제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

사용자 보안 모듈의 최근 기술 동향에 관한 연구

한종수*, 김근옥*, 서인석**, 정혜련**, 원동호*
*성균관대학교 정보통신공학부
**국가보안기술연구소
e-mail : : jshan@dosan.skku.ac.kr

A Study on The Latest Technologies Trend of User Security Module

Jong-Su Han*, Keun-Ok Kim*, In-Seok, Seo**, Hye-Ryoun Chung**, Dongho Won*
*School of Information & Communications Engineering, Sungkyunkwan University
**National Security Research Institue

요 약

최근 인터넷을 이용한 전자상거래가 활성화되면서 PKI 의 응용이 확대되고 있다. 이에 PKI 에서 활용되는 중요 개인 정보를 보다 안전하게 저장하고 휴대의 편리성을 보장하는 사용자 보안 모듈의 필요성이 요구되고 있다. 이에 본 논문은 대표적인 사용자 보안 모듈인 스마트 카드와 USB 기반 방식을 분석하고 현재 상용화되고 있는 제품 동향에 대해 분석하고자 한다.

1. 서론

정보통신 기술의 발달과 인터넷 사용자의 증가로 인해 인터넷을 이용한 뱅킹 서비스, 주식 거래, 온라인 쇼핑 등의 전자상거래가 급속히 발전하고 있다. 하지만 이러한 온라인상의 전자상거래는 비접촉, 비대면으로 이루어지기 때문에 거래 당사자간에 상대방의 신원과 거래의사의 정당성 등을 확인하기 어렵고, 타인으로 위장하여 문서나 내용을 변경하거나 다른 목적으로 사용할 수 있다는 문제점을 내포하고 있다. 이러한 문제점을 해결하고 전자상거래의 활성화 및 안전한 네트워크의 구현을 위해 많은 응용 분야에서 상대방의 신원을 확인하고 내용의 무결성을 확인할 수 있는 공개키 기반구조 (PKI : Public Key Infrastructure)의 활용이 필수요소로 자리잡고 있다. PKI 는 개인의 비밀키나 인증서를 통해 보안 서비스가 이루어지므로 불법 변조 방지 특성을 갖으면서 암호 알고리즘, 사용자의 키, 인증서 및 관련정보 등 중요 개인 정보를 보다 안전한 제 3 의 장소에 저장하여 휴대성, 안전성, 편리성 등을 모두 보장할 수 있는 별도의 사용자 보안 모듈의 필요성이 요구되고 있다. 본 논문에서는 대표적인 보안 모듈인 스마트 카드와 USB 기반의 보안 모듈에 대해 최근 기술 동향에 대해 알아보고자 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 대표적인 보안 모듈인 스마트 카드와 USB 에 대한 개요와 특징에 대해 알아 보고 3 장에서는 각 보안 모듈에 대한 관련 기술 표준에 대해 분석하고자 한다. 4 장에서는 현재 상용화 되고 있는 제품들을 각 표준에 따라 분류하여 알아보고 5 장에서는 결론 및 향후 연구 과제에 대해 설명한다.

2. 보안 모듈

무선 PKI 에 적용할 수 있는 보안 모듈은 크게 두 가지 방식으로 나눌 수 있는데, 하나는 스마트 카드 방식이고 다른 하나는 USB 기반 방식이다.

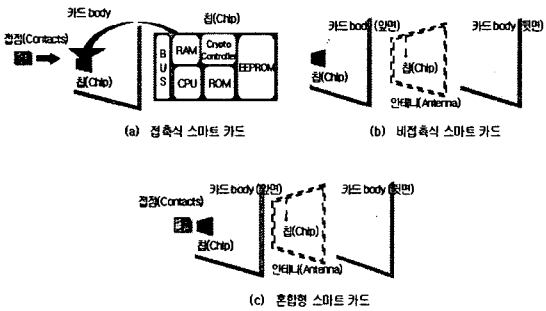
2.1 스마트 카드

스마트 카드는 데이터를 저장할 수 있는 마이크로 칩이 내장되어 있기 때문에, 암호 알고리즘을 제공하여 안전성과 신뢰성을 보장하며 전자서명, 인증, 암호화, 데이터 접근 통제 등의 기능을 제공한다는 장점으로 인해 현재 보안 모듈로 주로 사용되고 있다. 스마트 카드의 종류는 인터페이스 방식에 따른 분류와 마이크로 프로세서의 포함여부에 따른 분류, 진화단계에 따른 분류로 구별할 수 있으며 그 내용은 다음 [표 1] 과 같다[1].

