主題

전자상거래를 위한 IC카드 기술

한국전자통신연구원 한진희, 이창욱, 정교일, 손승원

차 례

요 약

전자상거래(Electronic Commerce)란, 정부나 기업 및 소비자 등 경제활동의 주체들이 전자적인 매체를 통신망과 결합하여 재화나 용역을 거래하는 제반 행위로 정의된다. 최근 이러한 전자상거래는 인터넷이나 네트워크 상에서 다양하게 발생되고 있는 추세이다. 하지만, 인터넷이나 네트워크 상에서 개인 정보의 유출이 빈번하게 발생되고 있기 때문에 이러한 개인 정보를 보호하기 위한 기술이 절대적으로 필요하다. IC 카드는 그를 위한 기술 중 하나로 알려져 있으며, 본 논문에서는 전자상거래를 보다 안전하게 수행할 수 있도록 개발된 IC 카드 기술에 대해 개략적으로 살펴보고자 한다.

Ⅰ. 서 론

전자상거래(Electronic Commerce)는 광의적 개념의 전자상거래와 협의적 개념의 전자상거래로 구분할 수 있다. 광의적 개념의 전자상거래는 전자상거래 주체인 정부, 기업, 개인간에 전자정보를 통하여 이루어지는 상거래 전반을 의미하고 광고, 수·발주, 개발, 구매, 결제 등 모든 경제 활동을 포함하며, 그 범주는 인터넷 전자상거래 뿐 아니라 전자문서 교환 (EDI : Electronic Data Interchange), 광속상거래 (CALS : Commerce At Light Speed)도 포함된다.

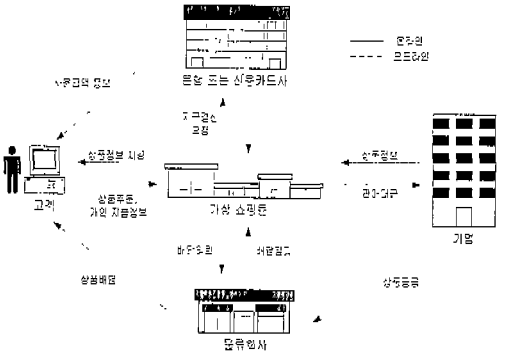

그림 1. 전자상거래 개념도

협의적 개념의 전자상거래는 인터넷이나 통신망을 통해 일반 소비자를 대상으로 상품관련 정보의 제공, 협상, 주문, 납품, 대금지불, 자금이체 등을 통해 마케팅, 판매활동을 수행하는 것을 말한다. 일반적인 전자상거래는 협의의 개념을 수렴한 것으로 그 수행과정은 그림 1과 같다.

협의적 의미의 전자상거래의 과정을 요약하면 고객이 인터넷에 연결하여 상인 서버에 접속 후 상품을 검색하는 단계, 구매 상품에 대한 지불단계, 상인으로부터 상품이나 서비스를 획득하는 단계, 상인 서버와 금융기관과의 통신으로 지불정보를 실제 화폐로 전환하는 단계로 구성된다[1][2].

전자상거래는 인터넷을 통해 거래가 이루어지기 때문에 현재 사용되고 있는 대면 거래와는 달리 비대면 거래로 이루어진다. 따라서 전자상거래가 활성화되고 현실화되기 위해서는 여러 가지 해결해야 할 선결 과제들이 있다. 첫째, 개인의 신용정보, 전자화폐(Electronic Cash), 계약서 등 송·수신되는 정보에 대한 정보보호체계의 확립의 필요성. 둘째, 법·제도·정책의 확립. 셋째, 네트워크 기술의 발전. 넷째, 표준화된 전자지불 시스템 구축 등이다.

통신망상에서는 정보 수집이 용이하므로 개인의 신상관련 정보들을 보호하는 것은 대단히 중요하다. 전자상거래에서도 이는 대단히 중요하게 다루어져야 한다. 최근 이러한 정보보호를 위해 IC(Integrated Chip) 카드가 사용되고 있다. IC 카드는 기존의 신용 카드와 비슷한 크기와 두께를 갖는 플라스틱 카드에 초박형의 마이크로프로세서(MicroProcessor) 및 ROM(Read Only Memory), RAM(Random Access Memory), EEPROM(Electrically Erasable Programmable Read Only Memory) 등의 메모리를 내장시킨 카드이다. IC 카드는 컴퓨터 등의 기기와 인터페이스를 통하여 통신이 가능하고 자체 프로세서를 내장하고 있어 가치 저장 및 연산이 가능하며, 메모리의 용량 및 안정성이 우수한 기록 매체로 사용되고 있다.

