무선 PKI 규격

이 용 • TTA 차세대이동통신프로젝트그룹 Vision 실무반 참관자
한국정보보호진흥원 전자서명인증관리센터 선임연구원

1. 서론

최근 휴대폰 등 무선단말기를 이용한 무선인터넷 사용이 급증하면서 무선인터넷 뱅킹, 증권거래 등 무선인터넷을 통한 전자거래가 확산되고 있고 기업의 시스템이 무선시스템으로 구축하는 사례도 늘고 있다. 향후 무선인터넷 사용자 서비스가 다양해질 것으로 판단되며 이와 더불어 유선인터넷과 동일한 수준의 정보보호 서비스에 대한 요구도 증대되어질 것으로 예상되어진다. 정보보호기술은 유선인터넷과 마찬가지로 안전한 전자상거래 서비스를 제공하기 위해서 통신정보에 대한 기밀성, 개체 인증기능 등의 정보보호를 위한 기능과 부인방지 기능 등을 제공해야 한다. 현재 웹 보안 프로토콜인 SSL(Secure Socket Layer)의 사용이 증가하면서 SSL의 핵심기술인 공개키 암호방식의 기반이 되는 PKI(Public Key Infrastructure)의 중요성이 강조되고 있다. PKI는 무선데이터 통신환경에서도 중요한 기반기술로써 작용할 것으로 예상된다.

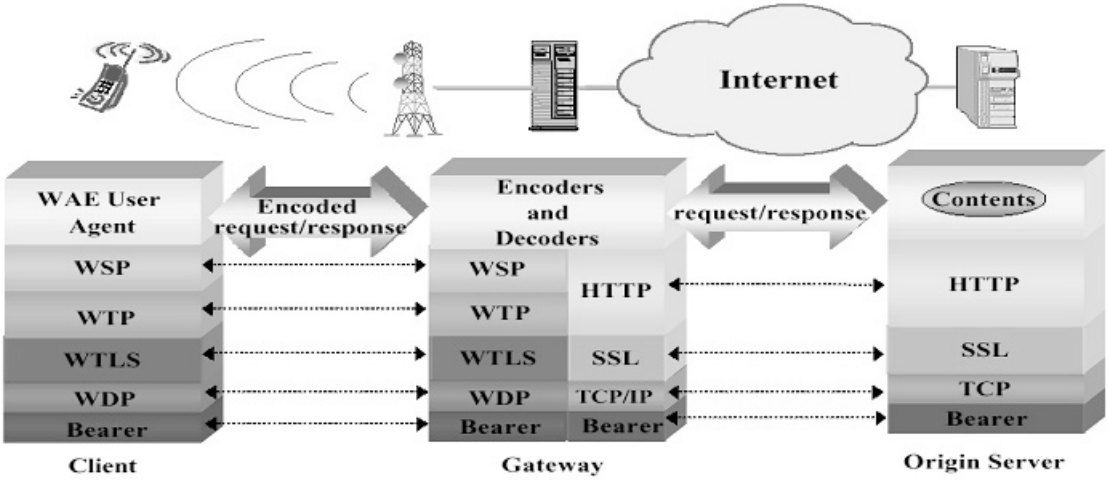
무선인터넷 환경은 유선인터넷 시스템과 달리 여러 가지 제약성을 가지고 있어 기존의 유선시스템에서 사용되던 보안 솔루션을 그대로 무선에 적용한다는 것은 아직까지 매우 어려운 실정이다. 무선시스템의 경우 낮은 대역폭, 시간지연, 연결의 불안전성 등 네트워크의 문제와 처리속도가 낮은 CPU, 적은 메모리, 배터리 시간, 작은 디스플레이, 입력장치 등 디바이스의 문제로 현재의 유선인터넷에서 이용되는 프로토콜 등을 무선단말기에 그대로 적용하는 것에는 많은 문제점들이 존재한다. 이러한 무선 환경의 제약성을 극복할 목적으로 무선인터넷을 위한 새로운 기술들이 개발되었다. 현재 무선인터넷 접속을 위한 기술은 WAP포럼에서 기존 유선인터넷에서의 프로토콜인 HTTP(HyperText Transport Protocol)에 기반하지 않고 새로이 개발한 WAP(Wireless Application Protocol), 그리고 마이크로소프트사, 퀄컴 등이 기존의 HTTP에 기반하여 무선데이터 서비스를 제공하고자 하는 경우인 MME(Microsoft Mobile Explorer), NTT-Docomo의 I-mode 등을 대표적으로 들 수 있다.

