특 집

전자화폐와 차세대 IC카드 기술

박 영 수, 전 성 익, 정 교 일
한국전자통신연구원 정보보호기반연구부

I. 서 론

전자화폐(Electronic Cash)의 등장[1]은 디지털 혁명 시대의 큰 변화인 경제 활동의 변화에서, 기존에 존재하던 많은 실물 시장은 가상 공간으로 이전하게 되고 이 속에서 디지털 데이터를 근간으로 하는 각종 구입, 판매 그리고 대금 지불이 이루어지게 된다. 이러한 환경에서 가장 중요하게 거론되고 있는 것은 지불 방법에 관한 문제이고, 기존의 지불 방법으로는 한계 즉, 사용 불편, 시간적·공간적 제약이 발생하게 된다. 따라서 인터넷 환경에 적합한 새로운 지불 방법이 요구되고 있으며 그 해결책으로 전자화폐가 등장하게 되었다.

전자화폐는 디지털 데이터 자체가 가치를 갖는 형태인 전자지갑(워크스테이션, IC카드, 개인 휴대 단말)에 저장되는 형태가 많다. 이 형태는 기존의 화폐가 가져야 하는 법적인 효력과 안전성에 관한 기능을 그대로 가지면서 IC카드와 같은 별도의 기기나 컴퓨터 등에 소프트웨어 형태로 존재하는 전자지갑에 의하여 관리된다.

전자화폐 종류는 전자상거래를 위하여 네트워크환경에서 사용 가능한 전자화폐와 신용카드 등과 같은 자기 플라스틱 카드를 대용하는 IC카드형 전자화폐가 있다. IC카드형 전자화폐는 사람이 직접 가지고 다니면서 현금이나 신용카드 대신 사용하는 화폐로서 전자상거래와는 일단 거리가 있지만, 최근 네트워크상의 전자상거래에 이용되는 전자화폐 시스템에서 IC카드 기능을 수용한 시스템이 나오고 있는데, IC카드가 안전한 가치의 저장, 거래 정보 저장, 그리고 사용자 인증 등을 위한 좋은 매체이기 때문이다.

본 고에서는 II장 IC카드 기술, III장 IC카드 표준, IV장 IC카드 시장 동향의 순서로 IC카드의 기술에 대하여 살펴본다.

II. IC카드 기술[2,3,4]

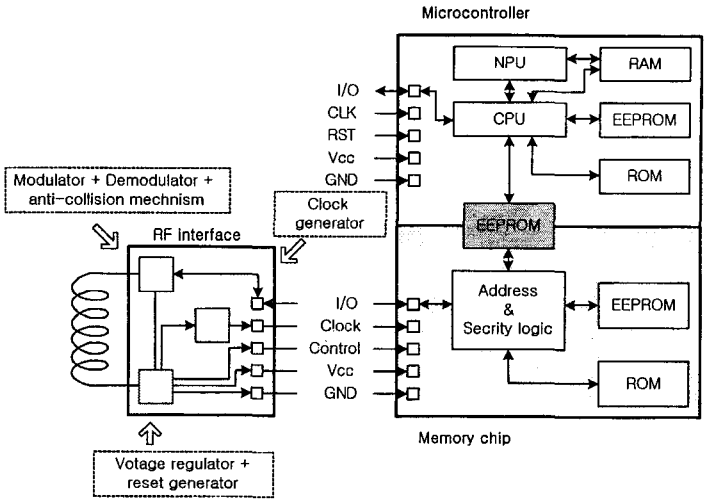
IC카드(혹은 스마트카드)는 마이크로프로세서와 메모리를 내장하고 있어서 카드 내에서 정보처리와 저장이 가능한 플라스틱 카드로 편리성/다기능성 및 보안성을 주요 특징[5]으로 한다.

