제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

PKI기반의 스마트카드를 이용한 무선 인터넷 보안

이경효*, 고혜선*, 오병균**
목포대학교 정보보호기술전공
e-mail: mediakh,demon@hanmail.net, obk@mokpo.ac.kr

Wireless Internet Security using Smart Card in Public Key Infrastructure

Kyoung-Hyo Lee*, Hyeo-Seon Go*, Byeong-Kyun Oh**
Department of information and protection Engineering,
Mokpo Nationnal University

요약

오늘날 인터넷 사용자의 급속한 증가와 데이터 중심의 무선 통신 기술의 빠른 성장으로, 중요한 정보를 비밀리에 전달하고자하는 보안성의 요구가 증가하고 있다. 무선인터넷은 데이터 공개성을 갖는 무선 매체를 사용한다는 점과 단말 혹은 사용자가 이동한다는 고유의 특성으로 인하여 제한된 CPU와 메모리 때문에 기존의 유선 PKI(Public Key Infrastructure)체계를 그대로 적용할 수 없는 기존 인터넷 보안 체계에 비해서 훨씬 복잡한 구조가 요구된다.[1] 본 논문에서는 이동하는 단말의 인증을 위한 효율적이고 유용한 식별자 적용기술인 스마트카드를 이용한 무선 인터넷 보안을 제공하기 위해 Mobile PKI 기반의 보안구조를 제안하여 보안을 강화하고자한다.

1. 서론

개인의 정보통신에 대한 수요가 증가하면서 무선 인터넷 및 Mobile commerce의 활성화 등으로 이동통신 단말기를 이용한 무선 시스템에서 다양한 서비스를 제공하기 위한 연구가 활발히 진행중이다. 이러한 Mobile commerce의 걸림돌은 기존 유선 인터넷과 이에 따른 애플리케이션 및 컨텐츠 측면에서 무선 상의 보안 서비스를 제공하는 것이 어렵고, 각종 암호 기술들이 단말기에서 완벽하게 수행되기 위해 필요한 CPU 및 메모리, 입/출력장치 등의 성능이 뒤떨어지기 때문에 효율적인 보안 서비스의 제공이 어렵다는 점이다. 이러한 단말환경의 열악한 환경을 극복하기 위해 무선 인터넷을 통한 Mobile commerce의 활성화와 보안을 위해 Mobile PKI기술을 통해 무선 서비스 이용자들이 공인 인증기관의 인증 서비스를 안전하게 제공받게 할 수 있어야한다. Mobile PKI기술은무선 인터넷환경에서 키관리 문제를 해결하고 무선 인터넷 접속기술로 사용되고 있는 WAP(Wireless Application Protocol)와 MME(Microsoft Mobilw Explorer)에 모두 적용할 수 있고 유선 PKI와 상호 연동성도 고려해서 개발되고있다. 본 논문에서는 스마트카드 기술관련 표준화 무선인터넷에서 스마트카드의 활용을 알아보고 스마트카드를 이용한 무선인터넷 환경에서 키관리 문제를 해결하고 다양한 보안서비스

를 제공하기 위하여 Mobile PKI기반의 새로운 보안을 위한 연구를 하였다.

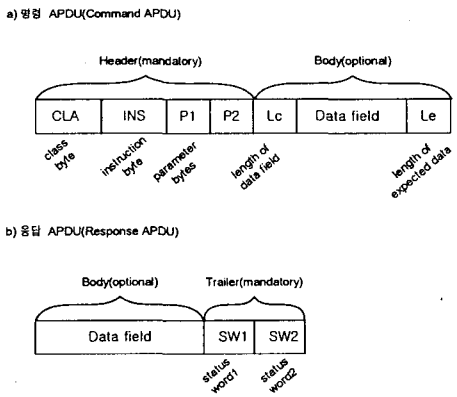
2. 관련연구

2.1 스마트카드와 무선인터넷 기술동향

신용카드와 같은 크기의 스마트카드는 고정고객 우대카드, 현금 차감카드, 학생신분증, GMS전화 등 광범위한 분야에 응용된다. 스마트카드는 비밀키 등과 같은 개인 비밀 정보의 저장장소로써는 최상의 조건을 가지고 있으며, 복잡한 암호 연산을 하나의 칩으로 구현된 암호 연산가속기의 장착으로 강력한 암호 연산 능력의 제공이 가능하고 이동성도 뛰어난다. 스마트카드에 전원이 공급되면 자신의 서비스를 제공할 준비가 되었음을 알리고 ATR(Answer to Reset)로 응답하고 전송프로토콜을 결정하게 된다. 또한 ART 송수신 이후에는 PPS(Protocol and Parameter Seletion) 절차를 통하여 스마트카드에서 응답한 전송프로토콜이 아닌 새로운 전송 프로토콜을 이용할 수도 있다.