[표 1] 스마트 카드의 종류

구분	분류
인터페이스	접촉식, 비접촉식, 혼합형(하이브리드, 콤비)
마이크로 프로세서	메모리, 마이크로 프로세서
진화단계	메모리, 단기능, 다기능, 네트워크, 컴퓨터

스마트 카드의 구성 요소는 CPU (Central Processing Unit)와 ROM (Read Only Memory), RAM (Random Access Memory) 그리고 데이터 저장을 위한 EEPROM (Electrically Erasable and Programable ROM) 등으로 구성되어 있다. 다음 [그림 1]은 스마트 카드의 인터페이스의 방식에 따른 분류의 구성을 나타낸 것이다[1].



[그림 1] 스마트 카드 구성

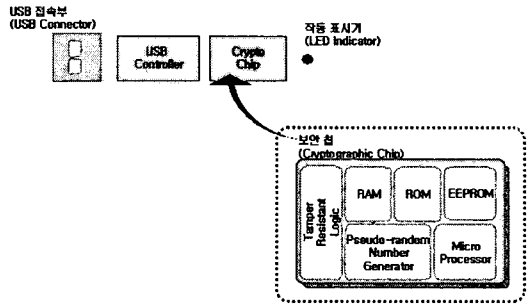
2.2 USB 기반 방식

USB(Universal Serial Bus)는 PC 를 열지 않고 각각의 주변장치를 쉽게 연결할 수 있도록 하는 장치를 말한다. USB 토큰 방식은 일반적으로 허브를 통해 컴퓨터 외부에서 쉽게 주변장치를 연결할 수 있고, PnP(Plug and Play) 기능과 전원이 켜진 상태에서도 장치를 설치· 제거할 수 있는 hot-plugging 기능을 지원하고 있다. 이러한 특징은 스마트 카드 방식이 보안 토큰에서 필요로 했던 별도의 카드 판독기의 필요성을 제거하였다. 또한 메모리 기반의 기존 제품과 달리 자체 프로세싱 기능을 갖춰 인증서 저장 뿐 아니라 자체에서 PKI 기능을 수행해 외부로 비밀키의 정보 유출을 차단할 수 있는 서비스를 제공 중에 있다. USB 기반 방식의 종류는 USB 드라이브, 토큰, 스마트 키로 구분할 수 있으며 다음 [표 2]는 이들의 특징을 정리한 것이다[2].

[표 2] USB 기반 방식의 종류

분류	특징
USB 드라이브	플래쉬 메모리를 통한 휴대용 데이터 저장장치
USB 토큰	EEPROM를 통한 휴대용 개인 보안 정보 저장장치
USB 스마트 키	스마트 카드+USB 방식의 휴대용 저장장치

USB 기반의 휴대용 보안 장치의 구성을 살펴보면, 외부 기기와 휴대용 보안장치를 연결할 수 있는 USB 접속부(USB Connector), 휴대용 보안 장치가 작동하고 있음을 알려주는 작동 표시기(LED Indicator), 그리고 USB 컨트롤러(USB Controller)와 보안 컨트롤러 (Cryptographic Chip)으로 구성되어 있다. 다음 [그림 2]는 USB 기반 방식 휴대용 저장장치의 구조를 나타낸 것이다[2].



[그림 2] USB 기반 방식 휴대용 저장장치 구조

3. 관련 기술 표준 동향

3.1 스마트 카드

스마트 카드 관련 표준은 스마트 카드의 규격과 물리적인 성질과 스마트 카드 판독기간의 통신 방법 등에 대해서 기술한 ISO/IEC 표준과, 세계적인 3 대 신용카드 업체들이 공동으로 개발한 차세대 IC 카드 기반의 신용· 직불카드 규격인 EMV 표준 규격이 있다. 또한 PC 환경 하에서 IC 카드에 관련된 표준을 정의한 PC/SC 규격과 소프트웨어의 발달을 위한 높은 레벨의 응용 프로그램 인터페이스와 카드 제조사들에게 제공되는 하드웨어 인터페이스의 표준을 제시함으로써 상호 운용성을 이루도록 한 OCF 명세서가 있다.

▣ ISO/IEC 표준

International Organization for Standardization /International Electrotechnical Commission 에서 만든 표준으로 ISO/IEC 7816, 10536, 14443, 15693 등이 스마트 카드의 규격부터 물리적인 성질과 전원을 얻을 때 사용하는 접점이나, 안테나, 스마트 카드와 스마트 카드 판독기간의 명령 형식에 대해서 자세히 기술하고 있다[3][4][5][6].

