

WAP을 위한 공개키기반구조 기술 기준
- 키분배 -

Public Key Infrastructure Technical Specification For WAP
- Key Distribution -

2001. 08(Ver1.5)

한국정보보호진흥원

<목 차>

1. 기준명	1
2. 기준의 개요	1
2.1 목적	1
2.2 적용범위 및 기대효과	1
2.3 내용 요약	1
2.4 참조권고	2
3. 약어	3
4. 키분배용 무선인터넷 PKI 기술 기준	3
4.1 키분배용 PKI 모델	3
4.2 키분배용 인증서 관련 기준	9
4.3 알고리즘	14

<그림 차례>

[그림 1] 무선 키분배용 X.509V3 인증서 발급신청 및 등록과정(안1)	4
[그림 2] 무선 키분배용 X.509V3 인증서 발급 및 등록과정(안2)	5
[그림 3] 무선 키분배용 인증서 검증과정(안1)	6
[그림 4] 무선 키분배용 인증서 검증과정(안2)	8
[그림 5] 인증서 비교	10

<첨부차례>

첨부 1. 무선 키분배용 X.509V3 인증서 프로파일	19
첨부 2. 무선 키분배용 X.509V2 인증서 효력정지 및 폐지목록 프로파일	21
첨부 3. 무선 키분배용 WTLS 인증서 프로파일	22
첨부 4. 무선 키분배용 X.509V3 인증서 DN 규격	23
첨부 5. 무선 키분배용 WTLS 인증서 DN 규격	25
첨부 6. WPKI URL 이용 사용자 인증서 획득법	27
첨부 7. 무선 키분배용 인증서 기술 기준(표)	28

1. 기준명

WAP을 위한 공개키기반구조 기술 기준 - 키분배 -
Public Key Infrastructure Technical Specification For WAP
- Key Distribution -

2. 기준의 개요

2.1 목적

무선인터넷의 키분배용 인증서 생성·처리 및 관련 기술 규격을 정의한다.

2.2 적용범위 및 기대효과

본 기준은 무선인터넷의 키분배용 공개키기반구조 모델, 인증서 및 알고리즘 관련 기준을 정의하고 있으며 인증기관 및 응용 프로그램의 인증서 생성·처리시 요구사항들을 명시하고 있다.

국내 무선인터넷 키분배용 기술기준을 정의함으로써 무선 인터넷 공개키기반구조 인증 관련 기술의 발전과 관련 응용 서비스 활성화에 기여할 것이다. 또한 전자상거래에 대한 신뢰성을 확보하여 전자상거래 시장을 자연스럽게 활성화시켜 나갈 것이다.

이 기준은 전자서명 인증관리체계내에서 무선인터넷상의 키분배를 위한 권고로 사용될 것이다.

2.3 내용 요약

한국정보보호센터는 무선 공개키기반구조를 구축을 추진하기 위해 3개 공인인증기관, 한국전자통신연구원, 이동통신서비스업체, 단말기 제조업체와 협의하여 키분배를 위한 키분배 기술기준을 개발하였다.

본 기준의 주요 내용은 무선 인터넷에서의 키분배 관련 기술기준으로서 인증서 생성 및 사용자의 인증서 처리시에 필요한 요구사항에 대한 내용을 기술하고 있다.

이 기준은 WAP Forum에서 제안한 WAP 인증서 및 인증서폐지목록 프로파일 (WAP-211-X.509), WAP 공개키기반구조 (WAP-217-WPKI), WAP WTLS (WAP-199-WTLS)에 기반을 두어 무선환경의 특성을 반영하여 기술되었다.

2.4 참조권고

- WAP Forum Proposed Version 9-Mar-2000, WAP-211-X.509 : WAP Certificate and CRL Profile
- WAP Forum Proposed Version 3-Mar-2000, WAP-217-WPKI, : Wireless Application Protocol Public Key Infrastructure Definition
- WAP Forum Version 18-Feb-2000, WAP-198-WIM, Wireless Application Protocol Identity Module Specification
- IETF RFC 2560(1999,6), X.509 Internet Public Key Infrastructure Online Certificate Status Protocols : FTP and HTTP
- IETF RFC 2510(1999,3), Internet X.509 Public Key Infrastructure Certificate Management Protocols
- ITU-T Recommendation X.509(1997), Information technology - Open System Interconnection - The Directory : Authentication Framework
- IETF RFC 2459(1999), Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- NIST/OSI Implementor's Workshop Publish Version(2.1:draft) 10-1999, PKCS#1, RSA Encryption Standard
- NIST/OSI Implementor's Workshop Publish Version(2.0) 3-1999, PKCS#5, Password-Based Encryption Standard
- NIST/OSI Implementor's Workshop Publish Version(1.2) 11-1993, PKCS#8, Private-Key Information Syntax Standard
- NIST/OSI Implementor's Workshop Publish Version(2.0) 2-2000, PKCS#9, Selected Attribute Types
- NIST/OSI Implementor's Workshop Publish Version(1.0) 11-1993, PKCS#10, Certification Request Syntax Format
- NIST/OSI Implementor's Workshop Publish Version(1.0) 6-1999, PKCS#12, Personal Information Exchange Standard
- ITU-T Recommendation X.520 (1997) | ISO/IEC 9594-6:1997, Information Technology Open Systems Interconnection The Directory: Selected Attribute types.

3. 약어

본 기준에서는 다음의 약어들이 적용된다.

- 가) CA : Certification Authority, 인증기관
- 나) CRL : Certificate Revocation List, 인증서 효력정지 및 폐지목록
- 다) CMP : Certificate Management Protocol, 인증서 관리 프로토콜
- 라) DN : Distinguished Name, 고유 이름
- 마) DER : Distinguished Encoding Rules, 인코딩 규칙
- 바) HTTP : Hypertext Transfer Protocol, 인터넷 전송 프로토콜
- 사) LDAP : Lightweight Directory Access Protocol,
- 아) OCSP : Online Certificate Status Protocol, 접속 인증서상태 프로토콜
- 자) POP : Proof of Possession, 소유 증명
- 카) PEM : Privacy Enhanced Mail, 인코딩 규칙
- 타) RA : Registration Authority, 등록기관

