스마트카드 칩 기술

이기한 | 서울여자대학교 정보통신대학 컴퓨터학부

교통카드, 전자화폐, 의료카드 등 다양한 기능과 뛰어난 보안성, 그리고 기존 IT산업과의 유기적인 결합 등의 장점을 갖는 스마트카드 산업은 2004년 세계 시장의 1/4 이상을 아태지역이 차지할 것으로 전망된다. 이번 특집에서는 교통카드 부문에서 세계적으로 독보적인 위치를 차지하고 있는 우리나라가 스마트카드의 다양한 분야에서 시장을 선점할 수 있도록 관련 표준화 기술 및 시장동향에 대해 살펴보고자 한다.

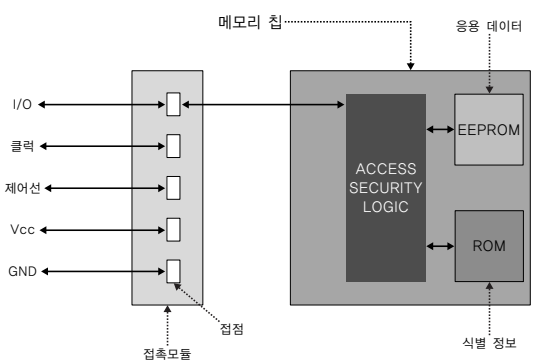
– 스마트카드 특집 순서 –

1. 개요

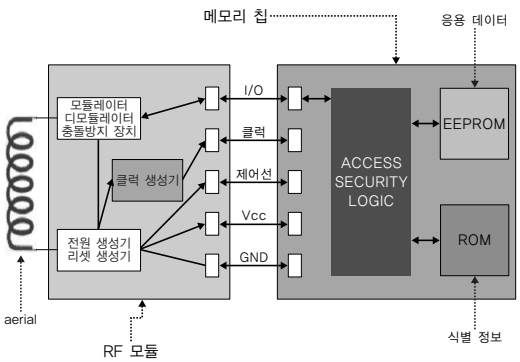
종이카드, 플라스틱카드, 마그네틱카드에 이어서 칩카드가 금융서비스, 교통서비스, 공공서비스, 그리고 의료서비스 등 여러 분야에서 사용되는 추세이다. ISO/IEC JTC1/SC17에서는 이러한 모든 분야에서 사용가능한 칩카드의 기본적인 국제 표준들을 정의하고 있다. 이러한 표준에 맞추어서 칩카드에서 사용되기 위한 칩의 개발이 많은 진척을 보이고 있다.

2. 칩 구성 요소들

칩카드에 장착되는 칩은 크게, 메모리 칩과 스마트 칩으로 구분된다. 메모리 칩은 〈그림 1〉과 같은 접촉식 메모리 칩과 〈그림 2〉와 같은 비접촉식 메모리 칩으로 구분된다. 접촉식 메모리 칩은 접근보안 논리회로(ACCESS SECURITY LOGIC), EEPROM, ROM 그리고 접점 등으로 구성되어 있다.



