情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

무선 PKI 환경에서 사용 가능한 사용자 보안 모듈의 개발 동향과 향후 전망

곽 진*, 이 승 우*, 오 수 현*, 원 동 호**

요 약

최근 이동통신 기술의 발전으로 이동통신 서비스의 발전과 함께 휴대폰과 노트북, PDA(Personal Digital Assistance)를 이용하여 무선 인터넷 이용자가 증가하고 있다. 또한 이를 이용한 뱅킹 서비스, 주식 거래, 온라인 쇼핑 등의 전자 상거래가 급속하게 발전하고 있다. 그러므로 무선 인터넷 환경에서 안전한 서비스를 제공하기 위해 유선 인터넷 환경에서와 같은 보안 서비스를 제공할 수 있는 무선 PKI(WPKI:Wireless Public Key Infrastructure)의 필요성이 대두되고 있다. 그러나 무선 인터넷 환경이 갖는 특수성과 사용하는 단말기의 제약 사항들로 인해 유선 인터넷 환경과는 달리 여러 문제점들이 있다. 이러한 무선 인터넷 환경에서의 문제점들을 해결하기 위해 사용자가 쉽게 사용할 수 있는 보안 모듈의 필요성이 대두되었다.

현재 대표적인 보안 모듈로는 스마트 카드 방식과 USB 기반 방식이 있으며, 본 고에서는 각 방식들에 관한 관련 표준과 최근 제품 동향에 대해 언급하고, 사용자 보안 모듈의 향후 전망에 대하여 살펴보도록 한다.

Ⅰ. 서 론

최근 들어 이동통신 서비스의 급속한 발전과 함께 개인의 휴대폰이나 노트북, PDA 등을 이용하는 무선 인터넷 사용자가 증가함에 따라, 무선 인터넷을 이용한 뱅킹 서비스, 주식 거래, 온라인 쇼핑 등의 전자 상거래가 급속히 발전하고 있다. 또한, 무선 인터넷 환경에서 안전한 서비스를 제공하기 위해 유선 인터넷 환경에서와 같은 보안 서비스를 제공할 수 있는 무선 PKI의 필요성이 대두되었다. 즉, 유선 인터넷 환경에서 제공되는 기밀성과 무결성, 부인봉쇄 등의 보안 서비스를 무선 인터넷 환경에서도 제공하기 위한 연구가 활발히 진행되고 있다.

그러나 무선 인터넷 환경이 갖는 특수성과 사용하는 단말기의 여러 제약 사항으로 인해, 무선 환경에서는 유선 환경과는 달리 많은 문제점들이 존재한다. 즉, 현재 무선 인터넷 환경에서 사용하고 있는 휴대폰이나 PDA와 같은 단말기의 연산 능력으로는 전자 서명의 생성·검증이나 인증서 검증과 같이 많은 시간이 소요되는 공개키 암호 관련 연산을 수행하기 어렵다. 또한, 무선 단말기의 메모리 크기의 제한으로 인해 많은 인증서를 저장하는 데에도 한계가 있으며, 단말기 분실시 인증서나 사용자의 비밀키와 같은 중요 정보를 분실할 우려도 있어 안전성 면에서도 문제점이 있다.

이러한 문제를 해결하기 위해 불법 변조 방지(tamper resistant) 특성을 갖으면서 암호 알고리즘, 사용자의 키, 인증서 및 관련 정보를 저장할 수 있는 별도의 보안 모듈의 필요성이 대두되었다.

보안 모듈이란 암호 시스템을 사용하는데 필요한 사용자의 비밀키 관련 정보나 개인 ID 등이 탑재되는 하드웨어 토큰으로, 단순히 메모리 기능만을 수행하는 것과 연산 능력이 있는 프로세서를 포함하는 것이 있다. 보안 모듈은 무선 단말기, 노트북 및 데스크 탑 PC, 네트워크 서버 등에 설치가 가능하고 보안 시스템의 관리를 매우 효율적으로 수행할 수 있다는 장점이 있다.

아직까지는 이러한 보안 모듈이 유선 PKI 기반의 제품에서만 활용되고 있지만, 앞으로 무선 인터넷의 활성화와 함께 무선 PKI 상에서도 보안 모듈

* 성균관대학교 전기전자 및 컴퓨터공학부 정보통신보호연구실 ({jkwak,swlee,shoh}@dosan.skku.ac.kr)
** 성균관대학교 전기전자 및 컴퓨터공학부 교수 (dhwon@simsan.skku.ac.kr)

이 널리 활용될 것으로 예상된다.

그러므로, 본 고에서는 PKI 환경에서 안전하고 효율적으로 사용 가능한 사용자 보안 모듈의 개발 동향과 향후 전망에 대하여 언급하고자 한다.

본 고의 구성은 다음과 같다. 먼저 제 2장에서는 무선 PKI 기술의 개요에 대하여 살펴보고, 다음으로 제 3장에서는 무선 PKI 환경에 적용할 수 있는 사용자 보안 모듈에 대해 기술한다. 사용자 보안 모듈은 크게 스마트 카드 기반 방식과 USB 기반 방식으로 구분할 수 있으며, 각 방식에 대해 관련 표준 규격과 최근 제품 동향에 대해 언급하고, 제 4장에서 사용자 보안 모듈의 향후 전만에 대하여 논한다. 마지막으로 5장에 결론을 맺는다.

Ⅱ. 무선 PKI 기술

본 장에서는 무선 PKI의 개요와 대표적인 무선 인터넷 접속 방식인 WAP(Wireless Application Protocol) 방식과 ME(Mobile Explore) 방식에 대하여 간략하게 설명한다.

1. 개 요

유선 인터넷 환경과 마찬가지로 무선 인터넷이 안전한 서비스를 제공하기 위해서는 기밀성, 무결성, 인증, 부인봉쇄와 같은 보안 서비스를 제공하기 위한 무선 PKI가 필요하다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용하며, 무선환경에 적합하도록 기능을 최소한 변화시킨 것이다. 즉, WAP 게이트웨이를 통한 무선 PKI 서비스에서는 기존의 유선 환경에서 사용하는 X.509 인증서에 비해 부피가 작고 간단한 구조로 구성되어 있는 WTLS (Wireless Transport Layer Security) 인증서를 사용한다. 이는 무선 환경에서 사용하는 소용량 단말기에서 암호화 및 인증 업무를 효율적으로 수행할 수 있도록 구성되었다.

2. 무선 PKI 구성요소

무선 PKI를 구성하는 요소로는 인증서를 발행하고 효력정지 및 폐지 기능을 수행하는 인증기관, 인증서 등록 및 사용자 신원 확인을 대행하는 등록기관, 인증서 및 인증서 폐지목록을 저장하는 디렉토리, 그리고 인증서를 신청하고 인증서를 사용하는 사용자로 분류될 수 있으며 각각의 특징은 다음과 같다.

- **인증기관 (CA : Certification Authority)**

인증기관은 공개키 기반구조를 구성하는 가장 핵심 객체로 사용자의 공개키 인증서의 발급·효력정지 및 폐지와 등록기관의 요청에 따라 인증서를 발급하는 기능을 수행한다. 또한, 인증서와 인증서 소유자의 정보의 관리, 인증서와 그 소유자의 정보를 관리하는 데이터 베이스의 관리, 인증서 효력정지 및 폐지목록, 감사 파일을 보관 등의 업무를 수행하는 핵심 기관이다.

- **등록기관 (RA : Registration Authority)**

등록기관은 인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자 사이에 설치하여 인증기관을 대신하여 사용자들의 인증서 신청 시 그들의 신분과 소속의 확인, 인증기관에 인증서 요청서 전송, 디렉토리로부터 인증서와 인증서 효력정지 및 폐지 목록 검색, 인증서 효력정지 및 폐지 요청 등의 기능을 수행한다.

- **디렉토리 (Directory)**

디렉토리란 인증서와 사용자 관련 정보, 상호인증서쌍 및 인증서 폐지목록의 저장 및 검색 장소로, 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP(Directory Access Protocol) 또는 LDAP (Lightweight DAP v2, v3)를 이용하여 X.500 디렉토리 서비스를 제공한다. 인증서와 상호인증서 쌍은 유효기간이 경과된 후에도 서명 검증의 응용을 위해 일정기간 동안 디렉토리에 저장된다.

- **사용자 (End entity)**

공개키 기반구조내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 말하며, 자신의 비밀키/공개키 쌍을 생성하고 검증, 공개키 인증서의 요청/획득, 전자 서명의 생성 및 검증, 특정 사용자의 인증서 획득 및 검증, 자신의 인증서 취소 등의 기능을 수행한다.

