무선 인터넷 환경에 적합한 PKI 기술 연구

이재일*, 정찬주*, 이용*, 송주석**

*한국정보보호진흥원, 전자서명인증관리센터
** 연세대학교, 컴퓨터과학과

A Study on the PKI technology for the Mobile Phone

Jae-il Lee*, Chanjoo Chung*, Yong Lee*, JooSeok Song**

*Korea Certification Authority Central, Korea Information Security Agency
**Department of Computer Science Yonsei Univ.

요 약

무선 단말기에서 인터넷 서비스를 제공하기 위한 인터넷 접속 프로토콜이 등장함에 따라 무선 인터넷 사용의 편리성과 특성에 대한 인식이 급속한 속도로 확산되고 있다. 무선 인터넷에서 전자상거래를 비롯한 데이터 서비스가 성공적으로 제공되기 위해서는 반드시 해결되어야 할 요소가 보안이다. 무선 인터넷의 안전한 전자상거래 서비스를 제공하기 위해서는 통신 정보에 대한 기밀성, 개체 인증 등의 정보보호를 위한 기능과 부인방지 기능 등을 제공해야 한다. 공개키기반구조 (Public Key Infrastructure, PKI)는 사용자에게 정보보호 기능과 부인방지 기능을 제공한다. 본 논문에서는 무선 인터넷 환경에 적용 가능한 공개키기반구조 적용 모델을 제안한다.

I. 서론

무선 단말기에서 무선 통신을 제공하기 위한 인터넷 접속 프로토콜이 등장함에 따라 무선 인터넷 사용의 특성과 편리성에 대한 인식이 급속한 속도록 확산되고 있다. 무선 인터넷이란 휴대형 단말기를 통해 무선으로 인터넷에 접속하여 인터넷 서비스를 이용하는 것을 말하며, 이는 사용자가 이동 중 무선망을 통하여 인터넷 서비스를 사용할 수 있는 기술을 말한다. 무선 인터넷은 유선 인터넷 환경의 시간, 공간적 제약을 극복할 수 있게 서비스 되고 있다.

무선 인터넷에서 전자상거래를 비롯한 데이터 서비스가 성공적으로 제공되기 위해서는 반드시 해결되어야 할 요소가 보안이다. 전자상거래 분야에 있어서 유선 인터넷과 마찬가지로 무선 인터넷이 안전한 전자상거래 서비스를 제공하기 위해서는 통신 정보에 대한 기밀성, 개체 인증 등의 정보보호를 위한 기능과 부인방지 기능을 제공해야 한다. 이러한 보안 요소들은 무선 단말기와 무선 인터넷 환경에 적용 가능한 기술이어야 하며 사용자에게 유선과 동일한 수준의 안전성을 제공할 수 있어야 한다.

기존의 무선 통신망에서 보안을 위해 사용되는 대부분의 알고리즘은 송·수신자 사이에 키 공유를 위한 사전 정보를 나눠 갖는 방식을 사용하고 있어, 다수의 사용자 환경에는 적용하기 어려운 문제점을 갖고 있다. 공개키기반구조 (Public Key Infrastructure, PKI)는 다수의 사용자 환경에서 공개키 암호방식을 사용하여 사용자의 공개키를 안전하고 신뢰성 있게 전달하는 수단을 제공한다.

무선 인터넷을 통한 전자상거래의 안전성을 보장하기 위해서는 무선 환경에 맞는 공개키기반구조에 대한 기술 개발이 필요하다. 이미 WAP (Wireless Application Protocol) 등의 대표적인 무선 인터넷 프로토콜에서도 보안을 위하여 공개키기반구조를 적용하고 있으며 이를 고려한 규격을 발표하고 있으나, 이는 아직까지 안전한 전자상거래의 제공에 필수적인 단대단 보안을 제공하지 못하고 있다[1][2].

본 논문에서는 무선 인터넷에 적용 가능한 공개키기반구조 적용 모델 제안과 기술들을 소개한다.

2장에서는 현재 제공되고 있는 무선 인터넷 프로토콜과 그 문제점을 제시한다. 3장은 무선 인터넷에 공개키기반구조를 적용할 경우 고려해야 할 사항들을 설명하고, 4장에서는 공개키 인증서 프로파일, 적용 가능한 알고리즘 등 무선 인터넷에 적용 가능한 무선 PKI 기술과 특징들을 설명하고, 5장에서 결론을 맺고자 한다.

