전자서명인증체계 디렉토리 프로토콜 규격

Lightweight Directory Access Protocol Specification

v1.11

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

전자서명인증체계 디렉토리 프로토콜 규격
Lightweight Directory Access Protocol Specification

1. 개 요

본 규격에서는 전자서명법 상에서 구축된 전자서명인증체계에서 공인인증기관이 제공하는 유·무선 PKI간 인증서비스의 상호연동을 위해 필수적으로 요구되는 디렉토리 프로토콜 규격을 규정한다.

2. 규격의 구성 및 범위

본 규격은 전자서명인증체계 내에서 이용되는 디렉토리 시스템에 적용되는 프로토콜과 디렉토리 스키마를 명시한다.

본 규격은 기본적으로 LDAP v3 및 관련 디렉토리 표준을 따르며, 국내 공인전자서명인증체계 내에서 사용되는 디렉토리 스키마와 디렉토리 공고와 관련된 최소한의 요구사항을 정의한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[RFC2251] IETF, RFC2251, *Lightweight Directory Access Protocol(v3),* December 1997

[RFC2252] IETF, RFC2252, *Lightweight Directory Access Protocol(v3) : Attribute Syntax Definitions,* December 1997

[RFC2256] IETF, RFC2256, *A Summary of the X.500(96) User Schema for use with LDAPv3,* December 1997

[RFC2587] IETF, RFC2587, *Internet X.509 Public Key Infrastructure LDAPv2 Schema*, June 1999

[RFC2798] IETF, RFC2798, *Definition of the inetOrgPerson LDAP Object Class,* April 2000

[RFC2119] IETF, RFC2119, *Key words for use in RFCs to Indicate*

Requirement Levels, March 1997

[X500] ITU-T Recommendation X.500 (1997) | ISO/IEC 9594-8:1998, *Information technology - Open Systems Interconnection - The Directory : Overview of Concepts, Models and Services*

[X501] ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-8:1998, *Information technology - Open Systems Interconnection - The Directory : Models*

[X509] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1998, *Information technology - Open Systems Interconnection - The Directory : Authentication Framework*

[X520] ITU-T Recommendation X.520 (1997) | ISO/IEC 9594-8:1998, *Information technology - Open Systems Interconnection - The Directory : Selected Attribute Types*

[X521] ITU-T Recommendation X.521 (1997) | ISO/IEC 9594-8:1998, *Information technology - Open Systems Interconnection - The Directory : Selected Object Classes*

3.2 국내 표준 및 규격

[KCAC.TS.CERTPROF] KISA, KCAC.TS.CERTPROF, v1.70, *전자서명 인증서 프로파일 규격*, 2009

[KCAC.TS.CRLPROF] KISA, KCAC.TS.CRLPROF, v1.50, *전자서명 인증서 효력정지 및 폐지목록 프로파일 규격,* v1.10, 2009

[TTAS-X509/R2] TTA, TTAS.IT-X.509/R2, *디렉토리 시스템 인증 프레임워크 표준*, 2000

[TTAS-X501] TTA, TTAS.IT-X.501, *디렉토리 기본표준*, 1993

[KCAC.TS.DN] KISA, KCAC.TS.DN, v1.21, *전자서명인증체계 DN 규격,* 2009

[KCAC.TS.CTL] KISA, KCAC.TS.CTL, v1.40, *인증기관간 상호연동을 위한 CTL 기술규격,* 2009

3.3 기타

해당사항 없음

4. 정의

4.1 전자서명법 용어 정의

본 규격에서 사용된 다음의 용어들은 전자서명법 및 동법 시행령, 공인인증기관의 시설 및 장비 등에 관한 규정(미래창조과학부 고시)에 정의되어 있다.

가) 인증서
나) 공인전자서명인증체계
다) 가입자

4.2 용어의 정의

본 규격에서 사용된 다음의 용어들은 [TTAS-X509/R2], [TTAS-X501], [KCAC.TS.DSCP], [KCAC.TS.CRL]에 정의되어 있다.

