IC Card 기술과 과제

유영갑
충북대학교 정보통신공학과 교수
주관심분야 :
computer architecture, memory testing,고속시스템설계,HDTV, ATM, 가변익 항공기 제어 등

요 약

전자 상거래 등에 널리 사용되는 IC 카드에 관련된 기술을 소개하고 전망에 대하여 기술하였다. 특히 암호기술에 대한 개관과 문제점을 제시하고 당면한 회로 기술상의 문제점도 지적하였으며, 국제 표준국이 제정한 관련 표준안에 대한 개요를 설명하였다.

1. 정보화와 전자신용

누가 화폐를 발행할 수 있을 것인가? IC 카드를 사용한 전자 상거래가 활성화되면서 다가오는 의문이다. 전자화폐의 형태는 다양하며 그 중에서도 IC 카드는 현실로 다가온 문명 전환기적인 현상인 것이다. 재화의 유통과 보유에서 매체상의 변혁인 것이다.

인류역사는 기록을 시작하면서 그 구체적인 사실들을 전달할 수 있었으며, 기록 매체의 변천은 정보와 전달과 재화의 교환에 결정적인 영향을 미쳤다. 종이에 의한 지폐, 플라스틱에 의한 신용카드가 지불수단으로 사용되다가 이제 IC 카드의 형태로 바뀌고 있는 것이다. 이것은 1974년 프랑스의 R. Morenork 출원한 특허에서 시작하여 프랑스를 중심으로한 유럽지역에서부터 전세계에 급속한 확산을 보이고 있다. 우리 나라에서도 이미 시내버스 요금 정산, 전화카드, 회사의 신분증 등에 사용되고 있으며, 한때는 주민등록증을 대체시키려는 논의와 준비가 활발하게 진행된 적이 있었다.

전자화폐의 물리적 형태로서의 IC 카드는 화폐로서의 몇 가지 특성을 요구받고 있으며, 이를 기술적으로 해결해야하는 요구에 직면해 있다. 그 중에서도 화폐로서의 기능 중에서 위조 방지 장치와 결제과정의 익명성을 들 수 있으며, 모든 이가 화폐로서 인정해줄 수 있는 기능과 물리적인 안정성 등이 핵심이라 할 수 있다. 위조 방지 기술, 공공성 그리고 거래의 익명성 등을 해결하기 위해서는 각종 암호 기술이 활용되고 있으며, 특히 공개열쇠 방식의 암호계가 갖는 편리함으로 실질적인 응용을 위한 기술 개발이 요구되고 있다.

안정성 등은 IC 카드의 물리적 구조와 카드제작에 사용되는 각종 재료의 개발이 이루어지고 있다. 또한 카드의 형태에 따라 비접촉식의 경우 무선주파수를 이용한 구동 전력의 확보는 패키징에서 상당한 기술적 대응이 필요하게 되었다. 카드에 탑재된 회로의 구동과 통신에 필요한 전력 프로파일을 충족시킬 수 있어야 하고, 이를 위하여 작은 카드형 기기에 효율 높은 안테나를 구현하는데 중요한 의미를 가지게 되었다.

이러한 기술들은 IC 카드의 공공성이 비추어 표준화가 중요한 의미를 갖는다. 상당한 표준안이 산업계에서 다듬어져 왔으며, 신기술의 등장은 기존의 표준에 대한 개정과 함께 새로운 범주의 표준을 끊임없이 제시하도록 요구하고 있다. 이들은 카드 제조사양에 직접적인 영향을 미치는 것으로 제품의 시장 진입에서 기술적으로 해결하여온 결과를 반영하는 것이다.

이 글은 IC 카드에 대한 소개와 현재 문제시되고 있는 핵심 기술에 대한 고찰을 하고자 하였다. 이 글의 2 장에서는 IC 카드의 기본적인 구조와 관련 기술을 소개하고, 3 장에서는 핵심 기술 중의 하나인 암호에 대한 개관을 하며, 4 장에서는 각종 표준안에 대하여 소개한다.

2. IC 카드의 구조

별도의 전지 없이 단일 칩만을 써서 필요한 정보를 식별하도록 하는 장치는 IC 카드뿐만 아니라 개별 식별 장치 등으로 보급되고 있다. 일반적인 식별 장치들이 차량 탑재나 동물 등의 체내 이식등의 방법으로 설치되는 반면

에 IC 카드는 특별히 신용카드 크기의 규격으로 포장되어 지갑이나 호주머니 등에 휴대가 간편하도록 한 것이다.