위에서 설명한 무선 PKI를 구성하는 4개의 중추적인 구성 요소 외에 무선 인터넷 사용자를 대신하여 인증서 상태 정보와 함께 인증 경로에 대한 검증 정보들을 제공하는 OCSP(Online Certificate

status Protocol)나, 무선 단말기의 계산 능력 저하로 인한 단점을 보완하기 위하여 사용되는 보안 모듈 등이 무선 인터넷 상에서 PKI를 구성하기 위한 부수적인 구성 요소이다. 더불어, 무선 PKI는 무선 인터넷 상에서 구성되어야 하므로, WAP 방식이나 ME 방식과 같은 무선 인터넷 접속 기술 또한 중요한 구성 요소이다. 각 접속 기술에 따라 PKI를 구성하는 인증서의 형식, 전송 포맷, 서명 알고리즘, 키분배 알고리즘 등이 각 방식에 적합하게 변형되어 사용된다.

3. 무선 PKI 모델

무선 PKI 모델에서 기본적으로 무선용 X.509 인증서를 사용하지만, 무선 CA 서버는 단말기의 검증 능력을 고려하여 WTLS 인증서를 사용하며, 무선 단말기의 저장공간 문제를 해소하기 위해 인증서를 발급 받을 경우 인증서의 URL을 이용하기도 한다.

단말기에서 무선용 X.509 서버 인증서의 검증 메커니즘으로는 CRL(Certificate Revocation List)이나 OCSP를 사용하도록 한다. 또한 무선에서는 최신의 CRL만을 모아놓은 Delta CRL을 옵션으로 사용한다.

무선 단말기에서 RSA를 사용하여 키 생성이 용이하지 않을 경우를 고려하여 ECDSA를 사용하여 키를 생성할 수 있는 기능이 추가로 제공되며, 서명 알고리즘으로는 RSA, ECDSA가 사용되고 키분배용 알고리즘으로는 RSA, ECDH 등이 있다.

III. 사용자 보안 모듈

본 장에서는 대표적인 사용자 보안 모듈인 스마트 카드(Smart card)와 USB(Universal Serial Bus) 기반 방식에 관련된 기술 표준 및 최근 제품 동향에 대해 기술한다.

1. 스마트 카드

스마트 카드는 인터넷의 사용이 급증하면서 통신, 금융, 교통, 그리고 전자 상거래 등의 분야에서 다양하게 활용되고 있다. 특히 반도체와 소프트웨어 기술의 발전과 함께 대용량 정보의 저장과 보안성을 바탕으로 스마트 카드의 응용 분야는 더욱 확대되고 있다. 스마트 카드는 단지 데이터만을 저장하는 메모리 카드와는 달리 데이터 저장뿐만 아니라 논리 연산 회로와 CPU(Central Processing Unit)가 내장되어 있어 메모리 카드에 비해 그 활용도가 높다.

본 절에서는 스마트 카드의 종류와 특징, 구성 요소, 그리고 관련 표준 규격에 대하여 설명한다. 스마트 카드 관련 표준은 ISO/IEC 7816을 기본으로 하며, 비접촉식 스마트 카드에 관한 표준인 ISO/IEC 10536, ISO/IEC 14443, ISO/IEC 15693 등이 있다.

1.1 스마트 카드 개요

스마트 카드는 SPOM(Self Programmable One Chip Microcomputer)의 개발을 시작으로, 고속 수학 연산을 위한 마이크로프로세서와 정보의 저장을 위한 메모리, 그리고 운영 체제 등이 내장되어 있는 카드로 발전하였다.

스마트 카드는 적용 범위에 따라 IC 카드, 칩(Chip) 카드, 마이크로프로세서 카드, CPU 카드 등 여러 가지로 사용되고 있으며, "마이크로프로세서, 운영 체제, 보안 모듈, 메모리 등을 포함하고, 트랜잭션 처리 능력을 지니고 있는 칩을 내장한 신용 카드 크기의 플라스틱 카드"라고 정의하는 것이 일반적이다. 대부분 신용 카드 크기의 스마트 카드가 주를 이루고 있지만 휴대용 단말기에서 사용할 수 있도록 크기가 매우 작은 카드들도 개발되고 있다.

특히, 스마트 카드에는 별도의 전원 공급 장치가 내장되어 있지 않으며, 정보의 저장과 처리에 필요한 전력은 외부로부터 제공된다. 스마트 카드에 내장되어 있는 메모리는 EEPROM(Electrical Erasable Programmable Read Only Memory)을 사용하여 별도의 전원이 공급되지 않아도 저장 내용의 유지가 가능하다.

1.2 스마트 카드의 구성요소

스마트 카드는 CPU와 ROM(Read Only Memory), RAM(Random Access Memory) 그리고 데이터 저장을 위한 EEPROM 등으로 구성되어 있다. 이러한 구성 요소들은 스마트 카드의 성능을 좌우하는 것으로 계속해서 발전해 나가고 있다. 흔히 마이크로프로세서라고 불리는 CPU의 처리 능력은 스마트 카드의 수행 능력을 결정하는 가장 중요한 요소로서 8비트의 CPU가 주로 사용되고 있으며, 암호 알고리즘의 고속 연산을 위해 16비트

와 32비트 CPU가 개발되고 있다. ROM은 운영 체제인 COS (Card Operating System)와 보안 알고리즘 등을 저장하기 위해 스마트 카드 제작시 포함되어 있는 요소로, 스마트 카드의 제작 후에는 수정이 불가능하다. 현재 주로 사용되고 있는 ROM의 크기는 16KB 이며 32KB 등으로 발전하고 있다. 스마트 카드에 전력이 공급되는 동안 데이터의 임시 보관 장소인 RAM은 I/O 버퍼, 레지스터, 암호화 작업 등의 공간으로 사용되고 있다.

EEPROM은 기존의 ROM에 비해 읽기와 쓰기, 지우기가 모두 가능하다는 장점을 가지고 있지만, 상대적으로 ROM에 비해 가격이 비싸며 수행 속도가 느리다는 단점이 있다. 하지만 64KB EEPROM이 개발과 함께 수행 속도 향상을 위한 연구가 활발히 진행되고 있다. 수학적인 고속 연산을 위한 보조 프로세서는 주로 암호화 연산을 수행하고 있으며 스마트 카드의 정보를 보호하기 위한 요소라 할 수 있다. RNG(Random Number Generator)는 스마트 카드 내부에서 암호 알고리즘의 응용에 필요한 난수를 생성하기 위한 것이며 대부분의 스마트 카드에서는 카드의 성능을 향상시키기 위해 난수 생성기를 칩 내부에 포함하고 있다.

〔그림 1〕은 접촉식, 비접촉식, 혼합형 스마트 카드의 내부 구조를 나타낸 것이다.

1.3 스마트 카드 종류와 특징

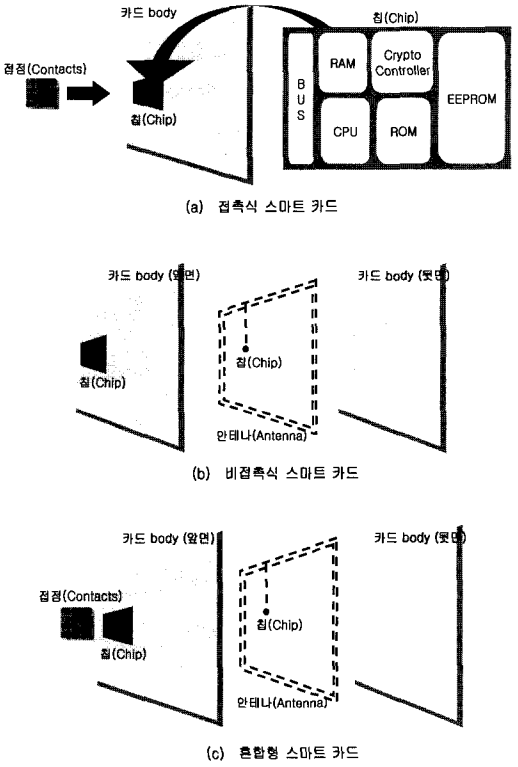
스마트 카드는 인터페이스 방식에 따라 접촉식과 비접촉식의 두 가지 방식으로 구분하는 것이 일반적이며, 마이크로프로세서의 포함 여부와 진화 단계에 따라 분류하기도 한다.