ISO/IEC 7816 은 접촉식 스마트 카드에 대한 국제 표준으로 ISO 7810 에서 정의한 ID 카드에 IC 칩을 추가한 형태로 스마트 카드 판독기와 직접 통신이 가능한 접점에 대한 설명이 되어 있는 표준이다[3].

ISO/IEC 10536 은 밀착형 스마트 카드에 대한 국제 표준으로 밀착형 비 접촉식 스마트 카드에 대한 설명과 이에 이용되는 케플링 에어리어의 위치 및 크기 등의 설명이 되어 있는 표준이다[4].

ISO/IEC 14443 은 리모트 형의 근접형 카드에 대한 국제 표준을 정의하고 있고 ISO/IEC 15693 은 리모트 형의 근방형 카드에 대한 국제 표준을 정의하고 있으며 이 두 문서는 근접형 비접촉식 스마트 카드에 대한 설명과 무선 주파수와 신호 인터페이스에 대한 설명이 되어 있다[5][6].

▣ EMV 표준 규격

세계적인 신용카드 업체인 Europay International Service Association, MasterCard International Inc, Visa International Service Association 이 공동으로 개발한 차세대 IC 카드 기반의 신용· 직불카드 기술 규격이다.

EMV 표준 규격은 지불 시스템을 위한 IC 카드 스펙에서는 스마트 카드와 장치들의 동작 및 상호 운용이 가능하기 위해 필요한 최소한의 기능을 정의하고 있으며, 지불 시스템을 위한 IC 카드 응용 스펙에서는 지불 시스템 트랜잭션을 수행하기 위해 필수적인 프로토콜을 정의하고 있다. 지불 시스템을 위한 IC 카드 단말기 스펙에서는 금융 서비스 시스템에서 인터페이스 장치가 스마트카드를 지원하기 위한 특정 요구 조건들을 정의하고 있다[7].

▣ PC/SC 규격

Microsoft, Hewlett-Packard, Simens Nixdorf 등이 개발한 규격으로 PC 환경에서 효율적으로 IC 카드 기술을 사용할 수 있도록 하였다. PC/SC 규격은 스마트 카드들과 판독기 간에 호환되는 인터페이스 요구사항, PC로 연결된 인터페이스 장치들의 요구사항, 인터페이스 장치 디자인 시 고려사항과 참고 디자인 정보, IC 카드 자원 관리자 정의, IC 카드 서비스 제공자 인터페이스 정의, 응용 도메인과 개발자 디자인 시 고려사항, IC 카드 보안과 프라이버시 장치들을 위한 주의사항 등으로 나누어서 설명하고 있다[8].

▣ OCF 표준 규격

3-International, Bull, Gemplus, First Access 등이 개발한 명세서로 높은 레벨의 응용 프로그램 인터페이스와 카드 제조사들에게 제공되는 하드웨어 인터페이스의 표준을 제시함으로써 상호 운용이 이루어질 수 있게 한 규격이다. ISO 7816 과 EMV, PKCS #11 등을 참조하여 설계한 OCF 표준 규격은 업체간의 표준화를 통해 다양한 솔루션의 호환성을 보장할 수 있다는 장점을 가지고 있다[9].

3.2 USB 기반 방식

USB 기반의 관련 기술 표준은 하나의 호스트와 여러 개의 주변장치들에 연결을 지원하고 이에 대한 전기적인 전송 규격과 프로토콜 같은 하드웨어와 소프트웨어 기술이 통합된 USB 1.1 과 USB 1.1 를 개정, 보완하여 USB 1.1 에서 사용하던 케이블과 커넥터를 그대로 이용하면서 최고 480Mbps(bit per second)를 지원할 수 있는 USB 2.0 이 있다. 또한 기존의 호스트 기반의 USB 2.0 과는 달리 USB 주변 장치 간의 단독 통신을 지원할 수 있는 USB OTG(On-The-Go)와 IEEE(The Institute of Electrical and Electronic Engineers, 국제전기전자기술자 협회)에서 지정한 1394 번째 표준인 IEEE 1394 가 있다[2][10][11][12].

▣ USB 1.1

1996 년 1 월 Intel, Compaq, NEC 및 Microsoft 등에 의해 USB 1.0 규격이 제정되었고, 이후 1998 년 전기적인 전송 규격과 프로토콜 같은 하드웨어와 소프트웨어 기술이 통합된 USB 1.1 규격이 발표되어 실제 실용화를 위한 규격으로 정의되게 된다. USB 1.1 은 캐이블이나 커넥터에 대한 단일 모델을 제공하고, Low speed 와 Full speed 두 가지 모드로 작동하며, Full speed 일 때 최고 12Mbps 까지 지원하게 된다. USB 1.1 은 동기식, 비동기식의 두 가지 전송 모드와 프로토콜 계층, 물리적· 전기적 구조 등에 대한 내용을 정의하고 있다[2][10].

