情 報 保 護 學 會 誌
第 16 卷 第 5 號, 2006. 10

금융 IC카드 보안과 EMV 인증

김 학 범*

요 약

신용카드의 보안을 해결하는 방안으로 IC카드의 도입이 활발히 진행되고 있으며, 국제적으로는 EMVCo가 IC 신용/직불 카드 규격을 공동으로 제정하여 이를 기반으로한 승인작업이 세계적으로 정착이 되고 있는데, 특히 IC카드에서는 EMV 승인을 받은 카드의 사용을 권장하고 있다. 본 고에서는 금융 IC카드 관련하여 기본적인 특징과 표준 현황을 살펴보며, EMV 규격의 보안 부분과 EMV 카드 인증에 대해서 기술한다.

Ⅰ. 서 론

전자상거래에서 카드 정보 유출을 방지하고 카드 이용자가 본인임을 확인할 수 있는 수단으로 안전결제 서비스 도입과 공인인증서 이용이 해결책으로 적용된 것처럼 오프라인 카드거래에서도 IC카드의 도입이 위·변조 거래를 예방하고 금융 보안을 해결할 수 있는 최선책으로 인식되고 있다[1].

IC(Integrated Circuit) 카드는 일반적으로 플라스틱 카드에 집적회로 칩이 부착된 카드로 스마트카드라고도 하지만, 실제 스마트카드는 IC카드의 한 종류로서 CPU와 논리연산회로가 내장되어 있어 정보의 저장과 처리가 가능한 카드이다.

IC카드를 이용한 서비스는 다양하지만, 지급 결제 수단으로 사용하는 금융카드 서비스로는 신용카드, 현금카드, 직불카드, 전자화폐, 선불카드 등이 있다.

국제적으로 EMVCo가 IC 신용/직불 카드 규격을 공동으로 제정하여 세계적으로 정착이 되고 있으며, 특히 아시아권에서는 M/S(Magnetic Stripe) 카드의 불법적인 사용액 증가로 인하여 비자/마스터카드에서는 2006년도까지 100% 보급계획과 한국, 태국, 대만을 우선 전환국으로 진행하고, 특히 IC 신용카드를 강력히 권장하고 있으며, IC카드에서는 반드시 EMV 승인을 받은 카드의 사용을 권장하고 있다[2].

국내에서도 2003년 3월 금융감독원이 수립한 '전자금융 및 IT부문 안전성 확보 대책'에 따르면, 국내 금융기관은 2005년도 말까지 현금카드를 IC카드로 교체 발급하고, 신용카드는 2004년 10%, 2005년 25%, 2006년 45%, 2007년 70%, 2008년 100% 비율로 전환하도록 되어 있다. 현재 이와 같은 일정이 엄격히 준수되고 있지는 않지만 세계적인 신용카드사인 비자와 마스터카드 역시 자사 브랜드의 카드를 EMV 기반의 IC카드로 전환한 것을 권고하고 있기 때문에 자기띠(M/S) 기반의 IC카드로의 전환은 거스를 수 없는 대세임이 분명하다[3].

본 고에서는 금융 IC카드 관련하여 기본적인 특징과 표준 현황을 살펴보며, EMV 규격의 보안 부분과 EMV 카드 인증에 대해서 기술한다.

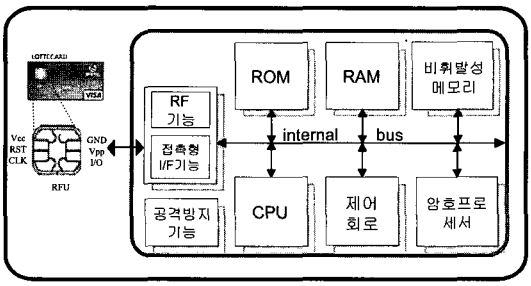
Ⅱ. 금융 IC카드의 이해 및 현황

1. 개 요

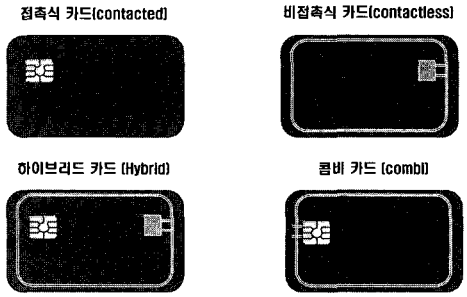
금융 IC카드는 일반적인 플라스틱 카드에 IC 칩을 부착하고 신용카드, 직불(현금)카드, 전자화폐 등의 기능을 저장하여 사용하는 카드이다. IC카드는 대량의 정보를 저장할 수 있으며 칩에 저장된 고유번호로 암호화 알고리즘을 구동시키기 때문에 카드를 복제하여도 사용할 수 없어 보안 측면에서 기존의 M/S 카드보다 훨씬 우수하다고 알 수 있다[1].

금융 카드에 부착되어 있는 IC카드는 그림 1과 같이 구성되어 있다.

* 순천향대학교 정보보호학과 (khb0305@sch.ac.kr)



〔그림 1〕 IC카드 구조



〔그림 2〕 IC카드의 외형적 유형

2. IC카드 분류

2.1 통신 방식에 따른 분류

IC카드는 카드에 부착된 IC칩과 카드 단말기의 물리적인 접촉여부에 따라 접촉식(Contact)과 비접촉식(Contactless) 카드로 구분되며[4] 표 1과 같다.

접촉식 카드는 칩 부분이 카드 리더기의 접점에 접촉되었을 때 작동하는 것으로서 높은 보안을 요구하는 금융 분야에서 주로 사용되며, 접점이 자주 접촉되어 물리적 손상의 우려가 있다.

