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

무선 PKI 기술 및 서비스 동향에 관한 연구

정영석*, 김수진*, 서인석**, 서상원**, 원동호*
*성균관대학교 정보통신공학부,
**국가보안기술연구소
e-mail : yschung@dosan.skku.ac.kr

A Study on Trends of Wireless PKI technologies and Services

Young-Seok Chung*, Soo-Jin Kim*, In-Seok Seo**, Sang-Won Seo**, Dongho Won*
*School of Information & Communications Engineering, Sungkyunkwan University
**National Security Research Institute

요 약

무선 PKI 환경에서는 단말기의 한계나 무선 환경이라는 제약 때문에 유선 PKI 환경에서 제공되는 다양한 서비스를 받기 위해 여러 가지 기술이 요구되며, 이를 위해 많은 기술 규격들이 개발되어 표준화가 진행 중에 있다. 본 논문에서는 현재 표준화가 완료된 무선 PKI 기술 표준과 표준화가 진행중인 무선 PKI 기술 규격에 대해 알아보고 이를 이용하여 제공되고 있는 서비스에 대해 알아본다. 또한, 향후에 무선 PKI 기반에서 제공될 수 있는 서비스와 무선 환경의 제약사항을 개선할 수 있는 방안을 제안한다.

1. 서론

최근 정보통신 기술의 발전과 휴대 단말기 사용의 보편화로 무선 인터넷의 사용자가 급격히 늘어났다. 그로 인해 무선 인터넷에 대한 수요가 증가하였고, 다양한 응용 서비스들을 사용할 수 있는 기술이 요구되고 있다. 현재 무선 인터넷 환경에서 제공되는 서비스는 대부분 전자 상거래 서비스인데, 이러한 서비스가 성공적으로 제공되기 위해서는 보안문제가 우선 해결되어야 한다. 즉, 유선 인터넷 환경에서와 마찬가지로 무선 인터넷 환경에서도 안전한 서비스를 제공하기 위해 메시지 기밀성, 메시지 무결성, 사용자 인증, 부인봉쇄와 같은 보안 서비스를 제공해야 하며, 이를 위해 무선 PKI(Public Key Infrastructure)가 필요하다.

그런데 무선 PKI 환경에서는 유선 환경과 달리 많은 제약조건이 있다. 디바이스의 적은 용량의 배터리, 작은 크기의 화면, 낮은 성능의 CPU, 적은 메모리 등의 디바이스 환경에서의 제약조건과, 무선망의 제한된 통신속도 , 높은 통신 에러율, 사용자의 편리성을 고려하지 못한 인터페이스, 제한된 종류의 디바이스 등의 무선 환경의 제약조건이 있다. [1]

이러한 제약조건을 극복하고자 무선 PKI 기술이 개발되었고, WMLScript(Wireless Markup Language Script) Crypto Library 에서 제공하는 signText() 함수를 이용하여 단대단 보안을 보장하고 있다. [2]

본 논문에서는 국내에서 세계 최초로 개발된 무선 PKI 기술 표준과 기술 규격을 분석하고, 이를 기반으로 이루어지고 있는 서비스에 대해 알아본다.

본 논문의 구성은 다음과 같다. 2 장에서는 무선 PKI 의 기반이 되는 무선 인터넷 기술과 무선 PKI 기술에 대하여 알아본다. 3 장에서는 현재까지 표준화가 완료된 무선 PKI 기술 표준과 표준화가 진행중인 무선 PKI 기술 규격에 대해 설명하고, 4 장에서는 무선 PKI 환경에서 실제 이루어지고 있는 서비스에 대해 알아본다. 5 장에서는 결론 및 향후 연구 계획에 대해 언급한다.

2. 관련 연구

무선 인터넷 기술에는 크게 WAP(Wireless Application Protocol) 방식과 ME(Mobile Explorer) 방식이 있는데, 무선 PKI 에서는 주로 WAP 방식에 기반을 두며, WAP 게이트웨이를 통한 무선 인터넷 서비스에서 인증 서비스를 운영한다.

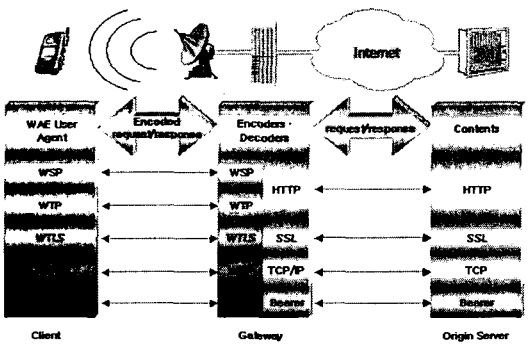
본 장에서는 두 방식에 대해 알아보고, 이를 이용한 무선 PKI 의 특징과 구조에 대해 알아본다.

