무선 WTLS 인증서 프로파일 규격

Wireless Transport Layer Security Certificate Profile Specification

2001. 8 (ver1.21)

한국정보보호진흥원

1. 규격명

무선 WTLS 인증서 프로파일 규격
(Wireless Transaction Layer Security Certificate Profile Specification)

2. 규격의 개요

2.1 목적

무선 키분배용으로 사용되는 WTLS인증서 생성·처리 및 관련 기술 규격을 정의한다.

2.2 적용범위 및 기대효과

본 규격은 전자서명인증관리체계내에서 키분배용으로 사용되는 WTLS 인증서 대한 프로파일을 정의하고 있으며 인증기관 및 응용 프로그램이 인증서를 생성 및 처리하는데 필요한 요구 사항들을 명시하고 있다.

본 규격은 인증 관련 기술의 발전과 관련 응용서비스 활성화에 기여할 것이며, 또한 전자상거래에 대한 신뢰성을 확보하여 전자상거래 시장을 자연스럽게 활성화시켜 나갈 것이다.

본 규격은 전자서명인증관리체계내에서 무선인터넷상의 키분배를 위한 규격으로 사용될 것이다.

2.3 내용 요약

본 규격의 주요 내용은 무선 인터넷에서의 키분배 관련 기술규격으로서 인증서 생성 및 사용자의 인증서 처리 시에 필요한 요구사항에 대한 내용을 기술하고 있다.

본 규격은 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 반

영하여 기술되었다.

3. 참조권고

3.1 국외 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.5.09 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 Direc tory: Selected Attribute types.

3.2 국내표준

- TTAS.IT-X.509/R2, 디렉토리 시스템 인증 프레임워크 표준
- TTA.IS-10118, 해쉬함수표준 - 제2부 : 해쉬함수알고리즘표준 (HAS-160)
- TTAS.KO/12.0012, 전자서명인증서프로파일표준

목 차

무선 WTLS 인증서 프로파일 규격
Wireless Transaction Layer Security Certificate Profile Specification

1. 개요

인증서의 표준은 ITU-T가 1988년 X.509를 제정한 이후로 지속적으로 개발되어 1993년 두 번째 판이 개정되었으며 1997년 세 번째 판이 개정되었다. 또한 IETF에서는 인증서에 대한 프로파일에 대하여 1999년 RFC 2459로 정의하여 권고하고 있다. 이에 따라 WAP 포럼에서도 WAP-211-X.509와 WAP-199-WTLS로 WTLS인증서 프로파일을 정의하여 권고하고 있다.

본 규격에서는 이를 기반으로 무선 키분배시 사용되는 WTLS 인증서 프로파일을 규정한다.

2. 규격의 구성 및 범위

본 규격은 전자서명인증관리체계내에서 인증서를 이용한 키분배용 무선 WTLS 인증서 프로파일 규격을 정의하고 인증기관 및 응용 프로그램의 인증서 생성·처리시 요구사항들을 명시하고 있다.

본 규격은 전자서명인증관리체계내에서 무선인터넷상의 키분배를 위한 규격으로 사용될 것이다.

3 관련 표준

3.1 국외 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-199-WTLS, Wireless Transport Layer Security 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.5.09 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, Infor--mation Technology Open Systems Interconnection The Direc tory: Selected Attribute types.

3.2 국내표준

- TTAS.IT-X.509/R2, 디렉토리 시스템 인증 프레임워크 표준
- TTA.IS-10118, 해쉬함수표준 - 제2부 : 해쉬함수알고리즘표준 (HAS-160)
- TTAS.KO/12.0012, 전자서명인증서프로파일표준

4. 정의

4.1 인증 프레임워크 정의

본 규격에서 사용된 다음의 용어들은 TTAS.IT-X.509/R2에 정의되어 있다.

가) 사용자 인증서(user certificate), 공개키 인증서(public key certificate), 인증서(certificate)
나) CA-인증서(CA-certificate)
다) 인증서 정책(certificate policy)
라) 인증서 사용자(certificate user)
마) 인증서 사용 시스템(certificate-using system)
바) 인증 기관(certification authority)
사) 인증 경로(certification path)
아) 최종 실체(end entity)
차) 해쉬 함수(hash function)
카) 키 일치 (key agreement)
타) 공개 키(public key)
파) 비밀 키(private key)
하) 신뢰(trust)
갸) 인증서 일련번호(certificate serial numbe

4.2 인증서 프로파일 정의

본 규격의 목적을 위하여 다음과 같은 용어들을 정의한다.

