通信情報保護學會誌
第 10 券 第 4 號, 2000. 12

WAP을 위한 국내 공개키기반구조(PKI)모델

이 재 일*, 박 정 환*, 송 주 석**

Public Key Infrastructure Model For Wireless Application Protocol(WAP)

Jae-Il Lee*, Jung-Hwan Park*, Joo-Seok Song**

요 약

무선 인터넷 서비스가 국내외적으로 크게 증가하고 있으며 2003년경에는 세계 무선 인터넷 사용인구가 6억 명에 이를 것이라는 전망이 나오고 있다. 그러나 무선인터넷이 보다 활성화되고 이를 이용한 뱅킹 서비스, 주식거래, 온라인 쇼핑 등의 전자상거래 서비스가 원활히 제공되기 위해서는 보안기술의 적용이 필수 사항이다.[6] 본 고에서는 WAP(Wireless Application Protocol)을 위한 전자서명인증 및 키 분배용 모델을 제시함으로써 국내 무선공개키기반구조 구축시 발생할 수 있는 혼란을 최소화하고 국내 무선 인터넷 인증 관련 기술의 발전과 응용 서비스를 활성화시키는데 기여하고자 한다.

Ⅰ. 서 론

정보통신부 자료에 의하면 국내 무선인터넷 가입자수가 2000년 8월로 1100만 명을 넘어섰고, 세계적으로 이동통신가입자 중 무선인터넷 사용비율이 2004년 기준 61%에 이를 것으로 예상되고 있다. 이러한 급속한 성장에 따라 무선인터넷 상거래의 안전성 문제가 함께 대두되고 있으며 이의 대응 방안으로 국내의 무선인터넷 보안기술연구가 활발히 진행 중에 있다. 무선인터넷에서의 정보 보호 서비스는 무선인터넷이 어떤 프로토콜을 기반으로 해서 동작하는지에 따라 제공 형태가 달라진다. 즉 WAP과 같이 새로운 프로토콜을 정의하는 경우에는 이에 적합한 새로운 정보보호 매커니즘이 개발되어야 하며, ME나 i-Mode와 같이 기존의 HTTP에 기반하는 경우에는 SSL (Secure Socket Layer)과 같은 유선인터넷에서 사용하고 있는 정보 보호 메커니즘의 수용이 가능하다. 이렇게 무선인터넷 솔루션은 〈표 1〉과 같이 크게 2가지 부류로 구분할 수 있다.[5]

표 1. 주요 무선인터넷 솔루션

구 분	WAP 기반	HTTP 기반	
		ME	i-Mode
기술언어	WML	M-HTML	C-HTML
전송 프로토콜	WSP/WTP/ WDP	HTTP	HTTP
브라우저	WAP 브라우저	Mobile Explorer	Compact NetFront
보안 메카니즘	WTLS	SSL	SSL

현재 HTTP에 기반한 방식은 마이크로소프트사의 ME(Mobile Explorer)와 NTT-Docomo의 i-Mode 서비스가 대표적이며, 다른 하나로는 WAP 포럼에서 개발을 주도하고 있는 WAP (Wireless Application Protocol)이 대표적이다. 사이버 증권, 온라인 쇼핑 등의 전자상거래 서비스를 무선상에서 원활히 제공하기 위해서는 유선인터넷과 마찬가지로 보안 문제가 우선적으로 해결되어야 하며 이

* 한국정보보호센터 전자서명 인증관리센터
** 연세대학교 컴퓨터과학과 교수

와 관련한 국제적인 표준화가 조속히 이루어져야 할 것이다. 이에 따라 본 고는 WAP을 위한 공개키기반구조 구축에 필요한 모델을 제시하고자 한다.

본 고는 다음과 같은 구성을 가진다. 2장에서 무선인터넷 보안을 위한 국내외 보안 기술 동향에 대해서 알아보고 3장에서는 국외 WAP 공개키기반구조 모델 현황을 4장에서는 WAP을 위한 공개키기반구조 구축에 필요한 전자서명인증 및 키 분배 모델을 제안하고, 마지막 5장에서 결론을 맺는다.

II. 국내·외 무선인터넷 보안 서비스 동향

이장에서는 국외 무선인터넷 보안업체인 Verisign, Baltimore, Sonera, Entrust 등에서 서비스하고 있는 무선 인증서비스 및 보안 솔루션에 대해 알아본다. 또한 국내 무선인터넷 접속 기술 및 보안 솔루션 개발 현황에 대해서도 알아본다.

1. 국외 보안기술 현황

현재 Verisign, Baltimore, Sonera, Entrust 등에서 WAP서버 인증서를 발급하는 서비스를 하고 있으며 무선 통신 사업자와 솔루션 제공업체, 인증기관이 상호 협력하여 무선 인증 서비스 및 보안기술개발을 활발히 추진 중에 있다.

