공인인증서 표시를 위한 기술규격

Notification Specification for Accredited Certificate

v1.11

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

공인인증서 표시를 위한 기술규격

Notification Specification for Accredited Certificate

1. 개요

전자서명법 제15조 제2항 9호의 규정에 따르면 공인인증서에 공인인증서임을 나타내는 표시가 포함되어야 한다. 이를 통해 이용자에게 전자서명법에 의한 법적 효력이 보장되는 공인인증서임을 표시함으로써 공인인증서에 대한 신뢰를 제고하고 이용 활성화에 기여 할 수 있다.

2. 규격의 구성 및 범위

본 규격은 공인인증서에 공인인증서임을 나타내기 위해 필요한 사항을 기술하고 있으며 크게 두 부분으로 나뉘어 진다. 첫 번째로 공인인증서 내 표시방법을 명시하고, 두 번째로 가입자 소프트웨어의 구현사항을 정의한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

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

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

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*, 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) 공인인증서
다) 공인인증기관
라) 전자서명인증관리체계
마) 가입자
바) 이용자
사) 가입자 설비

4.2 용어의 정의

정의하지 않음

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 DN을 생성하거나 처리하는데 따라야 할 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) CPS : Certification Practice Statement, 인증업무준칙
나) OID : Object Identifier, 객체 식별자
다) UTF8 : Universal Transformation Format, 8bit
라) ASN.1 : Abstract Syntax Notation One
마) RDN : Relative Distinguished Name

6. 공인인증서 내 표시방법

인증서 정책 확장필드의 UserNotice qualifier에 공인인증서임을 텍스트로 명시하여 해당 인증서가 공인인증서임을 나타낸다.

※ IETF PKIX RFC 3280의 CertificatePolicies 확장필드 구문에서 일부 발췌

```
Qualifier ::= CHOICE {
      cPSuri              CPSuri,
      userNotice          UserNotice }
CPSuri ::= IA5String


UserNotice ::= SEQUENCE {
      noticeRef           NoticeReference OPTIONAL,
      explicitText        DisplayText OPTIONAL}
```

```
NoticeReference ::= SEQUENCE {
        organization        DisplayText,
        noticeNumbers       SEQUENCE OF INTEGER }

DisplayText ::= CHOICE {
        ia5String           IA5String         (SIZE (1..200)),
        visibleString       VisibleString     (SIZE (1..200)),
        bmpString           BMPString         (SIZE (1..200)),
        utf8String          UTF8String        (SIZE (1..200)) }
```

본 규격에서는 CPSuri 및 UserNotice의 explicitText를 모두 사용하며, explicitText의 DisplayText 본문 구성은 다음과 같이 사용하여야 한다.

○ DisplayText = (한글) '이 인증서는 공인인증서입니다'
○ DisplayText = (영문) 'This certificate is licensed under Electronic Signature Act of the Republic of Korea'

한글의 경우 반드시 구현하여야 하며, 영문의 경우 선택적으로 구현 가능하다.

한글처리를 고려하여 DisplayText는 BMPString으로 생성하도록 한다. 현재 가장 널리 사용되는 MS explorer가 UTF8String 인코딩 방식의 DisplayText를 지원하지 못하므로 생성에서는 이를 고려하지 않는다. 응용어플리케이션은 DisplayText의 모든 타입을 처리할 수 있어야 한다.

DisplayText 타입	생성	처리
IA5String	o	m
VisibleString	o	m
BMPString	m	m
UTF8String	o	m

또한 인증서 정책 확장필드의 CPSuri에 공인인증기관의 CPS URI를 명시하여, 공인인증서를 사용하는 자가 해당 인증서의 정책정보를 획득할 수 있

도록 한다. CPSuri에 명시하는 CPS URI에 대해서는 https 또는 http를 이용하여 연결할 수 있다. 본 규격에서는 이용자에게 안전한 서비스 제공을 위해 https의 사용을 권고한다.