비접촉식 카드는 교통 분야와 같이 빠른 처리 속도를 필요로 하는 업무에 사용되는데 RF(Radio Frequency)라고 하는 무선주파수를 통하여 외부와 통신을 하는 비접촉식으로 기본적인 구조에 있어서는 접촉식 IC카드와 유사하다. 다만, 무선주파수 송수신을 위한 RF 안테나와 이를 처리하기 위한 RF칩이 내장되어 있고, 비교적 사용처가 단순하기 때문에 CPU와 같은 고성능 마이크로프로세서보다는 특정 기능을 구현한 전자회로에 의해 카드가 제어되는 것이 일반적이다. 접촉으로 인한 전기적 충격이나 손상이 없으며, 주머니에서 꺼내는 불편함이 없고 칩이 눈에 보이지 않는 장점이 있는 반면, 가격이 고가이며 아날로그와 디지털 회로의 집적화가 어렵다는 단점이 있다.

최근에는 기술발전에 따라 접촉식 카드와 비접촉식 카드를 하나의 카드로 지원할 수 있는 하이브리드(Hybrid) 카드와 콤비(Combi) 카드가 주종을 이루고 있으며 각 방식의 유형은 그림 2와 같으며, 각 방식의 특징은 표 2와 같다.

〔표 1〕 접촉식과 비접촉식 IC카드 비교

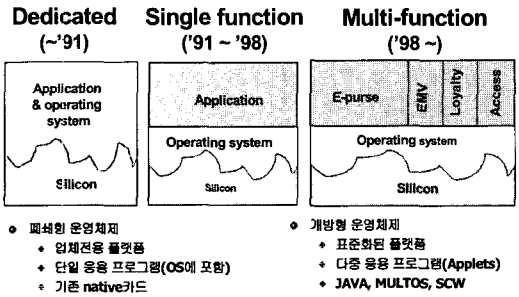
인터페이스	접촉식 (Contact)		비접촉식 (Contactless)	
CPU 유무	○	×	○	×
명 칭	Smart	Memory, Dummy	Smart	Memory, Dummy
특 징	보안성이 강함			편의성, 신속성이 장점
응 용	전자화폐, 직불, 응용, 신분증, 인터넷 인증 등	공중전화카드, 은행카드, 신용카드		교통, 출입통제 등
규 격	- ISO 7816 - Microprocessor(CPU) - Memory - COS 내장		- ISO 14442 - Memory - Antenna 내장	

〔표 2〕 IC카드의 외형적 유형에 따른 특성

구 분	특 성
접촉식 카드	전후면 관계없이 좌상측에 8개의 접점을 가진 금색판(GOLDEN PLATE)을 볼 수 있으며 그 이외의 부분은 카드 본체로 쓰이는 PVC, ABS 등의 재질이다.
비접촉식 카드	안테나코일,IC(Integrated circuit), 카드본체로 구성되어 있으며 외형적으로 볼 때 ISO 7810 ID1의 물리적 크기만 만족한다면 여타의 신용카드와 비교해 다른 면을 찾지 못할 것이다. 주로 사용되는 비접촉식카드는 13.56MHz R/W가능 Passive 메모리카드가 주로 사용된다. 마이크론사의 Mifare Card가 대표적인 경우이다.
하이브리드 카드	물리적으로 데이터를 공유하지는 못하나 한 장의 카드에 두 가지 이상의 기능을 탑재한 카드를 지칭한다. GEMPLUS사의 GEMTWIN Card의 경우 MPCOS 64K 접촉식카드와 GCL8K Mifare 비접촉식카드 기능을 동시에 수용한 HYBRIDE CARD가 좋은 예이다.
콤비카드	접촉식 Input/Output 모드와 비접촉식 Input/Output 모드를 동시에 가지고 있는 ONE CHIP (ONE CIRCUIT) 방식으로 물리적, 화학적으로 데이터를 공유할 수 있다. 일반적으로 가치(Value)는 접촉식 모드를 통해 입력되고, 저장된 가치는 비접촉식 모드에 의해 사용(출력)되는게 일반적인 예가 될 것이다.

2.2 플랫폼에 따른 분류

IC카드 운영체제는 COS(Chip/Card Operating System)라 불리며 초기 운영체제는 제한된 하드웨어 자원을 이용하는 Firmware와 같은 형태였으나 점차 카드 기술 및 메모리, 칩 공정 기술의 발달로 다양한 명령을 수행하고 코드 상에서 새로운 기능을 추가, 삭제할 수 있는 운영체제로 발전해 왔다(그림 3 참조).



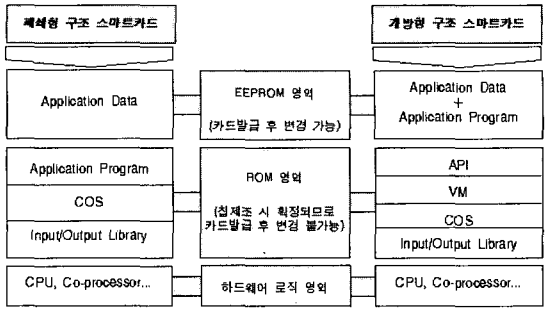
〔그림 3〕 IC카드 플랫폼 구조

폐쇄형 플랫폼은 플랫폼에 의존적인 특성으로 인해 응용 프로그램 개발이 어렵고 개발시간이 오래걸린다는 단점을 가지고 있지만 메모리 자원이 제한된 카드 환경을 효율적으로 이용함으로써 공간 오버헤드를 줄일 수 있고 카드 성능이 우수한다는 장점이 있다.

