전자서명 인증서 프로파일 규격

Digital Signature Certificate Profile

v1.70

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

전자서명 인증서 프로파일 기술규격
Digital Signature Certificate Profile

1. 개 요

본 규격에서는 전자서명법에 따라 구축된 공인전자서명인증체계의 공인인증기관이 유·무선 공인인증서비스를 제공하는데 있어 필수적으로 요구되는 전자서명 공인인증서(이하 인증서) 프로파일을 규정한다.

2. 규격의 구성 및 범위

본 규격은 [RFC3280]을 준수하여 전자서명인증체계에서 사용되는 X.509 v3 인증서에 대한 프로파일 규격을 정의하고 있다.

첫 번째로 본문에서는 인증서내 기본필드와 확장필드의 사용 목적 및 구조체 등을 정의하고 있으며, 두 번째로 부록에서는 최상위인증기관과 공인인증기관, 사용자 소프트웨어가 인증서를 생성하고 처리하기 위한 요구사항들을 명시하고 있다.

3. 관련 표준

3.1 국외 표준 및 규격

[X500] ITU-T Recommendation X.500 (1997) | ISO/IEC 9594-1:1998, *Information technology - Open Systems Interconnection - The Directory : Overview Of Concepts, Models and Services*

[X501] ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2:1995, *Information technology - Open Systems Interconnection - The Directory : Part 2 : Models*

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

[RFC2119] IETF RFC 2119 (1997), *Key Words for use in RFCs to Indicate Requirement Levels*

[RFC2459] IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure*

Certificate and CRL Profile

[RFC3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*

[WAPCert] WAP-211-WAPCert-20010522-a(2001), *WAP Certificate and CRL Profiles*

[RFC3850] IETF RFC 3850 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling*

3.2 국내 표준 및 규격

[KCAC.TS.DSIG] KISA, KCAC.TS.DSIG, v1.30, *전자서명 알고리즘 규격*, 2009

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

[KCAC.TS.NSACA] KISA, KCAC.TS.NSACA, v1.11, *공인인증서 표시를 위한 기술 규격*, 2009

[KCAC.TS.SIVID] KISA, KCAC.TS.SIVID, v1.21, *식별번호를 이용한 본인확인 기술 규격*, 2009

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

[KCAC.TS.HSMU] KISA, KCAC.TS.HSMU, v1.90, *보안토큰 기반 공인인증서 이용 기술 규격*, 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) 전자서명인증체계
다) 가입자
라) 가입자 소프트웨어
마) 공인인증서

4.2 용어의 정의

해당사항 없음

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어의 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) ASN.1 : Abstract Syntax Notation One, 추상적 구문 표기
다) CPS : Certification Practice Statement, 인증업무준칙

6. 전자서명 공인인증서 프로파일

6.1 인증서 기본 필드

인증서 기본필드는 인증서의 버전, 발급자, 유효기간 등 인증서의 기본 정보를 나타낸다. 아래 정의된 기본필드는 공인인증서에 모두 포함되어야 하며, 가입자

소프트웨어는 이를 처리해야 한다.

6.1.1 버전(Version)

버전 필드는 공인인증서 형식을 구별할 수 있는 기능을 제공하는데 본 규격에서는 정수 2값을 갖는 버전 3 인증서만 허용한다.

```
Version ::= INTEGER { v1(0), v2(1), v3(2) }
```

6.1.2 일련번호(Serial Number)

일련번호 필드는 공인인증기관이 발급하는 공인인증서에 부여하는 유일한 양의 정수이다. 이 값은 공인인증서 효력정지 및 폐지목록에서 더 이상 유효하지 않는 목록들에 대한 참조정보로 사용된다.

모든 인증서의 일련번호는 20바이트를 넘을 수 없으며, 가입자 소프트웨어는 최대 20바이트 길이의 일련번호를 처리할 수 있어야 한다.

6.1.3 서명 알고리즘(Signature)

서명 알고리즘 필드는 공인인증기관이 인증서를 생성할 때 사용하는 서명 알고리즘의 OID 값을 가진다. 사용하는 서명 알고리즘은 [KCAC.TS.DSIG]를 준수해야 한다.

6.1.4 발급자(Issuer)

발급자 필드는 공인인증서를 발급한 인증기관의 명칭을 DN 형식으로 표현하며 반드시 값을 가져야 한다. 여기서 DN 형식은 [KCAC.TS.DN]을 준수해야 한다.