● 마이크로프로세서의 포함 유무에 따른 분류

스마트 카드는 마이크로프로세서의 유무에 따라 메모리 카드와 마이크로프로세서 카드로 분류할 수 있다. 메모리 카드는 프로세서를 내장하지 않고 메모리만을 내장하고 있는 카드 형태를 말하며, 마이크로프로세서 카드는 메모리와 CPU를 포함하고 있는 것으로, 읽기와 쓰기 그리고 추가적으로 보안 기능까지 제공할 수 있다.

● 진화 단계에 따른 분류

진화 단계에 따라 스마트 카드를 분류하면 초기의 메모리 카드, 단기능 스마트 카드, 다기능 스마트 카드, 네트워크 스마트 카드 그리고 컴퓨터 스마트 카드 등의 5단계로 나눌 수 있다.



〔그림 1〕 스마트 카드의 구조

● 인터페이스 방식에 따른 분류

스마트 카드는 외부와의 접촉 방식에 따라 접촉식과 비접촉식, 하이브리드 방식, 그리고 콤비 방식으로 분류한다.

접촉식 스마트 카드는 카드 판독기(card reader) 안에 삽입하는 방식으로, 카드 판독기와의 접촉으로 전원을 공급받는다. 따라서 카드 판독기와의 물리적인 접촉으로 인해 전기적 충격이나 손상의 우려가 있으나 상대적으로 많은 데이터를 처리하는 인증과 전자 서명의 응용에 적합하다.

비접촉식 스마트 카드는 카드 내에 내장되어 있는 안테나를 이용하여 RF(Radio Frequency) 신호에 의해 통신하는 것으로 카드 판독기에 삽입할 필요 없이 일정 거리에서 카드 판독기 근처에 근접시키면 정보의 교환이 이루어지는 방식이다. 비접촉식 스마트 카드는 전원 공급 방식에 따라 정전 결합을 통해 전원을 공급받는 밀착형(CICC : Contactless IC Card)과 전자 유도를 통해 전원을 공급받는 리모트형(RCCC : Remote Coupling Communication

Card)으로 구분된다.

혼합형 카드로는 하이브리드 카드와 콤비 카드가 있다. 하이브리드 카드는 서로 다른 카드 종류들을 하나의 카드에 구성한 것으로, 접촉식과 비접촉식의 인터페이스를 모두 포함하고 있으며, 접촉식과 비접촉식의 양 인터페이스가 독립적으로 운영된다. 그렇기 때문에 독립적인 메모리와 별도의 운영체제가 존재한다. 주로 교통카드로 많이 이용되고 있다. 반면 콤비 카드는 하이브리드 카드와 마찬가지로 접촉식과 비접촉식의 인터페이스를 모두 포함하고 있지만, 같은 메모리를 사용하여 두 인터페이스가 상호 보완적으로 운영된다. 하지만 공유 메모리 영역의 훼손 시 두 가지 기능이 모두 마비되는 단점이 있다.

1.4 스마트 카드 관련 표준

스마트 카드 관련 표준으로는 ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) 표준과 EMV (Europay Mastercard Visa) 규격, PC/SC (Personal Computer/Smart Card) 규격, 그리고 OCF(Open- Card Framework) 규격 등이 있다. 본 고에서는 각 표준에 대하여 간략하게 설명하도록 한다.

- **ISO/IEC 표준**

스마트 카드 관련 국제 표준인 ISO/IEC (International Organization for Standardization/ International Electrotechnical Commission) 표준 문서는 스마트 카드와 스마트 카드 판독기간의 통신 방법인 인터페이스 방식에 따라서 접촉식과 비접촉식 그리고 이 두 방식을 혼합한 겸용 방식의 세 종류로 나눈다. 접촉식 방식은 칩의 동작을 위한 전원과 클럭 신호를 얻기 위하여 판독기와의 물리적인 접촉이 필요한 카드로, ISO/IEC 7816 표준 문서에 의해서 정의하고 있다. 비접촉식 방식은 카드 판독기 부근에 카드를 근접시켜 카드와 판독기 사이에 전원을 얻고 정보를 교환 할 수 있는 방식을 말한다. 비접촉식 카드에는 크게 정전 결합으로 전원을 얻는 밀착형(close coupling)과 전자 유도를 통해 전원을 얻는 리모트형 그리고 마이크로파형으로 분류할 수 있다. 밀착형은 ISO/IEC 10536에 기술되어 있으며, 리모트형은 ISO/IEC 14443에서 정의하고 있다. 하지만, 마이크로파형에 관한 표준안은 아직 제정되지 않았다. 또한 접촉과 비접촉식 방식을 혼합한 겸용 방식은 두 방식이 물리적으로 연결되었는지 독립적으로 연결되었는지에 따라 콤비 카드와 하이브리드 카드로 나눌 수 있다. 겸용 방식에 관한 구체적인 표준안 역시 현재까지는 제정되지 않았다.

- **EMV 규격**

EMV(Europay Mastercard Visa)는 세계적인 3대 신용 카드 업체들인 Europay International Service Association, MasterCard International Inc, Visa Inter- national Service Association 이 공동으로 개발한 차세대 IC 카드 기반의 신용·직불 카드 기술 규격이다. 기존의 자기 카드(magnetic stripe card)의 취약한 보안성을 극복하고 다양한 금융 서비스를 제공하기 위한 목적으로, 신용/직불 카드 서비스를 위해 자기 카드를 IC 카드화한 스마트 카드와 금융 거래 시스템 규격이라 할 수 있다.

이를 위하여 3사는 제조사, 경제 제도 그리고 카드가 어디서 사용되던 지에 상관없이 세계 공통으로 사용할 수 있는 칩 카드와 단말기 사이에 동작이 가능하도록 하는 일련의 표준 스펙을 연구하기 시작하였다. EMV 2.0 규격은 1995년 6월에 발표되었고, 다음 해인 1996년 6월에는 개정본인 EMV 3.0 규격이 발표되었다. 그 후, EMV'96 버전 3.1.1이 발표되었으며 EMV 버전 4.0이 2000년 12월에 발표되었다. EMV 버전 4.0에서는 가까운 미래에 저전압 카드에 응용할 수 있는 표준 규격을 제시하였으며, EMV 칩 카드가 보다 적은 접촉을 통해 인터페이스 되는 방법을 정의하고 있다.

EMV 규격에서는 "스마트 카드"라는 용어 대신 "집적 회로 카드(ICCs : Integrated Circuit Cards)"라는 용어를 사용하고 있으며, 신용/직불 카드 서비스 제공을 위한 IC 카드에 대한 규격을 기술하고 있다. EMV '96 Version 3.1.1까지는 "EMV '96 Integrated Circuit Card Specification for Payment Systems", "EMV '96 Integrated Circuit Card Application Specification for Payment Systems", "EMV '96 Integrated Circuit Card Terminal Specification for Payment Systems"의 3개 부분으로 구성되어 있었으나, EMV 버전 4.0 에서는 크게 변경되어

- Book 1 : Application independent ICC to Terminal Interface requirements
- Book 2 : Security and Key Management

- Book 3 : Application Specification
- Book 4 : Cardholder, Attendant, and Acquirer Interface Requirements

등의 4권의 책으로 구성되어 있다.

• **PC/SC 규격**

PC/SC(Personal Computer/Smart Card) WG (WorkGorup)은 불(Bull), 마이크로소프트(Microsoft), 휴렛패커드(HewlettPackard), 지멘스-닉스돌프(Siemens Nixdorf 사와 슬룸버거(Schlumberger)사 5개의 다른 분야의 회원들이 주도해서 1996년 9월에 처음으로 발족되었다. 컴퓨터 제조업체와 카드 운영체제 개발업체로 이루어진 이 그룹은 스마트 카드, 전자 상거래, 그리고 네트워크 컴퓨터(NC : Network Computer) 분야의 다른 기술 업체들을 참가시키면서 젬 플러스(Gemplus), IBM Corporation, 썬 마이크로시스템즈(Sun Microsystems), 도시바(Toshiba)와 베리폰(VeriFone) 등 새로운 회원을 추가하였다.

PC/SC 워크 그룹은 사용자 신분 확인과 보안의 향상을 위해 스마트 카드를 사용할 수 있도록 제안하였고, 이에 대한 회원들의 노력으로 1997년 12월 PC/SC 규격 버전 1.0이 나오게 되었다. PC/SC 규격 버전 1.0은 워크 그룹의 회원인 젬플러스사가 컴퓨터 제조자로서 스마트 카드를 구성하고, 마이크로소프트사는 스마트 카드 자원 관리자(smart card resource manager)로서 PC/SC 규격을 지원하는 윈도우 플랫폼을 만들면서 이 표준을 완성시키고 있다. 그리하여 이 표준은 제조회사가 서로 다른 스마트 카드와 카드 판독기사이에 상호 이용을 가능하게 하며, 다중 응용 간에 자원 공유를 가능하게 함으로써 카드 주변 프로그램 개발 비용을 절감시켜 주고 있다.