이러한 IC 카드를 특성별로 분류하면 칩의 기능에 따라서는 단지 데이터만 저장하는 메모리 카드와 데이터 저장뿐만 아니라 논리연산 회로와 CPU가 첨가된 IC 카드로 분류하며, 인터페이스에 따라서는 접촉형 카드와 비접촉형 카드로 분류하고, 카드 내부전원 유무에 따라서는 능동형 카드와 수동형 카드로, 칩의 수량에 따라서는 Single-Chip IC 카드와 Multi-Chip IC 카드로 분류한다[3].

본 고에서는 IC 카드의 규격 및 보안 기술을 자세히 소개하고, IC 카드를 이용한 전자상거래 활용 실태, 예를 들면 전자화폐 및 전자상거래 시스템 등에 대해 기술한 후, 향후 동향과 문제점 보완을 위한 해결책을 제안하고자 한다.

Ⅱ. IC카드 기술

1. IC 카드 규격

IC 카드는 ISO7816에서 규정한 IC 카드의 구조 및 통신규약을 따르고 있다. IC 카드의 규격은 그림 2와 같으며, 필요에 따라 암호연산용 보조 프로세서(Crypto-Coprocessor)를 내장하기도 한다[4][12].

각 외부 기기와 접촉하는 접점은 데이터 입출력 단자(Input/Output), 회로전압(Vcc), 프로그램 전압공급단자(Vpp), 외부클럭(Clock), 리셋(Reset), 접지(Ground), 예비용 단자 2개로 구성되어 있다. 데이터를 처리하는 데이터 부는 통상 8bit 마이크로프로세서가 내장되어 있어 메모리 읽기, 쓰기 및 외부장치와의 통신처리 기능이 수행된다. 메모리부는 카드 내부 운영체제인 COS(Card Operating System)를 내장한 ROM과 사용자 응용 프로그램과 데이터를 저장하는 RAM, EPROM, EEPROM이 있다.

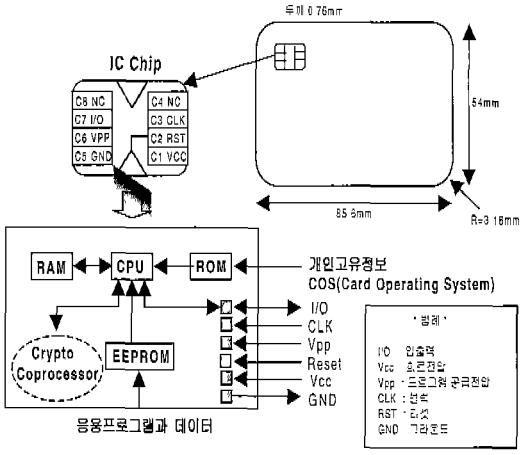

그림 2. IC 카드 규격

이러한 IC 카드의 특성을 보면, 카드 자체의 높은 보안성, 뛰어난 기억능력, 각종 서비스에 대한 융통성 및 기존의 타 종류 카드와의 통합이 가능하여 개인 정보의 분산처리와 통신망의 부담을 감소시켜준다. 하지만, 사용자가 카드 비용을 부담해야 하는 단점도 존재한다.

2. IC 카드의 보안기능

IC 카드는 자체 프로세서를 이용하여 인증 기능, 메모리 접근제어, 암호화연산 등을 제공한다. 카드 대칭/비대칭 암호 알고리즘 기술, 데이터 무결성 확인 기술, 카드와 단말기, 사용자와 카드, 카드와 서버간의 확인을 위한 인증 기술이 카드 보안을 위해 주로 사용되며, IC 카드 해독 방지 기술, 암호프로세서 설계 기술도 최근 중요한 요소로 자리잡고 있다[8][9][10].

2.1. IC 카드를 위한 물리적 보호장치

IC 카드는 우선 카드 자체가 위조가 불가능하도록 특수한 재질과 모양으로 설계되어야 한다. 카드 내부 IC 칩은 위조방지 장치를 적용하여 복제나 위조 노력 시 스스로 소멸하는 기능(Kill Bit Logic)을 도입하고 있고, 이중 금속층 회로(Double Metal Layer of Wiring)기술, 메모리 스캐터링(Scattering)기술, 외부에서 주파수나 광학으로 판독을 방지하는 장치 등으로 IC 칩 내부를 분석할 수 없도록 하고 있다. 이러한 기술은 IC 카드 내부에 저장된 개인 비밀 정보 및 데이터를 외부로부터의 공격에 대해 보호하는 방어 수단으로 사용될 수 있으며, 이러한 기술을 통칭 tamper resistance 기술이라고 정의한다.