1.1 베리사인(Verisign)

베리사인에서는 무선 인터넷용 WTLS서버인증서 ID를 판매하고 있으며, 이 인증서는 Motorola, Nokia, Phone.com의 WAP 서버에서 사용 가능하다. 이 제품은 기존의 유선 인터넷용 서버 인증서를 판매하고 있던 베리사인이 이를 WTLS용으로 수정하여 판매하는 것인데, 서버용 인증서의 형태로 Short-lived Mini Certificate를 제안하고 있다. 이는 클라이언트가 인증서 검증에 필요한 CRL을 참조하는 것이 무선환경에서는 쉽지 않으므로, 인증서의 유효기간을 유선에 쓰이는 CRL 주기와 비슷하게 발행함으로써 인증서의 상태검증을 대신하고자 하는 것이다.[1]

1.2 발티모어(Baltimore)

발티모어는 WAP 게이트웨이 서버와 전자서명 툴킷, 무선 PKI용 WAP CA를 개발하여 판매하고 있다. 현재 WAP에서의 무선 PKI 규격에 많은 제안을 하고 있으며, 제안하는 WAP을 위한 무선 PKI의 구조는 [그림 1]과 같다.[3]

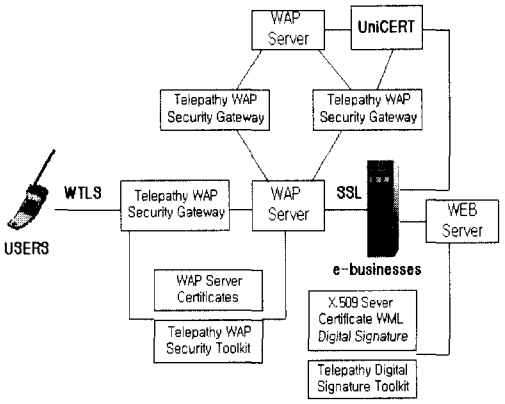


그림 1. Telepathy WAP Solution

Telepathy WAP 솔루션은 WAP 1.1 클라이언트와 서버 어플리케이션에서 정의되어진 WTLS 도구를 포함하고 어떤 네트워의 어플리케이션에도 WTLS 암호화 기능을 사용할 수 있게 해주며 기밀성과 무결성, 부인방지의 기능을 수행한다.

1.3 Sonera Smart Trust Solution

핀란드의 통신전문 회사인 Sonera는 무선 PKI 서비스 제품군과 이를 이용한 보안통신 솔루션을 개발하였다. Sonera가 제공하는 무선 PKI 서비스의 구조는 [그림 2]와 같다.[4]

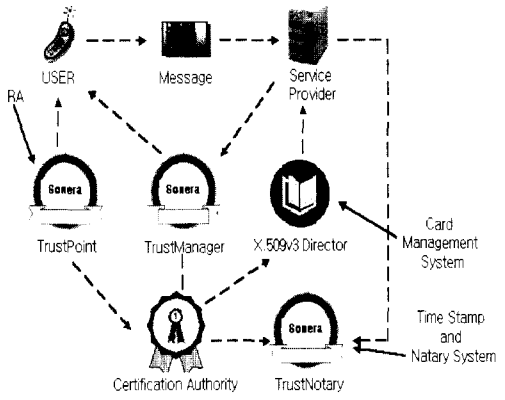


그림 2. Sonera PKI Solution

구성요소로서는 다음과 같다.

- TrustManager

S3 multi application smart card, GSM-SIM application 등 다양한 스마트카드를 지원하며 사용자, 서비스제공자, 이동전화 사업자들 간의 정보를 관리해준다. 이동전화사용자의 신분확인시 네트웍 ID로 확인한다.

- TrustPoint:Registration Authority Client

등록기관의 작업을 가능하게 해준다.

- TrustNotary

Sonera TrustNotary는 timestamp와 notary 서비스를 제공한다. timestamping을 받은 문서와 메시지는 참조를 위해 보관된다. 문서들은 Notary Service Web 사이트에서 전부 볼 수 있다.

1.4 Entrust(엔트러스트)

엔트러스트의 Mobile Solution은 WAP 서버용과 웹서버용 두 가지의 인증서를 상용서비스하고 있다. WAP과 GSM(Global System for Mobile Communications) 이동전화의 보안성을 발전시키는데 초점이 맞추어져 있으며, 개인 전자 장비나, e-commerce 서버, Beeper, 그리고 다른 이동장치도 포함한다.[2]

표 2. Entrust 무선 PKI 솔루션

Business	Services	Procucts
WAP Server 인증서	Entrust.net tm과 myEntrust.net tm(WAP 서버)	Entrust/PKI tm(WAP)
클라이언트 인증서	Entrust와 파트너 제공	Entrust/PKI tm (WAP Entrust/ AutoRA tm용
다른 어플리케이션을 위한 인증 제품	전문적인 서비스	Entrust/SecureControl tm
사업자 사이에 보안 네트웍이 필요할 때	엔트러스트와 파트너	Entrust/VPN, Entrust/Toolkit, Entrust Middleware Solution(BtoB용)
WTLS 어플리케이션	전문적인 서비스들	Entrust/Toolkit tm for WTLS

2. 국내 보안기술 현황

국내 무선인터넷 접속 기술은 크게 WAP계열과 ME계열로 나누어 볼 수 있다. SK텔레콤, 신세기 이동통신 및 LG텔레콤이 WAP 서비스를 제공하고 있으며 한국통신엠닷컴, 한국통신프리텔은 ME서비스를 제공하고 있다. 그러나 현재 제공되고 있는 무선 인터넷 서비스는 아직 PKI 서비스를 제대로 제공하지는 못하고 있는 실정이다. WAP계열 서비스의 경우 WTLS를 아직 적용하고 있지 않으며 ME의 경우는 한국통신엠닷컴이 주요 은행들과 SSL을 통하여 서비스 하고 있으나 보편적으로 이용되고 있지는 못하고 있는 실정이다. 하지만 무선 인터넷이 이슈가 되면서 [표 3]과 같이 많은 국내 업체들이 무선 인터넷을 위한 보안 제품을 개발 중에 있다.[5]

