TTA 표준소개

전자서명인증서 프로파일 표준

이재일
TTA 시스템보안연구반 참관자
한국정보보호진흥원 전자서명인증관리센터장

1. 서론

글로벌 정보통신망을 통하여 전자문서 교환 및 전자상거래의 안전·신뢰성을 보장하기 위해서는 공개키 기반의 인증서비스가 필요하다. 세계 각국은 자국의 통신 인프라의 안전·신뢰성보장을 위하여 공개키 기반구조(PKI, Public Key Infrastructure)를 구축하고 있다. 그러나 글로벌 환경에서 각 국이 구축한 공개키 기반구조를 이용하여 국제거래 또는 서로 다른 도메인간의 인증서비스를 수행하기 위해서는 인증기관간의 상호호환을 위한 상호연동 및 상호인증이 선결되어야 한다. 이러한 문제를 해결하기 위해서는 인증기관간의 기술규격 및 표준을 만들고 그를 준용함으로써 가능하다. 국제표준화기구인 ITU-T, 인터넷에 적합한 표준을 개발하는 IETF(Internet Engineering Task Force), 산업체 표준을 추진하는 PKCS(Public-Key Cryptography Standards) 등에서는 공개키 기반구조의 상호호환성 유지를 위한 기술규격 및 표준제정을 위하여 노력하고 있다.

인증서의 상호연동 및 상호인증을 위하여 가장 중요한 기술요소는 거래문서에 대한 전자서명 알고리즘, 인증서 및 인증서 폐지목록 프로파일, 인증서 발급 및 관리를 위한 프로토콜, 인증서의 유효성을 확인할 수 있는 인증서 경로 검증방법 등이 있다.

본 고에서는 PKI 상호연동에 있어 가장 핵심적인 표준인 전자서명인증서 프로파일에 대하여 설명하고자 한다.

2. 국외 표준 현황

현재 인증서와 관련한 국제표준으로는 X.509 V3이 있다. 1988년 ITU-T(International Telecommunication Union Sector - Telecommunication)에서 X.509 V1이 처음 제정되었으며, 1993년 ITU-T에서 X.509 V2가 제정되었고, 1995년 이후 ISO/IEC 9594-8 문서와 동일시되어 공동개발되고 있다. 1997년 이후 X.509 V3(ISO/IEC 9594-8)이 제정되어 널리 사용되고 있으며, 2000년 X.509 네 번째 판이 제정된바 있다. X.509 V2까지 정의된 인증서 영

(그림 1) X.509 V3 인증서 프레임워크

역을 기본영역이라 하며, X.509 V3부터 추가로 정의된 부분을 확장영역이라고 한다.

현재 인터넷 표준 단체인 IETF(Internet Engineering Task Force)의 PKIX(Public Key Infrastructure X.509) 워킹그룹에서도 인증서에 대한 프로파일 표준을 제정중에 있다.

X.509 V3 인증서 확장영역은 공개키 기반구조에 유연성을 주기 위해 버전 3에서 추가된 부분이다. X.509 버전 3을 이용한 여러 시스템 간의 상호연동성을 위해서는 X.509 확장영역에 대한 프로파일을 결정하는 것이 매우 중요하다.

3. 전자서명인증서 프로파일 표준

3.1 표준의 목적

본 표준은 전자서명법상에서 구축된 전자서명 인증관리 체계내에서의 인증서 생성 및 인증서 처리에 대한 상호연동성을 보장하고 국제적인 호환성을 유지하고자 하는데 그 목적이 있다.

3.2 적용범위

본 표준의 적용대상은 인증서를 생성하는 인증 서버와 인증서검증을 위하여 사용되는 사용자 소프트웨어 등에 적용하여 사용할 수 있으며 안전한 전자우편, 웹서버 인증 또는 가상사설 네트워크 등 인증서를 이용한 인증기술을 사용하는 모든 응용에 대해서도 다양하게 활용할 수 있다.

3.3 표준의 구성 및 범위

본 표준의 구성 및 범위는 전자서명인증 관리체계에서 사용되는 전자서명용 및 시점확인용 X.509 V3 인증서에 대한 프로파일 규격을 정의하고 있으며 인증기관 및 응용 프로그램이 인증서를 생성 및 처리하는데 필요한 요구사항을 명시하고 있다.