2.1. 전기적 구조

스마트 카드로도 불리는 IC 카드의 내부에는 일반적으로 마이크로 프로세서, 프로그램 메모리, 데이터 메모리, 입출력 단자 그리고 전원부로 구성되어 있다. 그림 1에 보여 진 바와 같이, 전형적인 IC 카드는 마이크로 프로세서, 메모리 등은 하나의 칩으로 구현되며, 입출력부와 전원부의 안테나 등이 별도의 부분품으로 만들어진다. 전원회로의 설계에 따라서는 에너지 저장을 위한 별도의 캐패시터를 부착하기도 한다. 프로그람 메모리에는 IC 카드 내부의 운영체제를 비롯하여 각종 서비스 프로그람이 들어 있다. 이들은 제조시에 기록된 후 변경이 필요 없으므로 보통 ROM 으로 만들어지며, 일반적인 데이터는 전원이 차단된 후에 지워지지 않도록 EEPROM 으로 만들어 진다. 현금 카드또는 전자 지갑의 경우 현재 쓰고 남은 잔액은 이 EEPROM 에 기록되는 것이다.

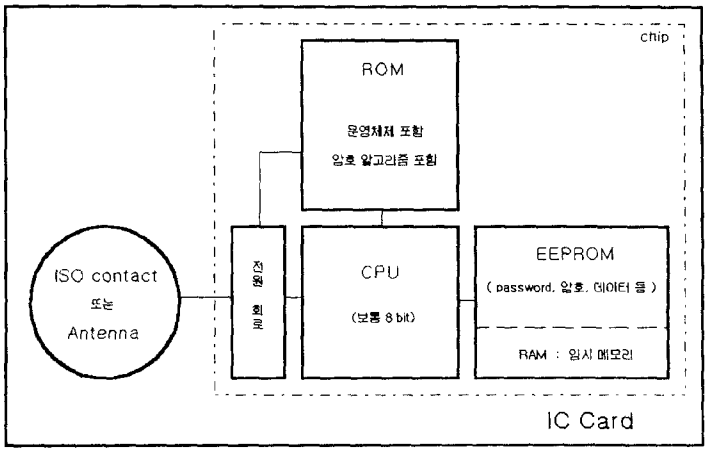

그림 1. 전형적인 IC 카드의 내부구조

IC 카드 내부의 움직임을 정의하는 운영체제는 먼저 초기화 과정, 통신 프로토콜이 처리되도록 하고 있으며, 전자지갑이나 현금카드의 경우 암호화 및 복호화를 위하여 상당한 부분이 할애되어 있다. 카드내부 정보에 대한 접근 제한이 체계적으로 설정되어 있어서, 카드 제조업자가 접근할 수 있는 영역, 은행이나 신용카드회사와 같은 카드 발급회사가 접근할 수 있는 영역, 그리고 말단 가맹점이 접근할 수 있는 데이터의 영역 등으로 구분하여, 이들 각각에 대한 특별한 보호를 하고 있다. 말단 가맹점은 카드에 들어 있는 현금을 입 출금할 수 있도록 하고, 카드 자체의 고유번호 등에는 접근할 수 없도록 한 것이다. 이는 화폐의 고유번호가 발권은행에 의해서만 통제되는 것과 같은 개념이다.

전원 회로와 입출력 단자는 비접촉식의 경우 함께 사용한다. 접촉식의 경우 전원단자와 통신용 단자는 구별되어 있다. 비 접촉식의 경우, 일정 기간 전원을 충전한 후에 초기화를 실시하고 통신을 실시한다. 이 경우 수신되는 신호에서 에너지를 동시에 추출할 것인지의 여부에 따라 전원회로의 복잡도는 상당히 달라지게 된다. 경우에 따라서는 판독기가 공급하는 클럭 신호를 추출하여 사용하기도 하는데, 이를 위하여 미세신호의 증폭기능이 들어가게 된다.