2.1 무선 인터넷 기술

무선 인터넷 환경에서는 디바이스와 무선 환경의 제약으로 유선 인터넷에서 사용되는 기술을 그대로 적용하기에 어려운 점이 있다. 따라서 무선 인터넷에서 사용되는 단말기의 제한된 자원을 효과적으로 사용하기 위한 무선 인터넷 기술이 개발되었으며, 대표적인 방식으로 현재 국내 표준으로 채택이 가장 유력시되는 WAP 방식과 유선 인터넷의 HTML 기술을 응용한 방법인 ME 방식이 있다.

● WAP

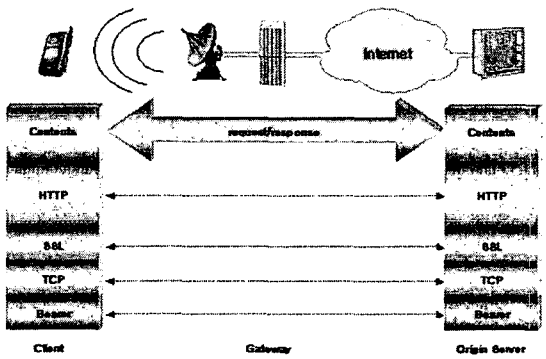
WAP 방식은 공개된 표준으로, 전세계적으로 사용자가 가장 많다. 그러나 기존의 HTTP 를 지원하지 않으며, 유· 무선 구간의 연결을 위한 별도의 WAP 게이트웨이를 필요로 하기 때문에 ME 방식에 비해 비용이 많이 든다는 단점이 있다. 반면에 기존 기술과의 호환성을 제공하고, 어플리케이션의 개발이 가능하기 때문에 다른 방식에 비하여 많은 유연성을 가지고 있는 서비스와 차별화 된 서비스를 개발하기에 유리하다는 장점을 가지고 있다. 또한 게이트웨이 내에서 WAP 과 HTTP 간의 변환 과정에서 발생하는 원문의 노출문제는 Crypto.signText()를 이용하여 해결하고 있다. WAP 방식의 구조도는 [그림 2-1]과 같다. [3][4][5]



[그림 2-1] WAP 방식의 구조도

● ME

ME 방식에서는 WAP 게이트웨이가 수행하는 작업을 무선 단말기 내의 브라우저가 수행하며, 일반 인터넷 표준인 HTTP 방식과 호환된다. 또한, HTML 을 축약한 m-HTML(micro Hypertext Markup Language)을 컨텐츠 기술 언어로 사용하기 때문에 이동통신사업자에게는 투자비를 절감할 수 있도록 해주고, 기존의 HTML 컨텐츠를 그대로 이용할 수 있다는 점에서 컨텐츠 제공자에게는 편의를 제공한다. ME 에서의 보안 메커니즘은 HTTP 에 기반하고 있으므로 유선 인터넷에서 사용되고 있는 SSL(Secure Sockets Layer) 정보보호 메커니즘의 수용이 가능하다. 또한, ME 는 운영 체제의 종류에 상관없이 사용 가능한 브라우저를 제공하는 장점이 있다. 반면 브라우저의 오버헤드가 크며, 브라우저에서 지원하지 않는 파일을 이용한 서비스를 제공하지 못하는 단점을 갖는다. ME 방식의 구조도는 [그림 2-2]와 같다. [5]



[그림 2-2] ME 방식의 구조도

2.2 무선 PKI 기술

무선 PKI 는 기존의 유선 PKI 의 구성요소를 그대로 이용하면서, 무선 환경에 적합하도록 기능을 최소화하였다. 즉, 기존의 유선 환경에서 사용하는 X.509 인증서에 비해 부피가 작고 간단한 구조로 되어 있는 WTLS(Wireless Transport Layer Security) 인증서를 사용한다. 이는 무선 환경에서 사용하는 소용량 단말기에서 암호화 및 인증 업무를 효율적으로 수행할 수 있도록 구성되었다.

