인증기관간 상호연동을 위한 CTL 기술규격

CTL Technical Specification for the Interoperability of Certification Authorities

v1.40

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

인증기관간 상호연동을 위한 CTL 기술규격

CTL Technical Specification for the Interoperability of Certification Authorities

1. 개 요

서로 다른 PKI 도메인의 인증서들간에 상호연동성을 확보하기 위해 인증서 신뢰 목록(CTL : Certificate Trust Lists)에 대한 기술규격을 정의한다.

인증서 신뢰 목록에 대한 상호연동 기술규격을 정의함으로써 다양한 분야의 인증 서비스간 상호연동성을 확보할 수 있으며, 이에 따라 인증 서비스의 활성화를 기대할 수 있을 것이다.

2. 규격의 구성 및 범위

본 규격은 전자서명인증체계 인증기관간 상호연동을 위한 인증서 신뢰 목록의 기능적 요구사항을 명시하고 있으며, 크게 두 부분으로 나뉘어진다.

첫 번째로, 인증서 신뢰 목록에 대한 개념과 프로파일을 정의한다.

두 번째로, 인증서 신뢰 목록의 생성, 배포, 검증 등의 운영방안을 정의한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[PKCS1] RSA Laboratories PKCS#1, *RSA Cryptography Standard v2.1,* 2001

[X509] ITU-T Recommendation X.509(1997) | ISO/IEC 9594-1:2001, *Information technology - Open Systems Interconnection - The Directory : Authentication Framework*

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

[RFC2119] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997

[PKCS7] RSA Laboratories PKCS#7, *Cryptographic Message Syntax Standard, v1.5,* 1997.5

[PKCS9] RSA Laboratories PKCS#9, *Selected Object Classes and Attribute Types v2.0,* 2000.2

[FIPS 180-1] NIST FIPS PUB 180-1, *Federal Information Processing Standards Publication (FIPS PUB) 180-1, Secure Hash Standard,* 1995.4

[FIPS 180-2] NIST, FIPS PUB 180-2, *National Institute of Standards and Technology,* 2002

3.2 국내 표준 및 규격

[TTA-120001] TTA, *TTAS.KO-12.0001/R1, 부가형 전자서명 방식 표준 - 제2부 : 인증서 기반 전자서명 알고리즘, 2000*

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

[TTA-120011] TTA, *TTAS.KO-12.0001/R1, 해쉬 함수 표준 - 제2부 해쉬 암호 알고리즘 표준(HAS-160),* 2000

[TTA-120012] TTA, *TTAS.KO-12.0012, 전자서명 인증서 프로파일 표준,* 2000

[TTA-120013] TTA, *TTAS.KO-12.0013, 전자서명 인증서 효력정지 및 폐지목록 프로파일,* 2001

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) 공인인증서
다) 공인인증기관
라) 전자서명인증체계
마) 가입자
바) 이용자
사) 가입자 설비

4.2 용어의 효력

본 규격에서 사용된 다음의 용어들은 전자서명인증체계 인증기관간 상호연동을 위한 인증서 신뢰 목록의 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 약어들에 대해 추가적으로 정의한다.