3.4 표준의 주요 내용

주요 내용으로는 전자서명인증 관리체계 내

에서 사용되는 인증서에 대한 규격으로서 기본 필드 및 확장필드중 인증서 생성시에 요구되는 필드의 내용과 사용자 소프트웨어 등에서 인증서 처리시에 요구되는 확장필드에 대하여 정의하고 있으며 확장필드에 대한 criticality를 정의한다. 또한 국제표준 및 단체규격 등과 호환가능하도록 정의하여 상호연동성을 보장한다. 본고에서는 표준의 주요 내용에 대해 중요한 필드 위주로 간략히 소개하고자 한다.

3.4.1 인증서 기본필드

○ 버전(Version)

버전 필드는 인코딩되는 인증서의 버전을 나타낸다. 인증서는 버전 3의 값을 가져야만 하며 이 값은 정수 2로 표현한다.

○ 발급자(Issuer)/소유자(Subject)

발급자/소유자 필드는 인증서를 발급한 인증기관의 명칭을 DN 형식으로 표현하며 반드시 값을 가져야 한다. 한글을 사용하는 경우에는 UTF8 형식으로 표현한다.

3.4.2 인증서 확장필드

3.4.2.1 표준 확장(Standard Extensions)

○ 키 사용목적(Key Usage)

키 사용목적 확장필드는 소유자의 공개키가 사용되는 목적을 명시하며 정의되는 사용목적은 다음과 같다.

digitalSignature, non-repudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly

공인 인증기관 인증서는 keyCertSign 및 cRLSign 비트의 조합을 사용하며 사용자 인증서는 digitalSignature 및 nonRepudiation 비트의 조합을 사용한다.

keyUsage 확장필드는 공개키가 사용되는 목적을 정의하며 전자서명 검증용이 아닌 암호화용 및 키 동의용에 대해서는 본 표준에서 언급하지 않는다.

이 확장필드는 critical로 설정되어야 하며 모든 인증서에 포함되어야 하고 지정된 사용목적 이외로 사용되지 말아야 한다. 모든 응용프로그램은 이 확장필드를 처리할 수 있어야 한다.

○ 인증서 정책(Certificate Policies)

한글을 사용하여 인증서 정책에 대한 추가적인 정보를 나타내고자 하는 경우에는 UTF8 형식으로 표현한다. 모든 인증서에 이 확장필드가 포함되어야 하며 응용프로그램은 이 확장필드를 처리할 수 있어야 한다. 이 확장필드는 critical 또는 non-critical로 설정될 수 있다.

○ 인증서 정책 매핑(Policy Mappings)

이 확장필드는 상호인증용 인증서에 대해서 선택적으로 사용될 수 있으며 모든 응용프로그램은 이 확장필드를 처리할 수 있어야 한다.

○ 소유자 대체 명칭(Subject Alternative Name)

소유자 대체 명칭 확장필드는 소유자의 추가적인 명칭을 나타내며 인증서비스 영역내에서 사용되는 고유한 식별정보를 나타낼 수 있다. 소유자의 실명은 한글로 표현되어야 하며 realName 하위필드에 UTF8 형식으로 표현한다. 소유자의 고유정보는 선택적으로 저장할 수 있으며 전자적으로 가공되어 addInfo 하위필드에 저장된다. 소유자 고유정보는 실명과 고유식별정보로 이루어지며 이를 저장하는 명칭형식은 다음과 같이 정의한다.

id-kisa-identifyData OBJECT IDENTIFIER ::= { 1 2 410 200004 6 1 }

모든 인증서에 이 확장필드가 포함되어야 하며 응용프로그램은 이를 처리할 수 있어야 한다. 이 확장필드는 non-critical로 설정되어야 한다.

○ 확장 키 사용목적(Extended Key Usage)

확장 키 사용목적 확장필드는 키 사용목적 확장필드에서 나타낼 수 있는 것 이외의 공개키 사용목적을 명시하며 각각의 사용목적에 대해 OID를 사용하여 나타낸다. 인증기관은 선택적으로 이 확장필드를 생성할 수 있으며 시점확인용 인증서에 대해서는 반드시 포함하여야 한다.