● 무선 PKI 의 구성 요소

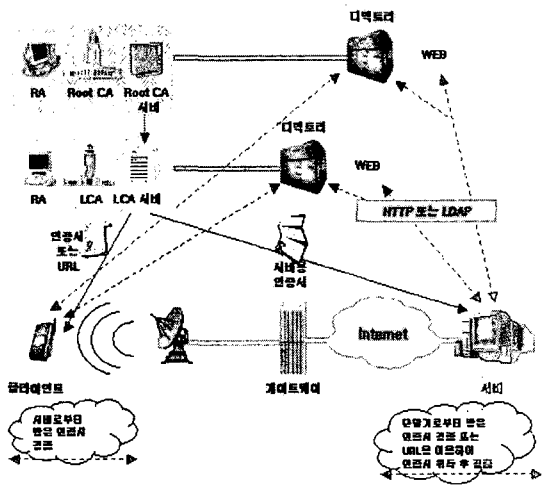
무선 PKI 를 구성하는 요소로는 인증서를 발행하고 효력정지 및 폐지 기능을 수행하는 인증기관(CA : Certification Authority), 인증서 등록 및 사용자 신원 확인을 대행하는 등록기관(RA : Registration Authority), 인증서 및 인증서 폐지 목록을 저장하는 디렉토리(Directory), 그리고 인증서를 신청하고 사용하는 사용자(EE : End Entity)가 있다. [6]

● 무선 PKI 모델

무선 PKI 에서는 단말기의 검증 능력과 메모리의 한계 문제를 고려하여 무선용 X.509 인증서, WTLS 인증서 또는 갱신 주기가 24~48 시간인 Short-lived 인증서를 사용하며, 인증서를 발급 받을 경우 인증서의 URL 을 이용하기도 한다. 또한, 단말기에서의 인증서 검증 메커니즘으로 OCSP(Online Certificate Status Protocol), 최신의 CRL(Certificate Revocation List)만을 모아놓은 Delta CRL 을 사용한다.

서명 알고리즘으로는 키 길이가 160 비트로 짧으면서도 보안강도는 1024 비트의 RSA 알고리즘 수준을

갖는 ECDSA(Elliptic Curve Digital Signature Algorithm)를 사용하며, 키분배용 알고리즘으로는 ECDH(Elliptic Curve Diffie-Hellman)를 사용한다. [그림 2-3]은 기본적인 무선 PKI 모델에 대한 구성도이다. [5]



[그림 2-3] 무선 PKI 모델

3. 무선 PKI 기술 동향

한국정보보호진흥원(KISA)은 공인인증기관, CA 개발업체, 이동통신사업자로 이루어진 무선 PKI 실무작업반을 구성하고, 공인인증기관 인증서의 상호연동을 보장하고 관련 제품간의 호환성을 확보할 수 있도록 무선 PKI 기술 규격을 개발하였으며, 2002 년 4 월 인터넷보안기술포럼(ISTF)에서 지금까지 제안된 무선 PKI 기술 규격 중 6 개의 규격을 표준으로 확정하였다. 무선 PKI 기술 표준과 규격은 무선 전자서명 인증관리체계의 인증기관 및 응용 프로그램에서 사용된다.

3.1 무선 PKI 기술 표준

무선 PKI 기술 규격 중 무선 PKI 기술 표준으로 확정된 것으로는 다음 6 개의 표준이 있다.[7][8][9][10][11][12]

- 무선 전자서명 인증서 프로파일 표준
  (Wireless Digital Signature Certificate Profile Standard)
  - 무선 전자서명 X.509 v3 인증서에 대한 프로파일 정의
- 무선 전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준
  (Wireless Digital Signature Certificate Revocation List Profile Standard)
  - 무선 전자서명용 인증서 상태확인을 위한 인증서 효력정지 및 폐지 목록 프로파일 정의
- 무선 WTLS 인증서 프로파일 표준
  (Wireless Transport Layer Security Certificate Profile Standard)
  - 키분배용으로 사용되는 WTLS 인증서에 대한 프로파일 정의
- 무선 전자서명 알고리즘 표준
  (Wireless Digital Signature Algorithm Standard)
  - 무선 전자서명 인증관리체계에서 지원하는 전자서명 알고리즘과 해쉬 알고리즘에 대해 기술
- 무선 키분배 알고리즘 표준
  (Wireless Key Distribute Algorithm Standard)
  - 키분배 인증서 서명에 지원되는 알고리즘과 해쉬 알고리즘에 대해 기술
- 무선 인증서 요청형식 프로토콜 표준
  (Wireless Certificate Request Format Potocol Standard)
  - 전자서명 및 키분배 인증서 요청형식 프로토콜 정의