II. 무선 인터넷 프로토콜

무선 인터넷은 유선 인터넷과 달리 여러 가지 제약성을 가지고 있다. 무선 단말기의 경우 PC와 같은 계산능력과 저장능력을 가지고 있지 않으며 무선 통신은 유선보다 낮은 데이터 전송률과 높은 에러률을 갖는다. 또한 화면크기, 배터리, 기억용량 등의 많은 문제점이 존재한다. 이러한 무선 환경의 제약성을 극복할 목적으로 무선 인터넷을 위한 새로운 기술들이 개발되고 있다.

현재 무선 인터넷 접속을 위한 기술은 WAP 포럼에서 기존의 유선 인터넷 프로토콜인 HTTP (HyperText Transport Protocol)에 기반하지 않고 새로이 개발한 WAP과 기존 HTTP를 무선환경에 맞게 수정하여 무선 데이터 서비스를 제공하는 마이크로소프트사의 ME (Mobile Explorer) 및 NTT-Docomo의 I-mode가 대표적이다[3]. 본 장에서는 WAP과 ME 방식에 대하여 알아본다.

1. WAP 방식

WAP은 WAP 1.x에 이어 WAP 2.0을 발표하였고[4], 현재 무선 인터넷에 적용되고 있는 것은 WAP 1.x이다. WAP 1.x에서는 무선망과 기존의 유선 인터넷망의 연동을 위하여 중간에 게이트웨이를 두고 있다. 사용자의 단말기와 게이트웨이 사이는 WAP에서 정의된 프로토콜로 통신이 이루어지고 게이트웨이와 유선 인터넷망은 기존의 인터넷 통신 프로토콜인 HTTP로 통신이 이루어진다.

WAP 1.x의 보안은 유선 인터넷의 SSL (Secure Socket Layer)에 대응하는 WTLS (Wireless Transport Layer Security)에 기반하고 있다[5][6]. WTLS는 IETF의 TLS (Transport Layer Security)를 기반으로 무선 환경에 적합하도록 개발된 보안 프로토콜이다[7]. WTLS는 단말기의 성능을 고려하여 여러 가지 관련 파라미터의 길이를 줄였으나 TLS을 기본으로 적용하였기 때문에 SSL 구조와 큰 차이가 없다.

WAP의 WTLS는 TLS와 거의 동일한 서비스를 제공하지만 단대단 보안은 제공하지 못하고 있다. WAP 서비스를 위해서는 중간의 게이트웨이를 거쳐야 하는데 WTLS구간에서 암호화된 데이터는 게이트웨이에서 복호화된 후 SSL로 다시 암호화되어 서버에 전달된다. 반대로 SSL로 암호화된 데이터는 게이트웨이에서 복호화된 후 WTLS로 다시 암호화하여 단말기에 전달된다. 이것은 게이트웨이의 보안에 문제가 생길 경우 심각한 보안의 취약점이 될 수 있다.

WAP 포럼에서는 다음 사항을 고려하여 WAP PKI 모델을 결정하였다.

- o 유선 PKI와의 변화를 최소화
- o 인증서 경량화를 고려한 무선용 인증서 채택
- o 인증서 검증 메커니즘 경량화
- o 인증서 폐지 목록 경량화를 위한 Short-lived 인증서 메커니즘 채택

WAP PKI 모델에서 서버 인증서는 WTLS 인증서를 사용하고 반면에 클라이언트 인증서는 X.509v3 인증서를 사용한다. 그러나 X.509v3 인증서가 클라이언트에게 보내지거나 클라이언트에 저장되지는 않는다. WAP PKI 모델은 그림 1과 같이 정의된다[2].