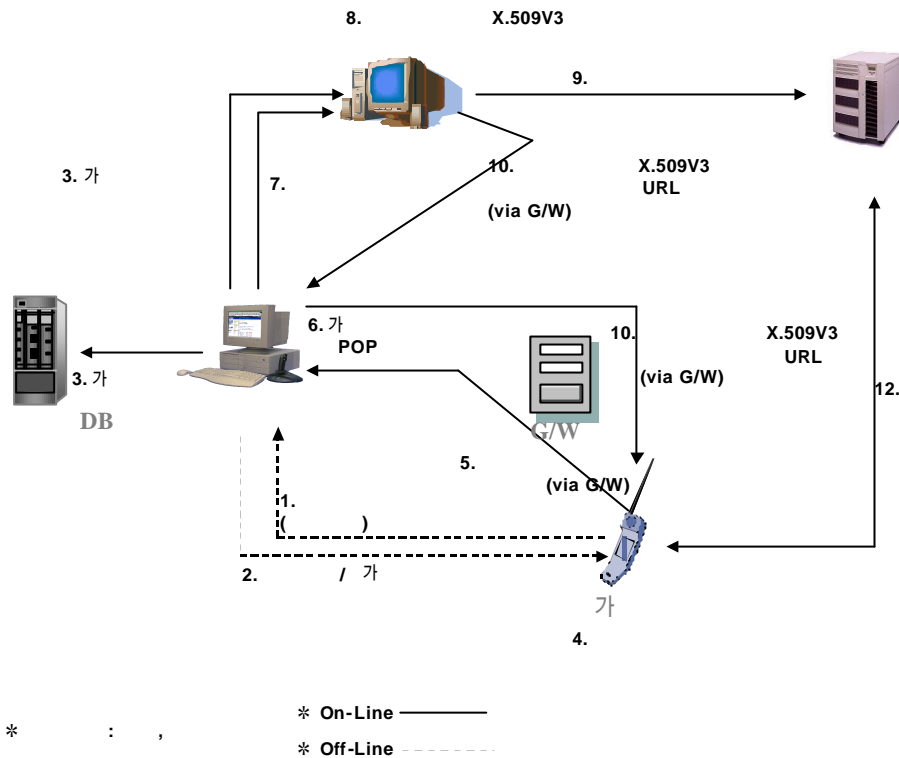
4. 키분배용 무선인터넷 PKI 기술 기준

4.1 키분배용 PKI 모델

4.1.1 인증서 발급신청 및 등록과정

가입자는 키분배용 인증서를 발급받기 위해 지역적으로 분산된 등록기관에서 직접 대면을 통한 신원확인을 하며 신원이 확인된 가입자는 등록기관으로부터 인증서 요청시 필요한 참조번호/인가코드(ID/Password)를 부여받는다. 가입자는 자신이 키분배를 위해 사용하는 키분배용 개인키(Private Key)와 키분배용 공개키(Public Key)를 생성한 후 개인 정보를 담은 무선 인증서 발급요청형식을 작성하여 인증기관(등록기관)으로 발급 요청을 한다. 인증기관은 자신의 전자서명생성키로 가입자의 키분배용 공개키에 대하여 서명함으로써 가입자 키분배용 인증서를 생성하여 가입자에게 인증서를 발행한다.

□ 인증서 발급신청 및 등록과정(안1)



[그림 1] 무선 키분배용 X.509V3 인증서 발급신청 및 등록과정(안1)

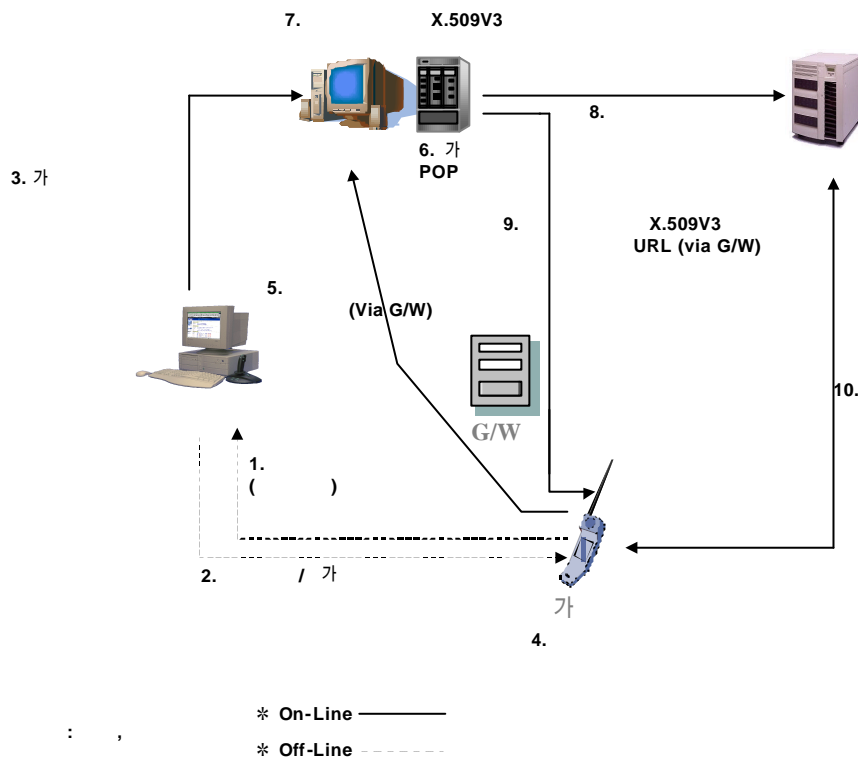
- 인증서 등록절차
 - 등록기관이 직접대면을 통해 사용자 신원확인을 한다.
 - 등록기관이 사용자의 신원확인 후 참조번호와 인가코드를 사용자에게 전달한다.
 - 등록기관은 자신의 database에 가입자를 등록하며 인증기관에 가입자의 정보를 인증기관으로 전송한다.
- 인증서 발급신청절차
 - 가입자는 인증서발급에 필요한 키분배용키쌍, 무선 인증서 발급요청형식을 생성한다.
 - 가입자는 자신의 키분배용개인키로 무선 인증서 발급요청형식을 서명한 후 등록기관에 전송한다.
 - 전자서명된 무선 인증서 발급요청형식을 받은 등록기관은 가입자의 서명을 통해 실제로 키분배용공개키에 대응하는 키분배용개인키의 소유여부를 확인(Proof Of Possession)한 후 발급요청형식을 인증기관에 전송한다.

- 인증기관은 무선 키분배용 X.509V3 인증서를 생성하여 자신의 디렉토리에 등록한 후 무선 키분배용 인증서 또는 인증서 URL을 등록기관으로 전송한다.
- 등록기관은 인증기관으로부터 받은 무선 키분배용 인증서 또는 인증서 URL 정보를 가입자에게 전송한다.

● 인증서 확인절차

- 인증기관으로부터 인증서를 받은 가입자는 자신이 받은 인증서의 이상유무를 확인한다.

□ 인증서 발급신청 및 등록과정(안2)



[그림 2] 무선 키분배용 X.509V3 인증서 발급 및 등록과정(안2)

● 등록절차

- 등록기관이 직접대면을 통해 사용자 신원확인을 한다.
- 등록기관이 사용자의 신원확인 후 참조번호와 인가코드를 사용자에게 전달한다.
- 등록기관은 가입자의 정보를 인증기관으로 전송한다.