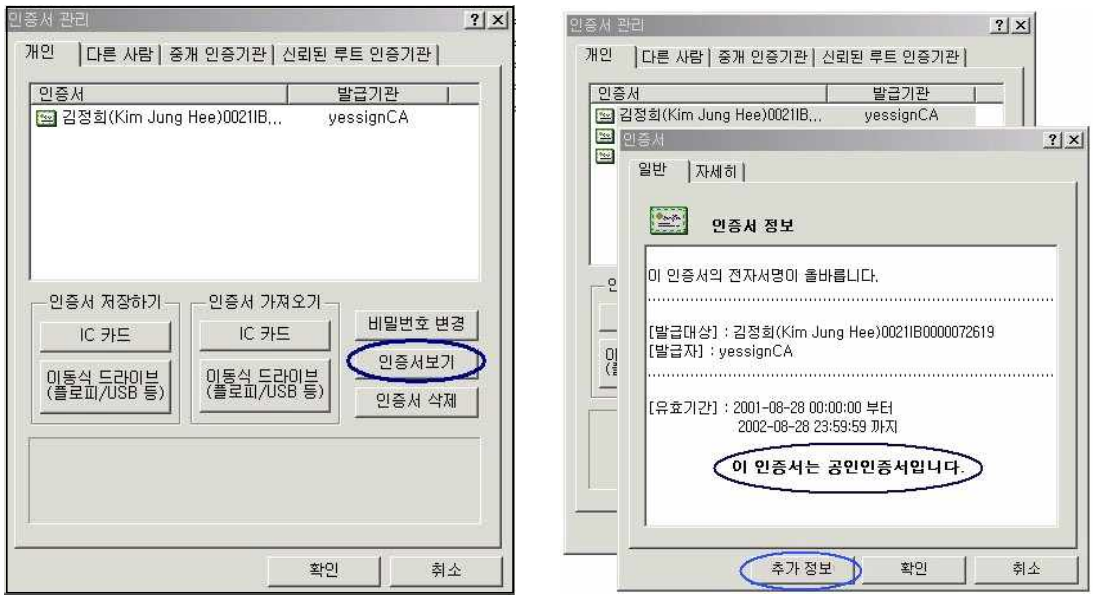
7. 구현

가입자 소프트웨어는 UserNotice의 explictText를 이용하여 이용자가 공인인증서 여부를 판별할 수 있도록 하는 기능을 제공하여야 한다. 수동으로 확인하는 방법은 반드시 구현하여야 하며, 자동으로 확인하는 방법은 선택적으로 구현 가능하다. 단, 자동으로 확인하는 방법을 구현하는 경우 본 규격에서 제공하는 사용자 인터페이스를 따를 것을 권고한다.

○ 수동으로 확인하는 방법

- 가입자 소프트웨어에서 '인증서 보기' 선택 시 인증서 메시지 창에 UserNotice의 explicitText 내용을 보여 줌

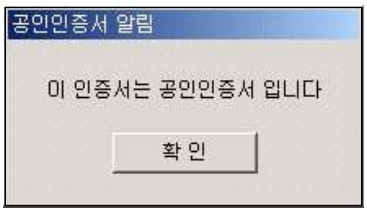
· 인증서 관리화면 및 인증서 화면 예



- '추가정보' 선택 시, CPSuri에 기술 된 인증업무준칙(CPS) 웹사이트를 제공함
  · 인증업무준칙(CPS) 제공 화면 예

○ 자동으로 확인하는 방법
- 인증서 발급 또는 인증서를 이용한 거래 시 UserNotice의 explicitText 내용을 팝업 창을 이용하여 보여 줌

· 팝업 창을 통한 공인인증서 표시화면



- 팝업 창에 대한 설정 및 해제 기능이 필요함
- '자동알림 설정'의 default는 '해제'로 함

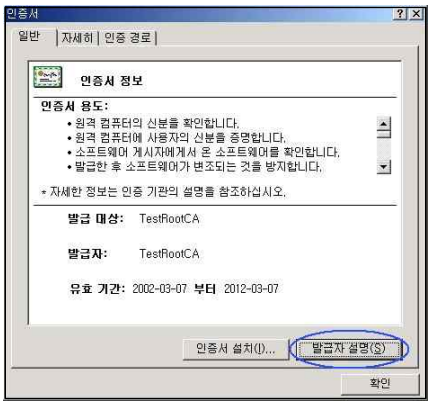
· 팝업 창 설정 및 해제 화면

8. 기술규격의 시행

본 기술규격은 2002년 9월 1일부터 시행한다.

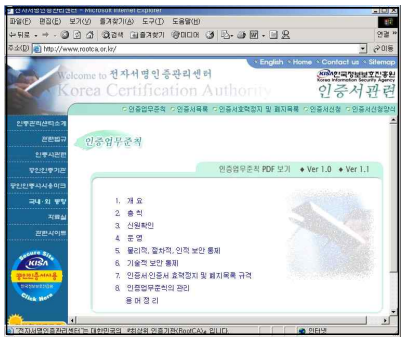
부록 1. MS Windows에서 공인인증서를 확인하는 방법

1. MS Windows에서 공인인증서 더블클릭하면, 다음과 같이 인증서를 보여줌



2. “발급자 설명” 선택 시, 새로운 창에 다음과 같이 사용자 알림 (userNotice) qualifier의 정보를 표시함

3. “추가정보” 선택 시, CPSUri에 기술된 인증업무준칙(CPS)으로 연결됨



부록 2. 규격 연혁

버전	제・개정일	제・개정내역
v1.00	2002년 5월	・"공인인증서 표시를 위한 기술규격"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