2. 국내 · 외 현황

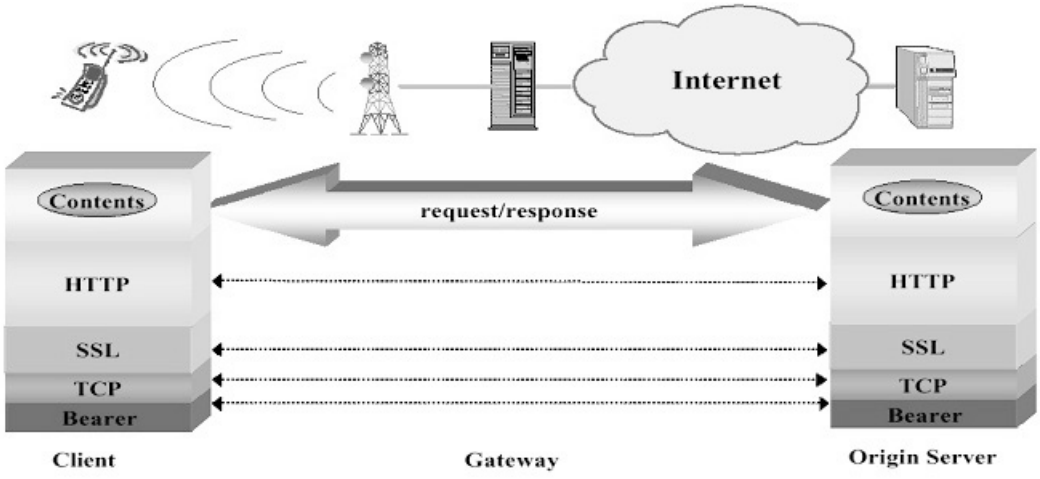
가. 표준화 현황

무선 PKI 표준화는 무선인터넷을 위한 표준화와 병행하여 진행되고 있다. 무선인터넷에 사용되는 단말기의 제한된 자원을 효과적으로 사용하기 위해 크게 WAP과 ME방식이 표준으로 제시되고 있다. WAP에서의 PKI기술은 기본적으로 WTLS (Wireless Transport Layer Security)계층의 보안을 전제로 WPKI 문서에서 전체 PKI를 설명하고 있고, ME에서는 SSL 기반의 보안을 전제로 PKI가 구축된다. 그러나 실제 구현에 있어서 국내 무선 PKI는 무선단말기의 성능상의 제약을 고려하여 WAP과 ME에서 정의된 규격이 국내 상황에 맞게 변형된 상태로 구축 · 진행중인 상태이다.

WAP표준은 현재 버전 2.0까지 발표되었으나, 현재 무선인터넷에 적용되고 있는 것은 WAP 1.x 기술이다. WAP 1.x는 무선망과 기존의 유선인터넷망을 연동하기 위한 WAP게이트웨이를 두고 있다. 사용자의 단말기와 게이트웨이는 WAP에서 정의된 프로토콜로 통신이 이루어지며, 게이트웨이와 기존



〈그림 1〉 WAP의 구성도



〈그림 2〉 ME의 구성도

유선망과의 통신은 HTTP를 통하여 이루어진다. WAP포럼에서는 무선환경에 적합한 프로토콜을 정의하고 있으며 보안을 위한 프로토콜로 WTLS가 있다. WTLS(Wireless Transport Layer Security)는 인터넷에서의 보안 메커니즘으로 잘 알려져 있는 SSL/TLS에 기반해서 작성되었고 기밀성, 사용자 인증, 메시지 무결성 등의 보안 서비스를 제공한다.

