전자서명인증체계 공인인증서 갱신 규격

Accredited Certificate Update Specification

v1.11

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

전자서명인증체계 공인인증서 갱신 규격
Accredited Certificate Update Specification

1. 개요

본 규격에서는 전자서명인증체계 최상위인증기관과 공인인증기관의 인증서 갱신을 위한 절차, 최상위인증기관 인증서의 신뢰방안 등을 명시하였으며 공인인증기관 및 사용자 소프트웨어는 본 규격을 준수하여 전자서명인증체계 공인인증서(이하 인증서)의 갱신방안을 마련해야 한다.

2. 규격의 구성 및 범위

본 규격은 전자서명인증체계에서의 인증서 갱신 절차를 정의하였으며 다음과 같이 두 부분으로 나누어진다.

첫 번째로 인증서 갱신의 용어 정의 및 갱신시점, 갱신시 인증서 프로파일 등 인증서 갱신을 위한 기본적인 요구사항을 정의하고

두 번째로 갱신된 최상위인증기관 인증서의 배포방안, 인증서 검증 절차 등을 명시하였다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[X500] ITU-T Recommendation X.500 (2001) | ISO/IEC 9594-1:2001, *Information technology - Open Systems Interconnection - The Directory : Overview Of Concepts, Models and Services*

[X501] ITU-T Recommendation X.501 (2001) | ISO/IEC 9594-2:2001, *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

[RFC2459] IETF, RFC2459, *Internet X.509 Punlic Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile,* January 1999

[RFC2510] IETF, RFC2510, *Internet X.509 Punlic Key Infrastructure Certificate Management Protocols,* March 1999

[RFC3280] IETF, RFC3280, *Internet X.509 Punlic Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile, April* 2002

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

3.2 국내 표준 및 규격

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

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

[KCAC.TS.UI] KISA, KCAC.TS.UI, v1.80, *공인인증기관간 상호연동을 위한 사용자 인터페이스 기술규격*, 2009

[KCAC.TS.CERTVAL] KISA, KCAC.TS.CERTVAL, v1.11, *공인인증서 경로검증 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) 전자서명인증체계
다) 가입자
라) 가입자 소프트웨어

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 : Certificate Policy Statement, 인증업무준칙

6. 인증서 갱신의 정의

본 규격에서 정의하고 있는 인증서 갱신은 다음과 같은 경우에 적용된다.

6.1 유효기간 만료

인증서의 유효기간 만료에 따라 만료 시점 이전에 유효기간을 연장하여 인증서를 갱신하는 것이다. 이 경우 인증서 갱신 시점은 7.1 공인인증서 갱신 시점을 준용해야 한다.

6.2 가입자 정보 변경

인증서 소유자의 DN 등 인증서 내의 가입자 정보가 변경된 경우 해당 정보를 변경하여 인증서를 갱신하는 것이다. 이때 인증서의 유효기간은 연장 또는 승계될 수 있다.

6.3 인증서 프로파일 변경

전자서명인증체계내 인증서 프로파일 규격이 변경되면 체계내 모든 인증서는 즉시 갱신되어야 한다. 이때 인증서 유효기간은 연장 또는 승계될 수 있다.

7. 인증서 갱신 발급

7.1 인증서 갱신 시점

최상위인증기관 인증서의 잔여 유효기간은 공인인증기관 인증서의 유효기간보다 같거나 길어야 한다. 만일, 발급된 공인인증기관 인증서 만료일이 최상위인증기관 인증서의 만료일보다 이후 시점이 되는 경우에는 인증서 검증에 문제가 될 수 있다.

따라서 최상위인증기관 인증서 만료일에서 공인인증기관 인증서 유효기간을 뺀 시점 이전에 최상위인증기관 인증서는 갱신되어야 한다.

인증서 갱신 시점 = 발급자 인증서 만료일 - 하위인증서 유효기간

사용자 인증서를 발급하는 공인인증기관 인증서의 갱신시점도 위와 동일하게 계산된다. 사용자 인증서의 종류에 따라 서로 다른 유효기간을 사용하는 경우에는 유효기간이 가장 큰 값을 하위인증서 유효기간 값으로 사용하여 갱신시점을 계산한다.