- o 디바이스에 저장되는 서버와 Root CA 인증서는 WTLS 인증서를 사용
- o 서버에 저장되는 클라이언트 인증서(WTLS와 응용을 위한)와 Root CA 인증서는 X.509v3 인증서[8]
- o OTA (Over-The-Air)를 통해 보내지거나 WAP 클라이언트 디바이스에 저장되는 클라이언트와 Root CA 인증서는 WAP Profile의 X.509v3 인증서
- o X.509v3 인증서가 OTA를 통해 전달되는 것을 원치 않을 경우 디바이스에는 인증서 URL을 저장[2]
- o 디바이스에 WIM과 같은 디바이스가 제공되지 않는다면, X.509v3 클라이언트 인증서를 저장하지 않음

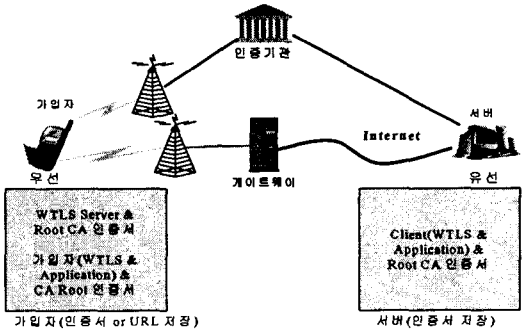

그림 1: WAP PKI 모델

2. ME 방식

ME는 마이크로소프트사에서 개발한 무선 단말기용 브라우저로 HTML 언어 전체를 사용하지 않고 일부만을 사용하므로 일반 HTML 브라우저에서 지원되는 모든 것들을 지원하지 않지만 기존의 컨텐츠를 사용할 수 있어 호환성이 뛰어나다. 내부적으로 기존 HTTP 방식과 호환이 되도록 HTML을 축약한 m-HTML을 사용하고 보안 메커니즘은 유선의 SSL을 사용하고 있다.

마이크로소프트사와 퀄컴사가 제휴하여 추진하고 있는 스팅거 프로젝트는 현재의 인터넷 표준을 지원함으로써 기존의 HTML 컨텐츠를 그대로 사용할 수 있어 호환성이 뛰어나다. 무선 구간을 위한 별도의 프로토콜을 정의하지 않고, 기존 TCP기반의 솔류션을 그대로 이용함으로써 유선 인터넷에서 사용된 기술을 그대로 적용하는 것이 가능하다.

Ⅲ. 무선 PKI 적용 시 고려사항

무선 인터넷 시스템의 경우 네트워크의 문제(낮은 대역폭, 시간 지연, 연결의 불안전성 등) 및 디바이스의 문제(낮은 연산 능력의 CPU, 적은 메모리, 배터리 시간, 작은 디스플레이, 입력 장치 등)로 현재의 유선 인터넷에서 이용되는 프로토콜을 무선 단말기에 그대로 적용하기에는 많은 문제점이 있다.

핸드폰과 같은 무선 단말기를 사용하는 무선 인터넷 환경에서 유선 인터넷 수준의 보안을 제공하기 위해 충족되어야 하는 요구사항을 다음과 같이 정의하여 보았다.

o 요구사항 1-무선에 적합한 PKI 모델 설계

무선 인터넷 환경에 맞는 인증서 검증 방식을 채택하여 처리율이 떨어지는 무선 단말기에서 인증서를 검증할 수 있도록 하여야 함. 무선 단말기의 CPU가 처리해야 할 데이터를 최소화하여 단말기 CPU의 처리 능률을 향상시키고, 무선 단말기 CPU에서 처리 가능한 서명, 검증, 암호화 알고리즘을 채택하여 무선 PKI 서비스의 효율성을 향상

o 요구사항2-무선 환경에 맞게 프로파일 및 알고리즘 등을 최적화

무선 단말기에서 처리 가능한 인증서, CRL (Certificate Revocation List) 프로파일 규격 및 사용되는 알고리즘 등의 최적화를 통하여 모듈 크기를 최소화

o 요구사항3-무선상에서 전송되는 데이터의 크기를 최소화

무선 단말기의 CPU가 처리해야 할 데이터를 최소화하여 단말기 CPU의 처리 능률을 향상

o요구사항 4-무선 환경에 적합한 프로토콜 설계

인증서의 발급, 저장, 처리, 검증 등에 필요한 프로토콜을 무선 단말기 환경에 맞도록 최적화하여 처리 시간을 단축

o요구사항 5-유선 PKI와의 상호연동 고려

유선 PKI와의 상호연동을 고려하여 설계

o요구사항 6 국제 호환성 고려

국제 표준을 준용함으로써 향후 국제 호환성을 갖도록 설계

Ⅳ. 제안하는 WPKI 구조

본 장에서는 무선 환경에서 유선과 같은 안전성을 제공하기 위하여 3장에서 언급한 요구사항을 만족하는 무선 PKI 모델을 제안한다. 제안하는 PKI 모델, 기술 및 특징에 대하여 소개한다.