ME방식은 WAP게이트웨이가 할 일을 무선단말기 내의 브라우저가 하도록 하고 있다. 내부적으로 기존의 HTTP방식과 호환이 되며 HTML을 축약한 M-HTML을 사용하고 있고 보안 메커니즘은 HTTP에 기반하므로 유선인터넷에서 사용되고 있는 SSL 정보보호메커니즘의 수용이 가능하다.

나. 국내 · 외 동향

국외의 경우, 베리사인(Verisign), 발티모어(Baltimore), 소네라(Sonera), 엔트러스트(Entrust) 등에서 WAP 서버 인증서를 발급하는 서비스를 제공하고 있으며 무선 통신사업자와 솔루션 제공업체, 인증기관이 상호 협력하여 무선 인증서비스 및 보안기술 개발을 활발히 추진중에 있다. 이러한 서비스는 WAP 표준에서 제시한 대로 WAP 게이트웨이를 중심으로 나뉘는 무선구간에는 WTLS를, 유선구간에는 SSL을 적용하고 단대단 보안을 제공하지는 못하고 있다. 또한 WAP에서 제시하는 short-lived 형태의 WTLS 인증서를 사용하고 X.509 인증서를 지원하지 못하고 있다.

국내의 경우, SK텔레콤 및 LG텔레콤이 WAP 서비스를 제공하고 있으며, 한국통신프리텔은 ME 서비스를 제공하고 있다. 현재 한국정보인증(주)이 LG텔레콤과 손잡고 무선 PKI 기술규격에 따라 무선 공인인증시스템을 구축하여 한국정보보호진흥원의 실질심사를 통과하고 시범서비스를 준비중이며, 한국통신프리텔과 SK텔레콤도 무선 PKI 기술규격에 따라 무선 공인인증시스템을 구축하여 실질심사를 받고 있는 중이다. 따라서 무선인터넷 사용자들은 금년중에 무선 PKI를 적용한 안전한 전자거래서비스를 받을 수 있을 것이다.

3. 무선 PKI

유선과 마찬가지로 무선인터넷이 안전한 전자상거래 서비스를 제공받기 위해서는 기밀성, 무결성, 인증, 부인봉쇄와 같은 서비스를 제공하기 위한 무선 PKI가 필요하다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용하며, 무선환경에 적합하도록 기능을 최소한 변화시킨 것이다. 무선 PKI를 구축할 경우에는 유선과는 달리 클라이언트와 서버간의 제한된 대역폭, 클라이언트의 처리능력, 클라이언트의 제한된 메모리를 고려해야 한다. 또한 기존 유선환경과는 달리 인증서 검증 메커니즘의 경량화 등을 고려하여야 한다.

가. 무선 PKI의 고려사항

휴대폰과 같은 무선단말기를 사용하는 무선인터넷 환경에서 유선인터넷 수준의 보안을 제공하기 위해서 고려해야 할 점은 다음과 같다.

- ○ 무선단말기의 CPU가 처리해야 할 데이터를 최소화하여 단말기 CPU의 처리능률을 향상시킬 수 있도록 구성하여야 하며, 무선단말기의 CPU에서 처리가능한 서명, 검증, 암호화 알고리즘을 채택하여 무선 PKI 서비스의 효율성을 높여야 한다.
- ○ 무선단말기에서 처리가능한 인증서, CRL(Certificate Revocation List, 인증서 폐지목록) 프로파일 규격을 정해야 하며, 사용하는 알고리즘의 최적화를 통하여 모듈 사이즈를 최소

한으로 줄여서 제한된 메모리를 갖는 단말기 환경에 맞춰야 한다.

○ 인증서의 발급, 저장, 처리, 검증 등에 필요한 프로토콜을 무선단말기 환경에 맞도록 최적화하여 모듈사이즈를 줄이고 처리시간도 줄여야 한다.

○ 무선인터넷 환경에 맞는 인증서 검증방식을 채택하여 처리율이 떨어지는 무선단말기에서 인증서를 제대로 검증할 수 있도록 하여야 한다.

○ 무선단말기의 메모리 제약을 고려하여 인증기관간 상호연동이 가능한 인증서 요청, 관리 프로토콜을 적용하여야 한다.