IC카드 종류는 마이크로프로세서의 포함 여부(마이크로프로세서, 메모리 카드), 인터페이스 방식(접촉, 비접촉, 하이브리드, 콤비카드) 등에 따라서 분류할 수 있다. 접촉식 카드는 판독기와 물리적인 접촉에 의하여, 비접촉 카드는 일정 거리 떨어져서 작동하는 카드이다. 하이브리드 카드는 서로 다른 카드의 종류를 하나에 구현한 것으로, 자기 카드에 스마트카드를 포함하는 형태나 접촉 및 비접촉식의 인터페이스를 모두 갖는 형태도 있다. 콤비 카드는 하이브리드와 같이 접촉·비접촉 인터페이스 모두 가지지만 같은 메모리를 가지며 상호 보완적으로 사용되는 점이 다르다.

1. 반도체 기술

카드 칩은 주문형 IC로 개발되어 공급되며 다음과 같은 구성 요소 및 제조 기술을 사용한다.

- CPU : 운영체제에 따라 명령어 수행, 어플



〈그림 1〉 콤비 카드 (듀얼 인터페이스 카드)[6]

〈표 1〉 접촉·비접촉 IC카드의 특징

분류 / 특성	접촉식	비접촉식			
		밀착형	근접형	근방형	마이크로파형
ISO 표준	ISO 7816	ISO 10536	ISO/IEC 14443	ISO/IEC 15693	미심의
접근거리	판독기 삽입	~2mm	~ 약 10cm	~ 약 70cm	~ 수 m
주파수대	3.57MHz	4.91MHz	13.56MHz	13.56MHz	2.45GHz
보안	◎	◎	○		
고속처리		◎	◎	◎	
전지	불필요	불필요	불필요	불필요	필요
메모리 용량	◎	◎	◎	○	○

주) ◎ : 매우 우수, ○ : 우수

리케이션 지원 등 여러 가지 다른 응용을 하나의 칩상에서 지원

- 암호처리 코프로세서 : 현행 DES 방식보다 안전성이 높은 RSA 방식은 연산량이 방대하여 8비트 프로세서로는 불가능하므로 별도의 전용 회로를 갖고 있는 코프로세서 또는 크립토 프로세서
- 메모리 : 데이터를 저장하기 위한 휘발성 메모리(DRAM, SRAM), 운영체제와 CPU 명령 저장 메모리(ROM), 그리고 운영체제에 다운로드되는 어플리케이션을 위한 메모리(EPROM, EEPROM, FRAM)
- 제조 기술 : 다기능 카드가 요구되면서, 더 큰 처리 능력과 메모리를 가진 새로운 반도체가 요구되고 IC카드의 중요성이 더해지면서 가장 진보된 서브미크론 공정 사용

2. 운영체제/API

운영체제는 소프트웨어 코드를 실행시키고 실리콘 하드웨어 기능을 활성화 시킬 수 있는 공통적인 플랫폼을 제공한다. 어플리케이션 개발 업체는 다년간, 다양한 고객의 어플리케이션을 위한 공통 플랫폼으로서 고유한 운영체제를 사용하였기 때문에 고객은 어플리케이션 개발 업체에 종

〈표 2〉 IC카드의 진화 단계별 반도체 기술

단계 / 기술	메모리카드 (1997~현재)	단기능카드 (1981~현재)	다기능카드 (1988~)	네트워크카드 (2001~)	컴퓨터카드 (2002~)
마이크로 컨트롤러	없음	8bit	8, 16, 32bit RISC	16, 32bit RISC (암호화지원)	32bit RISC, 암호화지원
사용 메모리	EPROM, EEPROM	EEPROM	EEPROM, Flash, FRAM	EEPROM, Flash, FRAM	EEPROM, Flash, FRAM
메모리 용량	수십~수백 bit	1~16KB	>8KB(8bit), >32KB (>16bit)	>256KB	>512KB
공정기술	>1 μm	0.5 μm(1998)	0.5 μm(8bit), 0.35 μm (>16bit, 1999)	0.25 μm(2000)	0.18 μm(2002)
차별화 요소	가격	좌동, 메모리 용량	좌동, 처리속도	좌동, 암호처리	좌동, 디지털신호처리, 생체측정, 사용자 interface
응 용	전화카드, 1회용금액카드	은행·보건카드, 충전식카드, GSM카드	은행·보건카드, 충전식카드, GSM카드포함 다중 응용	네트워크식별, 인증/보안거래 중점의 다중 응용	데이터처리중점의 다중 응용

속되어 다른 업체로부터 새로운 코드를 카드로 다운 받을 수 있는 기회가 없고, 카드 운영체제와 온-카드 어플리케이션 사이의 단단한 결합을 제공하였다.