비접촉식 IC 카드에서는 전원에 사용할 안테나의 설계도 중요하다. 안테나의 설계는 보통 통신에 사용될 동작 주파수를 결정하고, 이를 바탕으로 LC 탱크회로를 설계하게 되며, 이때 에너지 송출 능력을 적절한 R 값을 선정하여 반영하게 된다. 송신 주파수와 수신 주파수를 달리하는 경우 안테나의 주파수 범위를 넓혀야 하는 부담도 고려된다. 또한 탱크회로의 인덕턴스 값은 카드에 내장할수 있는 코일의 턴수에 관계되는데, 수백 번씩 감은 권선이 사용되기도 한다. 일반적으로 고주파 대역에서 동작하게 되면 인덕턴스의 값은 수 mH 정도가 사용되고 주파수에 따라 상응하는 캐패시턴스 값을 계산하여 사용한다. 대부분의 비접촉식의 경우, IC카드와 판독기간의 신호교환에 사용되는 변조방식으로는 FSK (frequency shift keying)이나 ASK (amplitude shift keying) 등이 사용된다. FSK 는 탱크회로나 안테나 회로의 대역폭에 부담을 주는 반면, ASK 는 주어진 반송주파수를 그대로 유지하는 관계로 부담이 줄어들 것으로 보인다.

비접촉식 카드의 제약은 주로 전원에서 온다. 카드에 내장된 마이크로 콘트롤러의 동작은 무선을 통하여 수신된 신호의 에너지를 정류하여 사용하게 되므로 전력이 많이 소요되는 고속 연산 등을 수행하는데 어려움이 있게 된다. 느린 마이크로 콘트롤러의

동작에 의하여 외부와의 통신도 느려질 수 밖에 없게 된다. 일반적으로 비접촉식이 접촉식 카드보다 속도가 느린 이유가 바로 이 전원의 제약 때문인 것이다. 따라서 보다 많은 에너지를 받아들이기 위하여 카드에 내장된 루프 안테나의 효율과 내부 전원 회로의 효율을 높이려는 노력이 있게 마련이다. 이런 노력에도 불구하고 전원 전압은 칩 내부의 회로가 동작하고 외부에 정보를 송신하게 되면 상당히 내려가게 된다. 전원설계는 회로동작기간 동안의 전원전압 변동에 대한 윤곽을 설정하여 이를 만족시키는 방향에서 실시된다. 또한 칩 내부 회로도 전원 전압의 상당한 변동에도 안정적인 동작이 가능하도록 설계되어야 한다.

2.2. 기계적인 구조

카드의 크기는 국제적인 규격으로 규정되고 있는 카드의 크기는 $85.9 \times 54.18\ mm^2$ 이며 두께는 $0.76\ mm$ 이다. 카드는 불필요한 외부의 자극에 있어서 내부의 정보와 칩 그리고 안테나 회로등이 망가지지 않도록 충분한 보호가 되어 있어야 한다. 카드에 장착되는 집적회로의 기계적인 파손 위험을 줄이는 것도 중요하다. 카드에 내장되는 칩의 경우 마이크로 콘트롤러, ROM, EPROM 등이 포함되어 대략 그 크기가 $5 \times 5\ mm^2$ 정도이며, 제조 회사별로 약간씩 다르며, 반도체 칩 제조공정의 발전에 따라 줄어들고 있는 추세이다. 집적회로 칩은 그 두께가 500 마이크론 이내의 아주 얇은 것이어서 작은 충격이나 기계적인 힘에 의하여 부러지게 된다. 카드의 경우 주로 카드가 호주머니 속 등에서

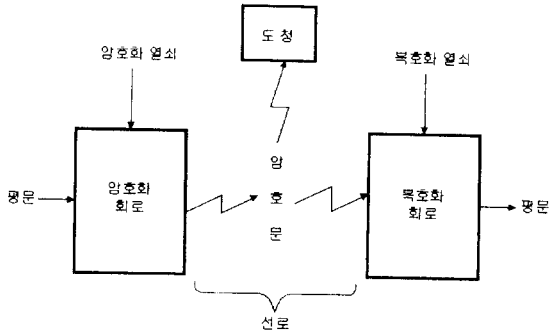

그림 2. 암호 통신 개념

휘게 되면 속에 든 칩이 파손되어 저장된 금전적인 정보 등이 망실될 위험이 있다. 이것을 방지하기 위하여 칩 주변에 강한 보강재를 사용과 칩의 소형화, 칩의 장착위치 선정 등을 통하여 해결하게 된다. 카드의 중앙에는 카드가 휠 때 가장 많은 힘을 받게 되므로 칩을 카드의 한편 구석으로 위치시켜서 같은 강도를 가진 구조에서도 보다 적은 기계적인 힘을 받도록 하는 것이다.

