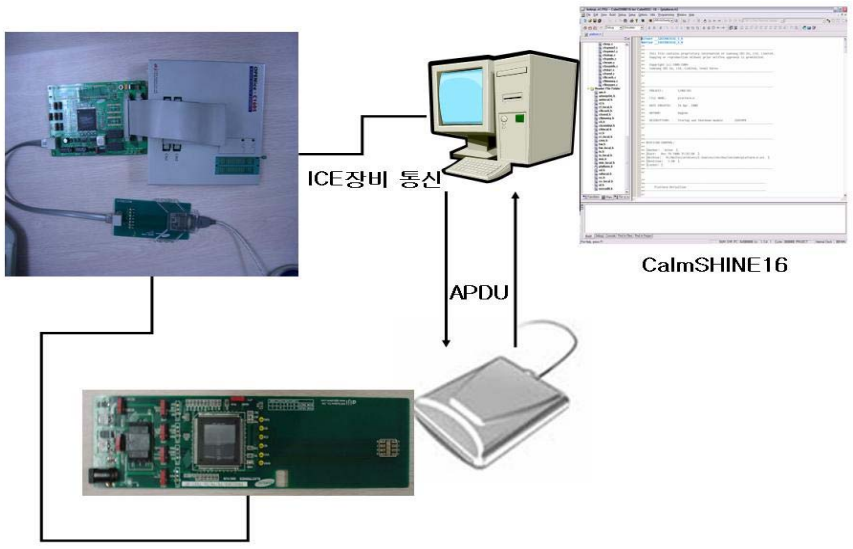
평가자의 시험결과는 평가제품이 설계문서에 서술된 대로 정상적으로 동작됨을 보증하였다.

8. 평가환경

평가자는 시험을 위해서 [ST]에서 명시된 환경구성과 일관성 있게 시험 환경을 [그림 3]과 [그림 4]와 같이 구성하였다.



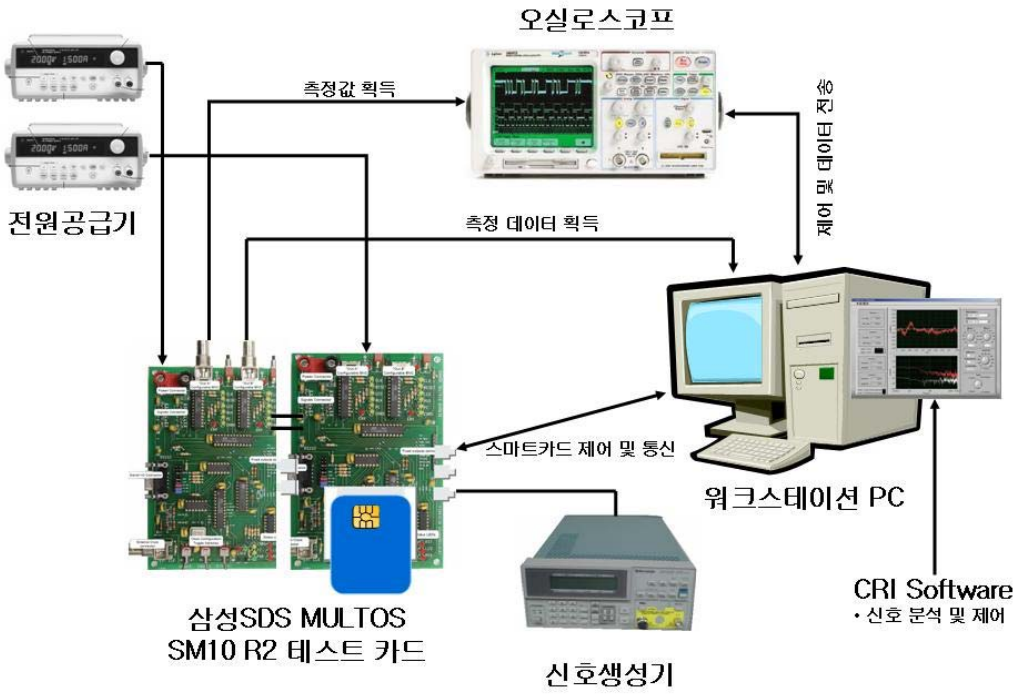
[그림 3] TOE 시험환경(DB를 이용한 기능시험)