6.1.5 유효기간(Validity)

유효기간 필드는 공인인증기관이 공인인증서의 상태를 보증해주는 기간을 나타낸다. 이 필드는 다음과 같이 공인인증서 유효기간의 시작을 나타내는 시작시각(notBefore)과 유효기간의 종료시점을 나타내는 종료시각(notAfter)에 시작 정보를 저장하여 유효기간을 표현한다.

```
Validity ::= SEQUENCE {
        notBefore       Time,
        notAfter        Time    }
```

시각 정보(Time)는 GMT로 표현하며 2049년까지 UTCTime 형식을 사용하고 2050년부터는 GeneralizedTime 형식을 사용해야 한다.

6.1.6 소유자(Subject)

소유자 필드는 공인인증서 소유자의 명칭을 DN 형식으로 표현하며 반드시 값을 가져야 한다. 여기서 DN 형식은 [KCAC.TS.DN]을 준수해야 한다.

6.1.7 소유자 공개키 정보(Subject Public Key Info)

소유자 공개키 정보 필드는 소유자의 공개키에 대한 알고리즘 및 공개키 정보를 나타낸다.

```
SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm           AlgorithmIdentifier,
        subjectPublicKey    BIT STRING  }
```

algorithm은 알고리즘의 고유 정보를 OID로 나타내며 사용되는 알고리즘은 [KCAC.TS.DSIG]를 준수해야 한다.

6.2 인증서 확장 필드

6.2.1 발급자 공개키 식별자(Authority Key Identifier)

발급자 공개키 식별자 확장필드는 인증서를 서명하는데 사용된 인증기관 개인키에 대응되는 공개키를 식별하기 위해 사용된다.

```
AuthorityKeyIdentifier ::= SEQUENCE {
  KeyIdentifier             [0]   KeyIdentifier       OPTIONAL,
  authorityCertIssuer       [1]   GeneralNames        OPTIONAL,
  authorityCertSerialNumber [2]   CertificateSerialNumber     OPTIONAL
}
```

발급자 공개키를 식별하기 위하여 KeyIdentifier와 authorityCertIssuer, authorityCertSerialNumber를 모두 사용해야 한다. KeyIdentifier는 발급자 인증서의 소유자 공개키 정보 확장필드의 subjectPublicKey 값을 SHA-1 알고리즘으로 해쉬한 160비트 값을 OCTET STRING 형태로 저장한다.

발급자 공개키 식별자는 공인인증기관과 사용자 인증서에 포함되어야 하고 가입자 소프트웨어는 이 확장필드를 처리해야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.2.2 소유자 공개키 식별자(Subject Key Identifier)

소유자 공개키 식별자 확장필드는 인증기관으로부터 인증 받은 공개키를 식별한다.

```
SubjectKeyIdentifier ::= KeyIdentifier
```

KeyIdentifier는 인증서내 소유자 공개키 정보 확장필드의 subjectPublicKey 값을 SHA-1 알고리즘으로 해쉬하여 160비트 값을 OCTET STRING 형태로 저장한다.

소유자 공개키 식별자는 인증서에 포함되어야 하고 가입자 소프트웨어는 이 확장필드는 처리해야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.2.3 키 사용 목적(Key Usage)

키 사용목적 확장필드는 인증서에 포함된 소유자의 공개키가 사용되는 목적을 명시한다.

```
KeyUsage ::= BIT STRING {
        digitalSignature    (0),
        nonRepudiation      (1),
        keyEncipherment     (2),
        dataEncipherment    (3),
        keyAgreement        (4),
        keyCertSign         (5),
        cRLSign             (6),
        encipherOnly        (7),
        decipherOnly        (8) }
```

인증기관 인증서는 키 사용목적 확장필드의 값으로 KeyCertSign과 cRLSign을 사용해야 하며, 사용자 인증서는 digitalSignature와 nonRepudiation을 사용해야 한다.

가입자 소프트웨어는 이 확장필드를 처리할 수 있어야 하며 이 확장필드는 critical로 설정되어야 한다.