2.2. 메모리 접근 통제 기술

메모리 접근 통제는 미리 결정된 조건이 합치할 경우에만 IC 카드가 데이터 메모리에 대한 접근을 허용하는 기능이다. 각 파일은 지정된 키에 의해서만 접근이 가능하며, 그 파일 내용을 갱신할 권한이 있는 기관에서 해당키를 생성하고 분배한다.

IC 카드의 보안성을 유지하기 위하여 가장 중요한 부분인 암호키나 PIN(Personal Identification Number)은 카드 내부에서만 읽을 수 있도록 비밀영역에 저장하여 제시될 때마다 내장된 카드 운영체제에 의하여 감시된다. 특히, IC 카드의 분실과 불법사용자에 의한 부정사용을 방지하고자 미리 정해진 회수이상 잘못된 비밀번호를 입력할 때에는 정당한 사용자가 아님을 인식하고 카드를 Lock 상태로 만들어 이후에는 카드 사용이 불가능하도록 하는 기능도 제공한다.

2.3. 암호 기술

암호화를 이용한 보호 기능은 카드 내부에 암호 알고리즘을 내장하여 데이터 암호화, 카드 및 카드로부터 생성되는 메시지에 대한 인증을 수행하는 기능이다. 이러한 암호 프로그램은 IC 카드 내부의 사용자 데이터를 보호하고 ATM(Automatic Teller Machine) 등의 단말기와 상호 인증을 제공하며, 메시지에 대한 암호화나 전자서명을 제공하는데 사용된다. 현재, 암호기능을 갖는 IC 카드는

관용 암호, 공개키 암호, 해쉬 기능을 탑재할 수 있는데 공개키 암호용 IC 카드인 경우에는 암호연산을 위한 암호 보조프로세서를 탑재하기도 한다.

2.4. 인증 기술

IC 카드의 인증 절차는 아래와 같이 크게 3가지로 분류된다. 우선, 카드에서 사용자를 인증하는 단계, 카드와 단말기간 상호 인증하는 단계를 거친 후, 마지막으로 인증을 마친 사용자가 원하는 응용 프로그램을 수행하기 위해 접근 대상 시스템과의 인증 과정을 거치게 된다. 그림 3은 IC 카드 상에서 발생되는 인증 절차 및 카드의 작동 과정을 보여준다.

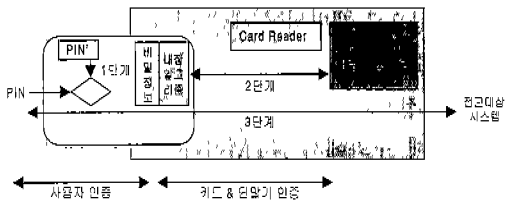

그림 3. IC 카드의 인증 절차

3. IC 카드 표준화 동향

IC 카드 표준은 ISO/IEC JTC1/SC17/ WG4와 ISO/IEC JTC1/SC17/WG8에서 주관하고 있으며, 각각 접촉형 IC 카드와 비접촉형 IC 카드에 대한 물리적 특성 및 전송 프로토콜, 리셋 절차, 데이터 송수신 관련 명령어 등에 대한 규격을 정의하고 있다. 최근에 접촉형 및 비접촉형 IC 카드의 테스트 표준은 10373-3, 10373-4, 6, 7의 표준번호로 제정되고 있다.

10373-3은 접촉형 카드 테스트 표준이며, 10373-4는 비접촉식 밀착형 카드 (Close-coupled Contactless Card)[5], 10373-6은 비접촉식 근접형 카드 (Proximity Contactless Card)[6], 10373-7은 비접촉식 근방형 카드 (Vicinity Contactless Card)[7]를 위한 테스트 표준이다. 표 1과 2는 WG(Wroking Group) 4와 WG8에서 담당하고 있는 표준 제정 목록을 나열하고 있다.