가) CA : Certification Authority, 인증기관
나) OID : Object Identifier, 객체 식별자

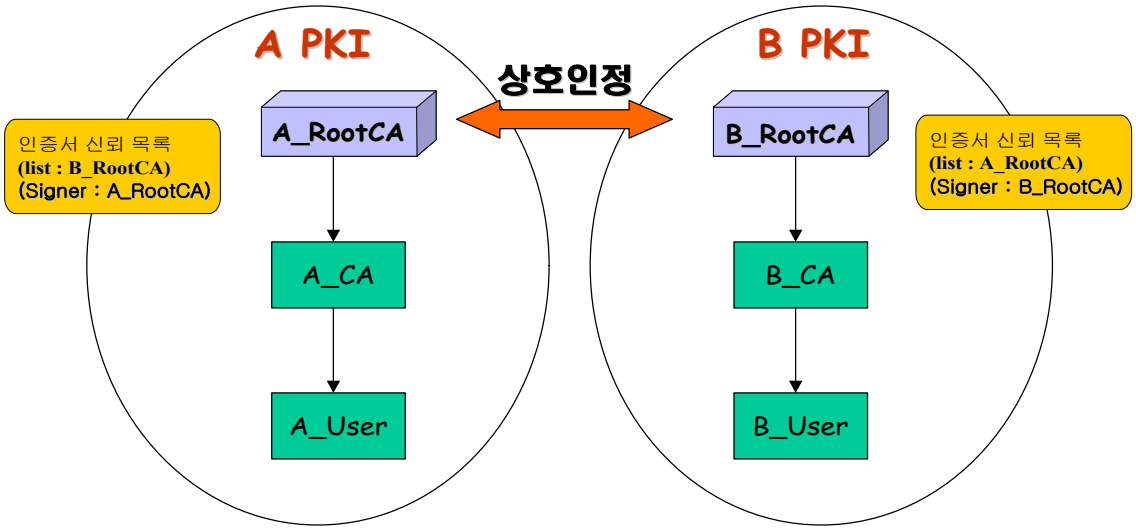
다) DN : Distinguished Name, 식별명칭
라) CN : Common Name, 객체 이름
마) PKCS : Public Key Cryptography Standard, 공개키 암호 표준
바) DAP : Directory Access Protocol, 디렉토리 접근 프로토콜
사) LDAP : Lightweight Directory Access Protocol, 경량 디렉토리 접근 프로토콜
아) CTL : Certificate Trust Lists, 인증서 신뢰 목록
자) ASN.1 : Abstract Syntax Notation 1, 추상적 구문 표기

6. 인증서 신뢰목록

6.1 인증서 신뢰목록 모델

인증서 신뢰 목록은 서로 다른 PKI 도메인간 상호연동의 한 방안으로써 상호연동 할 인증기관간 인증서를 배포하는 방안으로 이용되고 있다. 인증서 신뢰 목록은 인증기관들의 인증서 해쉬값을 리스트로 관리하며 [PKCS7]의 전자서명된 형태(SignedData)로 구성된다.

인증기관간 상호연동을 위하여 신뢰된 제 3자가 인증서 신뢰 목록을 발행하는 것이 아니라 각 PKI 도메인의 최상위 인증기관이 자신의 도메인에 인증서 신뢰 목록을 발행·관리한다.



[그림 1] 인증서 신뢰 목록 모델

6.2 인증서 신뢰목록 프로파일

6.2.1 인증서 신뢰목록 기본필드

6.2.1.1 버전(Version)

버전필드는 인코딩되는 인증서 신뢰목록의 버전을 나타낸다.

인증서 신뢰 목록의 버전은 1의 값을 가져야 한다.

6.2.1.2 주체사용(Subject Usage)

인증서 신뢰 목록의 사용목적을 명시하며 각각의 사용목적에 대한 OID로 나타낸다.

이 필드는 [TTA-120012]의 확장 키 사용목적(Extended Key Usage)과 같은 구조를 가진다.

해당 OID는 다음과 같다.

electronic-civil-application OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410) kisa(200004) npki-interoperability(8) ctl(1) subjectUsage(1) 1 }

6.2.1.3 식별자 나열(ListIdentifier)

인증서 신뢰 목록을 유일하게 식별할 수 있는 식별자로 Octet String으로 나타낸다.

본 규격을 준용하는 시스템은 이 필드를 사용하지 않아야 한다.

6.2.1.4 발급일자(This Update)

발급일자는 인증서 신뢰 목록이 인증기관에서 발급된 시점을 나타낸다.

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

6.2.1.5 다음 발급일자(Next Update)

다음 발급일자는 인증기관이 다음 인증서 신뢰 목록을 발급할 시점을 나타

낸다.

다음에 발급되는 인증서 신뢰 목록은 이 필드에서 지정한 일자보다 이전에 발급되어야 한다.

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

6.2.1.6 일련번호(Sequence Number)

일련번호 필드는 인증기관이 발급하는 인증서 신뢰 목록에 부여하는 양의 정수값으로 인증기관이 인증서 신뢰 목록 발행시 유일한 값이어야 하며, 인증서 신뢰 목록 사용자는 20 Byte까지 처리할 수 있어야 한다.