6.2.4 인증서 정책(Certificate Policy)

인증서 정책 확장필드는 인증서를 발급하는데 적용된 인증기관의 인증서 정책을 나타낸다.

```
certificatePolicies EXTENSION ::= {
        SYNTAX          CertificatePoliciesSyntax
        IDENTIFIED BY id-ce-certficiatePolicies }

certificatePoliciesSyntax ::= SEQUENCE SIZE(1..MAX) OF PolicyInformtation
        PolicyInformation ::= SEQUENCE {
                policyIdentifier    CertPolicyId,
                policyQualifiers    SEQUENCE SIZE(1..MAX) OF PolicyQualifierInfo OPTIONAL}
        CertPolicyID ::= OBJECT IDENTIFIER
        PolicyQualifierInfo ::= SEQUENCE {
                policyQualifierId   CERT-POLICY-QUALIFIER.&id
                                    ({SupportedPolicyQualifiers}),
                qualifier           CERT-POLICY-QUALIFIER.&Qualifier
                                    ({SupportedPolicyQualifiers}{@policyQualifierId}) OPTIONAL}
```

policyIdentifier 하위필드는 인증서 정책에 대한 OID를 값으로 갖는다. policyQualfiers 하위필드는 [KCAC.TS.NSACA]를 준수하여 cPSuri와 userNotice를 사용해야 한다.

이 확장필드는 최상위인증기관 인증서의 경우에는 non-critical로 설정하고, 공인인증기관 및 사용자 인증서의 경우 critical로 설정할 것을 권고한다. 다만, 사용자 인증서가 전자우편 보안용으로 사용되는 경우에는 non-critical로 설정할 것을 권고한다.

가입자 소프트웨어는 이 확장필드를 처리할 수 있어야 한다.

6.2.5 인증서 정책 매핑(Policy Mappings)

인증서 정책 매핑 확장필드는 인증서비스 영역간의 상호 인증시 상대방 인증서비스 영역의 인증서 정책을 받아들이고자 하는 경우에 사용된다.

인증서 정책 매핑 확장필드는 상호인증을 위해 최상위인증기관 인증서에서 선택적으로 사용될 수 있으며, 가입자 소프트웨어는 이 확장필드는 처리할 수 있어야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.2.6 소유자 대체 명칭(Subject Alternative Name)

소유자 대체 명칭 확장필드는 소유자의 추가적인 명칭을 나타내며, identityData 필드를 사용하여 인증서비스 영역 내에서 사용되는 고유한 식별정보를 나타낼 수 있다. 식별정보의 생성 및 주입 위치는 [KCAC.TS.SIVID]를 준수해야 한다. 만일 공인인증서를 전자우편 보안용으로 사용하고자 하는 경우, rfc822Name에 사용자의 이메일 주소를 포함하여야 한다.

```
SubjectAltName ::= GeneralNames
GeneralNames := SEQUENCE SIZE(1..MAX) of GeneralName
GeneralName ::= CHOICE{
        otherName                   [0]   OtherName,
        rfc822Name                  [1]   IA5String,
        dNSName                     [2]   IA5String,
        X400Address                 [3]   ORAddress,
        directoryName               [4]   Name,
        ediPartyName                [5]   EDIPartyName,
        uniformResourceIdentifier   [6]   IA5String,
        iPAddress                   [7]   OCTET STRING,
        registeredID                [8]   OBJECT IDENTIFIER }

id-kisa-identifyData        OBJECT IDENTIFIER ::= { id-attribute 1 }
identityData ::= SEQUENCE {
        realName      UTF8String,
        userInfo      SEQUENCE SIZE (1..MAX) OF
                      AttributeTypeAndValue OPTIONAL }
```

공인인증기관 및 사용자 인증서는 소유자 식별정보를 사용하여 본 확장필드를 사용해야 하며, 가입자 소프트웨어는 이 확장필드를 처리할 수 있어야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.2.7 발급자 대체 명칭(Issuer Alternative Name)

발급자 대체 명칭 확장필드는 인증기관의 추가적인 명칭을 나타내며 인증서비스 영역 내에서 사용되는 고유한 식별정보를 나타낼 수 있다.

인증기관의 고유정보를 나타내고자하는 경우에는 6.2.7에서 정의한 형식을 사용한다. 발급자 대체 명칭 확장필드는 공인인증기관과 가입자 인증서에서 선택적으로 포함될 수 있으며, 모든 가입자 소프트웨어는 이 확장필드를 처리할 수 있어야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.2.8 기본 제한(Basic Constraints)

기본 제한 확장필드는 사용자가 인증기관의 역할을 수행하는 것을 방지하며 이를 위하여 인증기관의 여부 및 인증경로의 길이를 제한한다. 이 확장필드는 인증기관용 인증서에만 포함되며 사용자 인증서에는 포함되지 말아야 한다.

```
BasicConstraintsSyntax ::= SEQUENCE {
        cA                    BOOLEAN DEFAULT FALSE,
        pathLenConstraint     INTEGER (0..MAX) OPTIONAL }
```

최상위인증기관과 공인인증기관의 인증서는 cA 하위필드의 값으로 TRUE를 가진다. 공인인증기관 인증서는 pathLenConstraints 하위 필드의 값으로 0을 가진다. 이 확장필드는 critical로 설정되며 모든 가입자 소프트웨어는 이 필드를 처리해야 한다.