표 3.국내 무선 인터넷을 위한 보안 제품 개발 동향

회사명	주요개발내용
드림시큐리티	WTLS 구현 제품인 Trust-M 무선 CA 서버 개발 등
소프트포럼	MSSL 개발완료 (ME 적용)
MI시큐리티	WAP PKI 제품 개발중
이니텍	RSA사와 공동으로 WTLS 툴킷 개발중
시큐아이닷컴	무선 뱅킹, 무선 전자상거래 등에 필요한 에이전트 개발 중
K-Sign	WAP PKI 제품 개발 중

무선 인터넷이 활성화되기 위해서는 국내 무선 인터넷 PKI가 구축되어야 하며 이를 위한 기술규격 및 표준에 대한 개발, 관련제도 및 절차 개발, 평가기술 및 운용기술 개발 등이 이루어져야 하겠다.

Ⅲ. 국외 WAP공개키기반구조 모델

현재 WAP에서의 보안기능에는 WTLS(Wireless Transport Layer Security)세션을 이용해 Transport레이어에서 가입자와 서버간 암호채널을 생성하여 통신하는 방법과 WMLScript (Wireless Markup Language Script)를 사용하여 어플리케이션 레벨에서 보안을 구현하는 방법등이 있다. 이 장에서는 WAP 공개키기반구조 구축에 필요한 보안 요구사항에 대해서 알아본다.

1. WTLS Class 2 공개키기반구조 모델

WAP 전송 프로토콜 레이어상에서 작동하는 보안 프로토콜을 WTLS라고한다. WTLS를 통하여 Socket 레이어에서의 암호화와 MAC 방식의 무결성, 서버인증 및 가입자(단말기)와 게이트웨이간의 안전한 정보전송 기능을 제공한다. Class 2는 사용자 인증을 제공하지 않고 있다.[8][10]

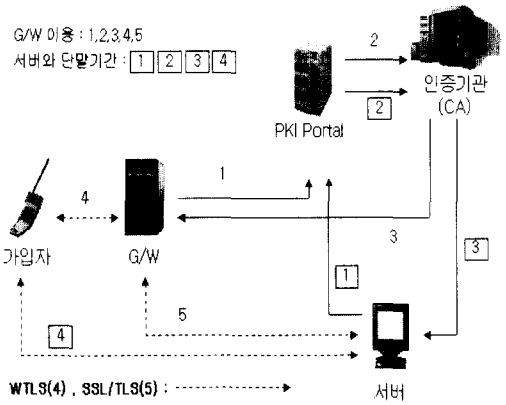


그림 3. WTLS Class2 PKI 모델

- G/W를 이용한 안전한 채널형성 방식(Two Phase Security)
  ① 게이트웨이는 인증서 발급에 필요한 키분배용키쌍과 인증서발급요청형식을 생성하여 PKI Portal에 보낸다.
  ② 등록기관은 게이트웨이의 ID를 확인하고 인증서요청형식을 인증기관에 보낸다.
  ③ 인증기관은 게이트웨이의 인증서를 게이트웨이에 보낸다.
  ④ 가입자(단말기)와 게이트웨이간 WTLS 세션을 형성한다. 이때 사용되는 암호화 알고리즘은 RC5(40,56,128), IDEA(40,56,128), DES (40,56), 3DES(168)등을 사용하고 해쉬알고리즘은 MD5, SHA1사용을 권고하고 있다.
  ⑤ 게이트웨이와 서버간 SSL/TLS세션을 형성한다.

- 서버와 단말기간에 직접적으로 이루어지는 안전한 채널형성방식(End to End Security model)
  ① 서버는 인증서 발급에 필요한 키분배용키쌍 인증서발급요청형식을 생성하여 PKI Portal로 보낸다.
  ② 등록기관은 서버의 ID를 확인하고 인증서발급요청형식을 인증기관에 전송한다.
  ③ 인증기관은 서버의 인증서를 서버로 보낸다.
  ④ 가입자(단말기)와 서버사이에는 WTLS 세션을 형성한다. (게이트웨이를 통한 라우팅만 될뿐 게이트웨이와 가입자 혹은 서버간 통신을 하지는 않는다.)

2. SignText 공개키기반구조 모델

WAP1.2에서는 전자서명 함수(SignedText)라는 WMLScritpt를 정의하여 어플리케이션 레이어에서 End-to-End 전자서명 기능을 제공하고 있다.[7][8][9]