가) 인증기관
나) 인증서 효력정지 및 폐지목록
다) 인증서 신뢰 목록
라) 디렉토리 정보 트리(DIT)
마) 디렉토리 스키마
바) 디렉토리 엔트리
사) 객체 부류
아) 속성
자) 식별명칭

4.3 디렉토리 관련 용어 정의

본 표준을 위하여 다음과 같은 용어들을 정의한다.

가) 완전한 인증서 효력정지 및 폐지목록(완전한-CRL : Complete CRL) : 특정한 인증서 범위(인증기관 인증서, 사용자 인증서, 폐지 사유 등)에 해당하는 모든 폐지된 인증서를 포함하고 있는 목록

4.4 용어의 효력

본 규격에서 사용된 다음의 용어들은 전자서명인증체계 디렉토리 프로토콜의 구현

정도를 의미하는 것으로 [RFC2119]를 준용하며 다음과 같은 의미를 지닌다.

가) 해야한다, 필수이다, 강제한다 (기호 : M)
반드시 준수해야 한다.
나) 권고한다 (기호 : R)
보안성 및 상호연동을 고려하여 준수할 것을 권장한다.
다) 할 수 있다, 쓸 수 있다 (기호 : O)
주어진 상황을 고려하여 필요한 경우에 한해 선택적으로 사용할 수 있다.
라) 권고하지 않는다 (기호 : NR)
보안성 및 상호연동을 고려하여 사용하지 말 것을 권장한다.
마) 금지한다, 허용하지 않는다 (기호 : X)
반드시 사용하지 않아야 한다.
바) 언급하지 않는다, 정의하지 않는다 (기호 : -)
준수 여부에 대해 기술하지 않는다.

5. 약어

본 규격에서는 다음의 약어가 이용된다.

가) DN : Distinguished Name, 식별명칭
나) CRL : Certificate Revocation List, 인증서 효력정지 및 폐지목록
다) IDP : Issuing Distribution Point, 인증서 효력정지 및 폐지목록 발급 분배점

6. 디렉토리 프로토콜

디렉토리 프로토콜은 [RFC2251]을 준용해야 하며, 디렉토리 정보 트리의 DN 구성은 [KCAC.TS.DN]을 준용해야 한다.

7. 디렉토리 스키마

본 절에서는 각 엔트리에 대한 속성 및 객체 부류를 분류하고, 국내 공인전자서명인증체계 내에서 사용되는 속성에 대한 최소한의 요구사항을 정의한다.

7.1 가입자

디렉토리에서 가입자 엔트리에 이용되는 속성 및 객체 부류는 다음과 같다.

7.1.1 속성

가입자 엔트리는 [X.520], [X.509] 및 [RFC2587]에서 정의하는 commonName 및 surname, userCertificate의 속성을 가져야 한다.

```
commonName ATTRIBUTE ::= {
    SUBTYPE OF    name
    WITH SYNTAX   DirectoryString
    ID     joint-iso-ccitt(2) ds(5) attributeType(4) commonName(3)}

surname ATTRIBUTE ::= {
    SUBTYPE OF    name
    WITH SYNTAX   DirectoryString
    ID     joint-iso-ccitt(2) ds(5) attributeType(4) surname(4)}

userCertificate  ATTRIBUTE ::= {
    WITH SYNTAX                Certificate
    EQUALITY MATCHING RULE     certificateExactMatch
    ID  joint-iso-ccitt(2) ds(5) attributeType(4) userCertificate(36)}
```