6.2.1.7 주체 알고리즘(Subject Algorithm)

신뢰 주체들 안에 포함되는 인증서를 해쉬하는 알고리즘에 대한 식별정보를 OID로 나타낸다.

이 필드는 [TTA-120011]에서 정의하고 있는 HAS-160 해쉬 알고리즘, [FIPS 180-1]에서 정의하고 있는 SHA-1 해쉬 알고리즘 혹은 [FIPS 180-2]에서 정의하고 있는 SHA-256 해쉬 알고리즘의 구조를 가져야 한다.

해당 OID의 정의는 다음과 같다.

```
has160 OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) korea(410) kisa(200004) npki-alg(1) 2 }

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

SHA-256 OBJECT IDENTIFIER ::= {
    iso(1) country(16) USA(840) US(840) company arc(1) US
    Government(101) Computer Security Objects Register(3)
    nistAlgorithms(4) 1 }
```

6.2.1.8 신뢰 주체들(TrustedSubjects)

인증서 신뢰 목록에 포함되는 인증서들의 해쉬값과 부가적인 속성값을 저장할 수 있다.

인증서의 해쉬값 계산에 사용되는 알고리즘은 '주체 알고리즘(Subject Algorithm)'에 명시된 해쉬 알고리즘을 이용하여야 한다.

6.2.2 인증서 신뢰 목록 확장필드(Extensions)

인증서 신뢰 목록을 실제로 운영함에 있어 요구되는 부가적인 정보들을 저장한다.

각각의 확장필드에는 criticality가 표시되어야 한다.

6.3 인증서 신뢰 목록 생성

서로 다른 PKI 도메인간 상호연동을 위한 상호인정 후 인증서 신뢰 목록을 생성하기 위해 필요한 상대 PKI 도메인의 인증기관 인증서의 해쉬값을 획득해야 한다. 인증기관 인증서의 해쉬값은 사전에 협의된 절차(예: 대면확인 방법)에 따라 교환하여야 한다.

각각의 인증기관은 획득된 인증서를 리스트로 가지는 인증서 신뢰 목록을 생성한다. 인증서 신뢰 목록의 발행자는 생성된 인증서 신뢰 목록을 [PKCS7]의 SignedData 형태로 전자서명 하여야 한다.

6.4 인증서 신뢰 목록 배포

인증서 신뢰목록은 디렉토리에 공고되어 사용자에게 배포되어야 한다.

사용자는 상대 도메인이 발행한 인증서 검증시, DAP 또는 LDAP을 통해 자신의 인증기관 디렉토리로부터 인증서 신뢰 목록을 획득한다. 인증서 신뢰 목록에 대한 디렉토리 스키마는 다음과 같이 정의하여 이용하고, certificateTrustList의 처리 속성은 바이러리 형식(certificateTrustList;binary)을 이용하여야 한다.

- Object-class : pkiCTL

```
pkiCTL OBJECT-CLASS ::= {
        SUBCLASS OF  { top }
        KIND  auxiliary
```

```
            MUST CONTAIN  { certificateTrustList }
            ID npki-interoperability(8) ctl(1) oc(2) pkiCTL(1)
    }
  - Attribute : certificateTrustList
    certificateTrustList ATTRIBUTE ::= {
            WITH SYNTAX  ContentInfo
            ID  npki-interoperability(8) ctl(1) at(3) certificateTrustList(1)
    }
  ※ ContentInfo는 [PKCS7]의 SignedData를 의미

pkiCTL OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410) kisa(200004)
      npki-interoperability(8) ctl(1) oc(2) 1 }

certificateTrustList OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410)
      kisa(200004) npki-interoperability(8) ctl(1) at(3) 1 }
```

6.5 인증서 신뢰 목록 갱신

인증서 신뢰 목록의 갱신은 다음과 같은 상황에서 일어날 수 있고, 이러한 경우 새로운 인증서 신뢰 목록을 발행해 디렉토리에 공고하여야 한다.

- 인증서 신뢰 목록에 포함된 인증서가 폐지될 경우
- 인증서 신뢰 목록에 새로운 인증서가 등록될 경우
- 인증서 신뢰 목록의 유효기간이 만료되었을 경우
- 인증서 신뢰 목록 필드의 값이 변경되었을 경우

6.6 인증서 신뢰 목록을 이용한 인증서 경로검증

6.6.1 검증 절차

[그림 2]는 인증서 신뢰 목록을 이용한 인증서 경로검증절차를 설명한 것이다.