○ 현재의 무선단말기가 이후 모듈변경이 어려운 점을 고려하여 확장성과 유선 및 국제 호환성을 고려하여야 한다.

나. 무선 PKI 모델

위의 고려사항을 감안하여 국내에서는 <그림 3>과 같은 무선 PKI 모델을 적용하였다.

○ 무선 PKI 모델에서는 기본적으로 무선용 X.509 인증서를 사용하지만, 무선 CA 서버는 단말기의 검증능력을 고려하여 Short-lived 인증서인 WTLS인증서를 사용하며, 단말기의 경우 저장공간의 문제로 인증서를 발급받을 경우 인증서의 URL을 이용한다.

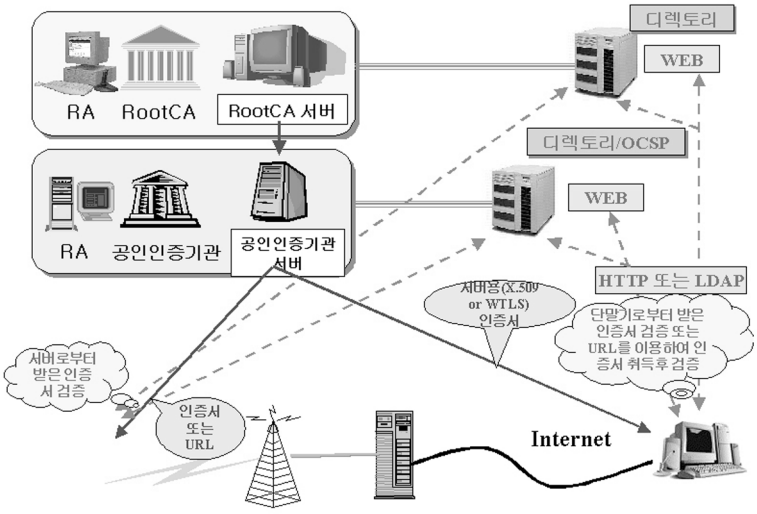
○ 단말기에서 무선용 X.509 서버 인증서의 검증 메커니즘으로는 CRL이나 OCSP를 사용하도록 한다. 또한 무선에서는 CRL를 잘게 쪼개서 최근 CRL를 가져와서 검증할 수 있는 메커니즘인 Delta CRL이 옵션으로 사용된다.

○ 무선단말에서 RSA를 사용하여 키 생성이 용이하지 않아 ECDSA를 사용하여 키를 생성할 수 있는 기능이 무선에서 추가되었으며, 서명알고리즘으로는 RSA, ECDSA가 사용되며, 키 분배용으로는 RSA, ECDH가 사용된다.

○ 무선에서는 무선환경에 맞는 인증서 요청 및 관리 프로토콜 규격을 사용한다.

4. 무선 PKI 기술규격

무선 PKI 모델에 따라 국내에서 개발된 무선 PKI 기술규격은 다음과 같다.



〈그림 3〉 무선 PKI 모델

가. 무선 전자서명 인증서 프로파일

WAP · ME에 모두 적용가능하고 이를 기반으로 무선 전자서명 인증관리 체계에서 사용되는 무선 전자서명 X.509V3 인증서에 대한 프로파일 규격을 정의하고 있으며, 인증기관 및 응용프로그램이 인증서를 생성하고 처리하는데 필요한 요구사항들을 명시하고 있다. 인증서의 기본필드 및 확장필드 중 인증서 생성시에 요구되는 필드의 내용과 사용자 소프트웨어 등에서 인증서 처리시에 요구되는 확장필드에 대하여 정의하고 있으며 확장필드에 대한 criticality를 정의한다.

나. WTLS인증서 프로파일

무선 전자서명 인증관리 체계에서 키 분배용으로 사용되는 WTLS 인증서 대한 프로파일을 정의하고 있으며 인증기관 및 응용 프로그램이 인증서를 생성 및 처리하는데 필요한 요구사항들을 명시한다. WTLS인증서 프로파일은 WAP 인증서 및 인증서 폐지목록 프로파일, WAP 공개키 기반구조, WAP WTLS에 기반을 두어 무선환경의 특성을 반영하여 작성되었다.