카드를 휴대할 때 발생하는 마찰 전기로부터 내부 집적회로를 보호하는 것도 상당히 중요한 문제이다. 보통 플라스틱 카드가 호주머니 속에서 발생할 수 있는 정전기는 수천 볼트가 되며 경우에 따라서는 일시에 방전되므로 이런 경우에는 집적회로의 내부 회로에 상당한 전류가 순간적으로 흐를 수 있는 것이다. 이러한 순간 전류에 대한 보호회로의 설계와 그 효과를 실측하는 문제가 있다.

3. IC 카드의 암호

암호화는 일상적인 정보의 표현을 변형하여 특수한 형태의 암호문으로 만들어서 주는 과정이며, 암호문을 다시 일반형태의 평문으로 바꾸는 과정은 복호화라고 한다. 그림 2 에는 암호화 과정을 보이고 있다. 암호는 정보의 발신자와 수신자 사이에 주고 받은 정보를 제 3 자가 듣지 못하도록 하는 도청 방지기능 이외에도 제 3 자로 하여금 발신자를 증명시켜주는 인증기능도 있다. 일반적으로 비밀 통신에서는 도청 방지 기능이 주가 되지만 IC 카드처럼 일정한 정보를 가지고 있으며 정보의 안정성이 중요한 경우에는 주로 인증의 기능을 부여할 수 있다.

IC 카드에 사용되는 암호는 카드의 용도에 따라 다양한 종류가 사용된다. 신분증을 대용하는 경우 본인 증명에 필요한 암호가 사용되며, 현금 카드의 경우 변조 또는 복제 방지를 위한 암호가 필요하다.

암호문의 비밀을 지키기 위해서는 도청하는 사람이 해독하기 어렵게 해야하고, 이를 위해서는 암호화하는 과정을 비밀로 해야 하지만, 차츰 여러 사람들이 같은 방식을 사용하게 되면 자연히 그 방식이 알려지게 된다. 따라

서 암호화는 방식은 알고리즘으로 공개하여 모든 이가 알 수 있도록 하되, 주어진 알고리즘을 이용하여 암호화 할 때 사용하는 아주 작은 정보, 즉 열쇠만을 비밀로 유지하는 것이 일반화되어 있다. 따라서 암호화 열쇠를 비밀로 보호하는 것이 현대암호 체제에서는 매우 중요한 것이다.

암호방식에는 크게 두 가지가 사용되고 있다. 하나는 관용(conventional)암호계와 공개열쇠(public key) 암호계가 그것들이다.

3.1. 관용 암호계

관용 암호계로서 널리 활용되고 있는 것이 DES (Data Encryption Standard) 로 알려진 알고리즘이다. 이것은 주로 글자의 위치를 서로 바꾸는 환자와 한 글자를 다른 글자로 대체하는 치환 과정을 여러 차례 조직적으로 반복하는 것이다. 이 알고리즘에서는 덧셈이나 다른 수학적인 연산을 과다하게 요구하지 않기 때문에 암호화와 복호화가 빠르고, 상당히 높은 비밀보호 능력을 가지는 것이다.

관용암호계에서는 암호화와 복호화에 같은 암호화키를 사용한다. 따라서 암호화는 비밀 통신을 원하는 두 사람만이 간직해야 비밀이 유지되기 때문에 IC 카드처럼 사용자가 많아지면 키의 개수도 늘어나는 불편함이 있다. 10 사람이 서로 완벽하게 비밀을 유지하려면 총 90쌍의 비밀키가 따라다니게 되며, 인원수의 제곱에 비례하여 늘어나게 된다. 따라서 관용암호계를 사용하는 현행 IC 카드의 경우 불특정 다수간의 비밀 유지를 위하여는 지극히 불편한 암호체계를 가지고 있는 것이 현실이며, 이 문제는 암호화에서 풀어야할 큰 숙제로 되어 있다.