7.1.2 객체 부류

가입자 엔트리는 [RFC2587], [X.521], [RFC2798]에서 정의하는 pkiUser 및 organizationalPerson, inetOrgPerson 등의 객체 부류를 가질 수 있다.

```
pkiUser OBJECT-CLASS ::= {
    SUBCLASS OF   { top }
    KIND          auxiliary
    MAY CONTAIN   { userCertificate }
    ID            joint-iso-ccitt(2) ds(5) objectClass(6) pkiUser(21)}

organizationalPerson OBJECT-CLASS ::= {
```

```
        SUBCLASS OF   { person }
        MAY CONTAIN   { LocaleAttributeSet ¦ PostalAttributeSet ¦
                      TelecommunicationAttributeSet ¦
                      organizationalUnitName ¦ title }
        ID  joint-iso-ccitt(2) ds(5) objectClass(6) organizationalPerson(8)}

    inetOrgPerson OBJECT-CLASS ::= {
        SUBCLASS OF   { organizationalPerson }
        MAY CONTAIN   { audio ¦ businessCategory ¦ carLicense ¦
                      departmentNumber ¦ displayName ¦ employeeNumber ¦
                      employeeType ¦ givenName ¦ homePhone ¦ homePostalAddress ¦
                      initials ¦ jpegPhoto ¦ labeledURI ¦ mail ¦ manager ¦
                      mobile ¦ o ¦ pager ¦ photo ¦ roomNumber ¦ secretary ¦
                      uid ¦ userCertificate ¦ x500uniqueIdentifier ¦
                      preferredLanguage ¦ userSMIMECertificate ¦ userPKCS12 }
        ID     joint-iso-ccitt(2)     country(16)     USA(840)     company(1)
               netscape(113730) ldap(3) objectclass(2) inetOrgPerson(2) }
```

7.2 인증기관

디렉토리에서 인증기관 엔트리에 이용되는 속성 및 객체 부류는 다음과 같다.

7.2.1 속성

인증기관 엔트리는 [X.520], [X.509] 및 [RFC2587]에서 정의하는 commonName 혹은 organizationalUnitName, cACertificate의 속성을 가져야 한다.

```
    organizationalUnitName ATTRIBUTE ::= {
        SUBTYPE OF    name
        WITH SYNTAX   DirectoryString
        ID  joint-iso-ccitt(2) ds(5) attributeType(4) organizationalUnitName(11)}

    cACertificate  ATTRIBUTE ::= {
        WITH SYNTAX                Certificate
        EQUALITY MATCHING RULE     certificateExactMatch
```

```
    ID   joint-iso-ccitt(2) ds(5) attributeType(4) cACertificate(37)}
```

인증기관 엔트리에 인증서 효력정지 및 폐지목록을 공고할 경우, 인증기관 엔트리는 authorityRevocationList 혹은 certificateRevocationList의 속성을 가져야 한다.

```
authorityRevocationList  ATTRIBUTE ::= {
    WITH SYNTAX                CertificateList
    EQUALITY MATCHING RULE     certificateListExactMatch
    ID   joint-iso-ccitt(2) ds(5) attributeType(4) authorityRevocationList(38)}

certificateRevocationList  ATTRIBUTE ::= {
    WITH SYNTAX                CertificateList
    EQUALITY MATCHING RULE     certificateListExactMatch
    ID   joint-iso-ccitt(2) ds(5) attributeType(4) certificateRevocationList(39)}
```

7.2.2 객체 부류

인증기관 엔트리는 [X.509] 및 [RFC2587], [RFC2798]에서 정의하는 pkiCA 및 inetOrgPerson, certificationAutority의 객체 부류를 가질 수 있다.

```
pkiCA OBJECT-CLASS ::= {
    SUBCLASS OF   { top }
    KIND          auxiliary
    MAY CONTAIN   { cACertificate ¦ certificateRevocationList ¦
                  authorityRevocationList ¦ crossCertificatePair }
    ID            joint-iso-ccitt(2) ds(5) objectClass(6) pkiCA(22)}

certificationAuthority  OBJECT-CLASS ::= {
    SUBCLASS OF   { top }
    KIND          auxiliary
    MUST CONTAIN  { cACertificate ¦ certificateRevocationList ¦
                  authorityRevocationList }
    MAY CONTAIN   { crossCertificatePair }
    ID  joint-iso-ccitt(2) ds(5) objectClass(6) certficationAuthority(16)}
```

7.3 인증서 효력정지 및 폐지목록 분배점

디렉토리에서 인증서 효력정지 및 폐지목록 분배점 엔트리에 이용되는 속성 및 객체 부류는 다음과 같다.