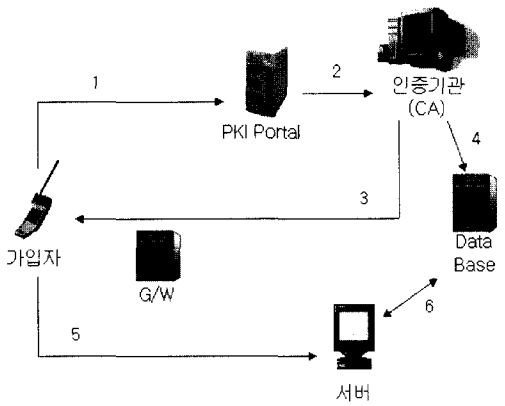


그림 4 SignText PKI 모델

① 가입자(단말기)는 인증서발급에 필요한 전자서명키쌍과 인증서발급요청정보를 생성하여 전자서명생성키로 서명한 후 등록기관에 보낸다. 키쌍 생성시 사용할 알고리즘은 RSA (Rivest, Shamir, Adleman), ECDSA (Elliptic Cu rve Cryptosystem)을 권고하고 있다. 키 길이는 RSA의 경우 1024bit 이상 ECDSA는 160 bit이상 사용을 권고하고 있다. 해쉬알고리즘은 SHA1 사용을 권고하고 있다.
② 등록기관은 가입자(단말기)의 ID를 확인하고 사용자의 인증서발급요청형식을 인증기관에 보낸다.

③ 인증기관은 가입자(단말기) 인증서(X.509 V3 인증서) 또는 WTLS인증서를 생성한 후 가입자(단말기)에게 인증서URL을 보낸다. (인증기관이 인증서전체를 가입자(단말기)로 보낼 시에는 WIM카드를 사용한다)

④ 인증기관은 가입자(단말기)의 인증서를 Database에 등록한다.

⑤ 가입자(단말기)는 전자문서를 서명 한 후 서명문서와 인증서URL을 서버에게 보낸다.

⑥ 서버는 가입자(단말기)로부터 받은 인증서URL를 통해 Database로부터 가입자(단말기)의 인증서를 가져온다.

현재 End-to-End의 전자서명은 단지 서명생성뿐이지 서명검증이나 암호화기능들에 대해서는 아직 정의하고 있지 않은 상태이고 이러한 기능은 향후 정의될 예정이다.[8] 인증서검증을 위해서 OCSP를 유력한 대안으로 보고 있으며 인증서 프로파일에 OCSP처리를 위한 필드를 별도로 두고 있다.[7]

Ⅳ. 국내 WAP 공개키 기반구조 모델

국내 무선환경에서의 WAP을 위한 전자서명 인증 및 키 분배 모델을 다음과 같이 제안한다.

1.WAP을 위한 전자서명인증 모델

WAP를 위한 전자서명인증 관련 기술규격 및 인증서 생성, 사용자의 인증서 처리시에 필요한 요구사항에 대해 알아보고 관련모델을 제안한다.[7][8][9]

1.1 인증서 발급신청 및 등록

가입자는 인증서를 발급받기 위해 지역적으로 분산된 등록기관에서 직접대면을 통한 신원확인을 하며 신원이 확인된 가입자는 등록기관으로부터 인증서 요청시 사용할 본인확인을 위한 참조코드(ID/Pas sword)를 부여받는다. 가입자는 자신이 서명에 사용하는 전자서명 생성키(Private Key)와 자신의 서명 검증에 사용하는 검증키(Public Key)를 생성한 후 전자서명 검증키와 개인 정보를 담은 인증서 발급요청정보를 작성하여 인증기관(등록기관)으로 발급 요청을 한다. 인증기관은 자신의 전자서명 생성키로 가입자의 전자서명 검증키에 대하여 서명함으로써 가입자인증서를 생성하여 가입자에게 인증서를 발행하게 된다.

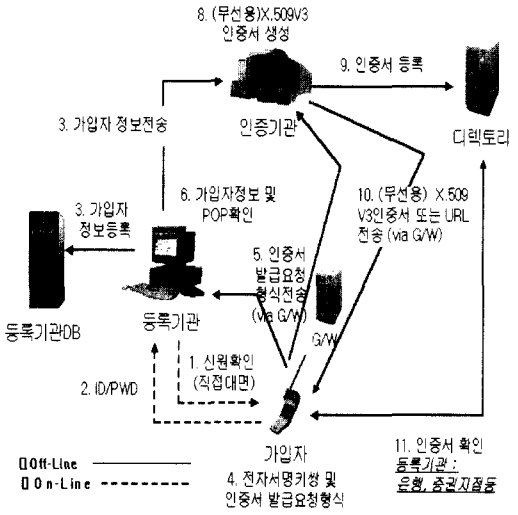


그림 5. (무선용)X.509V3인증서 발급신청 및 등록과정

1.1.1 인증서 등록절차

① 등록기관이 직접대면을 통해 사용자 신원확인을 한다.

② 등록기관이 사용자의 신원확인후 ID와 Password를 생성하여 사용자에게 전달한다.

③ 등록기관은 자신의 Database에 가입자를 등록하며 인증기관에 가입자 정보를 전송한다.