6.2.9 명칭 제한(Name Constraints)

명칭 제한 확장필드는 소유자 필드 및 소유자 대체 명칭 확장필드에서 사용되는 명칭의 범위를 제한한다.

```
NameConstraintsSntax ::= SEQUENCE {
        permittedSubtrees[0]       GeneralSubtrees OPTIONAL,
        excludedSubtrees[1] GeneralSubtrees OPTIONAL }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree
```

```
GeneralSubtree ::= SEQUENCE {
        base            GeneralName,
        manimum[0]      BaseDistance DEFAULT 0,
        maximum[1]      BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)
```

명칭 제한은 계층적인 구조를 가지는 명칭에 대해서만 반영되며 6.2.7에서 정의한 소유자 고유정보 관련 명칭 등에는 적용되지 않는다. 이 확장필드는 사용자 인증서에는 포함되지 말아야 하며, 인증기관은 선택적으로 생성할 수 있다.

이 확장필드는 critical로 설정되며 모든 가입자 소프트웨어는 이 필드를 처리해야 한다.

6.2.10 정책 제한(Policy Constraints)

정책 제한 확장필드는 인증서 정책 검사의 요구 및 인증서 정책 매핑에 대한 금지 등에 대한 정보를 나타낸다.

```
policyConstraintsSyntax ::= SEQUENCE{
        requireExplicitPolicy       [0]    SkipCerts OPTIONAL,
        inhibitPolicyMapping        [1]    SkipCerts OPTIONAL }

SkipCerts ::= INTEGER (0..MAX)
```

이 확장필드는 공인인증기관 인증서에만 critical로 설정되어 포함되며 requireExplictPolicy 하위 필드값으로 0을 사용하여 사용자 인증서의 인증서 정책을 검증하여야 한다.

모든 가입자 소프트웨어는 이 확장필드를 처리해야 한다.

6.2.11 확장 키 사용목적(Extended Key Usage)

확장 키 사용목적 확장필드는 키 사용목적 확장필드에서 나타낼 수 있는 것 이외의 공개키 사용목적을 명시하며 각각의 사용목적에 대한 OID로 나타낸다.

```
extKeyUsage EXTENSION ::= {
        SYNTAX          SEQUENCE SIZE(1..MAX) OF KeyPurposeId
```

```
        IDENTIFIED BY id-ce-extKeyUsage }
KeyPurposedId ::= OBJECT IDENTIFIER

id-kp-timeStamping          OBJECT IDENTIFIER ::= { id-kp 8}
id-kp-OCSPSigning           OBJECT IDENTIFIER ::= { id-kp 9}
```

공인인증기관의 OCSP 서버용 및 시점확인용 인증서인 경우 이 확장필드를 반드시 사용해야 하며 critical로 설정되어야 하고, 모든 가입자 소프트웨어는 이 확장필드를 처리해야 한다.

또한, 가입자 전자서명 인증서의 전자서명키가 [KCAC.TS.HSMU]을 준용한 보안토큰에서 생성될 경우 이를 인증서에 표시하기 위해 id-kisa-HSM 식별자를 사용한다. 이 경우 확장필드는 non-critical로 설정되어야 하고, 가입자 소프트웨어에서 이 확장필드의 처리는 선택사항으로 한다.

```
id-kisa-HSM                 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
            korea(410) kisa(200004) npki(10) attributes(1) kisa-HSM(2) }
```

6.2.12 인증서 효력정지 및 폐지목록 분배점(CRL Distribution Points)