Sun, MAOSCO, 그리고 Microsoft는 이를 극복하고, 판매 업체와 어플리케이션 경계를 넘는 유니버셜 칩카드 OS를 제공하려고 시도해 왔다. 즉, 어플리케이션 개발 업체들이 카드 발행업체와 독립적으로 어플리케이션을 만들 수 있게 하며, 궁극적으로 카드 사용자들이 사용 카드에 포함되기를 원하는 어플리케이션 프로그램을 결정할 수 있게 해준다. 이것은 카드의 호환성과 다기능 카드에는 좋은 징후이나 카드 보안과 오작동에 관한 한 불안 요소이다.

3. 보안 기술

스마트카드에 있어서 매우 중요한 특징이며, 가장 중요한 요소 기술의 하나이다. 가시적인 보안 특징들뿐만 아니라 칩, 운영체제, 네트워크, 어플리케이션 등에 있어서 보안 기능을 갖는다. 가시적인 보안 특징은 IC카드를 육안으로 식별할 수 있도록 사진 부착, 서명 띠, 홀로그램, 양각 및 초미세 인쇄 등의 방법이 있다. 칩의 보안 특징으로는 칩의 생산 과정에서 미세회로를 이용하여 시험한 후 외부로부터 직접 내부 액세스하는 것이 불가능한 모드로 전환시킨다. 칩 깊숙이 액세스 불가능한 위치에 소자를 묻는 방법으로 분해공학(reverse engineering)을 방지한다. 또한 주요 구성 요소를 연결하는 데이터 버스는 스크램블 시킨다. 메모리 셀에서 방출되는 전기적인 신호를 외부에서 감시되는 것을 막기 위하여 이 영역을 금속차폐물로 코팅하고 자외선이 메모리 내용을 지우는 것을 방지하기 위하여 보호막(passivation layer)으로 코팅한다. 이것 이외에도 외부로부터 칩의 변경(tampering)을 탐지하기 위한 회로로 너무 높거나 낮은 전압, 클럭 주파수, 온도 등을 검출해내는 회로가 있다.

운영체제의 경우, 모든 메모리 접근은 CPU를 경유해야 하므로 논리적인 수준에서 카드의 보안을 구현하는 것이 카드 운영체제의 설계에 상당

〈표 3〉 카드 칩 운영체제 및 API 특징

운영체제	장 점	단 점
JavaCard	- Java 지식기반은 스마트카드 어플리케이션을 넘어 확장 - JavaCard SIM의 GSM 사용 - PicoJava에 최적화된 프로세서 코어의 라이센스하에 이용 가능 - Java는 OS에 독립적인 인터프리트 언어	- 인터프리트 언어 방식이 실행시간 제한 - 라이선스 비용으로 인해 가입자 제한 - 관리 및 보안 산업의 우려 - PicoJava 실리콘 라이선스가 오직 4개 업체에만 발행됨
MultOS	- 안전한 어플리케이션에 대해 안전한 관리 절차가 선호됨 - 일부 은행에서 선호, MasterCard 편애 - 8비트 마이크로컨트롤러에 최적화된 OS	- VisaCash SVC가 JavaCard Open Platform을 선택 - 유럽의 CEP가 MultOS와 전쟁 - Mondex 전자지갑 외 시험운영이 제한적 - 라이선스 비용으로 가입자 제한
Windows Card (SCfW)	- Microsoft 제품이 널리 사용됨 - 판촉 및 지원되는 저가의 개발 도구 - Windows 2000 로그온 절차에 맞게 최적화됨	- 늦은 시장 진출 - 산업으로부터 관리 및 보안 우려 - US에서 시작된 제품은 금융 어플리케이션 침투가 제한될 수 있음
업체 고유	- 독특한 코드는 보안 어플리케이션과 ITSEC 승인에 선호됨 - 코드가 이미 특정응용에 맞도록 시험 및 최적화가 됨	- 카드 판매업체에 특징적, 이식성 결여 - 이용가능/생존 가능한 개발도구의 결여 - 대부분 고유 OS는 다기능에 맞게 설계되지 않음