시점확인용에 대한 확장 키 사용목적 OID는 다음과 같다.

id-kp-timeStamping OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 3 8 }

모든 응용프로그램은 이 확장필드를 처리할 수 있어야 한다. 이 확장필드는 critical 또는 non-critical로 설정될 수 있으며 특히 시점확인용 인증서에 대해서는 critical로 설정되어야 한다.

○ 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 위치정보를 나타낸다. 이 확장필드는 적어도 하나의 인증서 효력정지 및 폐지목록 분배점 위치정보를 포함하여야 한다. 이 확장필드는 모든 인증서에 포함되어야 한다. 인증기관 및 응용프로그램은 이 확장필드를 생성, 처리할 수 있어야 한다. 이 확장필드는 non-critical로 설정되어야 한다.

3.4.2.2 기타 인증서 확장필드

○ 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.

○ 대리인 (Procuration)

대리인 확장필드는 인증서 소유자로부터 권한을 대행받은 대리인이 존재하는 경우에 해당 대리인에 대한 정보를 포함한다. 이 확장필드에서는 대리의 유형 및 대리인에 대한 정보 등을 저장하며 다음과 같이 정의된다.

```
procuration EXTENSION ::= {
        SYNTAX                  ProcurationSyntax
        IDENTIFIED BY   id-kisa-at-procuration }
 id-kisa-at-procuration OBJECT IDENTIFIER ::= { 1 2 410 200004 4 1}
 ProcurationSyntax ::= SEQUENCE OF {
        country             PrintableString(SIZE(2)) OPTIONAL,
        typeOfSubstitution  TypeOfSubstitution OPTIONAL,
        signingFor                  SigningFor }
 TypeOfSubstitution         CHOICE {
        regType  DirectoryString,
        otherType SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER }
 SigningFor ::= CHOICE {
        thirdPerson                 GeneralName,
        certRef                     IssuerAndSerial }
 IssuerAndSerial ::= SEQUENCE {
        issuer                      GeneralNames,
        serial                      CertificateSerialNubmer }
```

권한 대행에 대한 정보는 국가코드를 나타내는 country, 대리 유형을 나타내는 typeOfSubstitution, 그리고 대리인을 나타내는 signingFor로 구성된다. 국가코드인 country 하위 필드는 권한대행을 부여한 국가에 대한 국가코드를 의미한다.

typeOfSubstitution 하위 필드는 대리인의 권한대행에 대한 유형을 나타내며 country 필드에서 지정한 국가에서 정한 대리 유형을 명시한다.

대리인을 나타내기 위해서는 signingFor 하위 필드를 이용하며 대리인의 정보는 대리인 명칭(thirdPerson) 또는 인증서(certRef)로 나타낼 수 있다. 이 확장필드는 사용자 인증서에만 사용될 수 있으며 인증기관 및 응용프로그램은 선택적으로 생성, 처리할 수 있다. 이 확장필드는 non-critical로 설정되어야 한다.

표 1. 인증기관 인증서 프로파일

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	m
Subject Key Identifier	n	m	m
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	m
Authority Information Access	n	o	o
Procuration	-	-	-

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

4. 결론

국내에서도 전자서명법의 시행과 공인인증기관 지정제도가 실시됨에 따라 활발한 인증서비스 제공이 기대되며 이를 기반으로 한 다양한 응용서비스가 개발될 것으로 예상된다. 또한 인증서비스 및 이와 관련된 수요가 증가하고 국제간 호환성을 보장하는 인증시스템의 개발이 시급하게 요구되고 있다. 이 시점에 인터넷 보안기술분야 민간업체들의 요구사항을 대폭 반영하여 독자적으로 인증서의 생성 및 처리에 대한 규격을 개발함으로써 상호호환성 및 국제 상호인증을 위한 기술력을 확보하였다고 할 수 있다.

본 표준은 국내 전자서명 인증관리체계가 구축되어 나가는데 발생할 수 있는 혼란을 최소화하고 인증 관련 기술의 발전과 관련 응용서비스 활성화에 기여할 것이다. 또한 전자상거래에 대한 신뢰성을 확보하여 전자상거래 시장을 자연스럽게 활성화시켜 나갈 것이다.