1. 무선 PKI 모델

WAP 포럼의 WPKI는 WTLS 스택을 사용하여 단대단 보안을 제공하지만, 제안하는 모델에서는 WTLS을 사용하지 않고 기밀성을 제공하기 위하여 응용계층에서 보안 기능을 제공한다[2][6]. 제안하는 모델의 가입자의 장비는 이동 전화기(핸드폰, PDA 등), 컨텐츠 제공자(Content Provider) 장비는 서버를 주요 모델로 가정한다. 단말 가입자(User)간의 통신은 제외하며, 단말 가입자와 컨텐츠 제공자(CP)간의 통신을 기본 모델로 정의한다. 제안하는 모델은 최상위 인증기관, 인증기관 그리고 가입자를 각각의 계층으로 갖는 3레벨 구조를 기본 모델로 가정한다.

단말 가입자는 통신하는 상대방의 인증서에 대한 유효성 검증을 수행한다. PKI에서 인증서 검증은 반드시 수행되어야 하고 신뢰성을 판단하기 위한 중요한 요소이다. 단말기의 부담을 줄이기 위하여 인증서 상태 검증OCSP 서버를 통한 인증서 상태 검증을 기본 방식으로 채택한다. 제안하는 WPKI 모델은 그림 2와 같다.

2. 인증서 및 CRL 프로파일

제안하는 무선 PKI 모델에서 사용되는 인증서 및 CRL 프로파일은 인증기관과 가입자용으로 분류할 수 있다. 인증기관의 경우 전자서명용 X.509v3 인증서 프로파일과 암호용 WTLS 인증서 프로파일이 있다. 가입자의 경우 전자서명용 X.509v3 인증서와 암호용 X.509v3인증서(단말 가입자, 컨텐츠 제공자) 및 WTLS 인증서 프로파일(컨텐츠 제공자)이 존재한다[8][9].

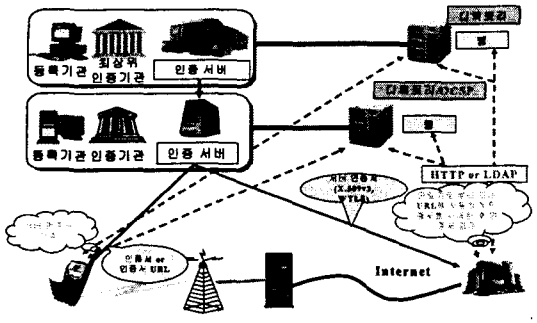

그림 2: 제안하는 WPKI 모델

인증기관 인증서와 가입자 인증서의 기본필드는 X.509v3 필드와 동일하다.

무선 전자서명 인증서 프로파일에서는 단말기에서 인증서 처리 부담을 감소시키고자 확장필드 중에서 잘 사용도지 않고 있는 기관키 식별자(Authority Key Identifier)와 주체 키 식별자(Subject Key Identifier) 필드 처리를 선택으로 정의하였다[8]. 또한 인증서 검증과 관련하여 OCSP 서버를 통한 인증서 상태 확인 기능을 제공하기 위하여 기관 정보 접근 (Authority Information Access, AIA) 필드와 도메인 정보 (Domain Information, DI) 필드를 추가하였으며, 이를 통하여 단말기에서 온라인 인증서 상태 확인 프로토콜 (Online Certificate Status Protocol) 기능을 제공할 수 있도록 하였다[8][11]. DI 필드만을 사용하는 경우에 URL 정보를 제공할 수 있는 방법이 제공되지 않는 문제점이 있어 IETF private 확장인 AIA 필드를 통해 OCSP 서버 위치 정보를 제공하도록 정의하였다[9].

무선 단말기가 전체 CRL을 가지고 와서 인증서 상태를 검증하기에는 CRL의 크기가 커서 부담이다. 이를 해결하기 위한 방식으로 CRL을 분할하여 최신의 CRL을 구성하는 Delta-CRL 방식과 여러 개의 CRL-DP 를 사용하는 방식이 있다[12]. WTLS 인증서 프로파일은 단말기에서 인증서 상태 확인의 부담을 줄이기 위하여 short-lived WTLS 인증서를 사용할 수 있도록 정의하였다[9].