한편 개방형 플랫폼(Open Platform)은 표준 API 규격에 맞게 응용 프로그램을 개발하기 때문에 응용 프로그램 개발이 쉽고, 운영체제 계층 위에 존재하는 가상 기계로 인해 다양한 응용 프로그램을 카드 한 장에 탑재하여 사용할 수 있다. 하지만 기존 카드 플랫폼에 비해서는 공간 최적화, 성능 부분에서는 다소 뒤떨어지는 단점이 있다. 개방형 플랫폼은 카드가 발행된 후 주어진 카드에 새로운 응용 프로그램 기능을 추가할 수 있도록 허용하므로 표준 언어와 개방형 API를 사용하는 새로운 응용 프로그램은 칩으로부터 독립적으로 새로운 칩 기술을 사용하기가 용이하여 다중 응용 프로그램과 시스템간 격리/분리가 이루어질 수 있다[5].

개방형 IC카드 플래폼에는 Multos, 자바 카드, Smart Card for Windows 등과 같은 세가지 솔루션이 존재한다.

폐쇄형 운영체제와 개방형 운영체제의 특징을 비교하면 그림 4와 같다.



〔그림 4〕 폐쇄형 플랫폼과 개방형 플랫폼 비교

Ⅲ. 금융 IC카드 관련 표준

1. 금융 IC카드 표준

국내 은행이 IC 현금카드를 발급하기 위해서 적용하고 있는 표준으로 금융 IC카드 표준이 있다. 마그네틱 현금 카드를 위조하여 고객의 예금을 인출한 사고가 다수 발생하면서 IC현금 카드의 도입 여론이 형성되었고 이를 위해 금융정보화추진분과위원회 은행소위원회가 금융 IC카드 표준(개방형, 폐쇄형)을 제정하였다.

개방형 금융 IC카드는 접촉식 IC카드의 국제표준인 ISO 7816[6]을 참조하여 EMV V4.0, 자바의 개방형 카드 규격을 기반으로 현금카드 이외에 직불카드, 전자화폐(K-Cash), 공인인증서까지 다양한 금융 서비스를 추가할 수 있다. 금융 IC카드에 적용되는 현금카드와 신용카드 이외의 서비스는 각 금융기관이 자율적으로 추진하기로 하였다. 다만 금융 IC카드 표준은 은행 공동의 표준이기 때문에 IC 현금카드가 금융 공동망에서 이용되기 위해서는 금융결제원의 금융 IC카드 표준 인증을 받아야 하며, 인증을 받지 못한 카드는 발급 은행에서만 이용할 수 있다[1].

2. EMV 규격

EMV 규격의 개발은 카드 회사인 벨기에의 Europay, 미국의 Mastercard와 Visa사가 기존의 M/S 카드 기반의 신용/직불카드를 IC카드화 하기 위한 작업반을 형성하면서부터 시작되었다. '95년 6월 EMV2.0 버전이 발표된 이후, EMV3.0('96년 6월), EMV3.1.1('98년 5월), EMV4.0(2000년 12월), EMV4.1(2004년 5월)로 개정되었다. 본 고에서는 가장 최근 자료인 EMV4.1의 보안 및 키 관리 위주로 살펴본다.

2.1 규격의 구성

EMV 규격은 기본적으로 ISO의 IC카드 표준인 ISO 7816을 참조하고 있으며, 표준은 크게 IC카드에 관련된 사항, 보안에 관련된 사항, 신용/직불 응용에 관련된 사항, 단말기에 관련된 사항으로 나눠져 있으며, 4.1버전의 세부 구성은 표 3과 같다[7~10].

〔표 3〕 EMV 4.1 규격의 구성

규격명	주요 내용
BOOK 1 : Application Independent ICC to Terminal Interface Requirements	- Part I : General - Part II : Electromechanical Characteristics, Logical Interface, and Transmission Protocols - Part III : Files, Commands, and Application Selection
BOOK 2 : Security and Key Management	- Part I : General - Part II : Security and Key Management Techniques
BOOK 3 : Application Specification	- Part I : General - Part II : Data Elements and Commands - Part III : Debit and Credit Application Specification
BOOK 4 : Application Specification Cardholder, Attendant, and Acquirer Interface Requirement	- Part I : General - Part II : General Requirements - Part III : Software Architecture - Part IV : Cardholder, Attendant, and Acquirer Interface

2.2 보안 및 키 관리

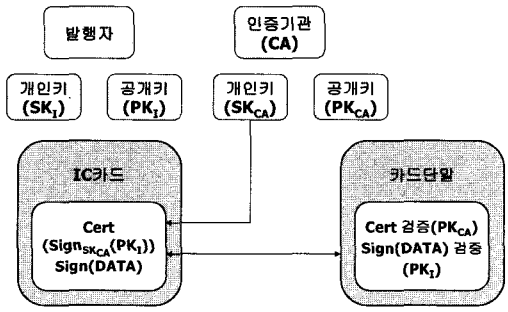
보안 및 키 관리 문서에서는 IC카드와 단말기 사이에서 정확한 동작 및 상호운용성을 위한 최소한의 보안요구사항을 정의한다. 또한, 추가적인 요구사항 및 권고사항들로 IC카드와 발급기 사이의 온라인 통신, 단말기 암호키 관리, 지불시스템의 보안등급 등을 제공한다.

보안 및 키 관리 요구사항은 오프라인 정적 데이터 인증, 오프라인 동적 데이터 인증, 오프라인 PIN 암호화, 응용 암호문과 발행자 인증, Secure Messaging, 인증기관의 공개키 관리 원칙 및 정책, 단말기 보안 및 키관리 요구사항을 다루고 있다.

(1) 오프라인 정적 데이터 인증(SDA)

오프라인 정적 데이터 인증(SDA : Static Data Authentication)은 공개키 기술에 기반한 전자서명 기법을 사용하는 터미널에 의해 수행된다. 이는 개인화(personalization) 후에 중요한 칩 내부에 저장되어 있는 정적인 데이터의 인가되지 않은 변경을 검출하기 위해 사용된다. SDA에는 발행자의 공개키를 서명하기 위한 매우 안전한 암호 설비인 CA(인증기관)가 요구된다. 터미널에 의해 인식되는 각 응용에 대하여 적절한 CA의 공개키가 포함되어야 한다.