● 인증서 발급신청절차

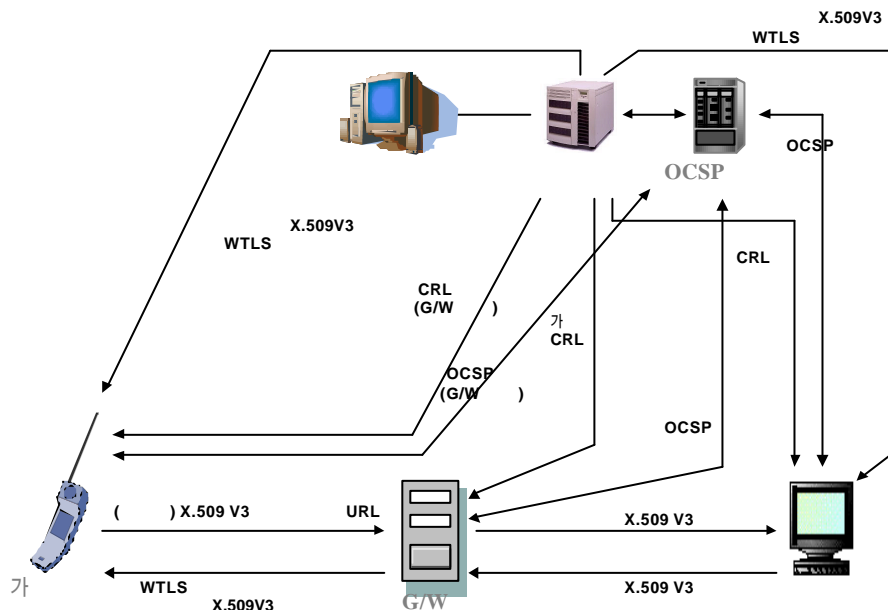
- 가입자는 인증서발급에 필요한 키분배용키쌍, 무선 인증서 발급요청형식을 생성한다.
- 가입자는 자신의 키분배용개인키로 무선 인증서 발급요청형식을 서명한 후 등록기관에 전송한다.
- 전자서명된 무선 인증서 발급요청형식을 받은 인증기관은 가입자의 서명 검증을 통해 실제로 키분배용공개키에 대응하는 키분배용개인키의 소유여부를 확인(Proof Of Possession)한다.
- 인증기관은 무선 키분배용 X.509V3 인증서를 생성하여 자신의 디렉토리에 등록하고, 이를 사용자에게 전송한다. 또는 인증서 대신 인증서를 획득할 수 있는 곳의 URL 정보를 전송할 수 있다.

● 인증서 확인절차

- 인증기관으로부터 인증서를 받은 가입자는 자신이 받은 인증서의 이상유무를 확인한다.

4.1.2 인증서 검증과정

□ 인증서 검증과정(안1)



[그림 3] 무선 키분배용 인증서 검증과정(안1)

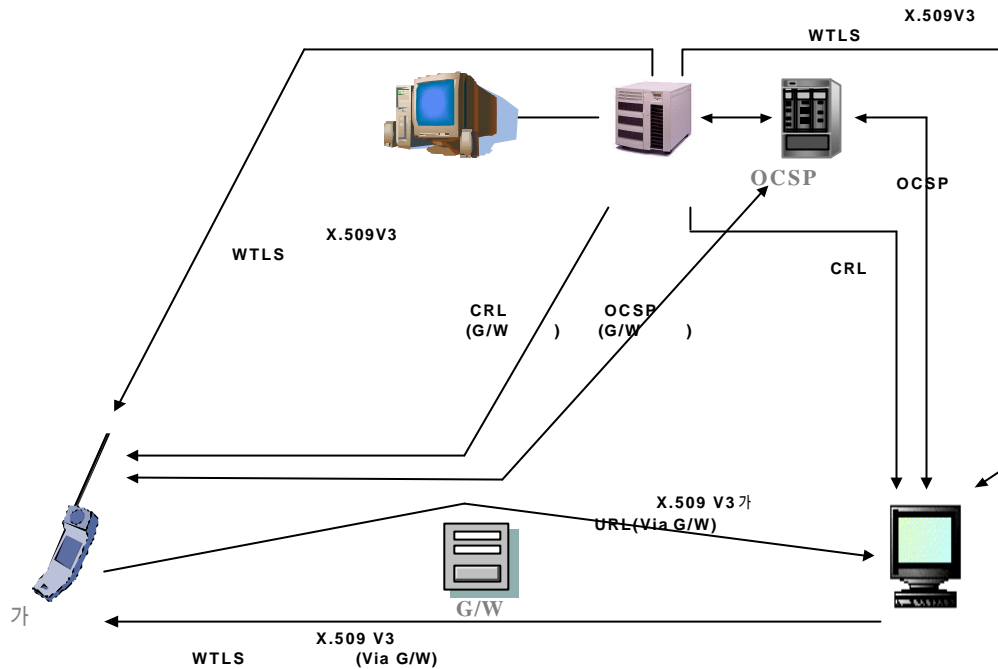
- 가입자가 G/W서버로부터 전송받은 인증서의 검증
 - G/W는 WTLS 서버인증서 또는 무선 키분배용 X.509V3 서버인증서를 가입자에게 전송한다.
 - 가입자는 G/W서버로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서 폐지목록(X.509V2)을 통해 인증서의 상태를 검증하거나 OCSP서버 등을 통해 인증서의 상태정보를 확인 할 수 있다. Short-lived WTLS 서버 인증서의 경우에는 상태 검증 행위를 한 것으로 간주한다.

- G/W서버가 가입자로부터 전송받은 인증서 또는 해당 URL에 있는 인증서 검증
 - 가입자는 자신의 인증서[무선 키분배용 X.509V3] 또는 인증서 URL을 G/W서버에게 전송한다.
 - G/W서버는 가입자로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서 폐지목록(X.509V2)을 통해 인증서의 상태를 검증하거나 OCSP서버 등을 통해 인증서의 상태정보를 확인 할 수 있다. URL을 받은 경우는 디렉토리로부터 인증서를 받아서 검증에 이용할 수 있다.

- G/W서버가 서버로부터 전송받은 인증서의 검증
 - 서버는 자신의 무선 키분배용 X.509V3 인증서를 G/W서버에게 전송한다.
 - G/W서버는 서버로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서 폐지목록(X.509V2)을 통해 인증서의 상태를 검증하거나 OCSP서버 등을 통해 인증서의 상태정보를 확인 할 수 있다.

- 서버가 G/W서버로부터 전송받은 인증서의 검증
 - G/W서버는 자신의 무선 키분배용 X.509V3 인증서를 서버에게 전송한다.
 - 서버는 G/W서버로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서 폐지목록(X.509V2)을 통해 인증서의 상태를 검증하거나 OCSP서버 등을 통해 인증서의 상태정보를 확인 할 수 있다.