1.1.2 인증서 발급신청절차

① 가입자는 인증서발급에 필요한 전자서명키쌍 및 인증서발급요청정보를 생성한다. 키 쌍 생성시 사용할 전자서명 알고리즘은 현재 WAP과 국내 전자서명 알고리즘의 표준인 RSA (Rivest, Shamir, Ad leman) KCDSA (Korean Certificated Digital Signature Algorithem), ECDSA (Elliptic Curve Cryptosystem)을 사용할 것을 제안한다. 이 때 키 길이는 안전성을 고려하여 RSA와 KCD SA의 경우 1024bit이상을 사용하며 ECDSA의 경우는 160bit이상을 사용한다. 서명에 사용되는 해쉬 알고리즘은 안전성 및 국내외 표준을 고려하여HAS-160, SHA-1을 사용할 것을 제안한다. 인증서발급요청형식 생성과 관련해서는 가입자와 서버의 경우를 구분하여 정의할 수 있다. 가입자 경

우 RFC2511, PKCS#10, 또는 사용자가 보낸 발급요청 정보를 기반으로 등록기관(인증기관)이 대신 생성하는 세 가지 방법중 하나를 이용할 수 있으나 단말기 성능을 고려해 보면 등록기관(인증기관)이 대신 인증서발급 요청형식을 생성하는 세 번째 경우가 유력할 것이다. 서버의 경우는 PKCS#10, RFC 2511를 이용해 인증기관으로 직접 전송한다. 전자서명 생성키 저장은 가입자(단말기)인 경우 WIM카드를 사용할때는 WIM규격[9]을 따르고 소프트웨어를 사용할 경우는 PKCS #5[15]로 암호화하여 PKCS#8[16]형식으로 저장한다.

② 전자서명된 인증서요청정보를 받은 등록기관(인증기관)은 가입자의 전자서명 검증을 통해 실제로 전자서명 검증키에 대응하는 전자서명 생성키의 소유여부를 확인(Proof Of Possession)하고 가입자의 인증서요청형식을 인증기관으로 보낸다.

④ 인증기관은 (무선용)X.509V3인증서를 생성하여 자신의 디렉토리에 등록하고, 이를 사용자에게 직접전송하거나 혹은 등록기관을 통해 (무선용)X.509 V3인증서를 발급한다. 또는 인증서 대신 인증서를 획득할 수 있는 곳의 URL정보를 전송할 수도 있다. 이때 인증서의 DN규격은 WAP과의 호환, 현 유선과의 연동성을 고려하여 [표 4]의 DN규격 사용을 제안한다. 인증서의 규격은 [그림 6]과 같이 정의하고 있는 무선용 X.509V3인증서 규격과 유선의 X.509V3인증서 규격을 복수 기준으로 제안한다.[11][13][114]

표 4.무선 DN 속성 체계

속성	인식 여부	설명
commonName	□	객체명
serialNumber	□	일련번호
countryName	□	국가명(ISO 3166 코드)
stateOrProvinceName	□	도시명 또는 도명
organizationName	□	기관명
organizationUnitName	□	부서명 또는 기관 특성
domainComponent	□	
RFC2459 나머지 속성	△	

(□: MUST, △: SHOULD)

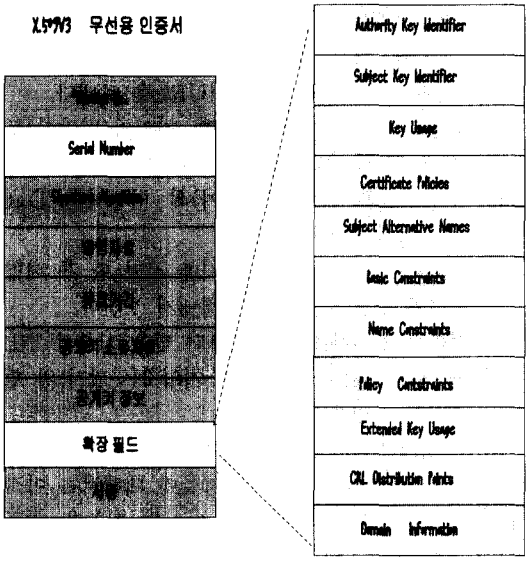


그림 6. 무선용 X.509V3 인증서

1.2 인증서 검증

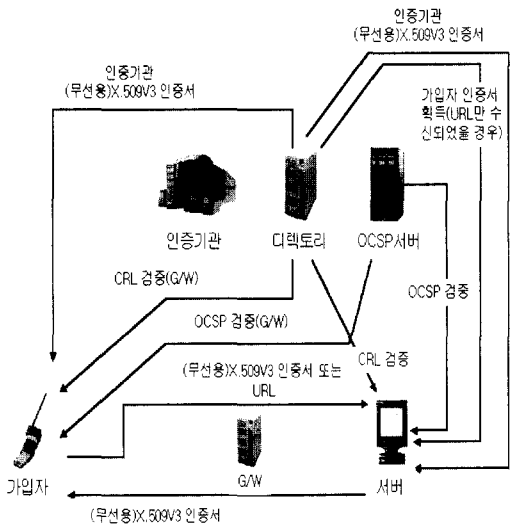


그림 7. (무선용)X.509V3 인증서 검증

1.2.1 가입자가 서버로부터 전송받은 인증서의 검증

서버는 자신의 인증서[(무선용)X.509V3]를 가입자(단말기사용자)에게 전송하고 가입자(단말기사용자)는 서버로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서폐지목록(X.509 CRL V2)를 통해 서버 인증서의 상태를 검증하거나 OCSP서버

등을 통해 인증서의 상태정보를 확인 할 수 있다. 현재 단말기의 전송성능을 고려해보면 CRL을 받는 것은 비효율적이며, 저장할 수 있는 메모리도 충분하지 못하다. 따라서 OCSP등을 이용하여 가입자(단말기 사용자)가 CRL 획득 없이도 쉽게 인증서의 상태 검증을 할 수 있어야 한다.