Ⅲ. 전자상거래를 위한 IC 카드의 활용

전자상거래에 있어서 인터넷 쇼핑시장의 가장 큰 문제는 보안 문제이다. 현재는 주로 신용카드를 통해 대금결제가 이루어지는데 이 과정에서 신용카드 번호와 비밀번호가 제3자에게 쉽게 노출되어 이용자들에게 큰 피해를 입히는 경우가 종종 있어왔다. 따라서 인터넷 시장의 성장에는 안심하고 거래할 수 있는 전자화폐와 같은 가상 화폐의 개발이 필수 요건이라 할 수 있다. 전자화폐란, 인터넷상에서만 존재하는 가상화폐이며 금전적 · 화폐적 가치가 전자적인 방법으로 IC 칩이 내장된 플라스틱 카드에 저장되어 있거나 또는 네트워크에 연결된 컴퓨터의 시스템 등에 저장되어 있는 화폐를 통틀어 말한다. 다시 말해 전자화폐는 가상은행 등에서 발행된 화폐가치가 전자적으로 저장된 전자화폐로 발행된 후, 이용자가 이를 구입하여 상품이나 서비스 등에 이용할 수 있도록 한 결제수단의 하나라고 볼 수 있다. 그러나 전자화폐는 아직은 기술적으로나 법적으로 해결해야 할 많은 문제점을 내포하고 있는 실정이다[2].

1. IC 카드형 전자화폐

플라스틱 카드에 은행예금의 일부를 전자적인 방법으로 이전 · 저장하였다가 단말기 등을 이용하여 현금처럼 사용하는 방식의 전자화폐로서 카드의 형태에 따라 접촉식, 비접촉식으로 분류될 수 있고, 카드의 종류에 따라 자기카드와 IC 카드로 분류된다. 접촉식 카드는 IC 카드를 단말기에 삽입 · 조작하면 저장된 전자화폐가 단말기로 이전되는 방식을 취하며, 원격지에서의 상품, 서비스 대금 지급 및 타인에

대한 자금이체가 가능하다. 반면, 비접촉식 카드는 IC 카드를 단말기와 접촉시키지 않고도 일정 거리 이내에서 카드와 단말기간에 통신이 이루어지게 된다.

2. IC 카드형 전자화폐 시스템 구성도

IC 카드형 전자화폐 시스템은 IC 카드, read-writer 혹은 응용 단말기, 발행 은행 호스트 컴퓨터, 매입 은행 호스트 컴퓨터, 통신망 중계 센터, 통신 시스템 및 통신회선 등의 구성요소로 이루어진다. 그림 4는 IC 카드형 전자화폐 시스템 구성도를 나타내고 있다.

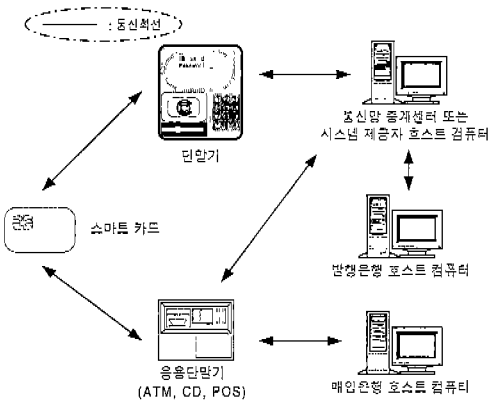

그림 4. IC 카드형 전자화폐 시스템 구성도

그림 4에서 단말기는 IC 카드의 데이터를 해독하거나 IC 카드에 데이터를 입력하고 소거하기 위해 터미널과 접속할 수 있는 장치를 말하며, 응용 단말기는 IC 카드를 사용할 수 있는 응용 단말기로 CD, ATM, POS(Point Of Sale)등이 있다. 또한, 발행 은행 호스트 컴퓨터는 카드의 발행 및 가치 저장 시 단말기와 통신을 담당하고 비밀키의 저장을 위해 명령 수행과 관련된 중요한 보안 기능을 수행하며, 매입 은행 호스트 컴퓨터는 판매자 단말기와 직접 통신을 담당하고, 구매와 관련된 비밀키의 저장 및 명령 수행 등의 보안 기능을 담당한다. 통신망 중계 센터 또는 시스템 제공자 호스트 컴퓨터는 보안 장비를 보유하고 구매 거래에 대한 데이터 수집 시 구매 단말기와 통신을 수행하며, 가치 저장 단말기와 발행 은행간 중계기능을 담당한다.

3. IC 카드형 전자화폐 개발 동향

IC 카드형 전자화폐는 유럽·북미 및 동남아 지역을 중심으로 개발 추진 중이며, 접촉식의 경우 현 은행간 차액 결제가 필요 없는 몬덱스(영국)형과 다수의 참가 은행이 발행에 참가하여 은행간 차액 결제가 필요한 프로톤(벨기에)형으로 구분된다. 유일하게 개방형으로 개발되어 세계 여러 곳에서 시범적으로 사용중에 있는 IC 카드 방식의 몬덱스는 진정한 의미의 전자화폐로 기대를 모으고 있다. 카드 사용자는 은행 구좌에서 ATM이나 전용전화선을 이용하여 자신의 카드에 화폐가치를 충전할 수 있으며, 전용 단말기가 있는 소매점, 주차장, 공중전화 등에서 주로 소액거래 시 사용할 수 있다. 이 때 사용된 금액이 IC 카드로부터 점포의 전용 단말기로 이동하여, 그만큼 IC 카드의 잔고가 줄어들게 된다. ATM을 통하여 금액의 재충전도 가능하고, 단말기를 이용하여 카드간의 금액이동도 가능하므로 거의 기존의 실물화폐와 기능 면에서 동일하다고 할 수 있다.