[그림 4] TOE 시험환경(디버깅을 이용한 기능시험)

TOE가 탑재된 스마트카드 또는 프로브 보드를 스마트카드 리더에 삽입하고 스마트카드와 통신을 위한 Card Communicator를 통해 MULTOS Test DB에 저장된 테스트 스크립터 및 평가자가 임의로 작성한 테스트 스크립터를 실행하게 된다.

또한, 평가자는 침투시험을 위해서 아래 [그림5]와 같이 구성하였다.



[그림 5] 침투시험환경

9. 평가결과

평가는 최신 공통평가기준, 공통평가방법론을 적용하였다. 평가는 평가제품이 공통평가기준 2부, ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_VLA.4가 추가된 EAL4 평가보증등급의 요구사항이 추가된 3부에 적합하다고 평가하였다. 자세한 평가결과는 평가보고서에 서술되어 있다.

- **보안목표명세서 평가 (ASE)**

평가자는 ASE 공통평가방법론 작업단위를 적용하여 평가하였다. 보안목표명세서에는 TOE 설명이 조리 있고, 내부적으로 일관성이 있으며, 보안목표명세서의 다른 부분과 일관성이 있게 서술되어 있다. 보안환경은 TOE와 TOE 보안환경에서 유도된 명확하고 일관된 보안 문제점의 정의를 제공하고 있고, 보안목적은 완전하고 일관성 있게 서술되어 있다. 보안목적은 식별된 위협을 만족시키며 식별된 조직의 보안정책을 달성하며, 서술된 가정사항을 만족시키고 있다. TOE 보안 요구사항과 IT 환경에 대한 보안요구사항은 완전하고 일관성 있게 서술되어 있고, 보안목적을 달성하기 위한 TOE의 개발에 알맞은 기반을 제공하고 있다. TOE 요약명세는 보안기능과 보증 척도를 정확하고 일관성 있는 상위 수준 정의를 제공하고, 서술된 TOE 보안요구사항을 만족하고 있다. 또한 보안목표명세서가 수용하는 보호프로파일을 정확히 실체화하고 있다.

- **형상관리 평가 (ACM)**

평가자는 ACM 공통평가방법론 작업단위를 적용하여 평가하였다. 형상관리에는 형상목록, 형상식별방법, 버전부여방법, 형상변경 통제 방법을 명시하고 모든 개발문서와 소스파일에 형상관리 체계를 적용하여 개발되었으며 형상항목의 생성 및 변경은 형상관리조직과 형상관리시스템을 통하여 이루어지고 있음을 확인하였다.

- **배포 및 운영 평가 (ADO)**

평가자는 ADO 공통평가방법론 작업단위를 적용하여 평가하였다. 배포 및 운영에는 TOE의 안전한 배포, 설치, 운영에 대한 대책, 절차를 서술하고 있고, 이를 통해서 TOE가 전송, 설치, 시동, 운영되는 동안 보안성이 손상되지 않음을 보장하고 있으며, 업체실사를 수행한 결과 문서의 내용이 적용되고 있음을 확인하였다.

- **개발 평가 (ADV)**

평가자는 ADV 공통평가방법론 작업단위를 적용하여 평가하였다. 개발에는 TOE 보안기능요구사항을 보안목표명세서의 TOE 요약명세 단계부터 실제 구현 단계까지 기능명세서, 기본설계서, 상세설계서, 구현의 표현을 이용하여 단계적으로 세분화하여 정의하고 있다. 또한 각 개발 단계에서 인접한 개발 표현간의 상관관계를 이용하여 요구사항을 정확하고 완전하게 구현하였음이 정확하게 서술되어 있다.