▣ USB 2.0

USB 2.0 은 고속의 인터페이스를 위해서 USB 1.1 을 개정, 보완하여 2000 년 4 월 발표되었다. USB 2.0 은 기존의 USB 1.1 의 특징들을 대부분 그대로 유지하면서 최고 480Mbps 까지의 성능을 낼 수 있다. USB 2.0 에서는 기존의 USB 1.1 에서 사용하던 프레임을 더 세밀하게 나눈 Micro Frame 이란 개념을 도입해서 좀 더 많은 양의 패킷을 자주 전송할 수 있도록 함으로써 대역폭을 효율적으로 사용할 수 있게 하였다. USB 2.0 은 USB 의 개략적인 구조와 데이터 흐름, 물리적· 전기적 구조, 프로토콜 계층, 허브 등에 대한 내용을 상세히 설명하고 있다[2][10].

▣ USB OTG

USB 규격을 제정하는 USB-IF(The Universal Serial Bus Implementers Forums)에서 USB 2.0 규격에 좀 더 이점을 부여하자는 데 착안하여 PC 에 연결되지 않은 USB 규격인 USB OTG 규격을 발표하였다. 기존의 USB 는 PC 와의 연결을 전제로 설계된 마스터-슬레이브(master-slave)의 구조를 가지고 있는 반면에 USB OTG 의 경우 PDA, 휴대폰, 휴대용 MP3 플레이어 등의 주변 장치 간의 통신이 가능하도록 하고 있다. 이에 USB OTG 표준에서는 주변 장치 간의 통신을 지원할 수 있는 Dual-role 디바이스의 개념과 SRP(Session Request Protocol), HNP(Host Negotiation Protocol)등을 정의하고 있다[11].

▣ IEEE 1394

IEEE 1394 는 "Firewire", "1394", "i.링크"라고 알려진 직렬 버스 구조를 지칭하는 규약으로 IEEE 에 의해 지정된 표준이다. 기존 USB 가 마스터-슬레이브(master-slave) 구조를 가지고 있는 반면 IEEE 1394 는 단대단(peer to peer) 구조를 가지고 있다는 특징을 가지고 있다. 또한 쌍방향 통신을 지원하며 PnP 와 Hot-plugging 서비스 지원이 가능하다. IEEE 1394 표준 문서는 구조와 프로토콜의 각 계층에 대한 기술적인 설명과 각 계층에서 수행하고 있는 서비스에 대한 내용이 표준문서에 포함되어 있다[12].

4. 제품 동향

4.1 스마트 카드

ISO/IEC 7816 표준의 제품으로는 일본 DNP 사의 RISONA CARDS 가 있으며, SchlumbergerSema 와 Easyflex City 와 Gemplus 의 MPCOS Pro 는 ISO/IEC 7816 과 ISO/IEC 14443 을 따르는 혼합형의 콤비 카드이다.

현재까지 EMV 인증을 받은 국내 기업은 한국정보통신(주), 사이버넷, 월마니어(주) 등이 단말기 인증을 받았으며, 삼성전자가 스마트 카드에 대한 EMV 인증을 획득하였다.

PC/SC 규격으로 제품을 만든 기업으로는 Nexsmart, SchlumbergetSema, Advanced Card system 등이 있고 국내 기업으로는 재익정보통신(주)이 있다.

OCF 규격을 지원하는 회사에는 Linux, Utimaco, Gemplus, IBM 등이 있다. Gemplus 사는 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. 다음 [표 3] 스마트 카드의 표준 문서에 따른 제품 동향을 나타낸 표이다.

[표 3] 스마트 카드 제품동향

표준	회사	제품명	그림	특징
ISO /IEC	SchlumbergerSema	Easyflex		• ISO/IEC 7816, ISO/IEC 14443 규격을 따르는 혼합 방식의 카드 • 3DES 암호 프로세서 사용
	DNP	RISONA CARDS		• ISO/IEC 7816을 따르는 카드 • DES와 3DES를 준용 • 상호인증이 가능한 스마트 카드
EMV	한국정보통신㈜	EMV 단말기		• 기존 자기 카드와 IC카드 공용가기 • 카드 삽입용 PIN PAD 부착으로 기존 자원의 재활용 가능
PC /SC	재익정보통신㈜	CSR-140		• PC/SC, Mondex, V-cash 호환 • 인터넷 뱅킹, 전자상거래, 전자서명 등에 사용
OCF	젬 플러스	JAVA 카드		• OCF 규격 지원 • Java card 2.1.1 지원 • 인터넷 뱅킹, 전자상거래 등에 사용

4.2 USB 기반방식

USB 1.1 과 2.0 은 키보드, 마우스, 휴대용 저장장치 등 다양한 주변 기기에 적용되어 개발되고 있다.