7.3.1 속성

인증서 효력정지 및 폐지목록 분배점 엔트리는 [X.520], [X.509] 및 [RFC2587]에서 정의하는 commonName 혹은 organizationalUnitName, certificateRevocationList 혹은 authorityRevocationList의 속성을 가져야 한다.

7.3.2 객체 부류

인증서 효력정지 및 폐지목록 분배점 엔트리는 [RFC2587] 및 [X.509]에서 정의하는 cRLDistributionPoint의 객체 부류를 가질 수 있다.

```
cRLDistributionPoint OBJECT-CLASS ::= {
    SUBCLASS OF   { top}
    KIND          structural
    MUST CONTAIN  { commonName}
    MAY CONTAIN   { certificateRevocationList |
                  authorityRevocationList |
                  deltaRevocationList }
    ID    joint-iso-ccitt(2) ds(5) objectClass(6) cRLDistriubtionPoint(19)}
```

7.4 인증서 신뢰 목록

디렉토리에서 인증서 신뢰목록 엔트리에 이용되는 속성 및 객체 부류는 다음과 같다.

7.4.1 속성

인증서 신뢰 목록 엔트리는 [X.521], [KCAC.TS.CTL]에서 정의하는 commonName, certificateTrustList의 속성을 가져야 한다.

```
certificateTrustList ATTRIBUTE ::= {
    WITH SYNTAX  ContentInfo
```

```
ID      iso(1) member-body(2) korea(410) kisa(200004)
        npki-interoperability(8) ctl(1) at(3) certificateTrustList(1)}
```

7.4.2 객체 부류

인증서 신뢰 목록 엔트리는 [KCAC.TS.CTL]에서 정의하는 pkiCTL의 객체 부류를 가질 수 있다.

```
pkiCTL  OBJECT-CLASS ::= {
    SUBCLASS OF  { top }
    KIND         auxiliary
    MUST CONTAIN { certificateTrustList }
    ID           iso(1) member-body(2) korea(410) kisa(200004)
                 npki-interoperability(8) ctl(1) oc(2) pkiCTL(1) }
```

8. 디렉토리 공고

본 절에서는 국내 공인전자서명인증체계에서 사용되는 인증서, 인증서 효력정지 및 폐지목록, 인증서 신뢰목록의 디렉토리 공고에 대한 요구사항을 정의한다.

8.1 인증서

대상 인증서의 소유자 DN과 동일한 엔트리에 공고해야 한다.

8.2 인증서 효력정지 및 폐지목록

대상 CRL이 완전한-CRL인 경우, CRL의 발급자 DN과 동일한 엔트리에 공고해야 해야 한다. 그렇지 않은 경우, CRL의 IDP 필드에 있는 인증서 효력정지 및 폐지목록 분배점과 동일한 엔트리에 공고해야 한다.

8.3 인증서 신뢰목록

인증서 신뢰목록은 ‘C=KR, O=KISA, OU=ROOTCA, CN=KISA-CTL’에 공고해야 한다.

부록 1. 규격 연혁

버전	제・개정일	제・개정내역
v1.00	2004년 5월	・“전자서명인증체계 디렉토리 프로토콜 규격”으로 제정
v1.10	2008년 10월	・관련 국내 표준 및 규격 갱신 내용 반영 ・법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.11	2009년 9월	・공인전자서명인증체계 기술규격 개정에 따라 본문 내용 중 관련 기술규격 참조 변경 사항 개정