PC/SC 버전 1.0이 제정된 이후에, PC/SC 버전 2.0이 웹 사이트를 통해서 드래프트가 되고 있으나 아직 새로운 버전이 제정이 되지 않은 상태이다. 또한, PC/SC 규격은 네트워크 컴퓨터와 스마트 카드의 호환성을 보장하기 위해 IBM의 주도로 오픈 카드 프레임워크(OpenCard Framework)와 협력하고 있다.

• **OCF 규격**

PC/SC보다 1년 뒤인 1997년에 만들어진 OCF (OpenCard Framework : 버전 1.1) 규격은 3-G 인터내셔널(3-G International), 아메리칸 익스프레스 여행 서비스사(American Express Travel Related Services), 불, 젬플러스, 퍼스트 액세스(First Access), 지세크&데브리언트(Giesecke & Devrient), IBM, 도시바, 토위토코(TOWITOKO), 슬룸버거, 지멘스, 썬 마이크로시스템즈, 유비큐(UbiQ Inc), 비자(Visa International), 엑스에이시 오토메이션(XAC Automation), 매니지먼트 보드(Management Board)로 이루어진 OCF 컨소시엄에서 제정하였다. 네트워크 컴퓨터, 스마트 폰(smart-phone), 셋탑 박스(set-top box) 등의 다양한 하드웨어 플랫폼이 스마트 카드 액세스를 위해 설계된 off-card용 객체 지향 소프트웨어 프레임 워크이다. 또한 OCF는 많은 소프트웨어와 하드웨어 플랫폼들에 대한 상호 작용 가능한 스마트 카드 솔루션들을 제공하고 있으며 개방된 카드(Open Card)에 관련된 환경 내에서 스마트 카드 관련 솔루션들을 만들어서 배치하는 응용의 서비스 제공자들과 개발자에게 가능한 응용 프로그램 인터페이스(API)와 구조를 제공하고 있다. 현재 OCF는 자바 컴퓨팅 플랫폼의 개척자이고 OpenCard 회원인 썬 마이크로 시스템의 전격적인 지원으로 전체적인 자바 응용 프로그래밍 인터페이스와 동반할 수 있는 기업표준에 적합성을 가진 자바언어로 프로그래밍되어 win95, 98, windows NT, Linux, IBM AIX 상에서 구현되어 있으며, PC 상으로의 접목을 위해서는 PC/SC 규격과 기타 ISO/IEC 7816, EMV, CEN, prEN 726, PKCS#11 등의 표준 및 규격을 참조하여 프레임 워크를 설계하였다.

1.5 스마트 카드 관련 제품 개발 동향

본 고에서는 스마트 카드 관련 표준에 따라 각 제품들의 개발 동향에 대하여 설명한다.

• **ISO/IEC 표준 관련 제품 개발 동향**

ISO/IEC 7816 접촉식 표준만 이용한 제품으로는 일본 DNP사의 RISONA Cards가 있으며, SchlumbergerSema사와 Easyflex City와 Gemplus사의 MPCOS Pro는 ISO/IEC 7816과 ISO/IEC 14443을 따르는 혼합형의 콤비 카드이다.

▪ SchlumbergerSema사의 <Easyflex City>

SchlumbergerSema사에서 만든 Easyflex City 카드는 국제 표준 문서 ISO/IEC 7816과

ISO/IEC 14443을 따르는 혼합 방식의 카드이다. 하나의 칩을 사용하는 마이크로프로세서 카드로서, 접촉식과 비접촉식이 모두 지원되며 마이크로프로세서가 인터페이스를 통제한다. 고속의 삼중 DES 암호 프로세서를 사용하며, 8 KB EEPROM과 SymbiOS 운영체제를 사용한다. ISO 7816-4에서 정의한 명령어와 파일 관리를 따른다.

접촉식 인터페이스는 ISO 7816 part 1, 2, 3, 4를 따르며, T=0 프로토콜을 사용하고 1MHz에서 5MHz를 위한 클럭 주파수와 최고 115 kbaud 데이터 통신 속도를 가지고 있다.

비접촉식 인터페이스는 ISO 14443 part 1, 2, 3, 4 유형 A를 따르며, 106kbaud의 데이터 통신 속도를 가지고 있으며, T=CL 프로토콜을 사용하고 보통 작동 중에 최고 10cm의 거리 범위를 가질 수 있다.

• DNP사의 <RISONA CARDS>

일본 DNP사에서 개발한 스마트 카드인 RISONA CARD는 국제 표준 문서인 ISO/IEC 7816의 part 1, 2, 3, 4를 따르고 있는 접촉식 스마트 카드이다.

8비트의 CPU와 256/1024 바이트의 사용자 메모가 있는 안전성 높은 스마트 카드이다. 암호화 알고리즘으로 DES와 triple DES를 사용하여 상호 인이 가능한 카드이다. 전송 프로토콜로는 ISO/IE 7816에서 정의한 T=1 비동기식 반이중 통신 프로콜을 이용한다.

• Gemplus사의 <GemCombi/MPCOS Pro>

Gemplus사의 GemCombi/MPCOS Pro 스마트 카드는 ISO/IEC 7816과 ISO/IEC 14443을 기반으로 하는 혼합 방식의 스마트 카드이다. 접촉식 표준으로 ISO/IEC 7816 part 1, 2, 3, 4를 따르며 비접촉식 표준으로 ISO/IEC 14443 part 1, 2, 3의 유형 A를 따르고 있고, 카드의 안전을 위해서 triple DES를 사용하였으며 응용에 유연하다.

● EMV 표준 관련 제품 개발 동향

현재까지 EMV 인증을 받은 국내 기업은 3, 4개 업체에 불과할 정도로 상당히 복잡한 인증으로 알려져 있다. 현재까지 한국정보통신(주), 사이버넷, 월마니어(주) 등이 단말기 인증을 받았으며, 삼성전자가 스마트 카드에 대한 EMV 인증을 획득한 것으로 알려 있다.

• 한국정보통신(주) <EMV 단말기>

한국정보통신(주)의 EMV 단말기는 기존 자기 카드와 IC 카드 공용이 가능한 최첨단 기기로 국내 최초, 세계적으로는 일본에 이어 2번째로 한국정보통신(주)가 개발에 성공하였다. 이 단말기는 기존의 신용 카드 단말기(EasyCheck)에 카드 삽입용 PIN PAD만 부착하면 되므로 기존 자원의 재활용이 가능하도록 하였다.

• 사이버넷 <EMV 단말기>

사이버넷은 세계에서 3번째, 국내 벤처 기업으로는 처음으로 EMV 인증을 획득하여 제품을 출시하였으며, EMV 응용을 업그레이드하기 용이하도록 개발하였다는 장점이 있다.

• 윌머니어스(주) <EMV 단말기>

윌머니어스(주)가 인증을 받은 EMV 단말기는 감열식 프린터 모듈을 기본으로 장착해 무선으로 현장에서 실시간으로 신용 카드 조회 및 결재를 할 수 있다. 또한, 기본 운영 체제를 리눅스로 채택하여 전원을 끄지 않고도 간단한 조작만으로도 영어, 일어, 한국어, 중국어 등 4개국 언어로 변경할 수 있어 국내뿐 아니라 해외에서도 인정받고 있다.

마스터, 비자 카드사는 위/변조의 위험이 높은 자기 방식의 신용 및 직불 카드를 보안성과 확장성이 큰 IC 카드로 대체하기로 하고, 2002년부터는 자기 카드, IC 카드 혼용으로 그리고 2005년부터는 IC 카드만 발급할 것으로 계획하고 있다.

국내에서는 SK텔레콤이 독자적으로 개발한 휴대폰 결재 기술을 비자와 공동으로 발전시켜 이를 비자의 국제 표준으로 채택하고, 전 세계에 공동 보급을 추진 중이다. 양사는 앞으로 스마트 카드형 신용 카드를 휴대폰에 장착하고 이를 적외선 금융 결제(IrFM) 표준에 따라 적외선 통신으로 결재하는 기술 개발을 공동 추진 중이며, 공동 개발된 기술은 근거리 무선 통신 결재 국제 표준 규격으로 삼아 전 세계의 이동 통신사와 금융사에 보급할 계획이다. SK텔레콤의 휴대폰 결재 기술은 스마트 카드 규격인 EMV 규격을 세계 최초로 적외선통신 방식을 통해 휴대폰에 구현한 기술이다.