3.2. 공개 열쇠 암호계

공개 열쇠 암호계는 관용 암호계가 안고 있는 열쇠관리의 문제를 근본적으로 해결하는 방식으로 선호되고 있다. 공개열쇠체제에서는 암호화에 필요한 열쇠는 공개하고 복호화 열쇠만을 비밀로 유지하면 되는 방식이다. 즉 암호화 열쇠로 평문을 암호문으로 바꾸었다하여도, 평문과 암호문을 비교하여 그 암호화 열쇠와 쌍을 이루는 복호화 열쇠를 찾아낼 수 없도록 고안된 것이다. 따라서 송신하는 사람은 암호화가 끝나면 그것을 다시 평문으로 되돌려 볼 수 없게 된 것이며, 오로지 수신자만이 그것을 평문으로 복원시켜 볼 수 있는 것이다. 암호화 키를 가지고도 복호화를 할 수 없기 때문에 각자 개인은 복호화 열쇠만을 비밀리에 보관하면 되는 것이다.

또한 공개암호계에서 복호화를 위한 비밀키를 이용하여 암호화하면 암호화키로 복호화가 가능하기 때문에 인증의 기능을 가질 수가 있다. 즉 비밀키를 써서 만든 암호문은 그 비밀키의 소유자만이 만들 수 있는 고유의 것이므로 변조나 위조가 불가능한 것이다. 따라서 이 인증 방식은 서명이나 날인의 경우와 같은 유일성을 보장하므로 법적인 효력을 충분히 가지게 된다.

공개열쇠방식의 암호계가 갖는 이러한 인증의 기능은 전자 신분증의 인증 기능에 그대로 적용가능하다. 이 원리는 전자도장이라 일컬어지는 인증시스템에도 그대로 적용된다. 도장의 원리는 날인한 사람의 원래의 평문을 수신한 사람이 변조할 수 없도록 함과, 그 문서가 날인한 사람으로부터 만이 발신되었다는 확실한 근거를 제공하는 것이다. 전자 신분증의 본인 증명에 필요한 인장이나 지문을 대신하여 소지자의 비밀키로 생성된 암호문을 삽입하므로써 본인임을 증명할 수 있는 것이다. 이는 법정에서의 본인의 날인을 부인할 수 없게 하는 부인봉쇄(non-repudiation) 기능이 가능한 것으로 관용암호계가 갖지 못한 중요한 장점으로 인증의 목표를 달성할 수 있도록 해주는 것이다.

공개열쇠 암호계의 제약은 그 계산량이 상당하다는 것이다. 일반적으로 관용 암호계에 비하여 1,000 배정도의 계산량을 요구하는 것으로 나타나고 있다. 공개열쇠방식으로 잘 알려진 RSA 방식의 경우, 주로 소수에 대한 지수계산의 어려움으로 비밀을 유지할 수 있으며, 충분한 기간동안 비밀을 유지하기 위하여는 많은 자리의 소수를 사용하여야 하는데, 자릿수가 많아지면 지수계산을 위해 엄청난 양의 연산을 요구하는 것이다. 이러한 계산을 실시간으로 수행해야 하며, 특히 비접촉식 카드의 경우 제한된 전원 에너지를 사용하는데는 해결해야하는 상당한 어려움이 있다.

4. 표준안

각종 응용분야에 따르는 표준안이 IC 카드의 종류별로 제정되고 있는데 국제 표준국 SC17을 중심으로 응용분야별 표준화를 수행하고 있다. 먼저 물리적인 규격은 ISO 7810에 규정되었는데 이는 흔히 사용되는 신용카드 등의 크기는 물론 마그네틱 띠의 규격도 정하고 있다. 이는 사용되고 있는 플라스틱의 성질과 카드의 내구성, 유연성 정도등을

규정하고 있다.

4.1. 접촉식 카드의 표준안

접촉식 IC 카드의 규격은 ISO 7816에 규정되어 있는데, 이는 마이크로 콘트롤러 칩이나 메모리등이 내장되어 있는 카드를 대상으로 하는 것이다. 이 표준안은 7 가지의 독립적으로 갱신, 편집되는 부분으로 구성되어 있으며, 기술적인 발전과 시장 현황등을 반영하도록 되어 있다. 예를 들면 제 1 부는 물리적인 특성을 기술하여서 크기라든가 동작환경 그리고 그 환경하에서의 내구성등을 기술하고 있으며, 최근에는 카드의 테스트 표준안인 ISO 10373 과 호환성을 유지하도록 개정되었다.