3. 전자서명 알고리즘

무선 단말기에서 RSA 1024bit 키 쌍을 생성하는 모듈은 CPU에 상당한 처리 부담을 주며, 이로 인하여 시간 지연에 따른 통신 중단의 문제점을 갖고 있다[12]. 제안하는 모델에서는 ECC 기반의 알고리즘을 채택하여 RSA 키 생성 문제를 해결하고자 하였으며, RSA 1024bit의 안전성에 준하는 타원곡선에 기반하는 163bit 키 쌍을 사용하는 것으로 정의한다. 무선 단말기에서 효율적인 전자서명 알고리즘으로 ECDSA 알고리즘을 정의하였고 [13], 추후 유선과의 연동성, USIM 등의 스마트 카드 및 단말기 성능 향상에 따라 RSA도 사용 가능하도록 RSA 전자서명도 정의하였으며, RSA 전자서명 검증은 가능하도록 설계하였다.

이에 따라, ECC 기반의 구현은 필드(GF(p), GF(2m) 및 GF(pm)마다 커브가 다양하고, 하나의 필드에서 다양한 커브들을 파라미터 값만 변경하여 동일 모듈로 구현하는 경우에는 메모리 크기 및 인증서에서 공개키 값 정보를 표기하는 방식이 달라지는 문제점이 있다. ECC 커브는 Basic 커브이면서 named 커브만을 선택하였다. 선택된 basic 커브는 3레벨 모두에서 생성 및 검증할 수 있도록 정의하였다. 국제 표준으로 공인된 커브를 사용함으로써 국제적 호환성을 제공한다.

4. 무선 인증서 요청 및 관리 프로토콜

제안하고자 하는 무선 인증서 요청 및 관리 프로토콜은 무선 단말기에 적용할 수 있을 정도로 최적화하여야 한다. 현재 유선 상의 관련 프로토콜은 구현 시 그 크기문제로 인하여 휴대폰과 같은 무선 단말기에 그대로 적용할 수 없는 문제점이 존재한다[14][15]. 또한 WTLS 게이트웨이 보안 문제를 해결하기 위해서는 응용계층에서 단대단 보안을 제공해야만 한다. 이를 위해 제안하는 인증서 요청 및 관리 프로토콜에서는 사용자 인증과 POP (Proof Of Possession)를 동시에 해결할 수 있는 요청형식을 참조번호, 인가코드 기반의 해쉬 함수를 통하여 구성한다. 해쉬 함수를 사용하여 인가코드의 기밀성을 제공하며, POP 및 인증을 SignText 함수에 기반한 전자서명으로 제공한다[10]. 표 1은 인증서 요청 및 관리 프로토콜 메시지 형식의 예이다.

표 1: 무선 인증서 요청 및 관리 프로토콜 메시지

분류	메시지 형식	서명되는 메시지
신규	M=type|PK|ID, N=PW	M|H(M,N)
재발급	M=type|PK_{new}|ID_{new}, N=PW_{new}	M|H(M,N)
갱신(키)	M=type|PK_{new}, N=nonce|SignValue	M|N
갱신	M=type|CN, N=nonce	M|N
효력정지	M=type|CertificateHold, N=nonce	M|N
폐지	M=type|ReasonCode	M

※ 자세한 표기 형식은 참고문헌 [16] 참조

제안하는 무선 인증서 요청형식 및 관리 프로토콜은 WAP Crypto Library에서 정의한 SignText 함수를 WTLS 인코딩 및 디코딩 기술을 이용하여 구현하였기 때문에 단말기 구현 코드 크기를 유선의 CMP를 구현하는 것보다 상당히 줄일 수 있다는 장점을 가지며, 3장의 요구사항 4를 만족한다.