인증서 효력정지 및 폐지목록 분배점 확장필드는 인증서의 상태정보를 확인하는 방법으로 인증서 효력정지 및 폐지목록을 사용하는 경우에 이를 획득할 수 있는 디렉토리 서버의 위치 정보를 나타낸다.

```
cRLDistributionPoints EXTENSION ::= {
        SYNTAX        CRLDistPointSyntax
        IDENTIFIED BY id-ce-cRLDistributionPoints }

CRLDistPointSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
DistribuiontPoint ::= SEQUENCE {
        distributionPoint   [0]   DistributionPointName OPTIONAL,
        reasons             [1]   ReasonFlags         OPTIONAL,
        cRLIssuer           [2]   GeneralNames        OPTIONAL }
DistributionPointName ::= CHOICE {
        fullName                  [0]   GeneralNames,
        nameRelativeToCRLIssuer   [1]   RelativeDistinguishedName }
```

공인인증기관과 사용자 인증서는 이 확장필드의 distributionPoint 하위필드를 반드시 포함해야 하며, 이 경우 DistributionPointName.fullName은 ldap 주소의 uRI 형태를 사용해야 한다. 해당 인증서의 CRL이 간접CRL인 경우에는 cRLIssuer 하위필드를 반드시 포함해야 한다.

이 확장필드는 사용해야 하며 non-critical로 설정되며, 모든 가입자 소프트웨어는 이 확장필드를 처리해야 한다.

6.2.13 발급자 정보 접근(Authority Information Access)

발급자 정보 접근 확장필드는 인증서를 발급한 인증기관에 대한 정보를 획득하고자 하는 경우에 사용되며 인증기관 정보에 접근하는 방법 및 위치정보 등을 포함한다.

```
AuthorityInfoAccessSyntax ::=
        SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE {
        accessMethod          OBJECT IDENTIFIER,
        accessLocation                GeneralName }

id-ad-caIssuers OBJECT IDENTIFIER ::= { id-ad 2 }
id-ad-ocsp OBJECT IDENTIFIER ::= { id-ad 1 }
```

이 확장필드는 사용자 인증서에 non-critical로 포함되며 모든 가입자 소프트웨어는 이 확장필드를 처리해야 한다. id-ad-ocsp를 사용하여 ocsp 서버에 접근하기 위한 URL을 나타내야 하며, id-ad-caIssuers를 사용하여 최상위인증기관 인증서 획득 정보를 포함할 수 있다.

7. 상호연동을 위한 요구사항

전자서명인증체계에서 사용되는 공인인증서는 이 규격에서 정의하고 있는 인증서 프로파일을 준수해야 한다.

만일, 상호연동용으로 사용되어 지는 공인인증서에 규격에서 정의되지 않은 확장

필드를 추가적으로 사용하고자 하거나, 확장필드의 값으로 규격에서 사용하도록 정의하고 있는 값 이외의 값을 추가적으로 사용하고자 하는 경우에는 해당 인증서의 상호연동성이 보장되어야 한다.

부록 1. 전자서명인증체계 공인인증서 프로파일 요약

가. 최상위인증기관 전자서명 인증서 프로파일

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x2(버전 3)	m	m	
2	Serial Number	INTEGER	자동할당	m	m	
3	Issuer		[KCAC.TS.DN] 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	[1]
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
4	Validity		최상위인증기관 CPS에 명시된 유효기간 준수	m	m	[2]
	notBefore	UTCTime		m	m	
	notAfter	UTCTime		m	m	
5	Subject		[KCAC.TS.DN] 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	[1]
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
6	Subject Public Key Info			m	m	
	algorithm	OID	전자서명인증체계 알고리즘 기술규격 준수	m	m	
	subjectPublicKey	BIT STRING		m	m	
7	Extensions	Extensions		m	m	
[1]	C=KR,O=KISA,OU=Korea Certification Authority Central,CN=KISA RootCA 숫자					
[2]	CA와 client는 UTCTime 및 GeneralizedTime 모두를 지원하는 것을 권고함					