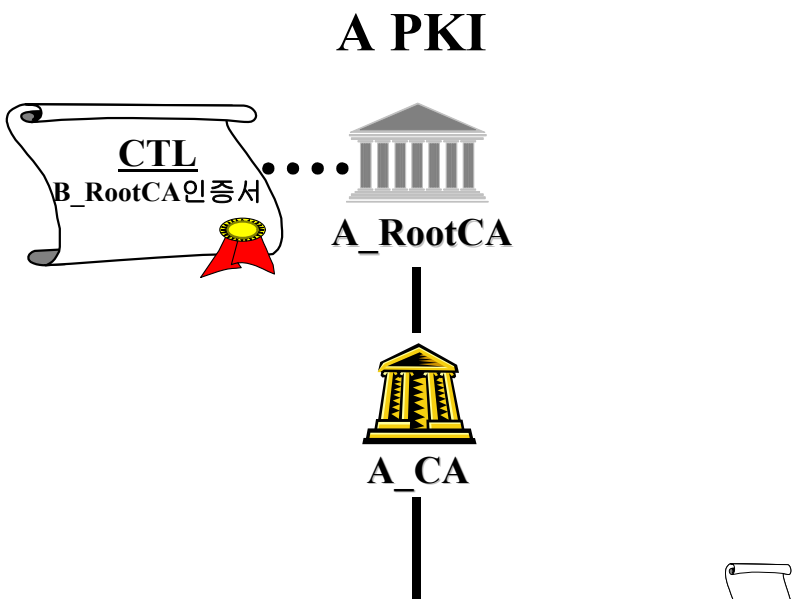
인증서를 검증하기 위해서는 먼저 인증 경로를 구성해야 한다. [그림 2]에서 A PKI의 A_User가 B PKI의 B_User 인증서를 검증할 때에 인증 경로는 다음과 같이 형성된다.

① B_RootCA 인증서
② B_CA 인증서

③ B_User 인증서

하지만, B_RootCA는 신뢰당사자인 A_User의 신뢰지점이 아니므로 자신의 신뢰지점인 A_RootCA 인증서와 A_RootCA가 발행한 인증서 신뢰 목록을 이용해, 다음과 같이 최종 인증경로를 생성하고 B_User 인증서를 검증한다.

① A_RootCA 인증서
② A_RootCA가 발행한 인증서 신뢰 목록
③ B_RootCA 인증서
④ B_CA 인증서
⑤ B_User 인증서



[그림 2] 인증서 신뢰 목록을 이용한 인증서 경로검증

신뢰당사자 A_User는 자신의 신뢰지점인 A_RootCA가 발행한 인증서 신뢰 목록에 B_RootCA의 인증서 해쉬값이 존재하는지 검증하고, 인증서 신뢰 목록은 A_RootCA의 인증서를 통해 검증하여야 한다.

6.6.2 인증서 신뢰 목록 검증

인증서 경로 검증시 인증서 신뢰 목록이 이용될 때 다음을 검증해야 한다.

① [PKCS7]의 ContentType이 SignedData에 해당하는 OID인지 검사
② [PKCS7]의 SignedData 및 SignerInfo의 버전 검사
③ SignedData→contentInfo→contentType이 CTL에 해당하는 OID인지 검사

④ SignerInfo→authenticatedAttributes의 속성값 검사
⑤ SingerInfo→encryptedDigest 검사(서명 검증)
⑥ 인증서 신뢰 목록의 버전 검사
⑦ 인증서 신뢰 목록의 유효기간 검사
⑧ 인증서 신뢰 목록의 이용범위 검사(Subject Usage : 주체 사용)
⑨ 해당 인증서가 인증서 신뢰 목록에 포함되는지에 대한 검사

7. 인증서 신뢰목록의 안전성 확보

인증서 신뢰목록은 공인인증체계의 전자서명키를 상향 조정하는 시점부터 본 규격 6.2.1.7절의 신뢰 주체들 안에 포함되는 인증서를 해쉬하는 알고리즘으로 256비트 이상의 출력값을 가지는 해쉬 알고리즘을 사용하여야 한다.