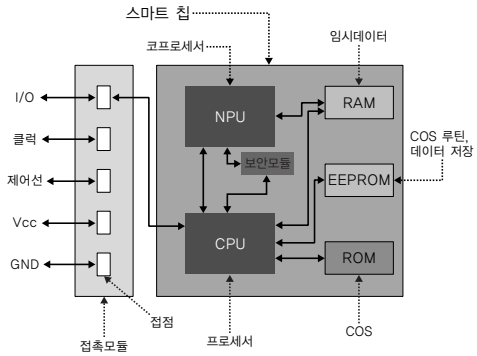
〈그림 1〉 접촉식 메모리 칩



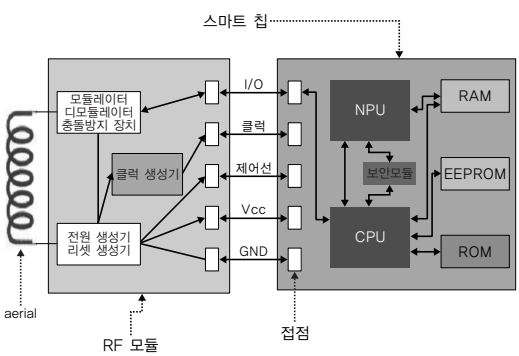
〈그림 2〉 비접촉식 메모리 칩

접근보안 논리회로는 EEPROM 및 ROM에 저장된 데이터 및 정보에 접점을 통한 외부장치에 또는 외부장치로부터의 접근 및 통제, 임의 변경과 삭제를 관장하는 부분이다. EEPROM은 메모리카드가 적용되는 서비스에 맞는 응용데이터를 저장하는 부분이고, ROM은 메모리 카드의 식별정보를 저장하는 부분이다. 접점은 메모리 칩과 외부장치로부터의 데이터의 입력/출력을 하는 통로이고, 클럭은 외부장치로부터의 클럭 신호를 입력받는 부분이며, Vcc 및 GND는 외부장치로부터의 전원을 받아들이는 부분이다. 접촉식 메모리 칩은 접촉 접점을 통해서 데이터 및 전원이 공급되어 동작하는 수동방식이다. 비접촉식 메모리 칩은 접촉식 메모리 칩에 RF 모듈이 첨부된 칩이다. RF 모듈을 통해서 전원 및 데이터의 전송이 이루어진다. 이러한 메모리 칩을 이용한 메모리카드는 단일 응용분야에 주로 사용된다. 주 사용분야는 전화카드, 선불카드, 주차카드, 교통카드, 로얄티카드 등에 사용된다.

스마트카드에 장착되는 스마트 칩은 메모리 칩과 마찬가지로 접촉식 스마트 칩과 비접촉식 스마트 칩으로 구분된다. 스마트 칩은 중앙처리장치인 CPU(Central Processing Unit), 코프로세서인 NPU(Numerical Processing Unit), 보안 모듈, EEPROM, ROM, RAM 등으로 구성되어 있다.



〈그림 3〉 접촉식 스마트 칩



〈그림 4〉 비접촉식 스마트 칩

CPU는 스마트 카드 사용시에 해당 연산을 처리하는 장치이다. NPU는 CPU의 산술 연산을 중점적으로 처리하는 장치로서 고속의 연산을 위해서 스마트 칩에 구현된다. 주로, 가격 때문에 구현되지 않는 경우가 보통이다. 보안모듈은 스마트 칩이 응용프로그램을 구동할 때에 보안기능을 담당하는 부분으로 하드웨어적으로 구현되는 경우도 있고, 아닌 경우도 있다. 보안모듈이 하드웨어적으로 구현되지 않는 경우에는 스마트 칩은 이 기능을 소프트웨어적으로 처리한다. ROM은 스마트 칩을 위한 칩 운영체제인 COS(Chip Operating System)가 탑재된다. EEPROM은 COS의 일부분과 응용프로그램이 탑재된다. RAM은 응용프로그램을 구

동할 경우에 임시 메모리로서 작용한다.

비접촉식 스마트 칩은 접촉식 스마트 칩에 RF 모듈이 장착된 칩이다. 이들 스마트 칩들은 메모리 칩과 마찬가지로 전원을 외부로부터 공급받아서 구동하는 수동방식이다.