발급기관이 IC카드를 개인화 할 때 카드에 전자서명 값이 카드번호, 사용자 이름, 주소 등과 같이 저장되며, 카드가 단말기에 삽입된 후 발행자의 공개키에 대한 CA의 서명값과 데이터에 대한 발행자의 서명값이 단말기로 전송되면 단말기는 미리 분배되어 있는 CA와 발행자의 공개키를 사용하여 서명값들을 검증함으로써, 카드에 대한 인증을 하게 되는 방식이다(그림 5 참조).



〔그림 5〕 IC카드와 터미널간의 통신

이 방식은 단지 저장된 값만을 이용하므로 IC카드 내에서의 공개키 암호 연산이 필요 없다는 장점이 있는 반면, 인증할 때마다 동일한 인증 정보를 사용하여 재사용 공격(replay attack)에 취약하다는 단점이 있다.

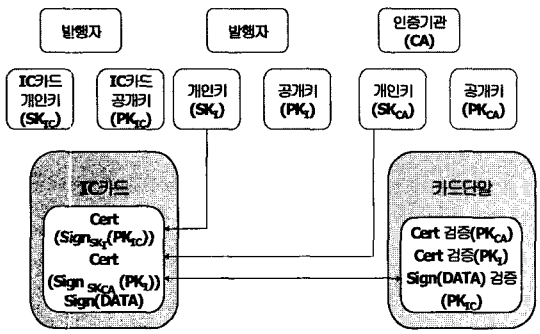
(2) 오프라인 동적 데이터 인증(DDA & CDA)

두가지 형태의 동적 데이터 인증이 존재하는데 DDA(Dynamic Data Authentication)은 카드 활동 분석 전에 수행되는 것이며, CDA(Combined Dynamic Data Authentication/Application Cryptogram Generation)는 첫 번째와 두 번째 AC 명령어 수행시에 수행된다.

카드 자체의 공개키와 개인키를 갖고 있으며, 거래시 단말기가 생성한 난수값을 포함한 동적인 데이터가 단말기로부터 전송되는 것으로부터 시작한다.

카드는 이 동적인 데이터에 자신이 가지고 있는 개인키로 서명한 뒤 카드의 공개키에 대한 발행자의 서명값, 발행자에 대한 CA의 서명값을 단말기에 전송하면 단말기는 미리 분배되어 있는 공개키들로 서명들을 검증하므로써 카드에 대한 인증을 수행한다.

카드에 암호 연산을 수행할 수 있는 프로세서가 탑재되어 있어야 하며, 정적 인증과는 달리 매 인증마다 변하는 데이터를 사용하기 때문에 재사용 공격에 안전하다는 장점이 있다. 오프라인 동적 데이터 인증은 그림 6과 같다.



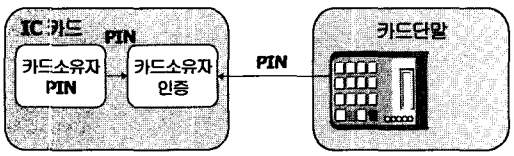
〔그림 6〕 오프라인 동적 데이터 인증

(3) 오프라인 PIN 암호화

오프라인 PIN 검증을 위한 PIN 암호화는 secure tamper-evident pad부터 IC카드까지 보안 전송을 보장하기 위한 암호화 메커니즘에 기반한 비대칭 알고리즘을 사용하는 터미널에 의해 수행된다.

PIN은 보통 4 자리의 숫자(0~9)로 사용하며 PIN이 터미널 키패드 또는 컴퓨터의 키보드를 통해 입력되면 그 정보는 카드로 보내어지게 되고 카드는 내부에 저장된 PIN 정보와 비교해서 그 결과를 터미널에 알려주는 방식으로 사용자를 인증한다.

PIN 입력시, 공격자가 간섭(Tampering) 공격을 함으로써 PIN 정보를 알아낼 수 있기 때문에 PIN 정보는 암호학적 기능을 갖춘 PIN Pad에 의해 암호화되어 전송된다. 터미널이 카드 소유자를 인증하는 방식은 그림 7과 같다.



〔그림 7〕 PIN을 이용한 방식

(4) 응용 암호문과 발행자 인증

이 절에서는 응용 암호문(TC, ARQC, AAR, AAC)의 생성을 위한 방법들을 제공한다. 응용 암호문은 IC카드와 인가응답 암호문(ARPC)에 의해 생성되고 ARPC는 발급자에 의해 생성되고 IC카드에 의해 검증된다.

두 가지 방법이 발급자 인증을 위해 사용된 ARPC의 생성을 위해 제공된다. 첫 번째 방법은 8바이트 ARPC를 생성하기 위한 방법으로 Triple-DES 알고리즘을 적용하며, 두 번째 방법은 4바이트 ARPC를 생성하기 위하여 MAC 알고리즘을 이용한다.

응용 암호문과 발급자 인증을 위한 메커니즘은 유일한 IC카드 응용 암호문 마스터키의 발급자에 의한 관리를 요구한다.

(5) Secure Messaging

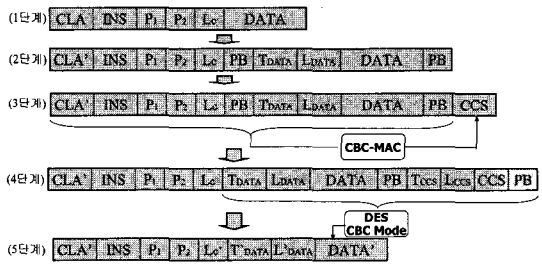
Secure Messaging의 목적은 데이터의 기밀성, 무결성 및 인증을 보장하는데 있다. 데이터의 무결성과 인증을 하기 위해서는 MAC 정보를 이용하고, 데이터 필드를 암호화하여 데이터의 기밀성을 확보하게 된다. 이는 통신사에서 가해질 수 있는 각종 위협에 대한 방어수단이다.