히 중요하다. EEPROM 메모리 내의 전용 파일(Dedicated File : DF)들의 논리적인 구성 즉, 하나의 DF가 선택될 때에 카드 운영체제는 다른 DF에 있는 데이터에 대한 접근 금지로 보안 장벽을 만들 수 있다. 또한 파일들에 대한 액세스는 개인식별번호(PIN)나 암호키를 이용하여 보호할 수 있다.

네트워크상의 손쉬운 접근은 IC카드의 접촉패드를 통해서 이다. 카드와 판독기 사이에 흐르는 데이터를 가로채기 위하여 변경된 판독기에 넣을 수 있다. 이러한 공격에 대하여 데이터의 무결성이 유지되기 위하여 통신 링크들은 부정한 조작으로부터 물리적으로 보호되어야 한다. 어플리케이션은 프로그램 자체에 많이 의존하며, 전술한 구성 요소들이 서로 결합되어 동작될 때 카드 시스템의 보안이 강화된다.

4. 안테나 및 무선통신 기술

비접촉식 카드는 모든 입출력, 전력까지도 RF 신호를 통하여 전송되므로 카드 내에 코일 안테나가 모듈의 크기나 칩 자체의 주변을 여러 번 감는 형태로 만들어진다. 신호는 125 kHz · 13.56 MHz 등의 지정된 주파수를 사용하며 RF 신호 변조에는 AM, FM, ASK, FSK 또는 BPSK 방식이 사용된다. 저전력 카드 칩의 필요에 의하여 낮은 주파수의 사용은 많은 전력이 전송될 수 있으나 데이터 전송 속도가 느린 반면 최고 1m 까지 통신 가능하다.

III. IC카드 표준[3]

1. 어플리케이션 표준

CEN(European Committee for Standardization)은 기기판독 카드 분야의 TC224, 전자지갑 분야의 WG 10을 통하여 운영되며 정보통신 기술 분야에서 방향을 설정하는 역할을

한다. CENELEC(European Committee for Electrotechnical Standardization)은 IEC (International Electrotechnical Commission) 표준이 적용 받지 않는 모든 전자기술분야에 대한 표준 개발을 담당한다. ETSI(European Telecommunications Standard Institute)는 텔레 커뮤니케이션 표준을 결정하고 만들어 내는 조직으로 특히, SMG9 위원회는 모바일 사용자가 스마트카드를 통해 글로벌 로밍에 접속할 수 있도록 공통 표준을 제공한다. ETSI GSM은 SIM(Subscriber Identification Modules)을 이용하는 GSM에 대한 표준 담당한다. EMV는 카드 접속, 보안 , 지불 기능의 상호 운용성을 구체화하여 기존 마그네틱 카드 교체를 위한 국제 개방 암호화 칩 카드 표준 개발을 위해 채택되었으며, ICC 및 ISO 관련 기기 표준에 기반을 두고 있다.

2. 하드웨어 표준

ISO(International Organization for Standards)에 의한 접촉식 스마트카드 표준을 비롯하여, 비접촉식 카드 및 ISO카드 관련 표준 등이 있다.

3. 인터넷 지불 관련 표준

SET(Secure Electronic Transaction)은 전자상거래에 대한 PC 키보드를 기반으로 한 지불 프로토콜로 마그네틱 카드 사용자가 인터넷을 통하여 데이터를 전송하기 위해 개발되었다. X.509는 SET을 사용한 거래의 수행 시 상인은 카드 사용자의 계정이 포함되지 않은 거래 은행으로부터 인가 코드를 받을 수 있는데, 이러한 문제는 신용카드 정보 접속을 방지하도록 신용카드 번호에 대한 X.509 인증의 대체로 해결되었다. C-SET(Chip-SET)은 SET과 상호 운용적이고 직불/신용 지불 및 전자지갑 지불 모두를 지원한다.