□ 인증서 검증과정(안2)



[그림 4] 무선 키분배용 인증서 검증과정(안2)

- 가입자가 서버로부터 전송받은 인증서의 검증
 - 서버는 WTLS 서버인증서 또는 무선 키분배용 X.509V3 서버인증서를 가입자에게 전송한다.
 - 가입자는 서버로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서 페이지목록(X.509V2)을 통해 인증서의 상태를 검증하거나 OCSP서버 등을 통해 인증서의 상태정보를 확인할 수 있다. Short-lived WTLS 서버 인증서의 경우에는 상태검증 행위를 한 것으로 간주한다.
- 서버가 가입자로부터 전송받은 인증서 또는 해당 URL에 있는 인증서 검증
 - 가입자는 자신의 인증서 [무선 키분배용 X.509V3] 또는 인증서 URL을 서버에게 전송한다.
 - 서버는 가입자로부터 받은 인증서를 검증한다. 이때 디렉토리에 있는 인증서페이지 목록(X.509V2)을 통해 인증서의 상태를 검증하거나 OCSP서버 등을 통해 인증서의 상태정보를 확인할 수 있다. 인증서 URL을 받은 경우는 디렉토리로부터 인증서를 받아서 검증에 이용할 수 있다.

4.2 키분배용 인증서 관련 기준

4.2.1 인증서 발급요청

가입자의 경우 인증서발급요청은 PKCS#10이나 무선 인증서 요청형식을 등록기관이나 인증기관으로 보낸다.

서버의 경우는 PKCS#10, RFC2511의 발급요청형식을 등록기관이나 인증기관으로 보낸다.

4.2.2 인증서 전송방법

인증서를 전송하는 방법은 인증서 자체를 전송하는 것과 인증서에 대한 URL만을 전송하는 것 두 가지로 나눌 수 있다.

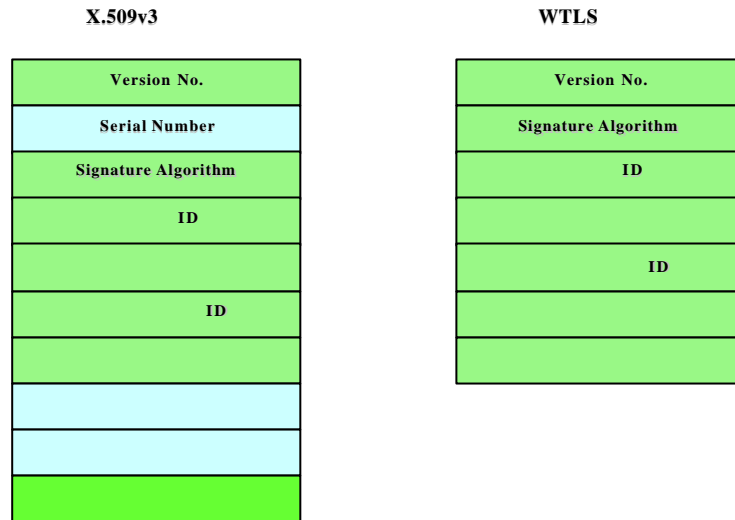
가입자(단말기)의 경우 저장용량의 부족 및 전송대역폭 제한 때문에 인증서 자체를 전송하는 방법이외에 인증서 URL만 전송하는 방법이 필요하다. 인증서 URL만 전송하는 경우 신뢰당사자는 URL을 참조하여 디렉토리로부터 가입자의 인증서를 획득하게 된다.

4.2.3 인증서 규격

키분배용 인증서란 키분배용공개키가 자연인 또는 법인이 소유하는 키분배용개인키에 합치한다는 사실 등을 확인·증명하는 전자적 정보를 뜻한다. 이러한 인증서 사용을 위해서는 인증서 규격을 정의해서 사용해야 한다. 인증서 규격은 인증서의 모든 필드의 내용과 표현 가능한 데이터 형식 등에 대하여 기술되어 있다.

가입자의 경우 인증서는 무선 키분배용 X.509V3 인증서 규격을 준용한다.

서버의 경우 WTLS 서버인증서를 필수로 무선 키분배용 X.509V3 인증서를 선택 기준으로 정의한다.



[그림 5] 인증서 비교

4.2.4 인증서 프로파일

인증서 프로파일은 인증기관 및 응용프로그램이 인증서를 생성하고 처리하는데 필요한 요구사항들을 명시하고 있다. 하지만 WTLS 서버인증서는 Serial Number도 확장영역도 없으므로 검증을 위한 정보를 제공하지 않는다. 그래서 이에 대한 방안으로 보증서 유효기간이 최대 48시간이내인 Short-lived 인증서를 발행하여 검증에 대한 문제를 대신하고 있다.

무선에서의 가입자인 경우 인증서 프로파일은 WAP 인증서 및 인증서 폐지목록 프로파일(WAP-211-X.509)를 준용한 첨부 1. 무선 기본배용 X.509V3 인증서 프로파일을 기준으로 정의한다.

서버인 경우 인증서 프로파일은 첨부 3.의 무선 기본배용 WTLS 인증서 프로파일을 필수로 첨부 1. 무선 기본배용 X.509V3 인증서 프로파일을 선택 기준으로 정의한다.

- ※ 첨부 3. 무선 기본배용 WTLS 인증서 프로파일
- ※ 첨부 1. 무선 기본배용 X.509V3 인증서 프로파일

4.2.5 인증서 효력정지 및 폐지목록규격

사용자는 인증기관에 의해 키분배용 공개키의 무결성을 보장받을 수 있다. 그러나 인증서에 포함된 키분배용 공개키에 대응되는 사용자의 키분배용 개인키가 노출되거나, 도난, 분실된 경우에는 큰 문제가 발생할 수 있다. 이러한 경우 인증서를 신뢰하여 상대방의 전자서명을 검증하는 신뢰당사자(Relying Party)가 선의의 피해를 입을 수 있다. 따라서 키분배용 개인키의 누출과 같은 키의 손상(compromise)이 발생한 경우 다른 사용자가 해당 키분배용 공개키에 대한 인증서를 사용하지 못하도록 함으로써, 키분배용 개인키의 누출에 따른 피해를 예방하여야 한다. 인증기관은 손상된 키분배용 개인키에 대응하는 키분배용 공개키의 인증서를 즉시 폐지하여, 이 사실을 인증서를 신뢰하여 사용하는 모든 신뢰당사자들이 알 수 있도록 하여야 한다. 이렇게 폐지된 인증서들에 대한 목록을 인증서폐지목록(CRL, Certificate Revocation List)이라고 하며, 인증기관의 저장소(Repository) 또는 디렉토리(Directory) 시스템 등에 등재하여 신뢰당사자가 언제든지 이 목록을 검색할 수 있도록 하여야 한다.

인증서 효력정지 및 폐지 목록은 인증서의 효력정지 및 폐지 여부를 인증서 사용자에게 알리기 위한 수단으로 개발되었으며 ITU-T가 1993년 X.509 인증서 효력정지 및 폐지 목록에 대한 첫 번째 표준을 제정한 이후로 1997년 두 번째 판이 개정되었다. 또한 IETF에서는 인증서 효력정지 및 폐지목록에 대한 프로파일을 1999년 RFC 2459로 정의하여 권고하고 있다.

무선 키분배에서의 인증서 효력정지 및 폐지목록은 X.509V2를 기준으로 정의한다.