1.2.2 서버가 가입자(단말기사용자)로부터 전송받은 인증서 또는 URL의 검증

가입자(단말기사용자)는 자신의 인증서[(무선용)X. 509V3] 또는 인증서URL을 서버에게 전송한다. 서버는 가입자로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서폐지목록(X.509 CRL V2)를 통해 인증서의 상태를 검증하거나 OCSP서버를 통해 인증서의 상태정보를 확인 할 수 있다. URL을 받은 경우는 디렉토리로부터 인증서를 받아서 검증에 이용할 수 있다.

2. WAP을 위한 키분배용 모델

WAP을 위한 키 분배 관련 기술규격 및 인증서 생성, 사용자의 인증서 처리시에 필요한 요구사항에 대해 알아보고 관련모델을 제안한다.

2.1 인증서 발급신청 및 등록

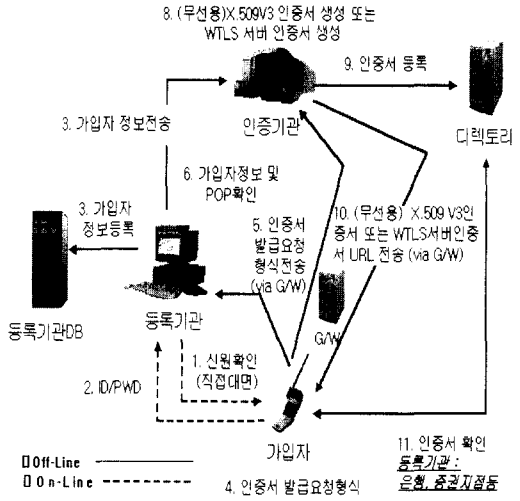


그림 8. 인증서 발급신청 및 등록과정

2.1.1 인증서 등록절차

① 등록기관이 직접대면을 통해 사용자의 신원확인을 한다.

② 등록기관이 사용자의 신원확인후 ID와 Password를 생성하여 사용자에게 전달한다.

③ 등록기관은 자신의 Database에 가입자를 등록하며 인증기관에 가입자의 인증서발급요청형식을 전송한다.

2.2.2 인증서 발급신청절차

① 가입자는 인증서발급에 필요한 키분배용키쌍 및 인증서발급요청정보를 생성한다. 키 분배 시 사용하는 알고리즘은 안전성 및 국내외 표준을 고려하여, RSA(Rivest,Shamir,Adleman), DH_KCDSA (Diffie-Hellman Korean Certificated Digita l Signature Algorithm), ECDH_ECDSA (Elliptic Curve Diffie-Hellman Elliptic Curve Digital Signature Algorithm)를 제안한다. 키 길이는 RSA와 DH_KCDSA의 경우는 768bit이상을 사용하고 ECDH_ECDSA의 경우는 160bit이상을 사용하는 것으로 한다. 인증서발급요청형식 생성시에는 가입자와 서버의 경우를 나누어서 정의한다. 가입자 경우 RFC2511, PKCS#10, 혹은 사용자가 보낸 발급요청 정보를 기반으로 등록기관(인증기관)이 대신 생성하는 세 가지 방법중 하나를 이용할 수 있으나 단말기 성능을 고려해보면 등록기관(인증기관)이 대신 인증서발급요청형식를 생성하는 세 번째 경우가 유력할 것이다. 서버의 경우는 PKCS #10, RFC2511를 이용해 인증기관으로 직접 전송한다. 키 저장은 가입자(단말기)인 경우는 WIM카드를 사용할때는 WIM규격[9]을 따르고 소프트웨어를 사용할 경우는 PKCS#5[15]로 암호화하여 PKCS#8[16]형식으로 저장한다.

② 전자서명된 인증서발급요청정보를 받은 등록기관(인증기관)은 가입자의 서명 검증을 통해 실제로 키 분배용 공개키에 대응하는 키 분배용 개인키의 소유여부를 확인(Proof Of Possession)한다.

③ 인증기관은 (무선용)X.509V3인증서 또는 WTLS 서버인증서를 생성하여 자신의 디렉토리에 등록하고, 이를 사용자에게 전송한다. 단말기 사용자에게는 인증서 대신 인증서를 획득할 수 있는 곳의 URL정보를 전송할 수도 있다. 이때 인증서의 DN규격은 〔표 4〕의 DN규격, 〔표 5〕의 WTLS 서버인증서 정의규격을 사용한다. 인증서는 〔그림 7〕의 WTLS 서버인증서, (무선용)X.509V3인증서를 사용할 것을 제안한다.