Ⅳ. IC카드 시장 동향[3]

메모리카드와 스마트카드로 이루어진 칩 카드 시장은 유럽을 중심으로 매우 활발하게 성장하고 있으며 전자상거래 등의 상거래시 지불의 편리성, 보안 및 인증의 용이성으로 이용 범위가 확산되고 있다. 메모리카드는 선불전화카드 어플리케이션, 스마트카드는 GSM SIM 어플리케이션에서 선호되고 있다. 카드 내에 내장된 운용체제와 API를 이용하여 카드 응용서비스 제공업자가 다양한 분야에서 적합한 형태로 프로그래밍이 가능한 형태를 제공하기 때문에 다기능 고부가 가치를 제공하는 스마트카드 관련 기술개발에 주력하고 메모리 카드의 경우 기존 시장을 중심으로 성장률이 둔화되는 추세이다.

2001년 전세계 칩 카드 선적[5]은 약 19억 개로 이중 스마트카드는 35% 정도이다. 전체의 77% 정도를 Gemplus, Schlumberger, Giesecke & Devrient, Oberthur Card Systems의 4개사가 출하한다. 칩 카드 반도체의 선적량은 약 22억 개, 마이크로 컨트롤러 35%와 메모리 65%이다. 마이크로 컨트롤러는 Infienon Technologies, STMicroelectronic, Philips Semiconductor, Hitachi의 4개사가 91% 이상을 차지하며, 메모리는 Infienon Technologies, STMicroelectronic, Philips Semiconductor의 3개사가 98% 이상을 점유한다.

1. 칩 카드 반도체 기술

반도체 업체들은 운용체제를 장착하는 스마트카드의 다기능성 및 다응용성을 만족시키기 위해 새로운 마이크로 컨트롤러[5] 개발에 주력하고 있다. 특히 칩의 다기능성과 거래시의 보안 및 인증에 대한 요구를 충족시키기 위한 다양한 기술을 선보이고 있다.

2. 칩 카드 업체

스마트카드 시장 진입을 시도하는 IT 벤더들은 기술주도의 제품을 공급하거나 서비스 제품을

〈표 4〉 스마트카드 마이크로 컨트롤러 실리콘 동향

실리콘 동향	효 과
0.5 마이크론 이하의 제조공정	웨이퍼당 다이수 증가와 추가 EEPROM 집적 가능
코드화된 물리적 제조공정	분해 공학에 의한 저항 강화
온칩 암호 코프로세서	트랜잭션 보안을 위한 DES, RSA, EC 암호화
메모리 관리 장치	다수 어플리케이션 사이의 메모리 firewall 제공
64KB 이상의 대용량 EEPROM	다중 어플리케이션 허용
플래시 메모리 집적	칩상 메모리 증가
강유전체 메모리, FRAM	저전압 동작으로 비접촉식 카드의 기능 향상
듀얼 인터페이스(ISO7816 & ISO14443)	교통/접근 기능의 추가적 어플리케이션 결합의 필요
JavaCard, MultOS, SCfW의 최적화	다중 카드 판매업체 설계 기회 확대

내세워 접근하고 있다. 기술 주도 제품은 Sun Microsystems와 ERG 의 플랫폼과 SecureNet, RSA, security & Baltimore Technologies 등의 금융서비스 솔루션, 디지털 인증 및 보안 솔루션을 제공하는 소프트웨어 형태이다. 서비스 제품은 금융서비스 시장을 목표로 컨설팅 및 시스템 통합 서비스와 멀티 어플리케이션을 위한 카드 발급과 트랜잭션 처리 서비스 등이다.