가) criticality : 인증서 생성시 확장필드에 부여되는 성질로서 critical과 non-critical이 존재함
나) critical : 인증서 사용 시스템이 critical로 설정된 확장필드를 처리할 수 없는 경우에는 인증서 및 인증경로 전체를 신뢰해서는 안됨
다) non-critical : 인증서 사용 시스템이 non-critical로 설정된 확장필드를 처리할 수 없는 경우에는 다음 확장필드를 처리하고 인증서 및 인증경로 전체의 신뢰도에는 영향을 미치지 않음
라) 신뢰당사자 : 인증서를 수령하여 해당 인증서를 신뢰하고 사용하는 자를 말함

마) 신원확인 : 인증서의 신뢰성 확보를 위하여 인증서 발급, 갱신, 효력정지, 효력회복 및 폐지 등의 신청시 신청인 및 신청 정보의 진정성 등을 확인하는 행위를 말함

바) 실명 : 실명이란 주민등록표상의 명의, 사업자등록증상의 명의 기타 금융실명제거래및비밀보장에관한법률 및 동시행령(대통령령 제15744호)에 정하는 실질명의를 말함

5. 약어

본 규격에서는 다음의 약어들이 적용된다.

가) CA : Certification Authority, 인증 기관
나) OID : Object Identifier, 객체 식별자
다) DN : Distinguished Name, 고유 이름
라) DER : Distinguished Encoding Rules, 인코딩 규칙
마) HTTP : Hypertext Transfer Protocol, 인터넷 전송 프로토콜
사) LDAP : Lightweight Directory Access Protocol, 디렉토리
아) POP : Proof of Possession, 소유 증명
차) PEM : Privacy Enhanced Mail, 인코딩 규칙
카) RA : Registration Authority, 등록기관
타) CMP : Certificate Management Protocol, 인증서 관리 프로토콜

6. 무선 WTLS인증서 프로파일

6.1 인증서 기본필드

6.1.1 인증서 버전(certificate_version)

버전 필드는 인코딩되는 인증서의 버전을 나타낸다.

WTLS v1 인증서는 버전 1의 값을 가져야만 하며 이 값은 정수 1로 표현한다.

응용 프로그램은 버전 1 인증서를 처리할 수 있어야 한다.

6.1.2 서명 알고리즘(signature_algorithm)

서명알고리즘 필드는 인증기관이 인증서 생성 시에 사용한 알고리즘에 대한 식별정보로 이 값은 정수로 표현한다.

6.1.3 발급자(issuer)

발급자 필드는 인증서를 발급한 인증기관의 명칭이 다음 사항을 포함한 DN 형식으로 표현하며 반드시 값을 가져야 한다.

- 필수사항 : Text 이름과 문자열집합(Textual name with character set)

  ※ Character_set은 IANA(Internet Assigned Numbers Authority) 규정 방식을 따른다.

- 선택사항 : X.509 DN, SHA-1 hash of the public key, binary identity.

한글을 사용하는 경우에는 UTF8 형식으로 표현한다.

모든 응용프로그램은 DN을 생성하고 처리할 수 있어야 한다.

6.1.4 유효시작시간(valid_not_before)

유효시작시간 필드는 인증서의 상태를 인증기관이 보증해주는 시작시간을 나타낸다.

시각 정보는 GMT로 표현하며 2049년까지 UTCTime 형식을 사용하고 2050년부터는 GeneralizedTime 형식을 사용한다.

6.1.5 유효종료시간(valid_not_after)

유효종료시간 필드는 인증서의 상태를 인증기관이 보증해주는 종료시간을 나타낸다.

시각 정보는 GMT로 표현하며 2049년까지 UTCTime 형식을 사용하고 2050년부터는 GeneralizedTime 형식을 사용한다.

6.1.6 소유자(subject)

소유자 필드는 인증서의 소유자 명칭이 다음 사항을 포함한 DN 형식으로 표현하며 반드시 값을 가져야 한다.

- 필수사항 : Text이름과 문자열집합(Textual name with character set)

※ Character_set은 IANA(Internet Assigned Numbers Authority) 규정 방식을 따른다.

- 선택사항 : X.509 DN, SHA-1 hash of the public key, binary identity.

한글을 사용하는 경우에는 UTF8 형식으로 표현한다.

모든 응용프로그램은 DN을 생성하고 처리할 수 있어야 한다.

6.1.7 소유자 공개키 타입(public_key_type)

이 정보 필드는 소유자의 공개키에 대한 알고리즘의 고유 정보를 식별정보로 이 값은 정수로 표현한다.

6.1.8 파라미터 식별자(parameter_specifier)

이 정보 필드는 인증서의 공개키 정보가 타원곡선 암호화 알고리즘을 사용할 경우 필요한 파라미터 값을 주기 위한 필드이다.

해당 곡선을 식별할 수 있는 파라미터 또는 해당 곡선의 대한 식별정보로 이 값은 정수로 표현한다.

6.1.9 공개키(public_key)

이 필드는 인증서를 통하여 인증되는 사용자의 공개키 값을 나타낸다.

부록 1 무선 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