2) 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier		최상위인증기관 인증서는 경로구축 대상이 아니므로 본 확장필드를 생성하지 않음	-	x	x	
	KeyIdentifier	OCTET STRING					
	authorityCertIssuer	GeneralNames					
	authorityCertSerialNumber	INTEGER					
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 정보의 160비트 해쉬값	n	m	m	
3	Key Usage	BIT STRING	KeyCertSing, cRLSign	c	o	m	
4	Certificate Policy			n	o	m	
	policyIdentifier	OID	최상위인증기관 인증서 정책		o	m	
	policyQualifiers				o	m	
	PolicyQualifierId	OID	CPS, UserNotice		o	m	
	Qualifier				o	m	
	CPSuri	IA5String	최상위인증기관 홈페이지 주소		o	m	
	UserNotice				o	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	공인인증서 표시규격 준수		o	m	
5	Policy Mappings		국가간 상호인증 고려	n	o	m	
	issuerDomainPolicy	OID					
	subjectDomainPolicy	OID					
6	Subject Alternative Names	otherName	id-kisa-identifyData에 한글실명	n	o	m	
7	Issuer Alternative Names	otherName	id-kisa-identifyData에 한글실명	-	x	x	
8	Basic Constraints			c	m	m	
	cA	TRUE			m	m	
	pathLenConstraint	INTEGER	국가간 상호인증 고려		o	m	
9	Policy Constraints			c	o	m	
	requireExplicitPolicy	INTEGER			o	m	
	inhibitPolicyMapping	INTEGER			-	-	
10	Name Constraints			c	o	m	
	permittedSubtrees	GeneralSubtrees					
	excludedSubtrees	GeneralSubtrees					
11	Extended Key Usage	OID		-	x	x	
12	CrlDistributionPoint			n	o	m	
	distributionPoint	DistributionPointName	ARL 획득 정보		o	m	
	reasons	ReasongFlags			o	m	
	cRLIssuer	GeneralNames	간접ARL발급시 사용		o	m	
13	Authority Information Access			-	x	x	
	accessMethod	OID	id-ad-caIssuers, id-ad-ocsp				
	accessLocation	GeneralName					

나. 공인인증기관 전자서명 인증서 프로파일

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x2(버전 3)	m	m	
2	Serial Number	INTEGER	자동할당	m	m	
3	Issuer		[KCAC.TS.DN] 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
4	Validity		최상위인증기관 CPS에 명시된 유효기간 준수	m	m	
	notBefore	UTCTime		m	m	
	notAfter	UTCTime		m	m	
5	Subject		[KCAC.TS.DN] 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
6	Subject Public Key Info			m	m	
	algorithm	OID		m	m	
	subjectPublicKey	BIT STRING		m	m	
7	Extensions	Extensions		m	m	

2) 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier		3가지 값을 모두 사용	n	m	m	
	KeyIdentifier	OCTET STRING			m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 정보의 160비트 해쉬값	n	m	m	
3	Key Usage	BIT STRING	KeyCertSing, cRLSign	c	m	m	
4	Certificate Policy			c	m	m	
	policyIdentifier	OID	공인인증기관 인증서 정책		m	m	
	policyQualifiers				o	m	
	PolicyQualifierId	OID	CPS, UserNotice		o	m	
	Qualifier				o	m	
	CPSuri	IA5String	공인인증기관 CPS 주소		o	m	
	UserNotice				o	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	공인인증서 표시규격 준수		o	m	
5	Policy Mappings			-	-	-	
	issuerDomainPolicy	OID					
	subjectDomainPolicy	OID					
6	Subject Alternative Names	otherName	id-kisa-identifyData에 공인인증기관 한글실명	n	m	m	
7	Issuer Alternative Names	otherName	id-kisa-identifyData에 최상위인증기관 한글실명	n	o	m	
8	Basic Constraints			c	m	m	
	cA	TRUE			m	m	
	pathLenConstraint	INTEGER	0		m	m	
9	Policy Constraints			c	m	m	
	requireExplicitPolicy	INTEGER	0		m	m	
	inhibitPolicyMapping	INTEGER			-	-	
10	Name Constraints			c	o	m	
	permittedSubtrees	GeneralSubtrees					
	excludedSubtrees	GeneralSubtrees					
11	Extended Key Usage	OID		-	x	x	
12	CrlDistributionPoint			n	m	m	
	distributionPoint	DistributionPointName	ARL 획득 정보		m	m	[1]
	reasons	ReasongFlags			o	m	
	cRLIssuer	GeneralNames	간접ARL발급시 사용		o	m	
13	Authority Information Access			-	x	x	
	accessMethod	OID	id-ad-caIssuers, id-ad-ocsp				
	accessLocation	GeneralName					
[1]	uri값으로 ldap://hostname[:portnumber]/dn[?attribute] 형식 사용						