- **설명서 평가 (AGD)**

평가자는 AGD 공통평가방법론 작업단위를 적용하여 평가하였다. 설명서에는 사용자가 평가제품에 접속시 제공되는 사용자 인터페이스와 동작방법을 예제를 들어 서술하고 있으며, 관리자설명서에는 관리자가 보안관리 인터페이스에 접속하는 방법과 보안관리 인터페이스에서 제공되는 각 메뉴에 대한 설명과 주의사항을 실례를 들어 서술하고 있다. 사용자/관리자설명서에서 서술된 내용이 정확하게 수행됨을 확인하였다.

- **생명주기 지원 평가 (ALC)**

평가자는 ALC 공통평가방법론 작업단위를 적용하여 평가하였다. 생명주기 지원서에는 TOE 개발의 모든 단계에 대한 절차 및 정책, 도구와 기법 등의 보안대책을 사용하여 개발 환경을 보호하고 있음을 타당하게 서술하고 있으며, 업체실사 과정을 통해서 실제로 적용되고 있음을 확인하였다.

- **시험 평가 (ATE)**

평가자는 ATE 공통평가방법론 작업단위를 적용하여 평가하였다. 시험서에는 보안목표명세서에 명시된 보안기능에 대해서 시험목적, 단계별 시험 절차 및 시험결과를 서술하고 결과를 예시하고 있다. 제공된 개발 과정별 기능시험과 모듈시험 등의 시험과정을 반복 수행하여 시험서에 서술된 시험 내용이 정확함을 확인하였으며 개발과정에서 구현된 보안기능의 동작이 일치함을 확인하였다. 또한 평가자 독립적인 시험을 수행하여 개발자 시험의 정확성을 확인하였다.

- **취약성 평가 (AVA)**

평가자는 AVA 공통평가방법론 작업단위를 적용하여 평가하였다. 취약성분석서에는 알려진 취약성에 대한 분석 및 대응방법, 오용가능성에 대한 분석 및 대응방법을 타당하고 정확하게 분석, 기술하고 있다. 또한 평가자 독립적인 취약성 시험을 수행하여 개발자 취약성 분석의 정확성을 확인하였다. 또한 보안기능 강도 분석에서 TOE 보안기능 강도가 보호프로파일/보안목표명세서에 정의된 기능강도 허용 수준을 만족함을 서술하고 있다.

10. 권고사항

- TOE는 중요 보안인 어플리케이션 탑재 및 삭제 등의 보안기능 실패시 설정된 실패회수를 확인해, 실패회수 초과 시 실패한 보안기능을 사용할 수 없도록 하는 기능이 있다. 실패회수는 TOE관리자가 설정하도록 되어 있으므로, 관리자는 실패회수를 10회 이내로 설정하는 것이 필요하다.
- 어플리케이션 삭제는 ADC(어플리케이션 삭제 인증서)를 통해 이루어진다. 만약, 어플리케이션 식별번호(AID)가 동일하면, 서로 다른 어플리케이션 삭제 인증서가 동일할 수 있으므로, 어플리케이션 개발시 식별번호는 반드시 다르게 설정하여야 한다.
- TOE는 어플리케이션 탑재시 사용되는 MSM 데이터 중 "Random seed" 값이 "0"인 경우 MSM의 인가없이 삭제된 어플리케이션을 재탑재 하는 것이 가능하므로, 어플리케이션 개발시 random seed값은 반드시 0이 아닌 값으로 설정하여야 한다.

11. 약어 및 용어 정의

아래의 약어 및 용어가 본 보고서에서 사용되었다.

(1) 약어

AID 어플리케이션 식별자(Application Identifier)
APDU 어플리케이션 프로토콜 데이터 유닛(application protocol data unit)
API application programming interface
ATM automated teller machine
ATR answer to reset
CAD Card Accepting Device
CC 공통평가기준(Common Criteria)
CLA class
COS 카드 운영체제(Card Operating System)
CRT Chinese remainder theorem
EAL 평가보증등급(Evaluation Assurance Level)
EEPROM electrically erasable programmable read-only memory
EF elementary file
FID file identifier
IC 직접회로(integrated Circuit)
IFD interface device
PP 보호프로파일(Protection Profile)
RAM random-access memory
ROM read-only memory
RNG random number generator
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)

(2) 용어

AAM (Application Abstract Machine) 어플리케이션 가상 플랫폼
가상 머신. OS에 구현된 가상 플랫폼에서 어플리케이션 개발자는 이 인터페이스에 따라 어플리케이션을 개발한다.