아울러 벤더간의 제휴 또는 협력 사업의 일환으로 멀티 어플리케이션 스마트카드를 위한 공동연구, 무선 어플리케이션과 스마트카드 어플리케이션을 연계, 그리고 스마트카드를 통한 금융 어플리케이션과 대량 트랜짓 어플리케이션 연결을 위한 제휴 작업들이 진행중이다.

3. 칩 카드 응용 분야

다양한 분야에서 이루어 지고 있지만, 금융, ID 인식 액세스의 세가지로 대별될 수 있으며, 신용/직불 카드, 교통, 네트웍 보안, ID/접속에 성장 전망이 밝다[4].

이외에 이동통신 단말용 스마트카드 모듈로는 SIM, R-UIM 및 USIM이 있다. SIM은 최고의 스마트카드 어플리케이션으로 새로운 가입자 수와 모바일 핸드셋 수를 증가시키고 있다. 가트너 조사에 따르면 아시아/태평양 지역의 중고 시장과 선불 서비스는 서유럽과 중국에서 SIM 수요를 자극하고 있다.

V. 결 론

스마트카드의 응용분야의 확산에 따라서 스마트카드의 보안성, 정보처리 능력 등의 특성을 바탕으로 하는 다기능 카드를 필요로 한다. 다기능 수용에 따른 메모리 용량 문제는 반도체 기술의 발전으로 해결 가능하고, 처리 능력의 강화를 위하여 저가의 고성능 마이크로 컨트롤러의 개발이 지속되고 있다. 보안성 강화는 반도체 기술과 비대칭 암호프로세서의 사용으로 더욱 강화되고, 듀얼 및 USB 인터페이스 적용과 같은 사용의 편리성을 위하여 기술적인 측면의 연구개발이 발전을 가속화 시키고 있다. 아울러 멀티 어플리케이션 제품을 통하여 시장을 창출하고 스마트카드 솔루션을 제공하는 순수 기술적 기능에 비즈니스 솔루션을 연계하여야 스마트카드 관련 산업의 성장을 기약할 수 있다.

참 고 문 헌

〔1〕 이만영 · 김지홍 · 류재철 · 송유진 · 염홍열 · 이임영, 전자상거래 보안 기술, 생능출판사, pp.275~317, 1999년 9월

〔2〕 한국전자통신연구원, 스마트카드 기술/시장 보고서, 30대 품목 기술/시장 보고서 시리즈,

1999년 12월
〔3〕 한국전자통신연구원, 스마트카드 기술/시장 보고서, 40대 품목 기술/시장 보고서 시리즈, 2000년 11월
〔4〕 한국전자통신연구원, 스마트카드 기술/시장 보고서, 50대 품목 기술/시장 보고서 시리즈, 2001년 12월
〔5〕 이윤철, 전세계 스마트 카드 기술 및 시장 동향, 주간기술동향 1068호, 2002년 10월 16일
〔6〕 W. Rankl, W. Effing, Smart Card Handbook Second edition, John Wiley & Sons, LTD, pp.15~25, 2000년

저 자 소 개

朴 永 秀
1985년 2월 중앙대학교 전자공학 학사, 1987년 2월 중앙대학교 대학원 전자공학 석사, 1990년 2월~현재 : 한국전자통신연구원 IC카드연구팀 선임연구원, 〈주관심 분야 : CAD 및 VLSI 설계, 암호 프로세서, IC카드 등〉

全 星 翼
1985년 2월 중앙대학교 전자계산학 학사, 1987년 2월 중앙대학교 대학원 전자계산학 석사, 1987년 2월~현재 : 한국전자통신연구원 IC카드연구팀장/책임연구원, 〈주관심 분야 : 운영체제, 시스템 소프트웨어, 스마트카드 기술 등〉

鄭 敎 逸
1981년 2월 한양대학교 전자공학 학사, 1983년 8월 한양대학교 산업대학원 전자계산학 석사, 1997년 8월 한양대학교 대학원 전자공학 박사, 1981년 12월~현재 : 한국전자통신연구원 정보보호연구본부 정보보호기반연구부장/책임연구원, 〈주관심 분야 : IC Card, Security, Biometrics, 국가기반보호, 신호처리 등〉