[표 4] USB 기반 방식의 제품 동향

표준	회사	제품명	그림	특징
USB	RAINBOW	iKey2000		• USB 1.1, 2.0 지원 • 토큰 내부에서 RSA 키 생성가능 • PKCS #11, MSCAPI 지원
	SecureCenter	SecureKey		• 사용자 비밀번호와 SecureKey를 사용하여 two factor 인증 만족 • USB 시리즈 A 커넥터 사용
	Securepia	MiKey		• 사용자 인증, 웹 로그인, 결제 및 저장장치로 사용
IEEE 1394	SONY	캠코더		• IEEE 1394 전체규격을 지원 • DV(Digital Video), DV Deck • 홈 네트워크 구현
	세로텍	외장하드 케이스		• 외장형 포토블 HDD 케이스 • IEEE 1394 인터페이스 • 최대 400Mbps 지원

그 중 휴대용 저장 장치는 RAINBOW, SecureCenter, Securepia, SafeDigm 등에서 개발되고 있다.

IEEE 1394 규격의 제품 현황을 살펴보면 칩 제조업체와 운용체계 개발회사, PC 주변장치 제조사들을 중심으로 접근이 이뤄지고 있다. 대표적인 회사로는 Sony, Fujitsu, Philips, Lucent 등을 꼽을 수 있다. 위의 [표 4]는 USB 기반 방식의 표준 문서에 따른 제품 동향을 나타낸 표이다.

5. 결론 및 향후 연구과제

앞서 살펴본 제품 동향에서와 같이 사용자 보안 모듈은 아직 유선 PKI 기반의 제품에서만 활용되고 있다. 하지만 앞으로 무선 인터넷의 활성화와 이동통신 서비스의 발전으로 무선 PKI 환경에서도 보안 모듈의 필요성이 예상된다. 더욱이 무선 인터넷 환경은 유선 인터넷 환경에 비해 전자서명의 생성·검증이나 인증서 검증과 같이 많은 시간이 소요되는 공개키 암호 관련 연산을 수행할 수 있는 단말기의 연산 및 저장 능력이 부족하고 단말기의 분실 시 인증서나 사용자의 비밀키와 같은 중요 정보를 분실할 우려도 있어 안전성 면에서 문제점이 있다. 이러한 무선 인터넷 환경이 갖는 제약조건과 무선 단말기의 단점을 보완하기 위해 보안 모듈의 사용이 확대될 것이다. 현재까지는 단순한 메모리 기능만을 수행하는 것과 단순 연산 능력이 있는 프로세서를 포함한 스마트 카드와 USB 기반 모듈의 사용이 대부분이다. 하지만, 앞으로 무선 PKI 환경에서 보안 모듈이 사용되어 안전한 보안 서비스를 수행하기 위해서는 더욱 향상된 연산 기능을 갖는 프로세서를 탑재한 강력한 기능을 갖는 보안 모듈의 연구 및 제품 개발이 활발히 이루어져야 할 것이다. 이에 무선 PKI 환경에 적합한 보안 모듈의 요구사항 분석을 통해 안전하고 효율적인 보안 모듈에 대한 연구가 계속되어야 하겠다.

참고문헌

[1] 강유성 외 2 인, "무선 인터넷 정보보호용 스마트 카드 기술 동향", 2000.6

[2] http://www.camcorder.co.kr/bjng/usb/

[3] ISO/IEC, "ISO/IEC 7816, Identification cards Integrated circuit(s) cards with contacts", 2000.6

[4] ISO/IEC "ISO/IEC 10536, Identification cards Contactless integrated circuit(s) cards", 2000. 4

[5] ISO/IEC, "ISO/IEC 14443, Identification cards Contactless integrated circuit(s) cards", 2000. 3

[6] ISO/IEC "ISO/IEC 15693, Identification cards Contactless integrated circuit(s) cards", 2000.3

[7] EMVCo , "EMV 2000 Spec. Book 1· 2· 3· 4"

[8] PC/SC work group, "PC/SC workshop Specifications 1.0", 1996.12

[9] opencard.org, "OpenCard Framework second edition", 1998.10

[10] USB-IF , "USB 2.0 Specification ENC", 2000.10

[11] USB IF, "On-The-Go Supplement to the USB 2.0 Specification" , 2001.12

[12] IEEE , "IEEE Std 1394-1995", 1995.12