ALU(Application Load Unit)
어플리케이션의 코드와 데이터가 포함된 유닛

APDU(Application Protocol Data Unit)
스마트카드와 단말기 사이의 통신을 위한 데이터 유닛

Codelet
보통의 어플리케이션은 EEPROM 에 탑재된다. 그러나 범용성이 있는 어플리케이션이나 공통으로 이용 가능한 어플리케이션 등은 ROM에 마스킹 할 수 있다. 이와 같이 ROM에 탑재된 어플리케이션을 코드 렛이라고 부름

EEPROM(Electrically Erasable Programmable Read-Only Memory)
전원 없이도 장기간 안정적으로 기억하는 비휘발성 기억 장치. 소거 및 프로그램 가능 읽기 전용 기억 장치(EPROM)의 변형으로 일단 기록된 데이터를 전기적으로 소거하여 재기록할 수 있다. 따라서 프로그램을 재기록하는 것이 필요한 응용에 편리하게 사용할 수 있다. 칩을 구성하는 소자의 전하를 전기적으로 변화시킴으로써 데이터를 기록, 소거한다. 전기적으로 판독이나 기록을 할 수 있어서 시스템 내에 내장된 상태로 프로그램을 다시 할 수 있음

에뮬레이션(Emulation) 보드
한 컴퓨터 시스템이 다른 시스템과 같이 작동할 수 있도록 하기 위해 특별한 프로그램 기술이나 기계적 방법을 사용할 수 있게 만든 보드

IC 칩(Integrated Circuit Chip)
스마트카드의 기능을 처리하기 위한 중요한 반도체이며, 마스크ROM(mask ROM), EEPROM, RAM과 I/O 포트 등 네 개의 기능 단위를 포함하는 처리장치

KMA
어플리케이션의 탑재, 삭제 등의 MULTOS에 필요한 각종 키에 관리하는 키 관리국

KTU(Key Transformation Unit)
어플리케이션 로드 유닛(ALU)의 일부로 비밀 ALU에 사용

MCD(MULTOS Carrier Device)
MULTOS OS가 탑재된 IC카드

MEL(MULTOS Executable Language)
MULTOS의 실행 가능언로로 MULTOS용으로 개발된 어셈블러언어

MISA(MULTOS Injection Security Application)
MISA는 KMA에 의해 배포되는 MULTOS 응용을 말하며, 각각의 MCD에 64byte의 보안 데이터를 주입하기 위한 안전한 방법을 의미

MULTOS(Multi-Application Operating System)
멀티 어플리케이션 IC카드용 운영시스템

MULTOS OS
MULTOS 스마트카드에서 구동되는 운영시스템

RAM(Random Access Memory)
램(RAM)은 컴퓨터 프로세서가 빠르게 접근할 수 있도록 하기 위하여, 운영체제, 어플리케이션 그리고 현재 사용중인 데이터를 유지하고 있는 저장소. 램은 하드디스크, 플로피 디스크, CD-ROM 등 다른 그 어떤 컴퓨터 저장장치보다 빠르게 읽고 쓰기를 할 수 있다. 그러나, 램에 저장되어 있는 데이터는 오직 컴퓨터가 작동하는 동안에만 유지되며, 컴퓨터의 전원이 꺼지면 램에 있는 데이터는 사라진다. 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 비교된다. 이는 컴퓨터의 전원이 끊어져도 그 내용이 변함 없이 유지되므로 보통 컴퓨터에 기본적인 운영체제 기능이나 언어의 해석 장치(interpreter)를 내장시키기 위해 이용됨

ADC (Application Delete Certificate) 어플리케이션 삭제 증명서
키 관리국이 발행자의(Issuer) 요구에 의해 발행하는 것으로 어플리케이션을 삭제하기 위한 증명서