비접촉식 IC 카드의 경우, 영국 및 스웨덴, 덴마크, 핀란드, 프랑스, 홍콩 등지에서 대중 교통(버스, 지하철, 기차 선박 등)요금의 지급 수단으로 사용되고 있으며, 노르웨이, 독일, 프랑스, 이탈리아, 미국의 경우에는 고속 주행 중인 자동차내의 IC 카드에서 도로 통행료가 공제되는 ETC (Electronic Toll Collection)가 시범 운영 중에 있다.

IC 카드를 사용하지 않는 네트워크형 전자화폐는 인터넷과 전자상거래의 급성장으로 이미 개발되어 사용되고 있거나, 개발이 활발히 추진되고 있지

표 1. ISO/IEC JTC1/SC17/WG4 표준 문서 현황

Project Number	Standard Number	Title	Actual (Date sent for Ballot/Published)					
			NWI	WD	CD	FCD	FDIS	IS
1.17.8.1	ISO/IEC 7816-1	Identification cards -Integrated circuit(s) cards with contacts - Part 1 Physical characteristics						97.07 98.10
1.17.8.2	ISO/IEC 7816-2	Identification cards -Integrated circuit(s) cards with contacts - Part 2 : Dimensions and location of the contacts			94.11			88.05 99.03
1.17.8.3	ISO/IEC 7816-3	Identification cards -Integrated circuit(s) cards with contacts - Part 3 · Electronic signals and transmission protocols						89.10 97.12
1.17.8.4 TF3	ISO/IEC 7816-4	Identification cards -Integrated circuit(s) cards with contacts - Part 4 · Interindustry commands for interchange	89.10	92.10	92.10		94.09	95.09
1.17.8.4	ISO/IEC 7816-4/ AM1	Impact of secure messaging on APDE structures		96.06	96 08		97.01	97 12
1.17.13 TF4	ISO/IEC 7816-5	Identification cards -Integrated circuit(s) cards with contacts - Part 5 : Registration system for applications in IC Cards	90.02	91.09	91.12		92.09	94.06
1.17.13	ISO/IEC 7816-5/ AM1	AM1 Proposal for a set of Registered Application provider identifiers (RIDs)	94.11	94.09	95.01		96.05	96.12
1.17.8.6	ISO/IEC 7816-6	Identification cards -Integrated circuit(s) cards with contacts - Part 6 · Interindustry Data Elements	92.10	93.10	94.07		95.03	96.05
1.17.8.6	ISO/IEC 7816-6/ AM1	IC Manufacturer registration	95.10	97.10	97.12	98.09		(99.03)
1.17.19	ISO/IEC 7816-7	Identification cards -Integrated circuit(s) cards with contacts - Part 7: Interindustry commands for Structured Card Query Language (SCQL)	94.03	96.06	96.08		97.02	99.03
1.17.20	ISO/IEC 7816-8	Identification cards -Integrated circuit(s) cards with contacts - Part 8 : Security architecture and related interindustry commands	94.03	96.12	97.01 97.07	98.01	98.12	(99.12)
1.17.20.1	ISO/IEC 7816-9	Identification cards -Integrated circuit(s) cards with contacts - Part 9 · Enhanced interindustry commands	96.10	97.12	98.04 98.12	99.06	(00.02)	(00.07)
1.17 8.10	ISO/IEC 7816-10	Identification cards -Integrated circuit(s) cards with contacts - Part 10 : Electronic signals and answer to reset for synchronous cards	95.12	96.08	96.08 97 06	98.09	99.05	(99.12)
1.17.23	ISO/IEC 15460	Identification cards -Integrated circuit(s) cards with contacts - Integrated circuits with voltages lower than 3 volts	97.09					
1.17.25	ISO/IEC 18020	Identification cards -Integrated circuit(s) cards with contacts - Personal verification through biometric methods in integrated circuit cards	99.06					
1.17.2.3	ISO/IEC 10373-3	Test methods - Integrated circuit(s) cards	94.11	96.10	96.12 98.08 99.08	(00.03)	(00.10)	(01.02)