EMV 규격의 실거래가 국내에서도 빈번히 이루어지자 비자·마스터 등 해외 신용 카드 브랜드와 국내 카드사·한국정보통신 등 사업자들도 본격적인

상용화에 대비해 시스템 정비를 서두르고 있다. 현재로서는 카드와 단말기간 승인 처리는 가능하지만 국제간 시스템 연동은 미비한 상태이며, 비자는 이를 완벽하게 온라인 처리할 수 있도록 한국 내 EMV 처리 환경을 연내에 구축할 계획이다.

● **PC/SC 표준 관련 제품 개발 동향**

PC/SC 규격으로 제품을 만든 외국 기업으로는 넥스마트(Nexsmart)사, 슐렘버저사, 어드벤스 카드 시스템(Advanced Card system)사 등이 있고 국내 기업으로는 스마트 카드 판독기와 라이터기를 만드는 재익정보통신(주)가 있다.

▪ 재익 정보통신 <CSR-120>

PC 내장형 스마트 카드 R/W 모듈인 CSR-120은 인터넷 뱅킹, 전자 상거래, 전자 서명, PC 보안등에 사용된다. 또한, ISO7816-1, 2, 3, 4가 지원되는 모든 스마트 카드를 지원하며 PC, Set-top Box 등의 단말기에 내장되고 PnP 기능으로 설치가 편리하다는 장점이 있다.

▪ 재익 정보통신 <CSR-130>

PC Serial(PC/SC) 접속형 스마트 카드 R/W인 CSR-130은, 인터넷 뱅킹, 전자 상거래, 전자 서명, PC 보안 등에 사용된다. ISO7816-1, 2, 3, 4가 지원되는 모든 스마트 카드에 지원되며, PC/SC, MONDEX, K-Cash, NETS 인증을 획득했고 PnP 기능으로 편리하게 설치할 수 있다. 또한, 별도의 전원 없이 키보드의 전원을 통하여 작동할 수 있다.

▪ 재익 정보통신 <CSR-140>

PC USB/Serial 접속형 스마트 카드 R/W인 CSR-140은 인터넷 뱅킹, 전자 상거래, PC 보안, 전자 서명, HTS 등에 사용된다. 별도의 전원 없이 USB/Serial 포트를 통하여 작동가능 하며, PC/SC, Mondex, V-cash 와 호환이 가능하고 PnP 기능으로 설치가 편리하다.

● **OCF 규격 관련 제품 개발 동향**

OCF 규격을 지원하는 회사에는 Linux, Utimaco, Gemplus, IBM 등이 있다. 젬플러스사는 OCF 규격을 사용하는 대표적인 회사로서 현재 OCF 규격으로 상용화된 제품에는 GemPC410, GemPC410-FD, GemPC410-SL, GemXplore CASE 3 for Java Card, GemXplore CASE Range, MPCOS-EMV 등이 있다.

▪ 젬플러스 <GamPC410>

Universal 스마트 카드 판독기인 GemPC410는 인터넷 뱅킹, 전자 상거래, 전자 서명 등에 사용된다. ISO7816-1, 2, 3, 4가 지원되는 모든 스마트 카드에 지원되며, OCF 규격 지원하고 RS- 232C 통신을 한다. TLP224, GLP 프로토콜을 사용하며 Serial Port와 Tower Casing을 사용한다.

▪ 젬플러스 <GamXplore CASE 3 for Java Card>

Java 카드인 GemXplore CASE 3 for Java Card는 인터넷 뱅킹, 전자 상거래, 전자 서명, 모바일 보안등에 사용된다. Java Card 2.1.1지원하고 ESTI GSM 03.19 R99 와 03.48 R98 규격을 지원한다. 또한, OCF 규격 지원하며 Visual Cafe, JBuilder를 사용하고 그래픽한 SIM 툴킷 응용 사용하며, Java Card 애플릿으로 다운로드와 조정이 가능하다.

▪ 젬플러스 <MPCOS-EMV>

마이크로프로세서 카드인 MPCOS-EMV는 전자 상거래, 전자 화폐, 신분 확인 등에 다양한 용도로 사용된다.

ISO7816-1, 2, 3, 4, 5를 지원하며, triple-DES 알고리즘을 사용하고 OCF, EMV 호환이 가능하며, 관리 명령어 집합을 지원한다.

그 중 제품 GemXplore CASE 3 for Java Card는 강력한 그래픽 인터페이스를 사용하는 Java GSM 카드로, 강력한 자바 도구 환경안에서 모바일 서비스가 빠르게 처리되도록 설계되어 있다는 특징이 있다.

2. USB 기반 방식

PC 환경에서 주변기기가 다양해짐에 따라 기존의 PC 환경에서 사용되던 카드방식으로 디바이스를 연결하는 슬롯과 프린터, 마우스 등의 주변기기를 연결하는 병렬포트나 직렬포트, IDE(Integrated Develop- ment Environment) 커넥터 등의 물리적인 공간이 부족하게 되었다. 뿐만 아니라 PC 환경에서 주변기기를 사용할 때 필요한 IRQ(Interrupt

Request)의 부족으로 많은 주변기기의 연결이 불가능하게 되었다.

또한 인터넷을 통한 각종 금융 거래나 전자 상거래가 확산되면서 본인 확인을 위한 개인정보가 크게 증가하고 있다. 그러나 인증서가 저장된 컴퓨터가 아니면 본인확인이 불가능하고 여러 사이트를 이용할 때마다 늘어나는 아이디(ID)와 비밀번호를 일일이 기억해야 하는 문제가 발생하였다. 이러한 문제점을 해결하기 위해, 인증서나 개인정보를 저장하여 필요할 때마다 이를 간편하게 사용할 수 있는 휴대용 저장장치가 개발되었으며, 이것이 USB (Universal Serial Bus) 방식의 드라이브, 토큰, 스마트 키이다.

1.1 USB의 개요

USB는 허브를 통해 컴퓨터 외부에서 쉽게 주변장치를 연결할 수 있게 하며, USB를 장착한 PC는 최대 127개의 주변장치를 연결할 수 있다. USB가 7비트의 어드레스 영역을 가지고 있기 때문에 128개의 디바이스까지 연결할 수 있게 된다. USB는 표준 규격을 바탕으로 인터페이스를 만들게 되므로, 새로운 인터페이스를 개발해야 하는 부담과 기존의 주변장치와의 충돌에 대한 부담을 줄일 수 있다. 그러므로 모든 주변기기가 동일한 USB 커넥터, 케이블로 연결되며 장착하는 순서와 전원 공급에 관계없이 장착과 분리를 쉽게 할 수 있는 Hot plug 기능을 지원함으로써 설치 작업을 보다 손쉽게 할 수 있다.

1.2 USB 휴대용 보안장치의 구성요소

USB 기반의 휴대용 보안장치는 외부 기기와 휴대용 보안장치를 연결할 수 있는 USB 접속부(Connector), 작동 표시기(LED Indicator), 그리고 USB 컨트롤러와 보안 칩(Cryptographic Chip)으로 구성되어 있다.

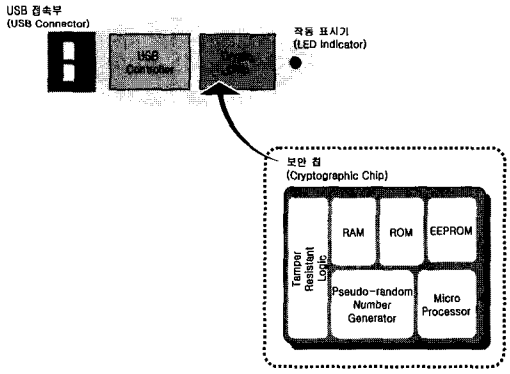
USB 컨트롤러는 보안 칩에서 사용하기 위한 정보의 전송과 외부 기기와의 정보 전송을 담당하며 스마트 카드 판독기와 같은 역할을 한다.