다. 무선 전자서명 인증서 효력정지 및 폐지 목록 프로파일

전자서명 인증관리 체계에서 사용되는 무선 전자서명용 인증서 상태확인을 위한 인증서 효력정지 및 폐지목록 프로파일에 대한 규격을 정의하고 있으며, 인증기관과 응용 프로그램이 인증서 효력정지 및 폐지목록을 생성 및 처리하는데 필요한 요구사항들을 명시하고 있다.

라. 무선 전자서명 알고리즘

무선 전자서명 인증관리 체계에서 지원하는 전자서명 알고리즘과 해쉬 알고리즘에 대하여 기술하며 관련 규격을 명시한다. 전자서명 알고리즘은 인증기관이 인증서와 인증서 효력정지 및 폐지목록을 생성하는 경우와 전자문서에 사용자가 전자서명을 하는 경우에 사용되며 RSA와 ECDSA(타원곡선에 기반한 DSA알고리즘)를 채택하고 있다.

마. 무선 키 분배용 알고리즘

무선 전자서명 인증관리 체계에서 지원하는 키 분배용 알고리즘과 암호화 알고리즘에 대하여 기술하며 관련 규격을 명시한다. 키 분배용 알고리즘은 RSA와 ECDH를 적용하며 암호화 알고리즘은 SEED와 Triple DES를 채택하고 있다.

바. 무선 전자서명 인증관리 체계 OID (Object Identifier) 규격

인증서에서는 전자서명 알고리즘, 인증서 정책, 확장필드 등의 전자적인 객체들에 대하여 고유의 식별자인 OID를 부여하여 사용한다. OID는 각 국가 및 기관에서 보유하고 있는 전자적인 객체들에 대해서 국제적으로 유일하게 식별할 수 있는 수단이며, 전자서명 인증관리 체계를 구축하는데 있어서 국내에서 독자적으로 보유하고 있는 전자객체에 대해서 국제적인 표준화단체를 통하여 고유한 OID를 부여하는 것이 필수적으로 요구된다. 전자서명 인증관리 체계 OID 규격은 무선 전자서명 알고리즘, 해쉬 알고리즘, 인증서 정책, 인증서 구성요소 등에 대한 OID를 체계적으로 구축하는데 활용될 것이다.

사. 무선 전자서명 인증서 DN(Distinguish Name) 규격

인증서 및 인증서 효력정지 및 폐지목록을 전자서명 인증관리 체계에서 고유하게 식별하기 위한 DN 규격을 정의하고 있다.

아. 무선용 인증서 요청 형식 프로토콜 및 관리 프로토콜 규격 등

인증기관간 상호연동을 제공하기 위하여 무선용 인증서 요청 형식, 인증서 관리 프로토콜 및 무선용 응용계층 보안 프로토콜 규격을 개발하였으며 이는 무선단말기에서 인증서 발급을 요청하고 인증서 관리에 필요한 갱신, 재발급, 효력정지, 폐지 등에 관한 절차를 무선용 인증서 관리 프로토콜에 정의하고 있다.

또한 WAP에서 게이트웨이 사용으로 인하여 발생하는 단대단 보안문제를 해결하기 위하여 무선 응용계층 보안 프로토콜을 정의하고 있다.

자. 무선 PKI 기술규격의 특징

최근 국내에서는 무선 전자서명 인증서 프로파일, 무선 전자서명 알고리즘 규격 등 6개의 무선 PKI 관련 표준이 제정되었다. 개발된 무선 PKI 표준의 주요 특징은 다음과 같다.