표 2. ISO/IEC JTC1/SC17/WG8 표준 문서 현황

Project Number	Standard Number	Title	Actual (Date sent for Ballot/Published)					
			NWI	WD	CD	FCD	FDIS	IS
1.17.11.1	ISO/IEC 10536-1	Identification cards - Contactless Integrated circuit(s) cards - Part 1 Physical Characteristics		89.09	89.11		91.07	92.09
1.17.11 1	Revision		97.10	98.10	98.11	99.03	(99.12)	(00.05)
1.17.11.2	ISO/IEC 10536-2	Identification cards - Contactless Integrated circuit(s) cards - Part 2 : Dimensions and location of coupling areas		92.10	92.11		93.11	95.12
1 17.11.3	ISO/IEC 10536-3	Identification cards - Contactless Integrated circuit(s) cards - Part 3 : Electronic signals and reset procedures	94.10	93.10	94.05		95 02	96.12
1.17.11.4	ISO/IEC 10536-4	Identification cards - Contactless Integrated circuit(s) cards - Part 4 : Answer to reset and transmission protocols	94.10	95.09	95.10 (99.05)	(00.03)	(00.10)	(01.03)
1.17.17.1	ISO/IEC 14443-1	Identification cards - Contactless Integrated circuit(s) cards - Proximity integrated circuit(s) cards - Part 1 : Physical Characteristics	93.05	96.10	96.12 97.03	98.07	(99 02)	(99.07)
1.17.17.2	ISO/IEC 14443-2	Identification cards - Contactless Integrated circuit(s) cards - Proximity integrated circuit(s) cards - Part 2 Radio frequency interface	96.10	98.07	98.11	99 05	(99.10)	(00.03)
1.17.17.3	ISO/IEC 14443-3	Identification cards - Contactless Integrated circuit(s) cards - Proximity integrated circuit(s) cards - Part 3 : Initialization and anticollision	96.10	98.10	98 12 99.02	99.06	(00.01)	(00.06)
1.17.17.8	ISO/IEC 14443-4	Identification cards - Contactless Integrated circuit(s) cards - Proximity integrated circuit(s) cards - Part 4 : Transmission protocols	97.10	(99.06)	(99.10)	(00.05)	(00.12)	(01.05)
1.17.17.4	ISO/IEC 15693-1	Identification cards - Contactless Integrated circuit(s) cards - Vicinity cards - Part 1 : Physical Characteristics	96.10	97 10	97.10	98.07	(99.02)	(99.07)
1.17.17.5	ISO/IEC 15693-2	Identification cards - Contactless Integrated circuit(s) cards - Vicinity cards - Part 2 : Air interface and initialization	96.10	98.10	98.11	99.03	(99 10)	(00.04)
1.17.17.6	ISO/IEC 15693-3	Identification cards - Contactless Integrated circuit(s) cards - Vicinity cards - Part 3 : Protocols	96.10	(99.06)	(99.10)	(00.03)	(00.10)	(01.03)
1.17.17.7	ISO/IEC 15693-4	Identification cards - Contactless Integrated circuit(s) cards - Vicinity cards - Part 4 : Registration of Applications/issuers	96.10	(99.09)	(99.10)	(00.03)	(00.10)	(01.03)
1.17.2.4	ISO/IEC 10373-4	Test methods - Contactless integrated circuit cards	94.11	96 10	96.12	(99.03)	(99.12)	(00.05)
1.17.2.6	ISO/IEC 10373-6	Test methods - Proximity cards	97.10	98.09	99.08	(00.03)	(00.10)	(01.03)
1.17.2.7	ISO/IEC 10373-7	Test methods - Vicinity cards	97.10	99.08	99.08	(00.03)	(00.01)	(01.03)

만, 아직 안전성에 대한 신뢰성 부족과 사회적인 인식 부족으로 이용이 미비한 실정이다.

국내에서는 정부의 정보통신망 구축, 대국민 서비스 향상 및 정보통신 산업 육성정책에 힘입어 SI (System Integration)업체들이 참여하여 금융, 통신, 교통, ID(Identification)분야 등의 산업분야를 주축으로 관련 제품의 상용화가 진행되고 있다. 금융카드는 마그네틱 카드의 위/변조 사례의 급증으로 인한 피해가 속출하고 있어 전자화폐 및 다기능 서비스 구현 등을 위해 도입이 추진되고 있으며, 광주은행, 동남은행, 부산은행 등 일부 지방은행들이 금융 IC 카드를 도입하고 있다. 현재 전자상거래기본법의 통과에 힘입어 전자화폐를 포함한 금융 IC 카드를 도입하기 위한 관련 기술, 행정의 표준화 및 법제화가 진행되고 있다.