IC카드와 터미널 사이의 데이터 전송은 IC카드의 I/O 접속단자를 통해 이루어지는데 전송 중에 있는 데이터가 그대로 전송된다면, 공격자가 전송되는 데이터를 도청 또는 위·변조하는 것이 가능하고, 수신자는 이러한 사실을 알지 못할 것이다. 안전한 전송을 위해서 데이터의 일부 또는 전체에 대한 인증, 필요하다면 기밀성이 보장되어야 하며 안전한 전송 프로토콜을 시작하기 전에 우선 IC카드와 단말기 사이에 RSA, DH, ECDH 등의 방식 사용하여 키 공유가 이루어져야 한다.

전송방법에 대해서는 ISO/IEC 7816-4에서 정의하고 있으며, 추가적인 기능은 7816-8에서 정의한다. 사용 방법에 따라 인증모드, 결합모드, 전송 수열 카운터 모드 등이 있는데 본 고에서는 결합모드만 살펴보도록 하겠다.

결합 모드는 인증모드에 비하여 더 높은 수준의 보안 전송방법으로 전송 데이터는 암호화하여 전송되며 인증모드를 보완한 방법으로 CCS(Cryptographic Checksum) 뿐만 아니라 암호화를 함으로써 안전하게 전송할 수 있으나, 암/복호화에 걸리는 시간이 필요하기 때문에 효율성이 떨어진다는 단점이 있다. 결합 모드의 단계는 다음과 같이 5단계로 진행되며 그림 8과 같다.

① 단계 1 : 전송 데이터에 APDU 형식의 헤더 부분을 추가함
② 단계 2 : 데이터를 TLV 코드화 형식으로 변환한 후, 8 바이트의 정수배가 되도록 패딩함
③ 단계 3 : DES를 이용하여 CBC-MAC으로서 8 바이트 CCS를 계산함
④ 단계 4 : 8 바이트의 정수배가 되도록 패딩 바이트를 추가하고, CBC 모드의 DES로 초기 APDU 형식의 헤더를 제외하고 암호화
⑤ 단계 5 : CCS 계산과 암호화에 사용된 PB를 제거한 최종 전송 데이터



〔그림 8〕 결합모드

(6) 인증기관의 공개키 관리 원칙 및 정책

인증기관 공개키는 일반적으로 아래의 단계를 거치게 된다.

① 계획(Planning)
② 생성(Generation)
③ 배포(Distribution)
④ 키 활용(Key Usage)
⑤ 폐기(Revocation)

계획 단계에서 가장 중요한 과정은 보안적인 측면에서 현재 키와 신규 키의 예상수명을 검토하는 것이다. 이 과정을 통해 신규 키의 길이와 만료일 뿐 아니라 사용중인 키의 길이와 폐기일자가 정해진다.

생성 단계에서는 CA가 앞으로 사용하기 충분한 공개키를 만들게 되는데 공개키 구현과 함께 CA는 고유의 비밀 키를 만들어야 한다.

배포 단계에는 CA가 새로운 CA 공개키를 각 발행자(Issuer: 은행)와 소유자(acquirer : 카드회사)에 배포하게 되는데 발행기관이 지불시스템이 제공하는 이 인증서를 확인하거나 소유자가 단말기에서 인증서를 안전하게 사용하기 위한 목적으로 사용된다.

키 활용 단계에서 CA 공개키는 상점에서 고정적, 가변적 데이터에 대한 인증을 하고, 오프라인으로 암호화된 PIN을 사용하기 위해서도 쓰이며, 발행자 공개키 인증서(Issuer Public Key Certificates)를 만드는 경우에도 사용된다.

폐기 단계에서 CA 공개키의 만료일이 되면, 키는 폐기되는데, 개인키와 함께 제공된 발행자 인증서 역시 사용할 수 없게 되어 발행자는 인증서가 제공된 IC 카드가 유효한지 만료일 전에 확인해야 한다. 또한 만료일 이전 일정시점부터 CA는 발행자 공개키 서명을 중단하여 더 이상 인증서가 발급되지 않도록 하고 만료일이 되면 가맹점은 공개키를 제거해야 한다.

이외에 규격에서는 다음과 같은 공동 원칙과 함께 각 단계에 필요한 원칙들을 규정하고 있다.

① 인증기관 공개키를 폐기하면 해당 신용/지불카드 재생산이 필요하다.
② 지불시스템은 공개 키 폐기를 위한 정책, 절차 및 일정을 결정해야 한다.
③ EMVCo, LLC는 공개키 폐기에 대한 공통된 개념과 회원간의 원활한 협의를 위한 공통 용어를 사용한다.

(7) 단말기 보안 및 키관리 요구사항

이 절에서는 평문 PIN 및 암호키와 같은 기밀 데이터를 다루기 위한 일반적인 단말기 요구사항을 기술하고 있으며, 특히 CA 공개키를 위한 핀 패드 보안 요구사항과 키 관리 요구사항에 대해서 다루고 있다.

먼저 단말기에 관한 요구사항은 다음과 같다.