공인인증체계의 전자서명키를 상향 조정하는 시점은 미래창조과학부가 별도로 고시하여 정한날로 한다.

부록 1 인증서 신뢰 목록 ASN.1 코드

```
CTL03 DEFINITIONS ::=

BEGIN

-- EXPORTS All

IMPORTS

   AlgorithmIdentifier, Extensions, AttributeTypeAndValue, Time FROM
   PKIX1Explicit88 {iso(1) identified-organization(3) dod(6) internet(1)
   security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-explicit-88(1)} ;

CertificateTrustList ::= SEQUENCE {
        version             Version DEFAULT v1,
        subjectUsage        SubjectUsage,
        listIdentifier      ListIdentifier      OPTIONAL,
        sequenceNumber      INTEGER,
        thisUpdate          Time,
        nextUpdate          Time,
        subjectAlgorithm    AlgorithmIdentifier,
        trustedSubjects     TrustedSubjects,
        extensions          Extensions          OPTIONAL }

Version  ::= INTEGER { v1(0) }

SubjectUsage ::= SEQUENCE SIZE (1..MAX) OF CTLPurposeId

CTLPurposeId ::= OBJECT IDENTIFIER

ListIdentifier ::= OCTET STRING

TrustedSubjects ::= SEQUENCE OF TrustedCertificate
```

```
TrustedCertificate ::= SEQUENCE {
    trustedCertificateHash          HashValue,
    trustedCertificateAttributes    TrustedCertificateAttributes    OPTIONAL }

HashValue ::= OCTET STRING

TrustedCertificateAttributes ::= SEQUENCE OF AttributeTypeAndValue

electronic-civil-application OBJECT IDENTIFIER ::= { iso(1) member-body(2)
        korea(410) kisa(200004) npki-interoperability(8) ctl(1) subjectUsage(1) 1 }

pkiCTL OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410) kisa(200004)
        npki-interoperability(8) ctl(1) oc(2) 1 }

certificateTrustList OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410)
        kisa(200004) npki-interoperability(8) ctl(1) at(3) 1 }

signedData OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840)
        rsadsi(113549) pkcs(1) pkcs-7(7) 2 }

cTL OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6)
        internet(1) private(4) enterprises(1) microsoft(311) 10 1 }

contentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
        rsadsi(113549) pkcs(1) pkcs-9(9) 3 }

messageDigest OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
        rsadsi(113549) pkcs(1) pkcs-9(9) 4 }

kcdsa1WithHAS160 OBJECT IDENTIFIER ::= {
        iso(1) member-body(2) korea(410) kisa(200004) npki-alg(1) 22 }

kcdsa1WithSHA1 OBJECT IDENTIFIER ::= {
```

```
        iso(1) member-body(2) korea(410) kisa(200004) npki-alg(1) 23 }

rsaWithHAS160 OBJECT IDENTIFIER ::= {
         iso(1) member-body(2) korea(410) kisa(200004) npki-alg(1) 20 }

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

sha256WithRSAEncryption OBJECT IDENTIFIER ::= {
        iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

has160 OBJECT IDENTIFIER ::=  {
        iso(1) member-body(2) korea(410) kisa(200004) npki-alg(1) 2 }

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

id-sha256 OBJECT IDENTIFIER ::= {
        joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)
        nistalgorithm(4) hashalgs(2) 1 }

END
```

부록 2 PKCS#7의 SignedData ASN.1 코드설명

```
ContentInfo ::= SEQUENCE {
        contentType ContentType,
        content    [0] EXPLICIT ANY DEFINED BY contentType OPTIONAL }
```

※ *contentType에 SignedData OID를 명시*

```
   signedData OBJECT IDENTIFIER::= { iso(1) member-body(2) us(840)
        rsadsi(113549) pkcs(1) pkcs-7(7) 2 }
```

```
ContentType ::= OBJECT IDENTIFIER

SignedData ::= SEQUENCE {
        version Version,
        digestAlgorithms DigestAlgorithmIdentifiers,
        contentInfo ContentInfo,
        certificates [0] IMPLICIT ExtendedCertificatesAndCertificates
        OPTIONAL,
        crls [1] IMPLICIT CertificateRevocationLists OPTIONAL,
        signerInfos SignerInfos }
```