무선 단말기와 스마트카드사이의 일반적인 동작인 명령-응답의 형태를 위한 송수신 데이터 단위는 APDU이며 이는 단말기에 의한 명령에 대한 카드의 응답으로 구분된다.

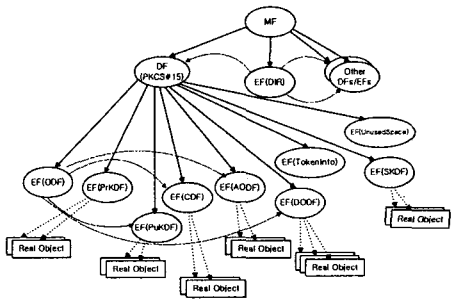
[그림1]은 이러한 APDU의 구성을 나타낸다.



[그림1]명령 및 응답 APDU형식

IP(Internet Protocol)기반의 휴대전화의 디지털화와 PHS의 출현에 의해 데이터 통신의 가능성이 커졌고 모바일 컴퓨팅개념의 등장으로 무선통신과 휴대 정보터널의 유기적인 결합이 더욱 강화되고 있다. 1999년 휴대전화로 인터넷을 통한 web엑세스, 전자메일, 온라인 상거래등이 가능한 서비스가 시작되었고, 2000년 IMT2000 통신에의해, 고속화와 멀티미디어화, 인터넷을 통한 서비스의 확산과 고도화를 지향하는 새로운 발전이 예견되고있다.[2]

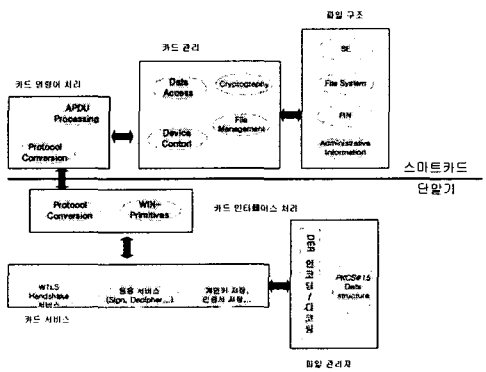
2001년에는 TCP/IP를 무선망에서 수용하도록 하는 WAP 2.0을 발표한 바 있고 WAP 2.0 규격에서는 기존의 WAP 1.X 규격을 위한 역행 호환성(backward compatibility)을 제공함은 물론 무선환경에 적합한 보안 서비스를 위한 TLS(Transport Layer Security)와 단말간 호환성을 제공하기위한 보안 토큰(cryptographic token) 규격을 만족한다.[2]



[그림2] PKCS #15내의 파일구조[5]

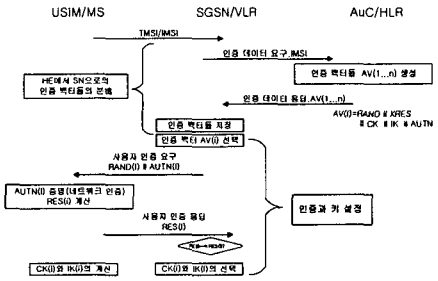
PKCS #15를 비롯한 PKCS 규격은 공개키를 사용하는 보안토큰의 정보 저장과 액세스에 대한 일관된 규칙을 적용함으로써 국제적인 호환성을 제공함은 물론, 하나의 스마트카드에 여러 응용을 탑재할 수 있는 다중 응용 카드 구현에 대한 지원과 기능 확장성을 제공할 수 있으므로 추후 무선 인터넷 단말에서는 반드시 만족하여야 할 것이다.[5][7]

현재로서는 무선 인터넷 보안을 제공할 수 있는 스마트 카드는 유럽에서는 3세대 이동통신에서의 대칭키 기반의 USIM과 인증서를 기반으로 하는 WAP포럼에서의 WIM으로 대별된다. 이에 대한 기술동향은 다음과 같다.



[그림3] WAP Identity Module을 이용한 정보보호 서비스 제공방식[8]

무선 인터넷 접속 프로토콜의 사실상 국제 표준이라 할 수 있는 WAP 프로토콜에서 사용하는 무선 인증 모듈인 WIM은 스마트카드 규격인 ISO/IEC 7816과 PKCS#15를 만족함은 물론, 전송계층 보안을 위한 WTLS 핸드쉐이킹과 응용계층에서의 전자서명을 지원하는 역할을 수행하며, 사용자 비밀키와 인증서 및 개인 비밀번호 등과 같은 중요정보를 저장하고 랜덤수의 생성 및 마스터 시크릿(master secret)을 계산하는 동작을 포함하는 ECC(Elliptic Curve Cryptography) 또는 RSA 방식을 수행한다.