표 5. WTLS서버인증서DN정의규격(X.500과의 연계)

필드	연관된 X.500 속성
servicename	Organization Unit(OU)
organization	Organization (O)
country	Country(C)
commonname	Common Name(CN)
extension	〈type〉

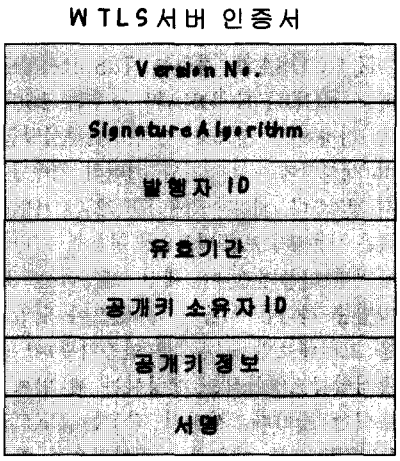


그림 9. WTLS 서버인증서

2.2 인증서 검증

2.2.1 인증서 검증(G/W를 이용하는 경우)

- 가입자가 G/W서버로부터 전송받은 인증서의 검증

G/W는 WTLS 서버인증서 또는 (무선용)X.509 V3서버인증서를 가입자에게 전송한다. WTLS서버인증서의 경우는 인증서의 최대 유효기간을 48시간 이내로 하여 매일 발행함으로써 가입자가 서버인증서의 상태검증을 대신한 것으로 간주한다. G/W서버로부터 받은 (무선용)X.509V3서버인증서를 검증할경우 디렉토리에 있는 인증서폐지목록(X.509V2)를 통해 인증서의 상태를 검증하거나 OCSP서버등을 통해 인증서의 상태정보를 확인 할 수 있다.

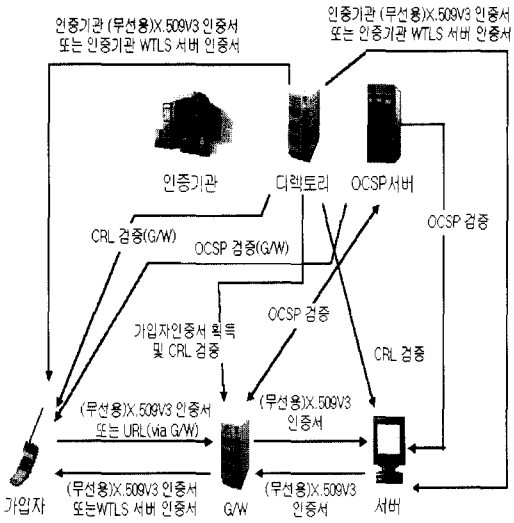


그림 10. 인증서 검증(G/W를 이용하지 않는경우)

- G/W서버가 가입자로부터 전송받은 인증서 또는 URL의 검증

가입자는 자신의 인증서〔(무선용)X.509V3〕 또는 인증서URL을 서버에게 전송한다. 서버는 가입자로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서폐지목록(X.509 CRL V2)를 통해 인증서의 상태를 검증하거나 OCSP서버등을 통해 인증서의 상태정보를 확인 할 수 있다. URL을 받은 경우는 디렉토리로부터 인증서를 받아서 검증에 이용할 수 있다.

- G/W서버가 서버로부터 전송받은 인증서의 검증

G/W서버는 서버로부터 받은 (무선용)X.509 V3 인증서를 검증한다. 이때 디렉토리에 있는 인증서폐지목록(X.509 CRL V2)를 통해 인증서의 상태를 검증하거나 OCSP서버등을 통해 인증서의 상태정보를 확인 할 수 있다.

- 서버가 G/W서버로부터 전송받은 인증서의 검증

서버는 G/W서버로부터 받은 (무선용)X.509 V3

인증서를 검증한다. 이때 디렉토리에 있는 인증서폐지목록(X.509 CRL V2)를 통해 인증서의 상태를 검증하거나 OCSP서버등을 통해 인증서의 상태정보를 확인 할 수 있다.

2.2.2 인증서 검증(G/W를 이용하지 않는 경우)

- 가입자가 서버로부터 전송받은 인증서의 검증

서버는 WTLS서버인증서 또는 (무선용)X.509V3 서버인증서를 가입자에게 전송한다. WTLS서버인증서의 경우는 인증서의 최대 유효기간을 48시간 이내로 하여 매일 발행함으로써 가입자가 서버인증서의 상태검증을 대신한 것으로 간주한다. 서버로부터 받은 (무선용)X.509 V3 서버인증서를 검증할 경우 디렉토리에 있는 인증서폐지목록(X.509 CRL V2)를 통해 인증서의 상태를 검증하거나 OCSP서버등을 통해 인증서의 상태정보를 확인 할 수 있다.

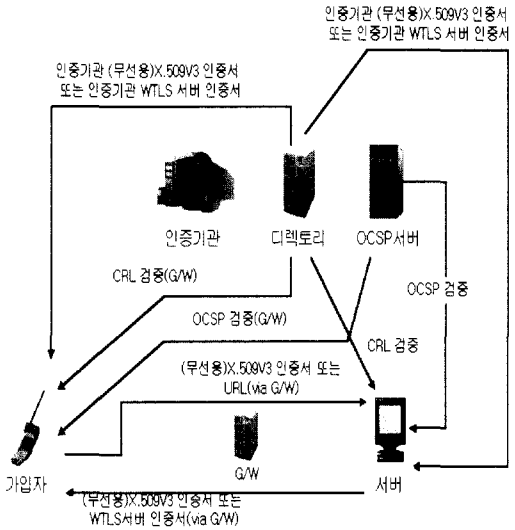


그림 11. 인증서 검증(G/W를 이용하지 않는경우)

- 서버가 가입자로부터 전송받은 인증서 또는 URL의 검증

가입자는 자신의 인증서[(무선용)X.509V3] 또는 인증서URL을 서버에게 전송한다. 서버는 가입자로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서폐지목록(X.509 CRL V2)를 통해 인증서의 상태를 검증하거나 OCSP서버등을 통해 인증서의 상태정보를 확인 할 수 있다. URL을 받은 경우는 디렉토리로부터 인증서를 받아서 검증에 이용할 수 있다.