보안 칩은 스마트 카드와 마찬가지로 EEPROM, ROM, RAM, 그리고 암호화 연산을 수행하기 위한 마이크로프로세서와 난수 생성기(Pseudo-Random number Generator) 등으로 구성되어 있으며, 키의 생성·관리 및 정보의 저장을 담당하고 있다. 보안 칩에서 생성된 정보는 인증서나 공개키와 같은 공개정보를 저장하는 영역과 비밀키 등과 같은 비밀 정보를 저장하는 영역으로 나뉘어 저장된다. 암호화 연산을 위해 필요한 DES, triple-DES, RC2, RC4, 그리고 RC5 등의 알고리즘이 휴대용 보안장치 제조 시 ROM에 내장되어 있다. 또한, 물리적인 보안 특성을 제공하기 위해 외부의 압력이나 충격 등에 의한 충격 감지(Tamper Resistant) 방식으로 설계되어 있다.

USB 기반의 휴대용 저장 장치의 구조는 [그림 2]와 같다.

1.3 USB 기반 방식의 종류와 특징

USB 방식을 기반으로 하고 있는 휴대용 저장장치는 USB 드라이브와 USB 토큰, 그리고 USB 스마트 키 등이 있다. USB 드라이브는 휴대용 데이터 저장장치 용도로 개발된 것으로, 개인정보는 물론 용량에 따라 문서 파일이나 멀티미디어 파일을 저장할 수 있는 용량이 큰 디스켓이라 할 수 있다. USB 드라이브의 저장매체는 플래시 메모리로 1MB에서 1GB 용량의 다양한 USB 드라이브가 개발되었다.



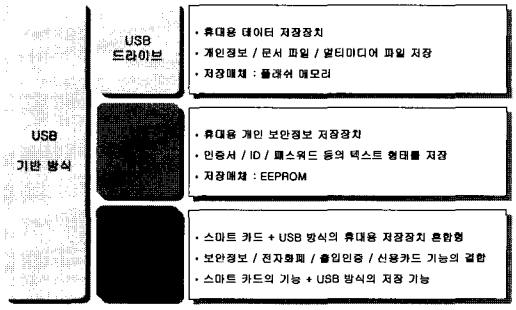
[그림 2] USB 기반 휴대용 보안장치의 구조

USB 토큰은 EEPROM을 저장매체로 사용하는 휴대용 보안장치로서, 용량은 8KB에서 16KB 정도로 1~3 개 정도의 인증서와 아이디, 패스워드 등의 텍스트 형태의 보안정보를 저장할 수 있다. USB 토큰은 인터넷의 발달과 휴대용 단말기를 이용한 인터넷의 사용이 증가하고, 특히 휴대용 무선 단말기를 이용하여 전자 상거래와 금융 거래를 안전하고 효율적으로 이용하기 위해 그 효용성이 증대되고 있다.

USB 스마트 키는 스마트 카드와 USB 방식의 휴대형 저장장치의 혼합형으로 보안정보 뿐만 아니라

전자화폐, 출입인증, 신용 카드 등의 모든 스마트 카드의 기능을 함께 사용할 수 있다.

〔그림 3〕는 USB 기반의 휴대용 저장장치의 종류를 나타낸 것이다.



〔그림 3〕 USB 기반 휴대용 보안장치의 종류

1.4 USB 기반 관련 표준

USB 관련 표준으로는 USB 1.1과 2.0, USB OTG(On-The-Go) 등이 있다. 본 고에서는 각각의 표준에 대하여 간략하게 설명한다.

• USB 1.1과 2.0

1996년 1월 인텔, 컴팩, NEC 및 마이크로소프트 등에 의해 USB 1.0 규격이 제정되었다. 처음에는 단순히 규격에 대한 정의만 이루어졌을 뿐 실제 실용화를 위해 개발되지는 않았다. 1998년에 전기적인 전송 규격과 프로토콜 같은 하드웨어와 소프트웨어 기술이 통합되어 새롭게 USB 1.1 규격이 발표되었다. 이와 동시에 여러 PC 메인보드용 칩셋 제작자들이 USB 포트를 지원하는 칩셋을 발표하고 메인보드 제작사들을 주축으로 지금처럼 PC에 USB 포트가 기본적으로 장착되기 시작했다.

그리고 2000년 4월에 기존의 USB 1.1 규격의 12Mbps보다 훨씬 빠른 속도인 480Mbps의 속도를 지원할 수 있는 USB 2.0 규격이 발표되면서 USB는 멀티미디어 컴퓨팅, 무선 LAN, 인터넷 정보가전 분야 등에서 중요한 역할을 하고 있다.

USB 1.1 시스템은 기본적으로 하나의 호스트와 여러 개의 주변장치들로 이루어진다. 그리고 호스트에는 루트 허브가 내장되어 있으며 호스트와 주변장치들은 외부 허브로 연결된다.

USB 2.0 허브에는 USB 2.0 주변장치와 USB 1.1 허브가 연결된다. 따라서 기존에 사용되던 USB 1.1 주변장치는 USB 1.1 허브를 통해 USB 2.0 허브로 연결된다.

• USB 1.1의 특징

USB 1.1은 1996년 1월에 발표된 USB 1.0을 실용화할 수 있도록 보완하여 1998년 9월에 최종 발표되었다. USB 1.1은 full-speed(12Mbps)와 low-speed (1.5Mbps) 두 가지 모드로 동작한다. USB 1.1의 특징은 다음과 같다.

먼저, USB 1.1은 케이블이나 커넥터에 대한 단일 모델을 제공하고, 자가 인식이 가능한 주변기기 및 드라이버 설정의 자동 매핑 기능을 가지고 있으며, 동적 부착이 가능한 재설정 기능을 가지고 있는 주변기기로 이루어져 사용자의 편의성을 제공한다.

또한, 기기의 버퍼링이 가능하도록 하여 넓은 범위의 패킷 사이즈와 다양한 데이터 속도를 지원한다. 버퍼 핸들링을 위한 제어가 프로토콜 내에서 구현되기 때문에 융통성이 있으며, 에러 처리 및 결점 복구가 프로토콜 내에 구현되어 있다. 기기의 착탈이 실시간으로 인식되며 고장난 기기를 자동으로 인식할 수 있는 기능을 가지고 있다.

USB 1.1은 다양한 대역폭(수 kbps~수 Mbps)을 갖는 기기에 적합하고, 동일 전송선에서 비동기식과 동기식 전송도 가능하다. 그리고 여러 주변 기기들 간에 동시 동작이 가능하며 대역폭이 허용하는 한도 내에서 127개의 기기를 연결할 수 있다.

PC를 호스트로 사용할 경우에는 PC의 PnP 기능과 호환되기 때문에 시너지 효과를 얻을 수 있으며, 특히 주변기기와 호스트 하드웨어의 최적화된 집적화가 가능하기 때문에 저렴한 가격의 주변기기의 개발에 적합하다. 그리고 하나의 시스템에 여러 호스트 컨트롤러를 지원할 수 있는 업그레이드가 가능한 구조를 가지고 있다.

• USB 2.0의 특징

USB 2.0은 고속의 인터페이스를 제공하기 위하여 USB 1.1을 개정 보완하여 2000년 4월에 발표되었다. USB 2.0의 가장 큰 특징은 기존의 USB 1.1에서 사용하던 케이블이나 커넥터를 그대로 사용하고 USB 1.1의 특징들을 대부분 그대로 유지하면서, high-speed(480Mbps)를 지원하는 것이다. 이를 backward 호환성이라 한다. 이 때, 접속된 두 디바이스 모두 high-speed를 지원하는 경우만 high- speed 전송이 가능하며, 한 쪽의 디바이스라도 full- speed/low-speed를 지원한다면 기존

의 full-speed나 low-speed로 데이터 전송이 이루어진다. 이를 forward 호환성이라 한다.

USB 2.0에서는 기존의 USB 1.1에서 사용하던 프레임을 더 세밀하게 나눈 마이크로 프레임이란 개념을 도입해서 좀 더 많은 양의 패킷을 자주 전송할 수 있도록 함으로써 대역폭을 효율적으로 사용할 수 있게 하였다. 표 1.은 USB 1.1과 USB 2.0의 특징을 비교한 것이다

〔표 1〕 USB 1.1과 2.0의 특징 비교

구분	USB 1.1	USB 2.0
대역폭(Mbps)	1.5 또는 12	480
최대 연결 주변기기 수(개)	127	127
PnP	가능	가능
Hot plug	가능	가능
케이블 최대 길이(m)	5	5
사용 케이블	4와이어 (데이터2,전원2)	4와이어 (데이터2,전원2)

• USB OTG

USB 규격을 제정하는 USB-IF(The Universal Serial Bus Implementers Forum)에서 USB 2.0 규격에 좀더 이점을 부여하자는 데 착안하여 PC에 연결되지 않는 USB 규격인 USB OTG (On-The-Go) 규격을 발표하였다. 이 새로운 내용을 후원하는 업체들로는 ACON, Cypress, Ericsson, Hewlett-Packard, InSilicon, Intel, MCCI, Microsoft, Motorola, NEC, Nokia, Onspec, OPTi, Palm, Philips, SoftConnex, Texas Instruments 그리고 TransDimension 등이 있다.