국내 IC 카드 산업은 발전 단계로 보아 도입기인데 비해 해외의 경우 성장기에 진입하고 있어 업체 및 기관들이 칩 제조업체, 카드 제조업체, 단말기 제조업체, 시스템 통합업체, 산업체 컨소시엄으로 세분화되어 있으며, 관련 산업군간, 업체간 협력 및 기술 공유에 의한 사업화가 추진되고 있는 실정이다. 표 3은 각 국의 전자화폐 개발 동향을 나타내고 있다[11].

현재, 전자화폐·전자상거래 결제시스템과 관련된 요소 기술은 이미 국내외적으로 각 분야에서 상당 수준 개발이 진척된 상황이며, 최근 제기되고 있는 핵심과제는 분산되어 있는 요소기술을 어떻게 잘 조합하여 편리한 사용 환경과 저렴한 사회적 비용으로 전자화폐 시스템을 구축하느냐 하는 데 있다.

4. IC 카드를 이용한 전자 지불 서비스

IC 카드는 다양한 응용 분야에 적용될 수 있다. 그 중에서도 금융분야, 통신분야, 교통분야, 생활 편의분야, 관광 레저분야 등에서 사용될 수 있고, 세부적으로 살펴보면 아래와 같다.

우선, 금융분야에서는 신용 카드, 직불 카드, 전자 지갑, 전자상거래 등으로 활용될 수 있으며, 통신분야로는 공중전화나 이동통신 단말기에 사용된다 (SIM : Subscriber Identity Module 카드).

최근, IC 카드의 최대 활용 분야는 교통분야로서 버스, 지하철, 택시, 주차장 사용료, 도로 통행료, 주유소 등 응용 범위가 매우 다양하다. 생활 편의 분야로는 병적 사항이나 혈액형 등을 저장한 의료카드, 백화점, 편의점, fast food점을 이용할 때 사용하는 카드로 활용할 수 있다. 또한, 관광 레저분야로 극장, 공원, 운동장 등의 입장료 지불 및 좌석 지정, 비행기 표 예매 및 좌석 지정 등에도 사용이 가능하다[13].

5. IC 카드형 전자화폐 표준화 동향

5.1 국내 표준화 동향

금융결제원이 제공하는 전자화폐 공동이용 서비스로 K-Cash가 개발되고 있는 중이며, 이를 위한 국내 규격(금융 IC 카드, PSAM 규격)이 제정되고 있다.

5.2 국외 표준화 동향

Mondex는 IC 카드를 이용한 전자지불 서비스로 영국의 NatWast은행과 Midland은행이 중심이 되어 95년 7월부터 시행된 은행 중심의 전자화폐

관련 단체 표준으로 EMV (Europay, Master, Visa) 와 달리 신용카드가 아닌 은행을 중심으로 서비스가 이루어진다. 현재는 Mondex International사가 개발에 참여하고 있으며, 전세계적으로 15개국, 1,270만개의 가맹점에서 운용중이다.

CEPS(Common Electronic Purse Specifications)는 CEPSCO Espariola A.I. E., Visa International, Europay International, ZKA, EURO Karten systeme에서 함

표 3. 각 국의 전자화폐 개발 현황

국 가	영국	미국, 호주	벨기에	독일	싱가폴	포르투칼	프랑스	일본	네덜란드	덴마크
명칭	Mondex	VISA MASTER	Proton	Geldkarte	NETS CashCard	MEP	Leponte-monnaie	미정	Chipknip	Danmont
추진 현황	'95.7 시험	미국 : '96년 개발 호주 : '95.10 시험	'94.10 시험	'95.10 도입	'94.2 시험	'95.2 가동	'89 도입	도입 예정	'95.2 시험	'96.3 도입
발행 기관	회원 은행	회원은행	은행 공동망, 회원 은행	직불 공동망, 회원 은행	은행 공동망, 회원 은행	직불, CD공동망, 회원은행	회원 은행	민간 은행	-	은행과 통신회사
수익 귀속	몬덱스사	발행은행	발행 은행	발행 은행	발행은행	발행은행	발행 은행	발행 은행	-	발행은행
차액 결제	×	○	○	○	○	○	○	-	-	○
카드간 자금 이체	○	×	×	×	×	×	×	-	-	×
사용 범위	소액 및 고액 거래	소액거래	소액 거래	소액 거래	소액거래	소액거래	소액 거래	-	-	소액 거래
거래시 비밀 번호 사용	×	×	×	-	×	×	×	-	-	×
카드 잠금 장치 사용	○	×	×	×	×	×	×	-	-	×

께 참여하였으며, 유럽 각국에서 추진됐던 독자 모델간의 호환성 확보를 위해 22개 국가들이 참여하여 만든 전자화폐 관련 단체표준이다. 현재 초안이 제정된 상태이며, CEPS기반 전자화폐 시스템은 2000년 초에 구축될 예정이다.