3.2 PKI 기술 규격

표준화가 진행중인 무선 PKI 기술 규격으로는 다음 5 개의 규격이 있다. [13][14][15][16][17]

- 무선 전자서명 인증서 DN 규격
  (Wireless Digital Signature Certificate Distinguish Name Specification)
  - 인증서 및 인증서 폐지 목록을 고유하게 식별하기 위한 DN 정의
- 무선 WTLS 인증서 DN 규격
  (Wireless Transport Layer Security Certificate Distinguish Name Specification)
  - WTLS 인증서를 고유하게 식별하기 위한 DN 정의
- 무선 전자서명 인증서 OID 규격
  (Wireless Digital Signature Certificate Object Identifier Specification)
  - 무선 전자서명 알고리즘, 해쉬 알고리즘, 인증서 정책, 인증서 구성요소 등에 대한 OID 명시
- 무선 인증서 관리 프로토콜 규격
  (Wireless Certification Management Protocol Specification)
  - 전자서명 및 키분배 인증서 재발급, 폐지, 갱신, 효력정지, 효력회복시 필요한 프로토콜 정의
- 무선 응용계층 보안 프로토콜 규격
  (Wireless Application Layer Security Protocol Specification)
  - 인증서 기반의 응용계층 프로그램간의 프로토콜을 위해 Crypto Library 와 단대단 보안 프로토콜 정의
  - 응용 프로그램이 암호화된 정보를 생성하고 처리하는데 필요한 요구 사항 명시

4. 무선 PKI 서비스 동향

아직 무선 PKI 시장이 국내는 물론 전세계적으로 초기 단계이기 때문에 무선 PKI 서비스가 본격적으로 제공되지는 않은 상황이지만, 공인인증기관과 이동통신사를 중심으로 공인인증서비스가 추진되고 있으며, KISA 와 PKI 솔루션 업체들은 기술 개발을 하고 있다. 또한, KISA 에서는 이미 지난해 6 월 WPKI 의 최상위 기관으로서 루트 CA 를 구축하였으며, 무선인증서비스

를 신청한 공인인증기관에 대한 실질심사를 맡도록 제도화 되어 있어 공인인증기관이 일반인을 대상으로 한 무선공인인증서비스를 하려면 KISA 의 실질심사를 통과해야 한다.

한편, 무선공인인증을 위해 이동통신사와 공인인증기관과의 협력이 필요한데, SK 텔레콤과 한국증권전산, LG 텔레콤과 한국정보인증, KTF 와 한국증권전산, 한국정보인증, 한국전자인증이 제휴를 맺어 무선인증시범서비스를 완료하였다. 한국증권전산의 경우 드림시큐리티가 KTF 에 무선공인인증시스템을 공급하여 SK 증권 등 6 개 증권사에 적용되고 있는 무선증권거래시스템인 모바일로(Mobilo)에 무선인증을 적용한 시범서비스를 추진하고 있다. 한편, 한국정보인증은 LG 텔레콤과 공동 개발한 무선공인인증시스템이 2002 년 3 월 KISA 의 실질심사를 통과함에 따라 테스트작업을 거쳐 6 월 한달간 시범서비스를 마친 상태이다. 또한, K-sign 은 8 월 한국전산원과 무선부문 인증시스템을 구축키로 합의했고, 9 월 한국증권전산에 무선 PKI 인증시스템을 구축하기로 발표함에 따라 SK 텔레콤, KTF 에 이어 LG 텔레콤에도 무선인증서비스를 제공하게 되었다. 금융결제원은 이동통신 3 사를 지원할 수 있는 통합된 형태의 WPKI 솔루션을 적용해 KISA 에 실질심사를 신청한 상태이어서 내년 상반기에는 시험운영 및 상용서비스에 들어갈 수 있을 것으로 예상된다.

KISA 에서 한국정보인증의 KTF 인증시스템에 대한 심사는 6 월말, 한국증권전산의 SK 텔레콤 및 KTF 인증시스템에 대한 심사는 각각 8 월과 9 월에 완료함에 따라 KTF, SK 텔레콤 순으로 1 개월간 시범서비스를 실시하여 9 월부터 국내 이동 3 사 전체가 무선 전자서명 인증 상용서비스를 실시할 것으로 보인다.