V. 결 론

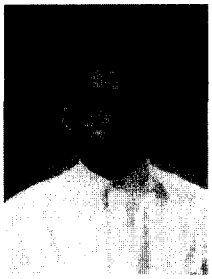
유선 인터넷과 마찬가지로 무선 인터넷을 이용하여 안전한 전자상거래 서비스를 제공받기 위해서는 기밀성, 무결성, 인증, 부인봉쇄 등의 정보보호서비스 제공이 필수적이다. 그러나 무선 인터넷 보안은 전세계적인 표준이나 기준이 완전히 확립되지 않아 경우에따라 업계가 자체적인 기준을 바탕으로 개발중이다. 따라서 본 고에서는 국내 WAP을 위한 공개키기반구조 모델을 제시함으로써 우리나라 무선 인증관리체계가 구축되어 나가는데 발생 할 수 있는 혼란을 최소화하고 무선 인터넷 인증 관련 기술의 발전과 응용 서비스를 활성화 하는데 기여하고자 한다. 본 고에서 제시한 모델은 유선 공개키기반구조와의 상호연동성도 최대한 고려하였으므로 유·무선 공개키기반구조 연동시에도 큰 도움이 되리라 생각하며 향후 관련된 무선보안기술을 개발하는데 있어서도 기여 할 수 있을 것으로 생각한다.

참 고 문 헌

[1] Verisign, http://www.verisign.com/ wireless/ index.html
[2] Entrust, http://www.entrust.net/wa pserver/ index.htm
[3] Baltimore, http://www.baltimore.co m/telepathy/ index.html
[4] Sorena, http://www.sonera.fi/englis h
[5] Internet&Comerce/기고/무선인터넷 시장현황과전망(1)(2)-http://www.itbiz.co.kr
[6] Mobile Internet Forum Korea 2000 conference(2000.9.26~9.27)
[7] WAP Forum Proposed Version 9-Mar-2000, WAP-211-X.509:WAP Certificate and CRL Profile
[8] WAP Forum Proposed Version 3- Mar-2000, WAP-217-WPKI,: Wire less Application Protocol Public Key Infrastructure Definition
[9] WAP Forum Version 18-Feb-2000, WAP-198-WIM, Wireless Application Protocol Identity Module Specification

[10] WAP Forum Version 18-Feb-2000 WAP-199-WTLS Wireless Application Protocol Wireless Transport Layer Security Specifi cation
[11] IETF RFC 2560(1999.6), X.509 Internet Public Key Infrastructure On-line Certificate Status Protocols : FTP and HTTP
[12] IETF RFC 2510(1999.3), Internet X.509 Public Key Infrastructure Certificate Management Protocols
[13] ITU-T Recommendation X.509 (19 97), Information technology-Open System Interconnection-The Directory : Authentication Framework
[14] IETF RFC 2459(1999), Internet X .509 Public Key Infrastructure Certificate and CRL Profile
[15] NIST/OSI Implementor's Work shop Publish Version(2.1:draft) 10-1999, PKCS#1, RSA Encryption Standard
[16] NIST/OSI Implementor's Work shop Publish Version(2.0) 3-1999, P KCS#5, Password-Based Encryption Standard
[17] NIST/OSI Implementor's Work shop Publish Version(1.2) 11-1993, PKCS#8, Private-Key Information Syntax Standard
[18] NIST/OSI Implementor's Work shop Publish Version(2.0) 2-2000, P KS#9, Selected Attribute Types
[19] NIST/OSI Implementor's Work shop Publish Version(1.0) 11-1993, PKCS#10, Certification Request Syntax Format
[20] NIST/OSI Implementor's Work sh op Publish Version(1.0) 6-1999, P KCS#12, Personal Information Ex change Standard
[21] ITU-T Recommendation X.520 (1997) | ISO/IEC 9594-6:1997, Information Technology Open Systems Interconnection The Directory : Selected Attribute types.
[22] 이재일, "무선인터넷을 위한 PKI 구축", 제 5회 정보보호 심포지엄, 한국정보보호센터 2000. 6
[23] 무선PKI(Public key Infrastructure) 기술기준(안) 한국정보보호센터 2000. 11

〈著者紹介〉



이 재 일 (Jae-Il Lee)

1986년 2월 : 서울대학교 계산통계학과 졸업
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월~1996년 6월 : 한국 IBM
1996년 7월~현재 : 한국정보보호센터 선임연구원/팀장
관심분야 : 유·무선 PKI, 전자상거래 보안

박 정 환 (Jung-Hwan Park)

1999년 2월 : 세종대학교 전산학과 졸업
1999년 2월~현재 : 세종대학교 전산학과 석사과정
2000년 9월~현재 : 한국정보보호센터 연구원
관심분야 : 무선 PKI, 전자상거래 보안,

송 주 석 (Song-Joo Seok)

1976년 2월 : 서울대학교 전기공학 졸업
1979년 2월 : 한국과학원 전기·전자 석사
1988년 2월 : Univ. of California at Berkeley 전산과학 박사
1979년 3월~1982년 2월 한국전자통신연구소 연구원
1989년 3월~현재 : 연세대학교 컴퓨터과학과 교수
관심분야 : 정보통신, 정보보호