- ○ 무선 전자서명 인증서 프로파일에서는 단말기에서 인증서 처리부담을 감소시키고자 확장필드 중에 Authority Key Identifier 필드와 Subject Key Identifier 필드를 option으로 정의함.
- ○ 인증서 검증과 관련하여 유선에서 제공하는 CRL 검증뿐만 아니라 OCSP(Online Certificate Status protocol) 서버를 통한 인증서 상태확인 기능을 제공하기 위하여 Domain Information을 필드를 포함하여 단말기에서 OCSP 기능을 제공할 수 있도록 함.
- ○ 현재 유선에서 정의하고 있는 RSA 알고리즘을 단말기에 사용하기에는 키 생성시간 등의 문제점을 해결하기 전에는 힘든 상황이므로, 무선 전자서명 알고리즘으로는 ECDSA 알고리즘을 정의하였고, RSA 알고리즘도 추후 기술발전에 따라 적용가능할 것으로 판단되어 단말기에서 서명, 검증이 가능하도록 정의함.
- ○ 무선 WTLS인증서 프로파일은 콘텐츠 제공자(Content Provider)의 키 분배용 인증서로 사용하기 위하여 정의하고 단말기에서 CRL 검증의 부담을 줄이기 위해 short-lived WTLS인증서를 사용할 수 있도록 함.
- ○ 유선의 인증서 요청 및 관리 프로토콜(CMP)을 무선단말기에 전부 탑재하기에 부담이 따르므로 무선단말기에서 온라인으로 인증서를 요청할 경우에 사용자 인증과 POP(Proof Of Possession)을 동시에 해결할 수 있는 요청형식을 참조번호, 인가코드 기반의 해쉬함수를 통하여 구성하였고, 무선인증서 요청 형식 및 관리 프로토콜은 WAP Crypto Library에서 정의한 Signtext 함수를 적용하여 단말기에 구현시 메모리 사용량 및 코드 크기를 최소화할 수 있도록 구성함.

5. 결론

현재까지는 무선 PKI에 대한 완전한 표준화 정립이 되어있지 않으며 자체적인 기술을 바탕으로 개발 · 연구중이지만, 한국정보보호진흥원에서는 이미 이동통신사와 연구소, 개발업체들로 구성된 무선 PKI 실무작업반을 구성하여 무선 PKI의 기술기준과 기술규격을 개발하여 국내 무선 PKI 구축에 적용하였다. 무선인터넷 PKI 구축을 위해서는 관련 제도 및 정책, 기술기준 및 표준, 응용기술, 평가기술

등의 개발이 요구되며 정부 공인 인증기관, 이동통신업체, 인증서버 개발업체, 학계 등과 협력체제 구성을 추진하여야 한다. 향후 무선망의 형태가 국제간의 로밍 등이 가능한 3세대 무선통신 시대로 변화하고 있는 실정에서 무선인터넷에서의 PKI도 이에 발맞춰 국제적인 표준화를 시급히 이루도록 해야 할 것이다.

참고문헌

- Wireless Application Protocol Public Key Infrastructure Definition, WAP-217-WPKI: 24-Apr-2001
- WAP Certificate and CRL Profile, WAP-211-X.509: 22-May-2001
- Wireless Transport Layer Security, WAP-261-WTLS-20010406p
- ITU-T Recommendation X.509(1997), Information technology - Open System Interconnection - The Directory : Authentication Frame work
- IETF RFC 2459(1999), Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- IETF RFC 2510(1999. 3), Internet X.509 Public Key Infrastructure Certificate Management Protocols
- IETF RFC 2560(1999. 6), X.509 In ternet Public Key Infrastructure On-line Certificate Status Protocols : FTP and HTTP
- Verisign, http://www.verisign.com/wireless/index.html
- Entrust, http://www.entrust.net/wapserver/index.htm
- Baltimore, http://www.baltimore.com/telepathy/index.html
- Sorena, http://www.sonera.fi/english
- 이 용, 무선인터넷을 위한 PKI 구축, 제6회 정보보호 심포지엄, 한국정보보호진흥원, 2001. 7
- 무선 PKI(Public key Infrastructure) 기술기준, 한국정보보호진흥원, 2001. 9
- 무선 PKI 기술규격 V1.21, 한국정보보호진흥원, 2001. 8

저자 약력

1997년	:	연세대학교 컴퓨터과학과(석사)
2001년	:	연세대학교 컴퓨터과학과(박사)
1993년 ~ 1994년	:	디지콤 정보통신 연구소 연구원
2001 ~ 현재	:	한국정보보호진흥원 전자서명인증관리센터 선임연구원