4.2.6 인증서 효력정지 및 폐지목록 프로파일

인증기관 및 응용프로그램이 인증서 효력정지 및 폐지목록 프로파일을 생성하고 처리하는데 필요한 요구사항들을 명시하고 있다.

무선에서의 인증서 효력정지 및 프로파일은 첨부 2의 전자서명 인증서 효력정지 및 폐지목록 프로파일을 기준으로 정의한다.

※ 첨부 2 무선 키분배용 X.509V3 인증서 효력정지 및 폐지목록 프로파일

4.2.7 인증서 인코딩

인증서 인코딩 방법에는 DER, PEM 등이 있는데 DER로 인코딩된 파일 확장명은 .der로 끝나며, 파일내용은 바이너리 형태이다. PEM은 안전하지 못한 방법으로 전송되는 E-Mail을 보호하기 위하여 전자서명 및 암호화 통신이 가능한 메일 프로토콜로 규정되어 되어 있다.

서버의 경우 (무선용)X.509V3 인증서의 경우 인코딩 규칙은 DER, PEM방식을 기준으로 정의한다.

무선 키분배용 WTLS 인증서는 WAP 공개키 기반 구조 (WAP-217-WPKI)에 정의된 WTLS 인증서 인코딩규격을 기준으로 정의한다.

가입자의 경우 인코딩 규칙은 DER방식을 필수로 PEM방식을 선택기준으로 정의한다.

※ 한글 코딩은 UTF-8를 사용한다.

4.2.8 이름 표기 (DN)

DN(Distinguished Name)은 인증서 및 인증서폐지목록을 전자서명 인증관리체계 내에서 고유하게 식별하기 위한 표준화된 이름이다. 즉 인증서 및 인증서폐지목록에는 소유자 및 발급자의 고유명칭에 대한 정보를 저장하게 되는데 이러한 명칭은 전자서명 인증관리체계내에서 고유하게 식별되어야 한다. 이를 위해서 ITU-T X.500에서 유선에 대한 DN를 정의하여 사용하고 있다.

가입자의 경우 DN 규격은 첨부4의 무선 키분배용 X.509V3 인증서 프로파일에 정의된 DN규격을 기준으로 정의한다.

서버의 경우 DN 규격은 무선 키분배용 WTLS 인증서를 사용할 경우는 첨부 5의 무선 키분배용 WTLS 인증서 DN 규격을 사용하고, 무선 키분배용 X.509V3 인증서를 사용할 경우는 첨부 4의 무선 키분배용 X.509V3 인증서 DN 규격을 기준으로 정의한다.

※ 첨부 4 무선 키분배용 X.509V3 인증서 DN 규격

※ 첨부 5 무선 키분배용 WTLS 인증서 DN 규격

4.2.9 인증서 유효기간

인증서 유효기간은 CA가 인증서 상태에 대한 정보를 유지하겠다고 보증하는 시간 간격을 의미하는데 각 날짜는 인증서 유효기간이 시작하는 날짜(notBefore)와 인증서 유효기간이 종료하는 날짜(notAfter)이다.

인증서의 유효기간은 UTCTime(시간 형식 : YYMMDDHHMMSSZ)이나 Generalized Time(시간형식 : YYYYMMDDHHMMSSZ)으로 인코딩되어 있을 수 있다. 2049년 까지의 날짜에 대해서는 인증서 유효기간을 반드시 UTCTime으로 인코딩해야한다. 또한 2050년 이후 날짜에 대해서는 GeneralizedTime으로 인증서 유효기간을 인코딩해야 한다.

무선에서의 가입자 또는 서버의 유효기간은 전자서명 인증관리체계에서 정의하고 있는 유효기간과 동일하다.

Short-lived WTLS 서버인증서 최대 유효기간은 48시간 이내로 한다.

4.2.10 인증서 및 인증서폐지목록 저장방식

가입자(단말기)의 (무선용)X.509V3 인증서 및 인증서폐지목록 저장방식은 WIM카드를 사용할 경우 WIM카드 규격을 따르고 소프트웨어를 사용할 경우 PEM형태로 저장하는 것을 필수로 DER형태로 저장하는 것을 선택기준으로 정의한다.

무선 키분배용 WTLS 인증서는 WAP 공개키 기반 구조에 정의된 키분배용 인증서 인코딩규칙을 필수기준으로 정의한다.

서버의 인증서 및 인증서폐지목록 저장방식은 PEM, DER형태로 저장하는 복수기준으로 정의한다.

4.2.11 키분배용 개인키 저장방식

가입자(단말기)의 경우 키분배용 개인키 저장방식은 WIM카드를 사용할 경우 WIM카드 규격을 따르고 소프트웨어를 사용할 경우 PKCS#5로 암호화하여 PKCS#8을 이용해 저장한다.

서버의 경우 키분배용 개인키 저장방식은 PKCS#5로 암호화하여 PKCS#8을 이용해 저장한다.

※ PKCS#5 : Password-Based Encryption Standard

※ PKCS#8 : Private-Key Information Syntax Standard

※ WIM : Wireless Application Protocol Identity Module Specification

4.2.12 키분배용 공개키 및 인증서, 인증서폐지목록 전달방식

가입자(단말기)의 키분배용 공개키 및 인증서, 인증서폐지목록 전달방식은 WIM카드를 사용할 경우 WIM카드 규격을 따르고 소프트웨어를 사용할 경우 PKCS#12를 사용하여 전달한다.

서버의 경우 키분배용 공개키 및 인증서, 인증서폐지목록 전달방식은 PKCS#12를 사용하여 전달한다.

※ PKCS #12 : Personal Information Exchange Syntax Standard

※ WIM : Wireless Application Protocol Identity Module Specification

4.2.13 인증서 및 인증서폐지목록 획득방식

가입자, 서버 모두 인증서 및 인증서폐지목록 획득방식은 첨부 6의 방식을 이용하여 획득한다.

※ 첨부 6. WPKI URL 이용 사용자인증서 획득법

4.2.14 인증서 관리 프로토콜

가입자의 인증서 재발급, 갱신, 효력정지, 폐지 요청을 할 때 무선 인증서 관리 프로토콜 규격에 따라 요청형식을 생성하거나 PKCS#10을 이용한다.

서버의 인증서 재발급, 갱신, 효력정지, 폐지 요청을 할 때 PKCS#10, RFC2511 등을 이용하여 요청형식을 생성한다.

4.3 알고리즘

무선 공개키 기반구조에서 지원하는 전자서명 알고리즘과 해쉬 알고리즘에 대하여 기술하며 관련 표준 및 규격을 명시한다.

4.3.1 전자서명 알고리즘(Signature Algorithms)

전자서명 알고리즘은 인증기관이 인증서와 인증서 효력정지 및 폐지목록을 생성하는 경우와 전자문서에 사용자가 전자서명을 하는 경우에 사용된다.

이를 위하여 전자서명 인증관리체계에서 지원하는 전자서명 알고리즘은 다음과 같다.