USB OTG는 USB 2.0 규격의 세부 규격으로 채택되었는데 지금까지의 USB는 PC와의 연결을 전제로 설계된 마스터 슬레이브의 구조를 가지고 있어 USB 장비끼리의 단독 통신은 지원되지 않았다. 이번 USB OTG의 채용으로 2대의 MP3 플레이어들간의 음악 전송, 디지털 카메라와 프린터의 직접 연결·인쇄, PDA와 다른 장비와의 연결과 같은 것이 가능하게 되었다.

USB OTG는 앞서 살펴본 것과 같이 USB 2.0의 세부 규격(On-The-Go Supplement to the USB 2.0 Specification)으로 채택된 것으로 세부구조와 특징 등은 USB 2.0과 거의 동일하다. 그 중 USB OTG에서 지원하는 서비스를 수행하기 위해 정의된 주요한 특징들을 살펴보면 다음과 같다.

• 두 가지 타입의 디바이스 정의

USB OTG에서는 두 가지 타입의 디바이스를 정의하고 있다. 하나는 일반적인 마스터-슬레이브 구조의 USB에서 사용되는 주변장치 디바이스이고 다른 하나는 USB 장비간에 통신이 가능한 Dual-role 디바이스로 이 두 가지 디바이스를 정의하고 있다. Dual-role 디바이스는 주변장치 역할 뿐만 아니라 제한적으로 호스트의 역할을 수행할 수 있고 "Targeted Peripheral List"를 통해 연결된 USB 장비가 Dual-role 디바이스로 사용되는 지 판단하고 그에 따른 서비스를 수행한다. 또한 SRP(Session Request Protocol)과 HNP(Host Negotiation Protocol)을 수행할 수 있다.

• SRP(Session Request Protocol) 수행

대기 상태에 있는 A-디바이스(호스트)에 SRP를 이용하여 B-디바이스(주변장치)는 버스의 초기화와 세션의 시작을 요청할 수 있게 된다. 요청방법으로는 "data-line pulsing"과 "VBUS pulsing"의 두 가지 SRP signaling 방법이 있다.

• HNP(Host Negotiation Protocol) 수행

호스트의 역할을 맡은 디바이스가 세션을 시작하게 되는데, HNP는 세션이 수행되는 중간에 호스트의 역할을 다른 dual-role 디바이스에게 전달할 수 있는 기능을 가진 프로토콜이다. 즉, 사용자의 편의에 따라 호스트와 주변장치의 역할을 케이블을 교환하는 번거러움 없이 호스트와 주변장치의 전환이 가능한 프로토콜이다.

• 커넥터

USB 2.0에서 정의한 Standard-A 플러그(plug)와 소켓(receptacle), Standard-B 플러그와 소켓 이외에 USB OTG에서는 Mini-A, B, AB 플러그와 소켓을 정의하고 있다. Mini-AB 소켓은 보드에 장착되어 있으며 Mini-A 타입이나 Mini-B 타입 플러그를 연결할 수 있다. 프로토타입 장치는 Mini-A 플러그가 연결되는 경우 USB 호스트 역할을 수행하고 Mini-B 타입 플러그가 연결되면 USB 주변장치로 동작하게 된다. 일단 한번 연결되면 두 디바이스들은 HNP에 의하여 호스트나 주변장치로 전환될 수

있다.

▪ 어댑터

USB OTG에서는 기존의 호스트 기반의 USB와의 호환을 위해 두 가지의 케이블 어댑터를 정의하고 있다. 기존의 호스트와 Mini-A 플러그를 연결하기 위한 "Standard-A 플러그와 Mini-A 소켓"과 dual-role 디바이스와 Standard-A 플러그를 연결하기 위한 "Mini-A 플러그와 Standard-A 소켓"이 있다.

1.5 USB 기반 관련 제품 개발 동향

• USB 1.1 및 2.0 관련 제품 개발 동향

USB 1.1과 2.0은 키보드, 마우스, 스캐너, 휴대용 저장 장치 등 다양한 주변 기기에 적용되어 개발되고 있다. 그러한 제품들 중 휴대용 저장 장치는 레인보우(RAINBOW)의 iKey2000, 시큐어센터(Secure Center)의 SecureKey, 시큐어피아(Securepia)의 MiKey, 세이프다임(SafeDigm)의 WiseClip 등이 개발되었다. USB 1.1/2.0 관련 제품 개발 현황은 〔표 2〕과 같다.

〔표 2〕 USB 관련 제품 개발 현황

제조사	제품명	특징
RAINBOV	iKey 2000	▪ USB 1.1과 2.0을 동시지원 ▪ FIPS 140-1 Level 2 획득 ▪ Taper-Proof 기능 ▪ 토큰 내부에서 1024bit RSA 키 생성 가능 ▪ PKCS#11, MSCAPI 지원
Secure Center	Secure Key	▪ 사용자 비밀번호와 SecureKey를 동시에 사용하여 Two-Factor 인증 기능 ▪ USB 시리즈 A 커넥터 사용
Securepi:	MiKey	▪ 사용자 인증, 웹 로그인, 절전 및 저장장치로 사용됨
SafeDigm	WiseClip	▪ 1024bit RSA 전자 서명 기능을 갖춘 Key-Token

Ⅳ. 향후 전망

사용자 보안 모듈은 스마트 카드 분야와 USB 기반 방식의 등장으로 급속히 발전하고 있다. 최근에는 자바카드(Java Card)나 SCfW(Smart Card for Windoes)를 이용한 다양한 응용카드의 개발과 무선 인터넷 환경에서 사용할 수 있는 USB 기반 방식의 휴대용 보안장치의 개발이 진행되고 있다.

스마트 카드의 표준화와 관련하여 ISO/IEC 7816과 ISO/IEC 14443 표준의 확립은 카드간의 호환성을 가능케 하여 다양한 응용을 발전시키고 있다. 특히 스마트 카드 시장은 유럽을 중심으로 매우 활발하게 성장하고 있다. 이에 각국에서는 특히 전자상거래 분야에서 편리성과 보안, 그리고 인증의 용이성으로 인해 그 이용이 급속히 확대되고 있는 추세이다.

USB 기반 방식의 드라이브와 토큰, 스마트키 등의 발전도 급속하게 진전되고 있다. 현재 국내에서도 USB 방식을 기반으로 하는 제품의 개발이 활발히 진행되고 있다. USB 기반 휴대용 저장장치는 보안성과 휴대성, 보관의 편리성을 바탕으로 하여 그 사용이 점차 확대되고 있으며 그 기능 또한 다양해지고 있다. 특히 인터넷을 이용한 전자상거래의 활성화와 함께 인증서의 저장과 개인의 비밀키 보관에 효과적으로 활용할 수 있다.

모든 통신 분야의 기술과 마찬가지로 무선 인터넷 환경에서의 사용자 보안 모듈은 사용자의 편의와 이동성을 제공하기 위해 발전해 나아갈 것으로 예상된다. 또한 개인 정보의 디지털화로 개인 정보의 안전한 저장과 신뢰할 수 있는 정보의 처리가 요구되면서, 스마트 카드나 USB 기반 휴대용 저장장치의 사용은 더욱더 증가하고 활성화 될 것으로 기대된다.

특히 이동통신 환경에서의 스마트 카드와 USB 기반 휴대용 저장장치는 사용자의 편리성을 제공하고 안전한 정보의 저장을 위해 매우 중요한 역할을 할 것이다. 스마트 카드와 USB 기반 휴대용 저장장치 분야의 기술은 공중전화카드와 교통카드, 회원카드, 선불카드 등과 같은 단일 기능을 가진 사용자 모듈에서 탈피하여 여러 기능을 통합하여 다중 기능을 가진 하나의 시스템으로 발전해 나가고 있다. 따라서 다중 응용 기능을 가진 스마트 카드와 USB 기반 휴대용 저장장치의 사용이 증가함에 따라 무선 인터넷 환경에서도 이를 사용하게 될 것으로 예상된다.