이 표준안의 제 2 부에 전기적 접촉을 위한 단자들의 위치와 크기가 규정되어 있고, 제조업체들이 이 규정을 준수하도록 촉구하고 있다. 이는 한 대의 카드 판독기를 써서 모든 카드를 다룰 수 있도록 하기 위한 조치이다. 접촉식 카드를 위한 단자의 크기와 모양은 회사마다 다르게 되어 있는데, 이는 규정된 접촉 단자의 최소 크기를 준수하면서도 각 회사의 독특한 문양으로 발전시키기 위하여 단자의 면적을 늘려 잡은 결과이다. 물론 이들 규정이 재정되기 전의 접촉식 카드를 수용하기 위한 방안도 제시되어 있어서 프랑스와 같이 시장에서 이미 상당수가 사용되고 있는 시장점유 업체들을 보호하기도 한다.

전기적인 신호와 프로토콜의 규정은 표준안 제 3 부에 포함되어 있다. 카드와 판독기가 신호를 주고받는 절차까지 기술되어 있는 것이다. 전기적인 신호의 변화가 반영되는 곳인데, 예를 들면 저전압 칩의 사용으로 3V 용의 신호의 사용이나 EEPROM 프로그람 전압의 제거 등이 반영되는 것이다. 이렇게 해서 불필요해진 단자들은 보다 고도의 카드 기능, 즉 양방향 통신 기능 같은 것을 수용하기 위하여 활용되도록 개정되는 것이다.

통신 프로토콜은 리셑 명령으로 시작되는데, 이는 핸드 쉐이크 기능의 도입과정에서 필요한 것이다. 카드를 초기화해서 카드 판독기와 통신을 시작하도록 준비시키는 것이다. 제 3 부에 카드가 판독기로부터 리셑 명령어를 받았을 때 취하게 되는 카드 자체 내부의 제반 활동이 규정되어 있다. 이 과정에서 동작 전압이라든가, 통신 방식, 마이크로프로세서의 동작속도 까지 결정되는 것이다.

카드와 판독기 사이의 정보교환에 관한 명령어 등에 대한 규정은 표준안 제 4 부에 표현되어 있다. 또한 신용카드 번호와 같은 금융기관별 고유 번호 관리에 관하여는 제 5 부에 규정되어 있으며 이들 번호는 카드 발급기관의 인식과 그에 따른 기관별 처리과정 등을 따르도록 하는 것이다. 현재는 덴마크의 전화회사인 PTT가 칩에 저장될 기관의 고유번호 발급과 처리를 관리하고 있다. 이 고유번호는 카드가 판독기에 삽입되었을 때 무슨 용도의 카드인지를 알려주는 역할을 하게 된다. 이 번호는 기능이 단순한 현재의 용도에서는 의미가 없지만, 향후 의료보험이나 신용카드와 같이 사용 범위가 확대되면 판독기가 이들을 처리해야하는 과정을 인식하도록 하는 역할을 하게 될 것이다. 즉 한 대의 판독기가 여러 종류의 카드를 처리하도록 도와주게 된다.

유효기간, 카드번호, 소지자 인적사항 등과 같은 카드정보를 기술하는 데이터 형식은 표준안 제 6 부에 규정되어 있다. 이것은 앞서의 4 부에서 규정된 명령어와 함께 카드내부의 운영체제하에서 처리될 데이터를 정의하는 것이다. 제 7 부에는 현행의 기능들이 향후에 개선될 각종 기능에서도 모두 처리되어 질 수 있도록 하는 상향호환성에 대하여 기술하고 있는데, 보안구조라든가 고급 명령어 등에 대한 것이다. 이들 규정의 각 부분은 비접촉식 카드에 대한 표준안의 제정의 근간이 되었다.

4.2. 비접촉식 카드에 대한 표준안

카드와 판독기 사이에 무선에 의한 정보 교환을 규정하는 표준안은 ISO 10536 과 ISO 14443 으로 구성되어 있다. 이들 규정은 접촉식 카드의 표준안인 ISO 7816 과 유사하게 정리되어 있다. 비접촉식의 경우 카드와 판독기 사이의 거리에 따라 세가지로 구분하고 있다: 카드와 판독기 사이의 거리가 1 mm 이내인 밀착식 (immediate proximity)과, 간격이 1 cm 까지 사용되는 근거리식 (close proximity), 그리고 3 - 5 m 까지 사용되는 원격식 (remote proximity) 이다. 이들의 경우 판독기에 대한 카드의 각도가 중요한데, 판독기와 카드 사이의 거리가 멀어질 수록 각도에 대한 여유가 넓어지며 원격식의 경우 각도에 구애되지 않게 된다.