AID (Application Identifier) 어플리케이션 식별자
ISO7816로 정의되는 어플리케이션의 식별자

ALC (Application Load Certificate) 어플리케이션 로드 증명서
키 관리국이 발행자의 요구에 의해 발행. 새로운 어플리케이션을 탑재하기 위한 증명서

ALU (Application Load Unit) 어플리케이션 로드 유닛
탑재가능한 로드 형식으로 변환한 어플리케이션

Application 어플리케이션
MULTOS의 실행 언어(MEL)로 쓰여진 프로그램 코드와 관련 데이터

Application Developer 어플리케이션 개발자
어플리케이션을 개발하는 사람(기업), 경우에 따라 어플리케이션 제공자나 어플리케이션 로드유닛을 제공하는 사람과 동일

Application Provider 어플리케이션 제공자
어플리케이션, 또는 어플리케이션 로드유닛을 발행자에게 제공하는 사람(기업)

APDU (Application Protocol Data Unit) 어플리케이션 프로토콜 데이터 단위
ISO7816에 정의되는 스마트카드의 기본 명령어

CA (Certification Authority) 인증국
필요한 키의 생성, 발행, 관리 및 ALC/ADC 및 MSM_CD등의 디지털 인증서를 제공하는 기관. KMA(Key Management Authority : 키 관리국)이라고 함

COB (Chip On Board)
반도체 칩을 플라스틱판에 탑재해, 금도금 된 전극에 접속, 레진으로 처리한 모듈

IFD (Interface Device) 단말장치, IC카드 리더/라이터
IC카드와 외부와의 접속 장치로 카드등과 데이터 통신 하는 기기

KTU (Key Transformation Unit) ALU내 암호키 탑재유닛
ALU내에 준비된 암호키 격납부에서 ALU를 암호화하는 경우에 이용되는 정보. 암호키나 암호화하는 범위등의 정보를 포함해, KTU 자신도 암호화되고 있다.

MCD (MULTOS Carrier Device) 멀토스 탑재 장치(MULTOS 제품)
MULTOS OS를 탑재한 반도체 칩 및 이 반도체 칩을 내장한 IC카드 등

MSM (MULTOS Security Manager)
MULTOS가 구현된 카드의 보안상태를 관리하며, MSM-CD에 의해서 설정 조건을 지정하고, 멀토스 카드를 사용 가능한 상태로 활성화(초기화) 한다.

MEL (MULTOS Executable Language) MEL 언어, 멀토스 실행 언어
MULTOS OS의 어플리케이션 실행 형식의 어셈블러언어

MULTOS (Multi-application Operating System)
멀티 어플리케이션을 위한 IC카드로 구현되는 OS의 명칭 및 멀토스 카드의 생명주기를 관리, 운용하는 스킴을 가리킨다.

M-SPI (MULTOS Service Provider Interface)
멀토스 KMA에 등록된 카드발행 또는 멀토스 KMA와의 서비스를 가능하게 하는 클라이언트 소프트웨어.

PIN (Personal Identification Number) 비밀번호
개인 인증용의 ID번호

Virtual Machine 가상 머신

OS에 구현된 가상 플랫폼에서 하드웨어 플랫폼(반도체 칩)에 의존하지 않는 어플리케이션 프로그래밍인터페이스(API)를 제공한다.

12. 참고문헌

인증기관은 아래의 문서를 사용하여 본 인증보고서를 작성하였다:

[1] 정보보호시스템 공통평가기준 (2005. 5. 21)
[2] 정보보호시스템 공통평가방법론 V2.3
[3] 국가기관용 개방형 스마트카드 플랫폼 보호프로파일 V1.0 (2004. 12. 28)
[5] 정보보호시스템 평가·인증 지침 (2005. 5. 21)
[6] 정보보호시스템 평가·인증업무 수행 규정 (2005. 9. 22)
[7] 삼성SDS MULTOS SM10 R2 보안목표명세서 V1.2 (2006. 3. 15)
[8] 삼성SDS MULTOS SM10 R2 평가보고서, 발행버전 1.0 (2006. 8. 9)