4.3.1.1 RSA

RSA는 소인수 분해 문제의 어려움에 기반한 알고리즘으로 Rivest, Shamir, 및 Adleman 등이 개발하였다.

RSA의 사용 가능한 전자서명 방식에 대한 OID 정의는 다음과 같다.

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {  
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }
```

RSA에서 지원하는 키의 길이는 1024비트 이상이어야 한다.

4.3.1.2 ECDSA

ECDSA는 타원곡선(elliptic curve)상에서 group을 정의하고 이에 대한 이산대수 계산의 어려움에 근거를 두고 있다. 타원 곡선 상에서의 이산대수문제는 일반적인 군에서 정의되는 이산대수 문제보다 훨씬 어려우며, 이에 따라, 작은 키로도 RSA 보다 높은 비도를 유지할 수 있다. ECDSA는 2000년 2월 8일에 발표된 FIPS 186-2 DSS에 새롭게 포함된 내용으로 타원곡선 전자서명 알고리즘이다.

ECDSA의 사용 가능한 전자서명 방식에 대한 OID 정의는 다음과 같다.

```
ecdsa-with-SHA1 OBJECT IDENTIFIER ::= {  
    iso(1) member-body(2) us(840) ANSI-X9-62(10045) signature(4) 1 }
```

ECDSA에서 지원하는 키의 길이는 160비트 이상이어야 한다.

4.3.2 공개키 정보(Subject Public Key Information)

4.3.2.1 공개키 알고리즘(Subject Public Key Algorithms)

공개키 알고리즘은 인증서가 포함하고 있는 공개키가 사용될 알고리즘이다.

이를 위하여 전자서명 인증관리체계에서 지원하는 공개키 알고리즘은 다음과 같다.

4.3.2.1.1 RSA

RSA의 사용 가능한 공개키 알고리즘에 대한 OID 정의는 다음과 같다.

```
rsaEncryption OBJECT IDENTIFIER ::= {  
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }
```

RSA에서 지원하는 키의 길이는 1024비트 이상이어야 한다.

4.3.2.1.2 ECDH

ECDH는 타원곡선(elliptic curve)상에서 DH 키분배 알고리즘이다.

ECDH의 사용 가능한 공개키 알고리즘에 대한 OID 정의는 다음과 같다.

```
id-ecPublicKey OBJECT IDENTIFIER ::= {  
    iso(1) member-body(2) us(840) ANSI-X9-62(10045)  
    id-public-key-type(2) 1 }
```

4.3.3 ECC 커브

ECC 커브는 ECDSA, ECDH 등에서 사용되는 ECC 커브이다.

이를 위하여 전자서명 인증관리체계에서 지원하는 ECC 커브에 대한 ASN.1 코드는 다음과 같다.

```
ecpkParameters ::= CHOICE {  
    ecParameters EParameters,  
    namedCurve OBJECT IDENTIFIER,  
    implicitlyCA NULL }
```

```
ecParameters ::= SEQUENCE {  
    version ECPVer,
```

```

    fieldID      FieldID,
    curve        Curve,
    base         ECPoint,
    order        INTERGER,
    cofactor    INTEGER OPTIONAL,
}

```

```

namedCurve ::= CHOICE {
    iso(1) identified-organization(3) secg(132) curve(0)
    ellipticCurve 1, -- ※ WTLS 3번 커브 --
    iso(1) member-body(2) us(840) ANSI-X9-62(10045) curves(3)
    characteristicTwo(0) c-TwoCurve 1, -- WTLS 5번 커브 --
    iso(1) identified-organization(3) secg(132) curve(0)
    ellipticCurve 8 -- WTLS 7번 커브 --
}

```

4.3.4 암호화 알고리즘

지원 가능한 암호화 알고리즘은 다음과 같다.

4.3.4.1 SEED

128비트 블록 암호알고리즘(SEED)은 128비트 암호키를 이용하여 메시지를 블록 단위로 암호·복호화하는 알고리즘으로 데이터의 비밀성 등과 같은 기능을 제공하기 위해 사용될 수 있다.

SEED에서 지원하는 키의 길이는 128비트이어야 한다.

4.3.4.2 TripleDES

TripleDES에서 지원하는 키의 길이는 168비트이어야 한다.

4.3.5 해쉬 알고리즘

해쉬 알고리즘은 기본적으로 메시지 인증에 사용되며 전자서명 알고리즘과 함께 전자서명 생성 및 검증에 사용된다.

지원 가능한 해쉬 알고리즘은 다음과 같다.

4.3.5.2 SHA-1

SHA-1은 미국 정부에서 개발하였으며 임의의 입력값에 대하여 160비트 해쉬값을 출력하는 해쉬 알고리즘으로 “Federal Information Processing Standards Publication (FIPS PUB) 180-1, Secure Hash Standard”에서 정의하고 있다.

SHA-1에 대한 OID의 정의는 다음과 같다.