Ⅳ. 결 론

본 고에서는 전자상거래를 위한 IC 카드 기술 및 IC 카드형 전자화폐 기술, 표준화 동향 등에 대해 살펴보았다. 앞서 언급한 바와 같이 전자거래 시 개인의 신상정보를 보호하는 것은 매우 중요하다. 최근에 이러한 개인정보를 보호하기 위해 IC 카드가 사용되고 있는데, IC 카드는 현금처리 비용과 사기에 의한 손실을 줄여주며, 계산대에서 고객거래를 신속히 처리하고 소비자에게 편리성과 안전성을 향상시켜준다. 하지만, 무엇보다 전자상거래가 활성화되고 현실화되기 위해서는 개인의 신용정보, 전자화폐, 계약서 등 송·수신되는 정보에 대한 정보보호 체계의 확립, 법·제도·정책의 확립, 표준화된 전자지불 시스템 구축 등이 선행되어야 할 것이다. 또한, 분산되어 있는 전자화폐 및 전자상거래 시스템의 요소기술을 잘 조합하여 편리한 사용환경과 저렴

한 사회적 비용으로 전자화폐 시스템을 구축하는 것도 중요한 과제라 할 수 있다.

※참고문헌

[1] 이만영 외 5명, *전자상거래 보안 기술*, 생능 출판사, pp. 275~317, 1999

[2] 장진연, "*전자화폐 결제제도에 관한 법적 연구*", 석사 학위 논문, 영남대학교, Dec. 1999.

[3] 정보보호 21C, *시큐리티 정보*, pp. 50-54, Jan. 2000.

[4] ISO/IEC JTC1/SC17/WG4 7816-1, 7816-2, IS

[5] ISO/IEC JTC1/SC17/WG8 10536, IS

[6] ISO/IEC JTC1/SC17/WG8 14443, IS

[7] ISO/IEC JTC1/SC17/WG8 15693, IS

[8] D. Naccache and D. MRaihi, *Cryptographic Smart Cards*, IEEE Micro, June 1996.

[9] S. Svigals, *Smart Card. The ultimate personal computer*, MacMillan Publ. 1985.

[10] 김호원 외 3명, "차세대 IC 카드 기술", pp. 74~83, no. 3, vol. 17, *한국통신학회 학회지*, 2000. 3.

[11] 김철환, 김규수, *전자상거래*, 문원출판, pp. 319~335, 1999

[12] W. Rankl, W. Effing, *Smart Card Handbook*, John Wiley & Sons, 1996

[13] M. Hendry, *Smart Card Security and Applications*, Artech House, 1997

한 진 희

1997년 숭실대학교 정보통신공학과 졸업 (공학사)
1999년 광주과학기술원 정보통신공학과 (공학석사)
1999년~현재 한국전자통신연구원 정보보호기술연구본부 IC 카드 OS연구팀, 연구원
관심분야 : IC Card, Internet Security, Biometry

정 교 일

1981년 한양대학교 전자공학과(공학사)
1983년 한양대학교 산업 대학원 전자계산학과(공학석사)
1997년 한양대학교 대학 원 전자공학과(공학박사)
1981년~현재 한국전자통신연구원 정보보호기술연구본부 IC 카드 구조연구팀 팀장/책임연구원
관심분야 : IC Card, Security, Biometry, 정보전, 신호처리

이 창 욱

1990년 한양대학교 전자공학과(공학사)
1992년 한양대학교 대학원 전자공학과(공학석사)
1997년 한양대학교 대학원 전자공학과(공학박사)
1997년~현재 한국전자통신연구원 정보보호기술연구본부 IC카드OS연구팀 팀장/선임연구원
관심분야 : IC Card, Network Security, Internet Appliance

손 승 원

1984년 경북대학교 전자공학과(공학사)
1994년 연세대학교 산업 대학원 전자공학과(공학석사)
1999년 충북대학교 대학원 전자공학과(공학박사)
1991년~현재 한국전자통신연구원 정보보호기술연구본부 정보보호응용연구부 부장/책임연구원
관심분야 : IC Card, Biometry, Network Security