① 변조방지장치 : 변조 방지 장치는 내부적으로 저장된 기밀 데이터로의 물리적 접속을 제한하고, 장비의 도용, 인가되지 않은 사용이나 변경을 막도록 설계되어야 할 것이다. 이러한 목적은 일반적으로 변조 방지, 변조 검출, 변조 표시, 혹은 시각적 혹은 청각적 경보와 같은 응답 메커니즘의 통합을 요구한다. 변조 방지 장치는 어떤 하나의 기능뿐만 아니라 어떤 여러 기능들의 조합도 단말기에서 수행되는 보안에 의해 명백히 허용되는 것을 제외하고 기밀 데이터를 노출시키는 결과를 가져와서는 안 되도록 설계되어야 한다. 합법적인 기능만이 사용될 때라도 기밀 데이터를 손상하지 않도록 논리적 보안이 충분하여야 한다. 이 요구사항은 통계자료의 내부 모니터링에 의해 혹은 기밀 기능 호출간의 최소 시간 간격을 부과함으로써 성취될 수 있다.
② PIN 패드 : PIN 패드는 변조 방지 장치이어야 한다. PIN 패드는 4~12 디지트 PIN의 입력을 지원하여야 한다. PIN 패드상에 표시장치가 있으면 각 디지트 입력의 표시가 디스플레이 되어야 한다. 그러나 입력된 PIN의 값들은 ISO 9564-1에 따

라 시각적 혹은 청각적 피드백 수단에 의해 표시되거나 노출되어서는 안된다.

키 관리 요구사항에서는 단말기에서 CA 공개키의 매입사에 의한 관리에 대한 요구사항을 명시하며 이 요구사항에는 다음과 같은 단계를 포함한다.

① CA 공개키 도입 : 지불시스템이 새로운 CA 공개키가 도입되어질 것임을 결정하게 되면 지불시스템으로부터 각 매입사에게 새로운 키의 분배를 보증하는 처리가 수행된다. 그러면 새로운 CA 공개키와 관련 데이터가 단말기로 전송되는 것을 보증하는 것은 매입사의 책임이다.

② CA 공개키 저장 : 오프라인 정적/동적 데이터 인증을 지원하는 단말기들은 이 명세서에 근거한 EMVCo 멤버등의 debit/credit 응용을 위해 RID (Registered Application Provider Identifier) 당 6개의 CA 공개키를 지원하여야 한다.

③ CA 공개키 사용 : 트랜잭션동안 CA 공개키의 사용은 이 명세서에 규정된 것과 같아야 할 것이다.

④ CA 공개 키 폐기 : 지불 시스템이 CA 공개키 중 하나를 폐기하기로 결정하면 매입사는 CA 공개키가 어떤 날짜부로 트랜잭션동안에 오프라인 정적/동적 데이터 인증을 위해 단말기에서 더 이상 사용될 수 없음을 보증하여야 한다.

〔표 4〕 터미널에 저장되어야 하는 CA 공개키 관련 데이터 요소의 최소 집합

필드 명칭	길 이	설 명
등록된 어플리케이션 개발업체 별자(RID)	5	CA 공개키와 연관된 지불시스템을 식별
CA 공개키 인덱스	1	RID와 관련된 CA 공개키를 식별
CA 해쉬 알고리즘 지시자	1	전자서명 방식에서 해쉬 결과를 창출하기 위해 사용되는 해쉬 알고리즘을 식별
CA 공개키 알고리즘 지시자	1	CA 공개키와 같이 사용되어질 전자서명 알고리즘을 식별
CA 공개키 모듈	가변(최대 248)	CA 공개키의 모듈부의 값
CA 공개키 지수	1 or 3	3 혹은 216+1와 동일한 인증기관 공개 키의 지수부의 값
CA 공개키 체크썸	20	SHA-1을 사용한 CA 공개키의 모든 부분(RID, CA 공개키 인덱스, CA 공개키 모듈, CA 공개키 지수)의 oncatenation 상에서 계산된 체크값

Ⅳ. 금융 IC카드 인증

이 장에서는 금융 IC카드 관련한 인증에 대한 내용을 살펴보며, 간단한 제품 인증 분류와 함께 EMVCo에서 수행하고 있는 EMV 인증에 대하여 자세히 살펴본다.

1. 제품 인증의 분류

IC카드 관련한 인증은 표 5와 같이 구분할 수 있으며[11], 본 고에서는 EMVCo에서 수행중인 EMV 인증을 살펴본다.

〔표 5〕 제품인증의 분류

분류 방법	세부 분류	내용
제품에 따른 분류	칩카드 인증	비자인터내셔날과 마스터카드 인터내셔날에서 인증서 발행기관의 역할
	단말기 인증	EMVCo에서 인증서 발행기관의 역할
사용 방식에 따른 분류	접촉식 카드 방식	
	비접촉(RF) 카드 방식	
인증에 따른 분류	카드 인증	칩하드웨어 인증, EMV Level1 및 어프리케이션 인증, Risk Review(위험성검토) 인증 등
	단말기 인증	EMV 단말기 인증, VLP 인증, PED(핀패드) 인증 등
	근거리 무선 방식 인증	비자 비접촉식 인증(MSD, 비접촉 VSDC, Visa Wave), 마스터카드 Paypass 등

2. EMV 인증

EMV 인증은 EMV Level1과 EMV Level2로 구분되며 단말기에 대한 인증은 EMVCo에서 관리한다. EMVCo, LLC는 EMV 규격을 만든 Europay, Master, Visa 신용카드 3사가 사가 동일한 지분으로 설립한 회사로 2002년에 Europay International이 Master 카드에 합병되면서 2004년 12월 일본의 카드사인 JCB international이 참가하고 있다.

EMVCo, LLC는 EMV 표준의 보급, 갱신 등의 제반관리 담당하고 있으며, 이사회 산하에 3사의 직원들로 구성된 7개의 워킹그룹(Card and Terminal WG, Security WG, Type Approval WG,

Interoperability WG, Common Core Requirements WG, Security Evaluation WG, Card Approval WG)만을 운영하며 업체에서 생산된 EMV 제품이 표준에서 정한 규격대로 준수하고 있는지 여부를 테스트하기 위한 인증절차를 제정한다. 이에 대한 실제 인증은 EMVCo가 승인한 인증센터에서 수행하며 현재까지 승인된 인증센터는 표 6과 같다[12].