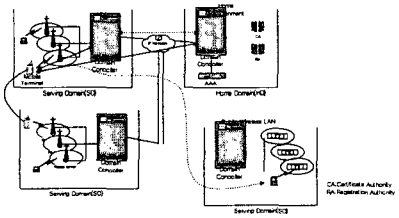


[그림4] Universal Subscriber Identity Modul에서의 인증 및 키 일치과정(AKA)

3.Mobile PKI(Public Key Infrastructure)시스템

최근 인터넷보안의 가장 중요한 이슈가 되고있는 것 중 하나가 PKI이다. PKI는 전자상거래에서 필수적인 전자서명을 비롯하여 공개키를 사용하는 모든 보안 문제에 대한 신뢰성있는 해답을 제시하기 위한 보안 서비스의 전반적 인프라 개념이라고 할 수있다. 인터넷과 같이 안전이 보장되지 않은 공중망에서 신뢰할 수 있는 기관에서 부여된 한 쌍의 공개키와 개인키를 사용하여 암호화와 전자서명 등의 암호화 알고리즘을 제공함으로써 사용자들에게 안전한 보안 환경을 제공하는 것이 공개키 기반구조이다. 또한 안전한 공개키 기반구조를 제공하기 위하여는 사용되는 키(공개키)의 생성과 분배, 저장, 폐기 등의 키관리와 공개키의 위조나 변조를 방지하기위한 인증서(Certification)관리 체계도 뒤따라야한다.[4]

이 모델은 차세대 이동 통신 시스템 구조를 도메인 구조로 일반화한 형태이다. 도메인은 MT에 직접적인 서비스를 제공해주는 SD과 MT의 인증 정보와 과금 등에 대한 관리를 하는 HD으로 나누어진다. SD은 다수의 노드로 구성되는데, 간략화를 위하여 무선 인터페이스를 제공하는 AP를 제외하고 나머지의 SD 핵심 노드들을 통합하여 DC라고 칭한다. 따라서 DC는 MT에 대한 위치 관리, 과금, 인증을 위한 기능을 포함하고 있어 GSM/UMTS의 GGSN(또는 SGSN)[8,9] 그리고, Mobile IP에서의 FA(Foreign Agent)와 유사한 기능을 수행한다. MT의 정보는 HD에서 관리하기 때문에 과금, 위치관리를 위한 노드 등이 HD에 포함되어 있다. SD의 DC와 구분하기 위해서 본 논문에서는 HD의 핵심 노드들인 DC와 AAA(Authentication, Authorization, Accounting)을 통합하여 HE(Home Environment)로 명칭한다. 각각의 도메인 인증 경로상에서 HE, MT, 또는 DC의 상위 노드인 서비스 제공자에 의해서 운영된다. 핵심망(core network) 은 AII-IP구조로 되어있고 과금 정보나 위치 정보는 모두 서비스 제공자에 의해서 운영될 수있으며 매우 다양한 보안 정책을 갖고 있는 SD사이를 핸드오버하면서 서비스를 받게된다. 하나의 서비스 운영자는 여러개의 도메인을 제공할 수 있다.



[그림5] Mobile PKI 시스템

이동 단말이 단대단 통신을 하기 위해서는 그림3에서 다음과 같은 여러 경로에 대한 신뢰성 확립이 필요한다.

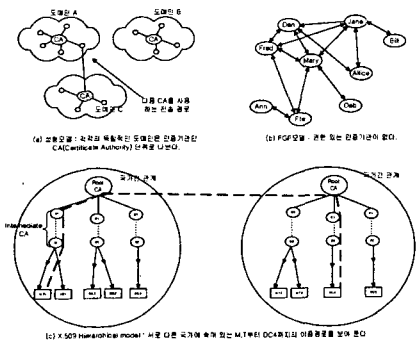
- MT↔SD 간의 상호 인증 ①
- HE↔SD 간의 상호 인증 ②
- HE↔MT 간의 상호 인증 및 과금 ③
- 사용자 노드간의 상호 인증 ④

핸드오버가 이루어질 경위 이러한 과정을 반복한 이후에 상대방과 통신을 재개할 수 있으므로 인증과 암호화·복호화의 반복에 의해 자원이 낭비된다. 따라서 MT가 도메인 내에서나 도메인 사이를 이동할 때 Mobile PKI 기반으로 상호 인증 및 신뢰성을 향상함과 동시에 효율적으로 시스템 및 네트워크 자원을 관리하고있다.