무선 인터넷 서비스를 제공하기 위한 WAP 방식에서도 무선 데이터 통신을 위해 스마트 카드에 탑재될 모듈의 규격을 WIM(WAP Identity Module)으로 제안하고 있다. 이렇듯 사용자 보안 모듈을 사용하여 무선 인터넷 서비스를 제공하는 것은 유선 인터넷 환경에서 제공하는 보안기능과 사용자 인증, 접근 제어 등의 서비스를 무선에서도 동일하게 제공하

기 위한 것으로 볼 수 있으며, 사용자의 편리성을 고려하여 쉽게 사용할 수 있도록 하기 위한 것이다.

위에서 언급한 바와 같이 사용자의 편리성을 장점으로 하여 개인 정보의 안전한 저장, 간단한 사용법 등을 바탕으로 하여 사용자 보안 모듈의 사용과 발전을 앞으로 더욱 급진전 할 것으로 예상된다. 또한 컴퓨터 사용의 일반화와 전자상거래의 발전과 함께 스마트 카드의 기능과 USB 기반 방식의 기능을 함께 사용할 수 있고, 단순한 정보의 저장뿐만 아니라, 무선 PKI 환경에서 효율적으로 사용할 수 있는 사용자 보안 모듈의 개발이 더욱 활발히 진행될 것으로 기대된다.

V. 결 론

무선 인터넷 서비스와 단말기의 발전으로 무선 인터넷을 이용하는 사용자가 점차적으로 증가하고 있다. 무선 인터넷 환경에서의 안전한 서비스를 제공하기 위해서는 유선 인터넷 환경과 같은 사용자 정보의 보안 서비스가 요구된다. 그러므로, 유선 인터넷 환경에서와 같이 무선 인터넷 환경에서도 PKI에 기반한 암호 시스템의 응용이 필수적으로 요구된다. 하지만 무선 인터넷 환경은 유선 인터넷 환경과 달리 휴대용 단말기의 제한적인 성능과 무선이라는 환경으로 인해 여러 가지 제약사항이 따른다. 따라서, 본 연구에서는 무선 인터넷 환경이 갖는 제약사항을 극복하고 안전한 무선 인터넷 서비스를 제공할 수 있도록, 무선 PKI 환경에서 사용자 보안 모듈의 활용 방안에 대해 연구가 보다 활발히 이루어져야 할 것이다.

본 고에서는 먼저, 안전한 무선 인터넷 서비스를 위한 무선 PKI 기술의 개요에 대해 알아보고, 무선 인터넷 환경이 갖는 여러 제약사항을 극복하기 위해 무선 PKI 환경에 사용할 수 있는 사용자 보안 모듈에 대해 기술하였다. 사용자 보안 모듈은 크게 스마트 카드 기반 방식과 USB 기반 방식으로 구분할 수 있으며, 각 방식에 대한 관련 표준 규격 및 최근 제품 개발 동향에 대해 설명하였으며, 마지막으로 사용자 보안 모듈의 향후 전망에 대하여 설명하였다.

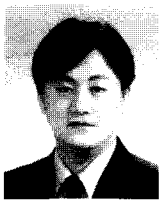
본 고의 연구 내용은 안전한 무선 PKI 서비스의 활성화와 더불어 무선 인터넷 뱅킹 서비스, 주식 거래, 온라인 쇼핑 등 무선 인터넷을 이용한 전자 상거래의 활성화에 기여할 것으로 기대된다.

참고문헌

[1] "디렉토리시스템 인증 프레임워크 표준", TTAS. IT-X509/R2, 한국정보통신기술협회, 2000.7
[2] "전자 서명 인증서 프로파일 표준", TTAS. KO-12.0012, 한국정보통신기술협회, 2000. 12
[3] "전자 서명 인증서 효력정지 및 폐지 목록 프로파일 표준", TTAS.KO-12.0013, 한국정보통신기술협회, 2001.6
[4] 권태경, "전자서명 활용을 위한 virtual smart-card 기술", 2001.9
[5] "Wireless PKI", 한국정보보호진흥원, 2001.5
[6] "Additional interindustry commands and security attributes", ISO/IEC 7816-9 ISO/IEC, 2000
[7] "Comparing Bus Solutions", Texas Inc. 2000.3
[8] "Developing Smart Card-Based Application using JavaCard", SunMicrosystem, 1998.9
[9] "Dimensions and location of coupling areas", ISO/IEC 10536-2, ISO/IEC, 1995
[10] "Dimensions and location of the contacts", ISO/IEC 7816-2, ISO/IEC, 1999
[11] "Electronic signals and answer to reset for synchronous cards", ISO/IEC 7816-10, ISO/ IEC, 1999
[12] "Electronic signals and reset procedures", ISO/IEC 10536-3, ISO/IEC, 1996
[13] "Electronic signals and transmission protocols", ISO/IEC 7816-3, ISO/IEC, 1997
[14] "EMV 2000 Spec. Book 1", EMVCo
[15] "EMV 2000 Spec. Book 2", EMVCo
[16] "EMV 2000 Spec. Book 3", EMVCo
[17] "EMV 2000 Spec. Book 4", EMVCo
[18] "Errata for USB 2.0 Revision", USB-IF, 2000.12
[19] "IEEE Std 1394-1995", IEEE , 1995.12
[20] "IEEE Std 1394a-2000", IEEE , 2000.3
[21] "Initialization & anticollision", ISO/IEC 14443-3 ISO/IEC, 1999
[22] "Interindustry commands for interchange", ISO/IEC 7816-4 ISO/IEC, 1997, 1995

[23] "Interindustry data elements", ISO/IEC 7816-6 ISO/IEC, 2000, 1996
[24] "Interindustry commands for structured card query language", ISO/IEC 7816-7 ISO/IEC, 1999
[25] "Numbering system and registration procedure for application identifiers", ISO/IEC 7816-5 ISO/IEC, 1994
[26] "On-The-Go Supplement to the USB 2.0 Specification", USB IF , 2001.12
[27] "Opencard Framework 1.0 White paper", opencard.org, 1998.5
[28] "OTG243", Transdimension Inc., 2001.3
[29] "P1394a Draft 5.0", IEEE , 2000.2
[30] "P139 4.1 Draft 0.16", IEEE , 2001.3
[31] "PC/SC Techinical Overview", PC/SC work group, 1996.12
[32] "PC/SC white paper :introducing the PC/SC specifications 2.0", PC/SC work group, 1999.11
[33] "PC/SC workshop Specifications 1.0", PC/SC work group, 1996.12
[34] "Physical characteristics", ISO/IEC 7816-1, ISO/IEC ,1998
[35] "Physical characteristics", ISO/IEC 14443-1 ISO/IEC, draft
[36] "Physical characteristics", ISO/IEC 10536-1 ISO/IEC, 2000
[37] "Physical characteristics", ISO/IEC 15693-1 ISO/IEC, draft
[38] "Radio frequency power and signal interface", ISO/IEC 14443-2, ISO/IEC, 1999
[39] "Security related interindustry commands", ISO/IEC 7816-8, ISO/IEC, 1999
[40] Dirk Husemann, "Standards in the smart card world", 2001
[41] "TBD Transmission Protocols", ISO/IEC 15693-3 ISO/IEC, 2000
[42] "Transmission protocols", ISO/IEC 14443-4 ISO/IEC, 2000
[43] "USB 2.0 Specification ENC", USB-IF, 2000.10
[44] "USB 2.0 Specification Revision", USB-IF, 2000.4
[45] "USB On-The-Go : A Totorial", Philips Semiconductors , 2002.1

〈著者紹介〉



곽 진 (Jin Kwak)
학생회원
2000년 8월 : 성균관대학교 바이오메카트로닉스공학과 공학사
2001년 3월~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 석사과정

이 승 우 (Seung-Woo Lee)
학생회원
2001년 2월 : 강남대학교 전자계산학과 졸업(공학사)
2001년 3월~현재 : 성균관대학교 정보통신공학부 석사 과정

오 수 현 (Soo-hyun Oh)
학생회원
1998년 2월 : 성균관대학교 정보공학과 졸업(공학사)
2000년 2월 : 성균관대학교 대학원 전기전자 및 컴퓨터 공학부 졸업(공학석사)
2000년 3월~현재 : 성균관대학교 정보통신공학부 박사 과정

원 동 호 (Dong-Ho Won)
종신회원
성균관대학교 전자공학과 (학사, 석사, 박사)
한국전자통신연구소 전임 연구원
일본 동경공대 객원연구원
성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 국무총리실 정보화추진위원회 자문위원
한국정보보호학회 이사, 부회장, 수석부회장
현재 : 성균관대학교 정보통신공학부 교수
성균관대학교 연구지원처장
한국정보보호학회 회장
정통부지정 정보보호인증기술연구센터 센터장