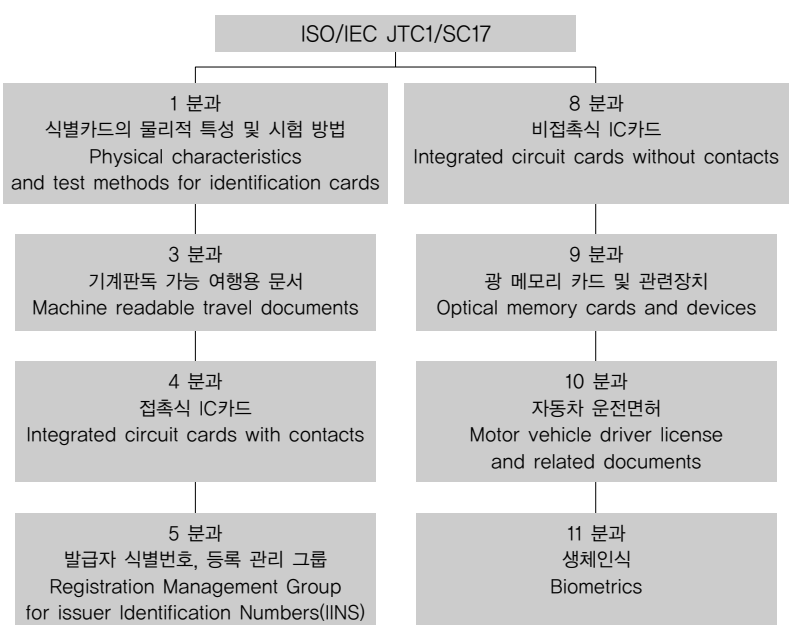
스마트 칩에 접촉식과 비접촉식의 모듈이 동시에 구현되어서 접촉식으로 또는 비접촉식으로도 메모리에 있는 데이터를 처리할 수 있으면, 콤비 칩이라 한다.

스마트 칩은 주로 8비트 프로세서가 사용되어지고 있으나, 32비트 또는 그 이상의 성능을 지닌 칩들도 등장하고 있다. 이들 프로세서는 주로 CISC(Complex Instruction Set Computer) 방식이 주종을 이루나, RISC(Reduced Instruction Set Computer) 방식을 채택하는 경우도 있다. CISC 방식의 8비트 스마트 칩은 모토롤라 6805나 인텔 8501에 기초하여 설계된다. RISC 방식의 16비트 스마트 칩은 히다찌의 H8 칩이 대표적이고, RICS 방식의 32비트 칩은 ARM 7M RISC 칩이 대표적이다.

스마트 칩은 사용용도에 따라서 다양하다. 특히, 보안모듈이 하드웨어적 또는 소프트웨어적으로 구현되어 있어서 보안기능이 필요한 경우에 주로 사용한다. (주)SUN의 자바 칩, 몬덱스의 MULTOS 칩은 오픈 플랫폼을 지양하는 대표적인 칩이다. GSM 방식의 통신용 단말기에 장착되는 SIM(Subscriber Identify Module)과 CDMA 방식에 장착되는 USIM (Universal Subscriber Identify Module), GSM과 CDMA에 장착이 가능한 R-SIM(Roaming Subscriber Identify Module) 또한 대표적인 스마트 칩이다.

3. 표준화

칩 자체에 대한 표준은 정해지지 않았지만, 스마트 칩이 사용되는 응용 분야에 따라서는 국제 표준이 정해져 있다. ISO/IEC JTC1/SC17은 이들 모든 표준의



〈그림 5〉 ISO/IEC JTC1/SC17 분과 구성도

근간이 된다. GSM과 EMV 또한 SC17에 근간을 두고 있다. ISO/IEC JTC1 SC17은 정회원이 32개국이며, 준회원은 10개국이다. ISO 내의 liaison은 TC68, TC171, SC23, SC25, SC27, SC31 등이며, 협력기관 분류 A등급은 AMEX, ECBS, ECMA, EUROPAY, IATA, ICAO, ICMA, MASTERCARD, 그리고 VISA 등이 있다. SC17은 〈그림 5〉와 같이 11개 분과로 이루어져있다. 여기서, 2분과, 6분과, 그리고 7분과는 더 이상의 아이템이 없어서 폐쇄되었다.

보안모듈은 금융 거래와 통신 분야에서 쓰이는 표준 암호 알고리즘으로서 DES나 T-DES가 사용되며, 국내에서는 SEED를 권장하고 있다. 특히, 스마트 카드나 스마트 칩과 단말기 사이에서의 인증을 위한 난수 생성기는 CPU에 통합되어 구현한다.

전원장치는 1분과의 ISO 7816-3 표준에 의하면, 그룹 A의 공급 전력은 5볼트이고 공급 전류는 100 미리 암페어를 초과하면 안되고, 그룹 B의 공급 전력은 3볼트이고 공급 전류는 50 미리 암페어를 초과하면 안된다고 규정하고 있다. GSM 11.11 규약에 의하면 GSM SIM 칩의 전류는 10 미리 암페어를 초과하면 안된다고 규정하고 있다.