다. 공인인증기관 시점확인 및 OCSP 서버용 인증서 프로파일

1) 기본필드 : 공인인증기관 전자서명용 인증서 프로파일과 동일

2) 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier		3가지 값을 모두 사용	n	m	m	
	KeyIdentifier	OCTET STRING			m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 정보의 160비트 해쉬값	n	m	m	
3	Key Usage	BIT STRING	Digital Signature, non-Repudiation	c	m	m	
4	Certificate Policy			c			
	policyIdentifier	OID	공인인증기관 인증서 정책		m	m	
	policyQualifiers				m	m	
	PolicyQualifierId	OID	CPS, UserNotice		m	m	
	Qualifier				m	m	
	CPSuri	IA5String	공인인증기관 CPS 주소		m	m	
	UserNotice				m	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	공인인증서 표시규격 준수		m	m	
5	Policy Mappings			-	-	-	
6	Subject Alternative Names	otherName	id-kisa-identifyData에 가입자 한글실명	n	m	m	
7	Issuer Alternative Names	otherName	id-kisa-identifyData에 발급기관 한글실명	n	o	m	
8	Basic Constraints			-	x	x	
9	Policy Constraints			-	-	-	
10	Name Constraints			-	-	-	
11	Extended Key Usage	OID		c	m	m	
12	CRL Distribution Point			n	m	m	
	distributionPoint	DistributionPointName	CRL 획득 정보		m	m	[1]
	reasons	ReasonFlags			o	m	
	cRLIssuer	GeneralNames	간접CRL발급시 사용		o	m	
13	Authority Information Access			n	o	m	[2]
	accessMethod	OID	id-ad-caIssuers				
	accessLocation	GeneralName					
14	OCSP No Check	OID	id-pkix-ocsp-nocheck	n	o	m	[3]
[1]	uri값으로 ldap://hostname[:portnumber]/dn[?attribute] 형식 사용						
[2]	OCSP 서버용 인증서를 공인인증기관이 발급하는 경우에는 반드시 생성 시점확인용 인증서의 경우에는 사용하지 않음						
[3]	OCSP 서버용 shortlived 인증서를 발행할 경우 사용 시점확인용 인증서의 경우에는 사용하지 않음						

라. 웹서버 보안 인증서 발급용 인증서 프로파일

1) 기본필드 : 공인인증기관 전자서명용 인증서 프로파일과 동일

2) 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier		3가지 값을 모두 사용	n	m	m	
	KeyIdentifier	OCTET STRING			m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 정보의 160비트 해쉬값	n	m	m	
3	Key Usage	BIT STRING	KeyCertSing, cRLSign	c	m	m	
4	Certificate Policy			n	m	m	
	policyIdentifier	OID	공인인증기관 인증서 정책		m	m	
	policyQualifiers				o	m	
	PolicyQualifierId	OID	CPS, UserNotice		o	m	
	Qualifier				o	m	
	CPSuri	IA5String	공인인증기관 CPS 주소		o	m	
	UserNotice				o	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	공인인증서 표시규격 준수		o	m	
5	Policy Mappings			-	-	-	
	issuerDomainPolicy	OID					
	subjectDomainPolicy	OID					
6	Subject Alternative Names	otherName	id-kisa-identifyData에 공인인증기관 한글실명	n	m	m	
7	Issuer Alternative Names	otherName	id-kisa-identifyData에 최상위인증기관 한글실명	n	o	m	
8	Basic Constraints			c	m	m	
	cA	TRUE			m	m	
	pathLenConstraint	INTEGER	0		m	m	
9	Policy Constraints			n	m	m	
	requireExplicitPolicy	INTEGER	0		m	m	
	inhibitPolicyMapping	INTEGER			-	-	
10	Name Constraints			c	o	m	
	permittedSubtrees	GeneralSubtrees					
	excludedSubtrees	GeneralSubtrees					
11	Extended Key Usage	OID		-	x	x	
12	CrlDistributionPoint			n	m	m	
	distributionPoint	DistributionPointName	ARL 획득 정보		m	m	[1]
	reasons	ReasongFlags			o	m	
	cRLIssuer	GeneralNames	간접ARL발급시 사용		o	m	
13	Authority Information Access			-	x	x	
	accessMethod	OID	id-ad-caIssuers, id-ad-ocsp				
	accessLocation	GeneralName					
[1]	uri값으로 ldap://hostname[:portnumber]/dn[?attribute] 형식 사용						