5. 인증서 검증

제안하는 무선 PKI 모델의 검증은 무선 단말기에서 서버 인증서 검증 방식과 컨텐츠 제공자(Content Provider, CP) 서버에서 단말기 인증서 검증 방식으로 분류된다. 무선 단말기에서 서버 인증서 검증은 CP 가 보내준 최상위 인증기관 ARL 및 CP 인증서를 이용하여 인증서 경로 구축을 한다. 유선 환경에서는 최하위 계층의 하나의 인증서를 이용하여 인증서 경로를 구축하지만, 무선 단말기에서는 유선의 CP 에게 인증서 경로 구축의 일부분을 위임 구축하여 인증서 경로 구축시 CA와 여러 번 통신해야 하는 통신회수를 줄이고, 그리고 이와 관련하여 검증request 및 response 메시지를 생성 또는 처리해야 하는 CPU의 부담 등을 낮추어 무선 단말기의 처리 부담을 줄인다.

무선 인증서 경로 검증은 유선 인증서 경로 검증에 비해 다음과 같은 특징을 갖는다. 그림 3은 유선 및 무선 가입자의 인증서 검증 과정을 비교한 것이다.

o 무선 단말기는 인증서 수신에 따른 대역폭의 낭비를 막기 위하여 최상위 인증기관 인증서를 사전에 보유

o 최상위 인증기관 전자서명키 신뢰성을 확보하기 위하여 최상위 전자서명키 해쉬값 (Trusted Certificate Information)을 볼 수 있는 기능을 제공

o CP 는 무선 단말 가입자에게 최상위 인증기관의 ARL 및 CP의 인증서를 전달함으로써 3단계 정도의 통신회수를 줄인다.

o OCSP를 이용하여 인증서 상태 정보를 전달 [16]

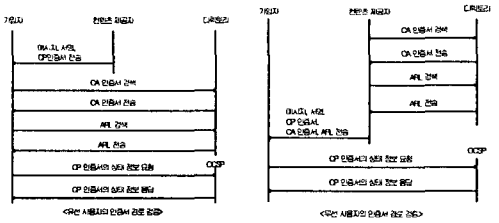

그림 3: 유선 및 유선 인증서 검증 과정 비교

CP는 인증서 검증을 위하여 무선 단말기로부터 전달 받은 URL 정보를 통하여 인증서를 다운로드 받아 인증서 경로를 구축하며, 이후의 과정은 유선 PKI에서 인증서 검증과정과 동일하다.

V. 결론

본 논문에서는 유선 PKI에서 제공하는 모델과 WAP 포럼에서 제시하는 WPKI 모델의 특징을 적용하여 무선 환경에 최적화된 무선 PKI 모델을 제안하였고, 효과적인 인증서 프로파일, 알고리즘 검증 기술에 대하여 제안하였다. 제안하는 무선 PKI 기술은 무선 환경 기반의 응용 서비스 개발에 적용할 수 있으며, 특히 안정적이고, 신뢰할 수 있는 서비스를 제공할 것으로 기대된다.

참고문헌

[1] WAP Forum, Wireless Application Protocol Architecture Specification, WAP-210-WAPArch-20010712.

[2] WAP Forum, Wireless Application Protocol Public Key Infrastructure Definition, WAP-217-WPKI.

[3] Microsoft Press, Microsoft Introduces Microsoft Mobile Explorer, http://www.microsoft.com/presspass/1999/Dec99/MobileExplorerPR.asp.

[4] WAP Forum, "Wireless Application Protocol WAP2.0 Technical White Paper", http://www.wapforum.org/what/WAPWhite_Paper1.pdf.

[5] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.

[6] WAP Forum, Wireless Transport Layer Security, WAP-261-WTLS-20010406-a.

[7] IETF RFC2246, The TLS Protocol Version 1.0.

[8] IETF RFC3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[9] WAP Forum, WAP Certificate and CRL Profiles, WAP-211-WAPCert.

[10] WAP Forum, WMLScript Crypto Library, WAP-161-WMLScriptCrypto-20010620-a.

[11] IETF RFC2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

[12] NIST/OSI Implementers Workshop Publish Version (2.1:draft) 10-1999, PKCS#1, RSA

Encryption Standard
[13] NIST, Digital Signature Standard (DSS): FIPS 186-2, Jan 27, 2000.
[14] IETF RFC2511, Internet X.509 Certificate Request Message Format.
[15] IETF RFC2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols
[16] 한국정보보호진흥원, 무선 PKI 기술규격 v1.21, 2001.8, http://www.rootca.or.kr