4. 칩 시험 · 인증

스마트 칩은 스마트카드의 핵심이다. 따라서, 스마트 칩에 대한 철저한 시험 · 인증은 스마트카드 사업의 모든 분야에 안정성 및 보안성에 많은 영향을 미친다. 스마트 칩의 시험 · 인증은 개발자 측면에서는 개발제품에 대한 객관적인 평가 및 인증을 만족시키고, 사용자 측면에서는 신뢰성과 안정성 요구를 만족시킨다. 스마트 칩의 시험 · 인증은 크게, 물리시험 인증과 보안시험 인증으로 구분한다.

4.1 칩 물리시험 인증

스마트 칩에 관련된 스마트카드의 물리시험 인증에 관한 국제 표준은 ISO 10373에 다음과 같이 정의되어 있다.

- ISO 10373-1 식별카드 - 검사방법 - Part 1 : 일반 구조 검사
- ISO 10373-3 식별카드 - 검사방법 - Part 3 : 접촉식 카드
- ISO 10373-6 검사방법 - Proximity cards
- ISO 10373-6/AM1 검사방법 - 근접형카드 (Proximity cards) - 부록 1 : 추가적인 PICC 검사방법
- ISO 10373-6/AM2 검사방법 - 근접형카드 (Proximity cards) - 부록 2 : 개선된 무선주파수(RF) 검사방법
- ISO 10373-7 식별카드 - 검사방법 - Part 7 : 원격형 카드(Vicinity cards)

특히, 이 중에서 스마트 칩에 관한 물리시험 인증부분을 정리하면 다음과 같다.

- 접점 저항 시험 · 인증
- 전기장 시험 · 인증
- 정전기 내성 시험 · 인증
- 전기적 특성 시험 · 인증
- 서지(SURGE) 시험 · 인증
- 전원전압 변동 시험 · 인증
- RF 방사전자 시험 · 인증
- RF 전조전자 시험 · 인증
- 자외선 시험 · 인증

접점 저항 시험 · 인증은 스마트 칩과 단말기의 오동작을 사전에 예방하고 신뢰성을 높여서 접점의 기능과

동작을 원활히 하는 것이 목적이다. 스마트 칩의 접촉식 모듈부분과 단말기의 접촉식 모듈의 접점저항은 특정 오옴 미만이어야 한다. 전기장 시험 · 인증은 스마트 칩에 자기장이 인가될 때 스마트 칩의 자기장 내성 여부를 확인하고 성능을 평가한다. 정전기 내성 시험 · 인증은 스마트카드의 사용자로부터 물체 근처에서 방전되는 정전기 방전에 영향을 받는 스마트 칩에 대한 내성여부를 평가한다. 전기적특성 시험 · 인증은 스마트 칩의 전기적 동작의 기능을 시험한다. 서지 시험 시험 · 인증은 과전압에 의하여 야기될 수 있는 서지를 스마트 칩의 전원선 및 상호접속선들에 인가시켜 스마트 칩의 성능 및 기능을 유지하는지를 평가한다. 전원전압 변동 시험 · 인증은 저전압 전원회로망에 접속되는 스마트 칩의 전압강하 및 전압변동에 대한 내성여부를 평가한다. RF 방사 전자시험 시험 · 인증은 스마트 칩에 RF를 방사시켰을 경우의 스마트 칩의 성능을 평가한다. 자외선 시험 시험 · 인증은 스마트 칩에 장착된 EEPROM이 자외선에 의해서 저장된 정보의 내용이 변화 또는 오동작이 발생하는지를 평가한다.

4.2 칩 보안인증

스마트 칩은 보안이 핵심이다. 따라서, 스마트 칩의 안전 및 신뢰성 검증은 필수항목이다. 보안에 대한 IT 분야의 평가는 ITSEC(Information Technology Security Evaluation Criteria)에서 진행한다. ITSEC은 다양한 상업적, 군사적 응용에 대한 보안평가를 제공하는 독립적인 조직이다. ITSEC에서 진행하는 평가는 하드웨어 및 소프트웨어에 대한 평가를 한다. 특히, ITSEC은 1994년부터 스마트카드에 대한 보안평가를 진행했다.