3.1 X.509 model

최근 인터넷 보안의 가장 중요한 이슈가 되고 있는 것 중 하나가 PKI이다. PKI는 전자상거래에 필수적인 전자서명을 비롯하여 공개키를 사용하는 모든 보

안 문제에 대한 신뢰성 있는 해답을 제시하기 위한 보안 서비스의 전반적 인프라 개념이라고 할 수 있다.



[그림6] PKI 모델

X.509에서 제안된 구조는 인증기관들이 계층적 구조를 갖는 형태 [그림6-c]이고 그 외에 일반적인 PKI 모델은 [그림6] 과 같다.[4]

그림[6-b]는 현재 유선망에서 인터넷 보안을 위해 주로 사용되고 있는 성형 구조의 독립된 도메인 형태를 갖는 모델이다. 성형구조는 여러 개의 인증기관이 존재하고, 각각이 발행하는 인증서가 웹 브라우저에 저장되어 있거나 새로이 추가할 수 있는 형태로 되어 있다. 이 구조의 가장 큰 특징은 인증기관들이 서로 완전히 독립되어 있기 때문에 단대단 통신의 보안을 위한 신뢰성 확립(상호 인증)을 위해서는 두 개체 모두 동일한 인증기관으로부터 인증서를 발급 받아야 한다는 것이다. [그림6-b]는 PGP(Pretty Good Privacy)에서 사용된 모델이다. PGP의 인증 모델은 PGP의 성공과 더불어 많은 사용자를 확보하고 있기는 하지만, 체계적인 관리 부족으로 인하여 확장성에 문제가 발생하기 때문에 소규모의 그룹에만 적당하다.

인증기관이 인증 도메인(보안 도메인)을 구성하는 주체이므로 X.509의 계층 구조를 이용하여 다양한 인증 정책을 펼 수 있는 장점이 있다. 이러한 계층구조는 또한 차세대 이동통신망과 같은 개방환경의 다중 도메인 구조에서도 적합한 구조이나, 그림에서 보듯이 MT와 HE는 동일한 CA의 하위 노드이고, DC까지의 인증 경로는 매우 다양하게 존재할 수 있다.[4]

4. 결론

스마트 카드기반 무선 인터넷의 대표주자인 WIM과 USIM에 대한 구조 및 이러한 무선 인터넷 스마트 카드의 방향을 알아보았다. 무선 인터넷에서 요구되는 네트워크 노드들간의 상호인증, 심층 네트워크 데이터 전송의 기밀성 등을 만족시켜주기 위한 PKI기반의 보안 프레임 워크인 Mobile PKI를 제안하고 Mobile Terminal이 도메인 내에서나 도메인 사이를 이동할 때 Mobile PKI기반으로 상호인증 및 신뢰성을 향상함과 동시에 효율적으로 시스템 및 네트워크 자원을 관리할 수 있음을 알 수 있었다. 또한 이동단말을 이용한 응용서비스, 즉 전자상거래 뱅킹, 홈트레이닝 등을 가능하게 할 수 있는 보안 구조와 기반을 마련하는 것은 매우 중요하며 자바카드와 같은 개방형 플랫폼을 지원하는 스마트 카드 기술에 대한 보다 적극적인 연구가 이루어져야 할 것이다.

참고문헌

[1] 서병기 김태연 "WAP환경에서의 안전한 키분배 프로토콜", [한국정보처리학회 추계학술발표회], 1997

[2] "Wireless Aplication Protocol Identity Module Specification, Part: Security, Version 12-July-2001," WAP 포럼 July 2001

[3] "Wireless Application Protocol Architecture", Version 12-July 2001, WAP 포럼, July 2001

[4] ITU-T Recommendation X.509: Information Technology-Open Systems Interconnection-TheDirectory: Authentication Framework.

[5] ISO/IEC 7816-3,"Information Technology - Identification cards - Integrated Circuit(s) cards with contacts - Part 4: Interindustry commands for interchange, International Organization for Standardization," Dec. 1995.

[6 ISO/IEC 7816-4,"Information Technology - Identification cards - Integrated Circuit(s) cards with contacts - Part3:Electronic signals and transmission protocols, International Organization for Standardization," Sep. 1995.

[7] ISO/ 7816-8,"Identification cards - Integrated Circuit(s) cards with contacts - Part 8: Security related interindustry commands, International Organization for Standardization," Oct. 1999.