마. 가입자 전자서명 인증서 프로파일

1) 기본필드 : 공인인증기관 전자서명용 인증서 프로파일과 동일

2) 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier			n	m	m	
	KeyIdentifier	OCTET STRING	발급자 인증서의 KeyID		m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 정보의 160비트 해쉬값	n	m	m	
3	Key Usage	BIT STRING	Digital Signature, non-Repudiation	c	m	m	
4	Certificate Policy			b			[1]
	policyIdentifier	OID	공인인증기관 인증서 정책		m	m	
	policyQualifiers				m	m	
	PolicyQualifierId	OID	CPS, UserNotice		m	m	
	Qualifier				m	m	
	CPSuri	IA5String	공인인증기관 CPS 주소		m	m	
	UserNotice				m	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	공인인증서 표시규격 준수		m	m	
5	Policy Mappings			-	-	-	
	issuerDomainPolicy	OID					
	subjectDomainPolicy	OID					
6	Subject Alternative Names	otherName	id-kisa-identifyData에 가입자 한글실명과 VID	n	m	m	
		rfc822Name	가입자 이메일 주소		o	m	[2]
7	Issuer Alternative Names	otherName	id-kisa-identifyData에 공인인증기관 한글실명	n	o	m	
8	Extended Key Usage	OID	보안토큰 식별자 (id-kisa-HSM)	n	o	o	[3]
9	Basic Constraints			-	x	x	
	cA	FALSE					
	pathLenConstraint	INTEGER					
10	Policy Constraints			-	-	-	
	requireExplicitPolicy	INTEGER					
	inhibitPolicyMapping	INTEGER					
11	Name Constraints			-	-	-	
12	CRL Distribution Point			n	m	m	
	distributionPoint	DistributionPointName	CRL 획득 정보		m	m	[4]
	reasons	ReasonFlags			-	-	
	cRLIssuer	GeneralNames	간접CRL 발급시 사용		o	m	
13	Authority Information Access			n	m	m	[5]
	accessMethod	OID	id-ad-caIssuers, id-ad-ocsp		m	m	
	accessLocation	GeneralName			m	m	
[1]	전자우편 보안에 사용하고자 하는 경우 non-critical설정, 이외에 critical 설정 권고						
[2]	전자우편 보안에 사용하고자 하는 경우 rfc822Name 생성 권고						
[3]	[KCAC.TS.HSM]의 보안토큰 기반일 경우 보안토큰 식별자(id-kisa-HSM) 사용						
[4]	uri값으로 ldap://hostname[:portnumber]/dn[?attribute] 형식 사용						
[5]	전자우편 보안에 사용하고자 하는 경우 id-ad-caIssuers 생성 권고						

부록 2. 규격 연혁

버전	제·개정일	제·개정내역
v1.00	2000년 2월	·"전자서명 인증서 프로파일"로 제정
v1.10	2004년 6월	· 무선 전자서명 인증서 프로파일 규격 v1.21 흡수 통합 · 전체적인 문서 형식 및 구성을 전자서명인증관리체계 규격 문서양식에 맞게 개정 · 6. 전자서명 인증서 프로파일을 RFC3280에 적합하게 내용 수정 · 부록 1. 전자서명 인증서 프로파일은 RF3280에 적합하게 내용 수정 및 최상위인증기관 인증서, OCSP 서버용 인증서 프로파일 추가 · 부록 2. 전자서명 인증관리체계 OID 구조 삭제 · 부록 3. 전자서명 인증관리체계에서 지원하는 알고리즘 삭제
v1.20	2005년 12월	· 6.2.4 인증서 정책 확장필드 속성을 critical에서 both로 변경 · 6.2.6 주체 대체 이름 확장필드에 사용자 이메일 주소 포함 · 6.2.13 발급자 정보 접근 확장필드의 ic-ad-caIssuers 이용방법 변경 · 부록 1. 전자서명인증체계 공인인증서 프로파일 요약 수정
v1.50	2007년 3월	· 가입자 전자서명 인증서의 경우 전자서명키가 보안토큰내에서 생성될 경우 확장 키 사용목적(Extended Key Usage)을 사용할 수 있도록 하되, 속성은 non-critical 및 처리는 선택사항으로 설정 · [부록1] 라. 가입자 전자서명 인증서 프로파일의 확장키 사용목적(extended key usage) 속성 변경 ※ 속성 : non-critical, 생성(o), 처리(o)
v1.60	2008년 10월	· 관련 국내 표준 및 규격 갱신 내용 반영 · 법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.70	2009년 9월	· 공인인증서 암호 체계 고도화에 따른 암호 알고리즘 변경 내용 반영 · 웹서버 보안 인증서 발급용 인증서 프로파일을 부록 1의 라항으로 추가