프랑스와 주요 카드제조사들은 이를 발전시켜서 CC(Common Criteria)/PP(protection Profile)를 제정하고 현재는 스마트 카드에 대한 보안을 진행하고 있다. CC/PP에서 인증하는 스마트 칩 보안인증 레벨은 국제적으로 EAL1 ~ EAL7까지로 구분한다. CC/PP를 인증하는 국가는 프랑스, 독일, 미국, 일본 등이 진행하고 있다. 한국은 한국정보보호진흥원이 준비중에 있다. 한국이 인증하는 레벨은 K1 ~ K7까지이며, 보안레벨이 높을수록 보안이 높다.

칩 보안인증은 칩 자체 보안인증, 칩에 탑재된 COS 보안인증, 그리고 칩에 탑재된 응용프로그램 보안인증으로 구분된다. 칩 보안인증의 평가대상은 칩 자체로서 환경상의 취약성을 분석하는데 그 목적이 있다. COS 보안인증의 평가대상은 칩에 적재된 COS의 신분확인, 접근통제등의 보안기능과 응용프로그램과의 인터페이스이다. 응용프로그램 보안인증의 평가대상은 평가신청자의 요청에 의해서 이루어지며, 평가 신청대상자가 원하는 기능을 평가한다.

CC/PP의 칩 보안인증을 받은 회사는 ATMEL, 삼성, 인피니온, 필립스 등이며, 삼성은 EAL4+ 등급을 획득하였다. CC/PP의 COS 보안인증을 받은 제품은 GemXpressp rpo E64 PK와 Multos다. 스마트 칩과 COS의 보안인증을 받은 제품은 히다찌 AE45C에 탑재된 Multos이다. 스마트 칩, COS 그리고 응용프로그램의 보안인증을 받은 제품은 히다찌 H8/3112에 탑재된 Multos 버전 3에 구현된 몬덱스 지불 응용프로그램이며, Schlumberger/Sema와 인피니온에 탑재된 자바에 구현된 CRISTAL이다.

5. 결론

메모리 카드와 스마트카드로 구성되는 칩 카드는 아직 활성화 단계에 있다. 스마트 칩이 장착된 스마트카

드는 사람들이 소지하고 다니는 열쇠, 지갑, 신분증 등 그 사용 가능성은 무한하다.

IMT-2000과 같은 이동전화 등의 통신기기에 장착되는 SIM 또는 USIM 카드는 단순 이동통신기기의 요금 결제를 벗어나서 무선 전자상거래에도 적용 가능하여 스마트 칩에 의한 탁월한 보안기능에 의해서 사용이 간편한 전자상거래 장치로 사용되게 될 것이다. 금융 분야에서도 2005년부터는 모든 신용카드를 비롯한 현금카드 및 직불카드들이 스마트 칩이 장착된 칩 카드가 사용되어야 한다. 모든 국가의 정부들이 전자정부를 구현하고자 하므로, 국가 차원의 전 국민 카드가 필요하다. 이러한 전 국민 카드는 주로 다기능을 요구하므로, 다기능 카드에 대한 인식도 필요하다.

전반적으로 카드 이용자들의 인식이 점차 뚜렷해지면서 보다 향상된 카드에 내장된 칩의 용량 및 처리능력, 인터페이스 등이 요구되어진다. 특히, 다기능을 요구하는 스마트카드는 메모리 용량과 고성능의 마이크로 컨트롤러 처리능력에 따라 급속하게 확산될 수 있고, 이들 칩 개발은 반도체 및 부품 기술에 의존한다. 따라서, 스마트 칩 반도체 분야는 다른 영역의 응용 반도체보다 훨씬 더 빠르게 진전될 수 있다. 특히, 보안용 스마트 칩 개발은 제조사 및 관련 벤더들에게 있어 여러 가지 이유로 보안시장의 점유에서 성공할 수 있는 필수적인 요소이다. TTA