이들 규정의 제 1 부에는 물리적인 크기가 규정되어 있으며, 제 2 부에는 무선장치의 위치와 크기가 규정되어 있고 ISO 14443 의 경우 무선 주파수에 대한 기술이 포함되어 있다. 나머지 부

분에는 전기적인 규격, 전송 프로토콜, 보안 시스템에 대한 표준이 들어 있다.

접촉식 카드와의 차이점은 무선 범위 내에 여러 장의 카드가 제시되었을 경우, 이를 처리하는 방식이다. 이것은 ISO 14443 의 제 4 부에 포함되어 있다. 이때에는 LAN에서 활용하는 충돌방지 알고리즘이 흔히 채택된다. 즉, 두 장의 카드가 동시에 카드 판독기와 통신을 시도하게 되면 충돌이 발생했다고 하는데, 이때 각 카드는 통신을 일단 중지하고 자체적으로 임의의 시간동안 기다렸다가 다시 통신을 시도하는 것이다. 카드별로 기다리는 시간이 다르므로 충돌이 다시 발생할 가능성이 줄어드는 것이다. 마치 동전던지기를 해서 통신을 다시 시도하는 것과 같다. 핸드쉐이크 초기에는 9600 bps 로 통신하도록 합의가 되어 있으며, 초기 리셀 과정을 거치고 나면 카드 판독기와 카드 상태에 따라 양측이 편리한 보드 율로 통신하게 된다.

5. 전 망

전자상거래의 활성화와 휴대형 상품의 광범위한 보급은 IC 카드 산업의 급격한 신장을 가져오고 있으며 이러한 추세는 당분간 지속될 것이다. 카드와 판독기간의 통신이 고주파에서 광에 이르는 다양한 매체가 활용될 것이며 관련되는 하드웨어의 제조 기술이 발전할 것이다. 이러한 응용분야의 확산은 정보의 보호와 안정성에 대한 고도의 기술을 요구하고 있다. 특히 암호화를 통한 개인 신상의 정보와 금전적 정보를 보호의 필요에 의하여 이 분야의 급속한 발전이 이루어 질 것이다. 또한 소형화와 데이터 처리용량의 확대에 따른 집적회로 기능이 고도로 발전할 것이다. 이러한 기술적인 변화는 표준안으로 정리되어 시장에서의 기기의 기능을 통일하고 신기술에 의한 카드기능의 개선이 광범위하게 이루어지도록 할 것이다.

광범위하게 보급되고 있는 IC 카드는 사회적 변화의 극적인 면을 더욱 강조하게 될 것이다. 전자화폐를 발행하고 있는 국가, 즉 영국의 Mondex, 독일의 GeldKarte, 미국의 VisaCash, 네델란드의 ChipKnip 등 여러의 경우를 보면, 고도의 인증기능과 신용 사회의 도래는 지불수단이나 화폐의 발행을 한정된 기관에 국한하지 않고 다양한 주체에 의하여 이루어지고 있으며, 이러한 추세가 전세계에 확산되는 것은 시간문제인 것이다. 국가기관이나 공공적인 성격의 기구 등에 의하여서만이 이루어지던 각종 증빙 활동도 그 주체가 더욱 확대되고 개인화하는 경향이 지속될 것이다. 이는 인류 문명에서의 전환기적인 사건으로 자리 매김 할 기술 현상의 하나인 것이다.

참고문헌

[1] D.C. Lynch and L. Lundquist, *Digital Money : the New Era of Internet Commerce,* John Wiley and Sons, Inc., New York, 1996

[2] H. Dreifus and J. T. Monk, *Smart Cards: a Guide to Building and Managing S mart Card Applications,* John Wiley & Sons, Inc., 1998

[3] J. Seberry and J. Pieprzyk *Cryptography: an Introduction to Computer Security,* Prentice Hall, 1989

[4] A. Saloma, *Public-Key Cryptography,* Springer-Verlag, Berlin, 1990

[5] U. Kaiser and W. Steinhag-en, "A low power transpon-der IC for high performance identi-fication systems," *IEEE J. Sol-id State Circ-ui ts,* vol. 30, no. 3, pp. 306-310, Mar, 1995

[6] 이필중, "암호화 신원인증으로 프라이버시 보장," *비둘기*, 10-11쪽, 1998년 6월호

< 전덕영 위원 >