```
id-SHA1 OBJECT IDENTIFIER ::= {  
    iso(1) identified-organization(3) oiw(14) secsig(3) algorithms(2) 26 }
```

첨부 1. 무선 기본배용 X.509V3 인증서 프로파일

[인증기관 인증서]

기본필드명	생성	처리
Version	m	m
Serial Number	m	m
Signature	m	m
Issuer	m	m
Validity	m	m
Subject	m	m
Subject Public Key Info	m	m
Issuer Unique ID	x	x
Subject Unique ID	x	x
Extensions	m	m

확장필드명	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	o
Subject Key Identifier	n	m	o
Key Usage	c	m	m
Private Key Usage Period	n	x	x
Certificate Policies	b	m	m
Policy Mappings	n	o	m
Subject Alternative Names	n	m	m
Issuer Alternative Names	n	o	m
Subject Directory Attributes	n	x	x
Basic Constraints	c	m	m
Name Constraints	c	o	m
Policy Constraints	c	o	m
Extended Key Usage	b	o	m
CRL Distribution Points	n	m	o
domain information	n	o*	o*
Authority Information Access	n	m	o
Procuration	-	-	-

o : critical n : non-critical b : critical or non-critical - : not defined
 m : mandatory o : optional x : not recommended

*OCSP를 사용할 경우 DI의 사용을 Highly recommend 함

[가입자 인증서]

기본필드명	생성	처리
Version	m	m
Serial Number	m	m
Signature	m	m
Issuer	m	m
Validity	m	m
Subject	m	m
Subject Public Key Info	m	m
Issuer Unique ID	x	x
Subject Unique ID	x	x
Extensions	m	m

확장필드명	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	o
Subject Key Identifier	n	m	o
Key Usage	c	m	m
Private Key Usage Period	n	x	x
Certificate Policies	b	m	m
Policy Mappings	-	x	x
Subject Alternative Names	n	m	m
Issuer Alternative Names	n	o	m
Subject Directory Attributes	n	x	x
Basic Constraints	c	x	x
Name Constraints	-	-	-
Policy Constraints	-	-	-
Extended Key Usage	b	o	m
CRL Distribution Points	n	m	o
Domain information	n	o*	o*
Authority Information Access	n	m	o
Procuration	n	o	o

c : critical n : non-critical b : critical or non-critical - : not defined

m : mandatory o : optional x : not recommended

*OCSP를 사용할 경우 DI의 사용을 Highly recommend 함

첨부2. 무선 기본배용 X.509 인증서 효력정지 및 폐지 목록 프로파일

기본필드명	생성	처리
Version	m	m
Signature	m	m
Issuer	m	m
This Update	m	m
Next Update	m	m
Revoked Certificates	m ¹⁾	m
User Certificates	m ¹⁾	m
Revocation Date	m ¹⁾	m
CRL Entry Extensions	m ¹⁾	m
CRL Extensions	m	m

인증서 효력정지 및 폐지 목록 확장필드명	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	m
Issuer Alternative Name	n	o	m
CRL Number	n	m	m
Issuer Distribution Point	c	o	m
Delta CRL Indicator	n	o	o

엔트리 확장필드명	critical	선택여부	
		생성	처리
Reason Code	n	m	m
Hold Instruction Code	n	o	o
Invalidity Date	n	o	o
Certificate Issuer	c	o	m

c : critical n : non-critical b : critical or non-critical - : not defined
 m : mandatory r : recommended o : optional x : forbidden or not recommended

1) 효력정지 및 폐지된 인증서가 없을 경우에는 효력정지 및 폐지 목록 필드가 인증서 효력정지 및 폐지목록에 나타나지 않음

첨부 3. 무선 기본배용 WTLS 인증서 프로파일

항목	WTLS 인증서 (서버용)	WTLS 인증서 (인증기관용)
certificate_version	V1	V1
signature_algorithm	ecdsa_sha, rsa_sha	ecdsa_sha, rsa_sha
issuer	<Text>	<Text>
valid_not_before	GMT	GMT
valid_not_after	GMT	GMT
subject	<Text>	<Text>
public_key_type	ecdh(3), rsa(2)	ecdsa(4)
parameter_specifier	option	option
publickey	ecdh 공개정보, rsa 공개키	ecdsa 공개키
Signature	ecdsa 서명값, rsa 서명값	ecdsa 서명값, rsa 서명값

기본필드명	생성	처리
certificate_version	m	m
signature_algorithm	m	m
issuer	m	m
valid_not_before	m	m
valid_not_after	m	m
subject	m	m
public_key_type	m	m
parameter_specifier	m °	m °
public_key	m	m

m : mandatory, x : not recommended, ° : use only when the public key type is elliptic curve algorithm

첨부 4. 무선 기본배용 X.509V3 인증서 DN 규격

가. 속성 정의

속성	OID	약칭	크기	공인 인증 기관	가입자		실 명
					법인	개인	
commonName	2.5.4.3	cn	64	○	○	□	객체이름 (예:실명)
surname	2.5.4.4	sn	32,768	△	△	△	사람의 '성(姓)'
serialNumber	2.5.4.5		64	○	○	○	일련번호
countryName	2.5.4.6	c	2	□	□	□	국가명(ISO 3166 코드)
localityName	2.5.4.7	l	128	△	△	△	지역이름
stateOrProvinceName	2.5.4.8	st	128	△	△	△	도시 또는 도(道) 이름
organizationName	2.5.4.10	o	64	□	□	○	기관 이름
organizationUnitName	2.5.4.11	ou	64	□	○	○	기관의 특성, 또는 (기관내) 부서 이름
title	2.5.4.12		64	△	△	△	(기관내) 사람 직위
businessCategory	2.5.4.15		128	○	○	○	(기관이 수행하는) 사업의 종류
givenName	2.5.4.42		32,768	△	△	△	사람의 '이름'
initials	2.5.4.43		32,768	△	△	△	사람이름의 약어표기
generationQualifier	2.5.4.44		32,768	△	△	△	사람이름의 접미어
dnQualifier	2.5.4.46		32,768	△	△	△	RDN(Relative DN)을 명확하게 하여주는 구분자
emailAddress	1.2.840.113549.1.9.1		128	○	○	○	전자우편 주소
DomainComponent	0.9.2342.19200300.100.1.25	dc		○	○	○	도메인 네임 구성요소 (RFC 2247)

※ □ : 필수, ○ : 권고, △ : 선택

※ OID : 속성(Attribute)에 대한 OID 체계는 joint-iso-itu-t(2)-ds(5)-attributeType(4)임 예를 들어, locality의 OID는 2.5.4.7이며, joint-iso-itu-t(2)-ds(5)-attributeType(4)-locality(7)로 표기 됨

나. DN 사용 방법

전자서명 인증관리센터

o c=kr, o=KISA, ou=RootCA, cn=cert|timestamp, [emailAddress]

- ※ **c** : Country (국가), **o** : Organization (기관),
ou : Organization unit (기관의 특성)
cn : Common name (인증서명)

공인인증기관

o c=kr, o=KICA, ou=LicensedCA, [businessCategory],
[serialNumber], [cn], [emailAddress]

o c=kr, o=KFTC, ou=LicensedCA, [businessCategory],
[serialNumber], [cn], [emailAddress]

o c=kr, o=KOSCOM, ou=LicensedCA
[businessCategory], [serialNumber], [cn], [emailAddress]