〔표 6〕 EMVCo가 승인한 Labs(2006년 10월 현재)

국가	인증센터	인증범위
한국	ICT Korea Co., Ltd.	Level 1 & 2
일본	TUV Japan Ltd., TUV SUD Group	Level 1 & 2
대만	FEIMA ltd. Taiwan Branch	Level 2 only
중국	Beijing Unionpay Card Technology Co., Ltd(Bank Card Test Center)	Level 1 & 2
영국	Radio Frequency Investigation Ltd.(RFI) Global Services	Level 1 & 2
	TUV Product Service Ltd (United Kingdom)	Level 2 only
프랑스	FIME European Test Center	Level 1 & 2
	Groupement Des Cartes Bancaire "CB"	Level 2 only
독일	Cetecom ICT Services GmbH	Level 1 & 2
	VOB-ZVD	Level 2 only
스페인	Applus+ Certification Technological Center	Level 1 & 2
	Sermepa	Level 2 only
	Sistema 4B	Level 2 only
이태리	Associazione Progetto Microcircuito	Level 2 only
덴마크	Danish Electronics Light & Acoustics(DELTA)	Level 1 & 2

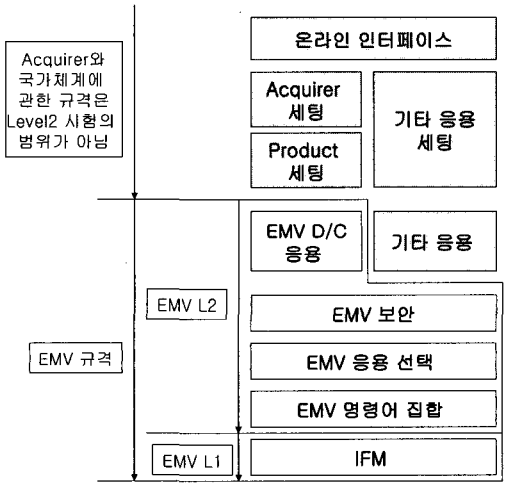
국내의 IC 신용카드 표준은 국제 호환성을 위하여 EMV 규격의 ICカード를 그대로 국내 표준으로 채택하였기 때문에 별도의 표준을 개발하지 않고 EMVCo 멤버의 전환 프로그램을 따라가게 되었다. EMV IC 신용카드 단말기는 EMVCo 멤버의 인증을 받아야 되는데 국내 전용으로만 사용되는 IC 신용카드는 EMV 규격을 적용하되 여신전문금융협회를 로컬 EMV 인증센터로 선정하여 국내에서 인증을 수행한다.

이외에 국내의 EMV 규격 카드 단말기에 대한 인증기관으로 EMVCo가 인증한 ICT Korea가 있는데, 2002년 10월부터 EMV 기반 단말기를 인증하였으며, 2004년 10월부터 EMV 규격 IC카드의 국내 인증 업무를 담당하고 있다.

2.1 EMV 인증의 종류

EMV 인증은 EMV Level1과 EMV Level2로 나뉘는데 터미널 구성요소 중 각각에 대한 시험범위는 그림 9와 같다[13][14].

IFM(Interface Module)은 Level1에 맞는지 평가되는 장치의 부분으로서 IFM 단독으로 운영가능한 장치를 구성하지 못한다면 IFM의 운영을 허용하는 다른 구성요소도 제출되어야 하지만, 시험과 승인은 IFM에만 한정된다.



〔그림 9〕 터미널 구성 요소 설명

EMV Level1 인증은 하드웨어에 관련된 안정성 시험으로 인증 대상 제품은 칩카드를 사용하는 모든 단말기다.

- 칩카드리더기(PC용 더미리더기)
- 카드조회기용 카드리더 모듈

EMV Level1 인증에는 또한 하드웨어에 대한 시험 환경(전압변동, 온/습도)에 대한 시험이 포함되어 있으며 주요 시험 내용은 다음과 같다.

- Electrical, Mechanical Tests
- Contact Sequencing
- Answer to Reset
- Protocol Test(T=0, T=1)

EMV Level2 인증은 제품의 소프트웨어에 대한

시험으로 제품의 어플리케이션(S/W)에 대한 신뢰성 및 정확성 시험이다. 인증 대상 제품은 칩카드를 이용하는 신용 및 직불거래 기능을 갖춘 모든 단말기이다.

- 카드 결제 조회기
- CD/ATM기 등

EMV Level2 인증을 위해서는 EMV Level1 인증을 사전에 받아야 하며 약 2천불의 비용이 소요되는데, 주요 시험 내용은 다음과 같다.

- EMV transaction flow
- Application selection
- Security aspects
- Terminal capabilities
- Terminal risk management

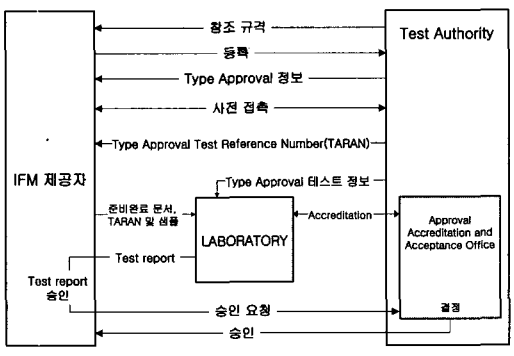
소프트웨어 구조, 식별 및 버전 통제는 EMV 규격의 범위를 벗어나며 요구되는 EMV 규격의 기능들을 지원하기 위한 소프트웨어 구성요소는 EMV 응용 커널(application kernel)이라 한다. 응용 제공자는 EMV 응용 커널을 확인해야 하며, 응용 제공자의 명명 규칙에 따라 유일한 이름을 붙여야 한다. 만약 승인된 부분에 대한 변경이 발생했을 경우는 Major 변경과 Minor 변경을 확인하여 Major 변경일 경우는 새로운 인증이 요구된다.