※ *SignedData→contentInfo→contentType필드에는 cTL OID를 명시*

```
   cTL OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) dod(6)
        internet(1) private(4) enterprises(1) microsoft(311) 10 1 }
```

※ *SignedData→contentInfo→content필드에는 CertificateTrustList가 포함됨*

※ *SignedData→certificates필드에는 SignedData에 서명한 인증서와 CTL에 포함되는 인증서를 포함할 수 있음*

※ *crls필드는 사용하지 않음*

```
DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

ExtendedCertificatesAndCertificates ::= SET OF ExtendedCertificateOrCertificate

ExtendedCertificateOrCertificate ::= CHOICE {
        certificate Certificate, -- X.509
        extendedCertificate [0] IMPLICIT ExtendedCertificate }
```

CertificateRevocationLists ::= SET OF CertificateRevocationList

SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
version Version,
issuerAndSerialNumber IssuerAndSerialNumber,
digestAlgorithm DigestAlgorithmIdentifier,
authenticatedAttributes [0] IMPLICIT Attributes OPTIONAL,
digestEncryptionAlgorithm DigestEncryptionAlgorithmIdentifier,
encryptedDigest EncryptedDigest,
unauthenticatedAttributes [1] IMPLICIT Attributes OPTIONAL }

※ *authenticatedAttributes필드에는 PKCS#9에서 명시된 contenttype, message digest속성을 포함해야함*

contentType OBJECT IDENTIFIER ::= { iso(1) member-body(2) us*(840) rsadsi(113549) pkcs(1) pkcs-9(9) 3 }*

messageDigest OBJECT IDENTIFIER ::= { iso(1) member-body(2) us*(840) rsadsi(113549) pkcs(1) pkcs-9(9) 4 }*

※ *unauthenticatedAttributes필드는 이용하지 않음*

IssuerAndSerialNumber ::= SEQUENCE {
issuer Name,
serialNumber CertificateSerialNumber }

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

EncryptedDigest ::= OCTET STRING

Attributes ::= SET OF Attribute

Attribute ::= SEQUENCE {
type AttributeType,
value AttributeValue }

```
AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= SET SIZE(1...MAX) OF AttributeValueItem

AttributeValueItem ::= ANY DEFINED BY AttributeType
```

부록 3. 규격 연혁

버전	제・개정일	제・개정내역
v1.00	2002년 4월	・"인증기관간 상호연동을 위한 CTL 기술규격"으로 제정
v1.10	2003년 11월	・전체적인 문서형식 및 구성을 전자서명인증체계 규격문서 양식에 맞게 개정 ・6.2.1.7절 주체 알고리즘(Subject Algorithm) 설명에 지원하는 해쉬 알고리즘 OID를 추가 함 - 전자서명 알고리즘은 본 규격이 인용하는 [PKCS1]과 [TTA-120001]에서 언급되고 있으므로 부록 3 제거 ・6.2.1.8절 신뢰주체들(TrustedSubjects) 설명에서 '상호연동할 인증서가 없을 경우에는 이 필드는 인증서 신뢰 목록에 나타나지 않는다' 문구 삭제 ・부록 1 인증서 신뢰목록 ASN.1 코드를 모듈형식으로 재구성하였고, 부록 4의 관련 OID를 부록 1에 흡수 통합 함 ・부록 1 인증서 신뢰목록 ASN.1 코드에서 CertificateTrustList 구조체내 trustedSubjects 변수의 'OPTIONAL' 조건 제거
v1.20	2004년 5월	・6.4 인증서 신뢰 목록 배포에서 인증서 신뢰목록의 배포위치를 디렉토리로 수정 ・6.6.1 검증 절차에서 인증서 신뢰목록의 발급과 배포는 앞절에서 논의되었으므로 삭제
v1.30	2008년 10월	・관련 국내 표준 및 규격 갱신 내용 반영 ・법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.40	2009년 9월	・공인인증서 암호체계 고도화에 따른 알고리즘 변경사항 반영