한편, 정보통신부에서는 이동통신사에 RA 자격을 부여하는 대신 이동통신사로 하여금 전적인 책임을 지게 하는 방안을 추진 중에 있다.

또한, 한국정보인증에서는 개인들이 공인인증서를 발급 받으러 등록기관에 직접 가야하는 번거로움을 덜어주기 위해 기존의 유선공인인증 사용자들이 직접 공인인증기관을 방문하지 않고도 네트워크를 통해 인증을 받을 수 있도록 별도의 유무선 공인인증통합서비스를 준비중이다. [18][19][20][21][22][23][24]

5. 결론 및 향후 연구 계획

본 논문에서는 무선 PKI 기술 표준 및 규격과 현재 이루어지고 있는 서비스에 대해 알아보았다.

현재 약 3000 만명에 이르는 국내 휴대폰 가입자들이 무선 인터넷으로 모바일 뱅킹, 온라인 증권거래, 사이버 트레이딩, 예약 및 티케팅 등을 하는 과정에서 본인확인 및 무선 데이터 보호를 통해 안전하게 전자상거래를 할 수 있게 되었다.

하지만 단말기 기능과 무선 PKI 기술의 발전에도 불구하고 단말기 분실의 위험과 단말기에 저장되어 있는 중요 정보의 유실로 인한 피해로부터 안전하지 못한 실정이다. 이를 보완하기 위해 기존의 기술을 그대로 이용하면서 스마트카드나 USB(Universal Serial Bus) 토큰과 같은 보안성이 뛰어난 하드웨어 토큰을 함께 이용하는 방법이 있다. 이는 단말기의 적은 저장공간과 낮은 연산 능력을 보완하여, 사용자의 비밀정보나 인증서와 같은 중요한 정보를 단말기에서 분리하여 저장하고, 복잡한 암호학적 연산을 가능하게 함으로써 보다 안전하고 효율적으로 서비스를 제공받을 수 있게 한다. 즉, 온· 오프라인 상의 모든 거래를 안전하게 할 수 있고, 신뢰성 있는 인증을 통해 전자결재, 전자 계약 등의 서비스를 제공 받을 수 있으며, 보다 효율적인 의료보험 서비스도 가능하게 될 것이다. 추후 하드웨어 토큰에 대한 많은 연구와 서비스의 다양화를 위한 요구 사항 분석이 이루어져야 할 것이다.

참고문헌

[1] 이석준, 정병호, 정교일, "무선 전자상거래를 위한 보안 기술", 정보보호학회지, pp. 1-13, 2002.6

[2] WAP Forum, " WMLScript Crypto API Library", 2001.6

[3] WAP Forum, "Wireless Application Protocol Architecture Sepcification", 2000.10

[4] WAP Forum, "WAP 2.0 Technical White Paper", 2002.1

[5] http://www.kisa.or.kr/K_trend/KisaNews/200108/special_report_01.html

[6] R. Housely, W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC 2459, 1999.1

[7] ISTF, "ISTF-012 무선 전자서명 인증서 프로파일 표준", 2002.4

[8] ISTF, "ISTF-013 무선 전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준", 2002.4

[9] ISTF, "ISTF-014 무선 WTLS 인증서 프로파일 표준", 2002.4

[10] ISTF, "ISTF-015 무선 전자서명 알고리즘 표준", 2002.4

[11] ISTF, "ISTF-016 무선 키분배 알고리즘 표준", 2002.4

[12] ISTF, "ISTF-017 무선 인증서 요청형식 프로토콜 표준", 2002.4

[13] 한국정보보호진흥원, "전자서명 인증서 DN 규격", 2001.8

[14] 한국정보보호진흥원, "무선 WTLS 인증서 DN 규격", 2001.8

[15] 한국정보보호진흥원, "무선 전자서명 인증서 OID 규격", 2002.7

[16] 한국정보보호진흥원, "무선 인증서 관리 프로토콜 규격", 2001.8

[17] 한국정보보호진흥원, "무선 응용계층 보안 프로토콜 규격", 2001.8

[18] http://www.signgate.com/index.htm

[19] http://www.kftc.or.kr/

[20] http://www.nca.or.kr/main/nca_main_intro.htm

[21] http://www.crosscert.com/

[22] http://www.koscom.co.kr/

[23] http://www.ktnet.co.kr/

[24] http://www.rootca.or.kr/