2.2 인증 절차 및 특징

기업에서 인증을 준비하거나 진행하기 위해서 가장 먼저 할 사항은 인증시험을 할 수 있는 시험소를 선정하여 사전에 필요한 사항을 준비하여야 한다.

2.2.1 인증 절차

EMV 인증을 위한 절차는 그림 10과 같다.



〔그림 10〕 제품 인증 절차

Level1과 Level2에 공통된 사항으로는 인증업체에 등록 신청(업체→EMVCo), 시험의뢰(업체), 시험시행(Lab.), 인증신청(업체→EMVCo), 승인(EMVCo)의 순서로 진행되며, Level2에 대해서는 EMV 승인 전에 EMVCo에서 ICS 승인후 진행하며 ICS Lab.에서 검토후 EMVCo에 발송하게 된다.

① Vendor 등록 : EMVCo에서 공인한 Test Lab에서 TA(Type Approval) Testing이 완료되기 전에 EMVCo에 업체 등록을 하여야 한다.
- 등록신청서(T1-Admin, T2-Admin:Appendix 1)를 작성하여 송부한다.
- EMVCo는 등록번호와 계약사항, 절차와 추가정보에 대해서 보내준다.

② EMVCo/Vendor 계약 : 계약에 대한 모든 내용은 모든 Vendor에 표준으로 제공되며 계약을 체결한다.

③ Testing Process : Testing은 반드시 EMVCo에서 공인된 Lab에서 실시한다.
- 선정한 Lab과 TA Test를 수행하기 위한 H/W, S/W, Documents 조건을 논의해야 한다.
- ICS(Implementation Conformance Statement)와 필요한 문서, Sample을 송부한다.
- Lab은 EMVCo Test Process에 부합하여 test하며 Test Report를 업체에 송부한다.

④ 승인 요청(Request for Approval)
- 제품에 대한 문서를 EMVCo에 제출하며, 승인 비용을 지불한다.
- EMVCo에서 시험결과를 평가한다.

⑤ EMVCo 승인(Approval)

V. 결 론

본 고에서는 신용카드의 보안을 해결하기 위한 방안으로 도입되고 있는 IC카드에 대한 기본 특징, 보안요구사항과 EMV 인증에 관련된 현재까지의 국·내외 추진 현황에 대해서 살펴보았다.

금융 IC카드의 향후 전망으로는 지속적인 이용 증가가 예상와 함께, 고전적인 카드 외형의 탈피를 들 수 있는데 유럽의 SIM(Subscriber Identity Module) 카드가 그 예이다. 또한 유비쿼터스와 디지털 컨버전스의 영향에 따라 휴대폰과의 결합, 생체인식 기능을 바탕으로 하는 새로운 기술의 발전을 예상할 수 있다[3]. 이에 따른 기능의 확장과 함께 관련 보안기술들도 역시 확보되어야 할 것으로 사료된다.

또한 제품의 호환성과 안전성을 확보를 위한 노력으로 콤비 카드를 대상으로 비접촉식 제품에 대한 인증이 준비되어 진행되고 있으며, 사용 중에 칩카드 손상을 방지하기 위한 카드의 내구성 시험에 대한 부분도 새롭게 연구되고 있다.

참 고 문 헌

[1] 백미연, "금융IC카드 이용 동향", 금융결제원 *지급결제와 정보기술*, 제20호, pp. 68-99, 2005.4.

[2] 김소연, "스마트카드를 이용한 금융카드 서비스 및 시장 동향", *TTA 저널 90호*, pp. 75-82, 2004.7.

[3] 장병환, "카드기반 지급결제수단의 이용현황 및 전망", 금융결제원 *지급결제와 정보기술*, 제24호, pp. 1-30, 2006.4.

[4] Wolfgang Rankl, Wolfgang Effing, *Smartcard Handbook*, John Wiely & Son, 3rd Ed., 2003.

[5] 한진희, 스마트카드 플랫폼 기술, TTA 저널 90호, pp 75-82, 2004.7.

[6] ISO 7816, *Identification Card - Integrated Circuit(s) Card with Contacts, Part 1-15*

[7] EMV Spec. V4.1 Book1, *Application Independence for ICC to Terminal Interface Requirements*, May 2004.

[8] EMV Spec. V4.1 Book2, *Security and Key Management*, May 2004.

[9] EMV Spec. V4.1 Book3, *Application Specification*, May 2004.

[10] EMV Spec. V4.1 Book4, *Cardholder, Attendant, and Acquirer Interface Requirements*, May 2004.

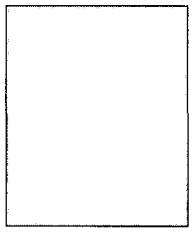
[11] 전정호, "EMV 인증과 기술동향", ICT Korea, 2006.3.

[12] www.emvco.com\

[13] EMVCo LLC v4.0. *EMVCo Type Approval Terminal Level 1 Administrative Process*, Feb. 2003.

[14] EMVCo LLC v1.3. *EMVCo Type Approval Terminal Level 2 Administrative Process*, Dec. 2004.

〈著者紹介〉



김 학 범 (Hak-Beom Kim)
종신회원
1990년 8월 : 중앙대학교 대학원 컴퓨터공학과 졸업(석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월 (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 (주)장미디어인터렉티브 상무이사
2005년 4월~현재 정보보호연구소 부소장
2001년 3월~현재 순천향대학교 공과대학 정보보호학과 겸임교수
관심분야 : 컴퓨터보안, 공개키 기반구조(PKI), 정보보호 표준화/평가, 스마트카드 보안, 유비쿼터스 보안