- ※ **businessCategory** : Business category (사업의 종류)

가입자

o 법인 :

c=kr, o=KISIA, [ou], [businessCategory], [serialNumber],
[cn], [emailAddress]

o 개인 :

c=kr, [o], [ou], [businessCategory], [serialNumber], cn=Hong
Kil-Dong, [emailAddress]

- ※ 가입자의 **cn** : 개인명 또는 법인명 = {영문명}

첨부 5. 무선 키분배용 WTLS 인증서 DN 규칙

가. 속성 정의

속성	공인인증 기관	법인	실 명
<servicename>	<input type="checkbox"/>	<input type="checkbox"/>	organization 안에 있는 entity의 service name, CA, subscriber 등.
<organization>	<input type="checkbox"/>	<input type="checkbox"/>	organization name
<country>	<input type="checkbox"/>	<input type="checkbox"/>	2-character ISO country name
<commonname>	<input type="checkbox"/>	<input type="radio"/>	fully-qualified domain name or IP address
<extension>	<input type="radio"/>	<input type="radio"/>	rfc2253 에 정의되어 있는 1차 또는 2차 속성형식, 추가로 SN (the attribute Subject Serial Number) 정의 가능

※ : 필수, : 권고

나. DN 사용 방법

공인인증기관 사용 예

- o <servicename>; <organization>; <country>; <commonname>; [<extension>]
- o "LicensedCA SignKorea KOSCOM; KOSCOM; KR; www.signkorea.com;
[serialNumber]" or
"LicensedCA SignKorea KOSCOM; KOSCOM; KR; 210.207.195.70;
[serialNumber]"
- o "LicensedCA SignGate KICA; KICA; KR; www.signgate.co.kr;
[serialNumber]" or
"LicensedCA SignGate KICA; KICA; KR; 211.35.96.13; [serialNumber]"
- o "LicensedCA YesSign KFTC; KFTC; KR; www.yessign.com; [serialNumber]
or
"LicensedCA YesSign KFTC; KFTC; KR; 203.233.91.44; [serialNumber]"

법인 사용 예

- o <servicename>; <organization>; <country>; [[<commonname>];

[<extension>]]

- o "Kookmin Internet banking; Kookmin Bank, Inc.; KR; [banking.kookmin.co.kr];[serialNumber]" or "Kookmin Internet banking; Kookmin Bank, Inc.; KR; [210.124.53.70];[serialNumber]"
- o "Lotte Shopping Mall; Lotte,Com; KR; [www.lotte.com]; [serialNumber] or "Lotte Shopping Mall; Lotte,Com; KR; [211.174.50.5]; [serialNumber]

※ WTLS인증서의 경우는 Text(M) 형태를 필수기준으로 정의하고 그 외의 , Key_hash_sha(o), binary(o), X.509_name(o)은 선택기준으로 정의하는 것으로 한다.

첨부 6. WPKI URL 이용 사용자 인증서 획득법

본 첨부에서는 무선 지원하는 사용자 인증서 획득법을 명시한다.

1. HTTP URLS

: HTTP GET 메시지로 전송하며 응답은 MIME 형식의 인증서이다.

http://<base URL>?ih=<issuer name hash>&sn=<serial number>

<base URL>

<issuer name hash> SHA-1의 해쉬값 20 octet, base64로 인코딩(28자)

<serial number> base-64로 인코딩된 인증서 번호

예)

http://www.somename.com/cert?ih=hvcNAQEFBQADgYEAghAGhYTRgkFj&sn
=EP9uEIY3KDegjlr

Content-type: application/x-x509-user-cert

<binary X.509>

2. LDAP URLS

: [LDAPURL]과[LDAPSrch] 규격을 따르며 응답은 MIME이다.

예)

ldap://ldap.wap/cn=Wap%20user,o=Wap%20Serches%20Inc.,c=US?userCertificate??
(userCertificate:2.5.13.34:=123456\$o=Wap%20LDAP%20Serches%20Inc.,c=US)

Content-type: application/x-x509-user-cert

<binary X.509 blob>

첨부 7. 무선 키분배용 인증서 기술 기준(표)

1. 알고리즘

항목	세부 항목	센터	비고
키분배용 알고리즘	가입자	· RSA(768/2048) · ECDSA(160/163)	※RSA (MIN:768 MAX: 2048) ※ECDSA (MIN:160 MAX:163)
	서버	· RSA(768/2048) · ECDSA(160/163)	※RSA (MIN:768 MAX: 2048) ※ECDSA (MIN:160 MAX:163)
암호화 알고리즘	가입자	· SEED(128) · 3DES(168)	
	서버	· SEED(128) · 3DES(168)	
해쉬 알고리즘	가입자	· SHA1	
	서버	· SHA1	

2. 기본배용 인증서 관련 기준

항목	세부 항목	센터	비고
인증서 규격	가입자	· X.509 V3	
	서버	· WTLS 서버인증서(M) · 무선 기본배용 X.509 V3(O)	※M(Mandatory) O(Option)
인증서 프로파일	가입자	· 첨부 1. 무선 기본배용 X.509 V3 인증서 프로파일	
	서버	· 첨부 1. 무선 기본배용 X.509 V3 인증서 프로파일 (O) · 무선 기본배용 WTLS 인증서 규 격 (M)	※M(Mandatory) O(Option)
CRL규격	가입자	· X.509 V2	
	서버	· X.509 V2	
CRL 프로파일	가입자	· 첨부 2. 무선 기본배용 X.509V3 인증서 효력정지 및 폐지목록 프 로파일	
	서버	· 첨부 2. 무선 기본배용 X.509V3 인증서 효력정지 및 폐지목록 프 로파일	

항목	세부 항목	센터	비고
코딩 방법	가입자	· DER(M) · PEM(O)	※ 한글 코딩은 UTF8 사용 ※ M(Mandatory) O(Option)
	서버	· 무선 키분배용 X.509V3 인증서 -DER, PEM · 무선 키분배용 WTLS 인증서 -WTLS인증서 인코딩 규격	※ 한글 코딩은 UTF8 사용
DN	가입자	· 첨부 4. 무선 키분배용 X.509V3 인증서 DN 규격	
	서버	· 무선 키분배용 X.509V3 인증서 -첨부 4. 무선 키분배용 X.509V3 인증서 DN 규격 · 무선 키분배용 WTLS 인증서 -첨부 5. 무선 키분배용 WTLS 인증서 DN 규격	
인증서 유효기간	가입자	· 유선과 동일	
	서버	· 유선과 동일 · WTLS 서버인증서 -48시간 이내	

※PKCS #9 : Selected Attribute Types

항목	세부 항목	센터	비고
인증 요청서	가입자	· PKCS#10 · 무선 인증서 요청 형식	
	서버	· PKCS#10 · RFC2511	
인증서 전송방법	가입자	· 인증서의 URL 전송 · 전체 인증서 전송	
	서버	· 전체 인증서 전송	
인증서 및 CRL 저장방식	가입자	· WIM카드 : WIM 규격 · DER 형태로 저장(M) · PEM 형태로 저장(O)	
	서버	· PEM, DER 형태로 저장	
전자 서명 생성키 저장방식	가입자	· WIM카드 : WIM 규격 · PKCS#5로 암호화하여 PKCS#8 형식으로 저장	
	서버	· PKCS#5로 암호화하여 PKCS#8 형식으로 저장	

- ※PKCS #5 : Password-Based Encryption Standard
- ※PKCS #8 : Private-key information Syntax Standard
- ※PKCS #10 : Certification Request Syntax Standard

항목	세부항목	센터	비고
전자 서명키 및 인증서, CRL 전달방식	가입자	· WIM카드 : WIM 규격 · PKCS#12	
	서버	· PKCS#12	
인증서 및 CRL 획득방식	가입자	· LDAP/HTTP · 첨부 6, WPKI URL 이용 사용자 인증서 획득법	
	서버	· LDAP/HTTP · 첨부 6, WPKI URL 이용 사용자 인증서 획득법	
인증서 검증방식	가입자	· CRL 혹은 delta-CRL · OCSP · Short-Lived Certificate	· 기본 필드 검증외에 인증서 상태검증을 수행하여야 함. · 경로검증방법: RFC2459 준용
	서버	· CRL 혹은 delta-CRL · OCSP	· 기본 필드 검증외에 인증서 상태검증을 수행하여야 함. · 경로검증방법: RFC2459 준용
인증서 관리 프로토콜	가입자	· PKCS#10 · 무선 인증서 요청 형식	
	서버	· PKCS#10 · RFC2511 등 사용	

※PKCS #12 : Personal Information Exchange Standard