최상위인증기관 인증서가 갱신되면 전자서명인증체계내 모든 사용자 소프트웨어는 갱신된 최상위인증기관 인증서를 즉시 배포 받아야 한다. 최상위인증기관 인증서의 배포방안은 8. 최상위인증기관 인증서 배포방안을 준수해야 한다.

7.2 전자서명키쌍과 인증서 DN

인증서 갱신시 전자서명키쌍은 교체할 수 있으며, 갱신후 인증서 유효기간 동안 키쌍의 안전성이 보장되면 동일한 키쌍을 사용하여 인증서를 갱신할 수 있다. 갱신되는 인증서의 DN은 갱신전 인증서 DN과 동일하거나 변경하여 발급할 수 있다.

7.3 인증서 프로파일

인증서 갱신시 준수해야 하는 인증서 프로파일은 [KCAC.TS.CERTPROF]이며, 인증서 유효기간 등과 관련된 자세한 사항은 최상위인증기관 CPS를 준용해야 한다.

8. 최상위인증기관 인증서 배포방안

인증서를 검증하고 활용하기 위해서는 최상위인증기관 인증서를 안전하고 신뢰성 있는 방법으로 배포해야 한다. 공인인증기관은 다음과 같은 방법을 사용하여 사용자에게 최상위인증기관 인증서를 배포할 수 있다.

8.1 CTL(Certificate Trusted List) 이용

최상위인증기관에서 발급하는 CTL에 갱신된 최상위인증기관 인증서를 추가하여 배포할 수 있다.

최상위인증기관은 갱신전 구 전자서명키와 갱신후 신 전자서명키를 모두 사

용하여 2개의 CTL을 발급·관리해야 한다. 구 전자서명키로 발급된 CTL은 최상위 인증기관 신인증서를 포함하고, 신 전자서명키로 발급된 CTL은 최상위인증기관 구인증서를 포함해야 한다.

최상위인증기관 구인증서가 만료되면 구 전자서명키로 발급된 CTL은 더이상 사용되지 않는다. 신 전자서명키로 발급된 CTL에 포함된 갱신전 최상위인증기관 인증서는 삭제되고 신 전자서명키로 발급된 CTL은 재발급되어야 한다.

CTL의 생성 및 검증, 디렉토리 스키마는 [KCAC.TS.CTL]를 준용해야 하며, CTL을 디렉토리에 배포할 때 신 전자서명키로 발급된 CTL은 구 전자서명키로 발급된 CTL과 동일한 엔트리(kisaCTL)에 공고된다.

CTL을 이용하여 최상위인증기관 인증서를 배포하는 경우 가입자 소프트웨어는 CTL을 획득, 처리할 수 있어야 한다. CTL 검증을 통해 신뢰성이 확인된 최상위 인증기관 인증서는 가입자 소프트웨어에 저장되어야 한다.

8.2 가입자 소프트웨어 기능 활용

공인인증기관은 가입자 소프트웨어의 업데이트 기능을 활용하여 최상위인증기관 인증서를 가입자에게 배포할 수 있다.

최상위인증기관 구인증서가 이미 설치된 가입자는 가입자 소프트웨어 업데이트 기능을 활용하여 최상위인증기관 신인증서를 배포 받을 수 있다. 이 경우에는 [KCAC.TS.UI]를 준용하여 최상위인증기관 인증서의 해쉬값 비교 후 해당 인증서의 신뢰성을 확인할 수 있도록 해야한다.

가입자 소프트웨어를 처음 설치하는 사용자의 경우에는 소프트웨어 초기 설치시 또는 소프트웨어 설치 후 업데이트 기능 활용 등의 방법을 통해 최상위인증기관 구인증서와 신인증서를 모두 배포 받을 수 있도록 해야 한다.

최상위인증기관 인증서의 신뢰여부 확인 기능과 관련된 자세한 사항은

[KCAC.TS.UI]를 준용해야 한다.

9. 인증서 검증

9.1 다수의 인증기관 인증서 관리

가입자 소프트웨어는 인증서 검증을 위해 갱신전 최상위인증기관 인증서와 갱신후 최상위인증기관 인증서를 모두 저장할 수 있어야 한다. 다수의 최상위인증기관 인증서 저장과 관련된 사항은 [KCAC.TS.UI]를 준용해야 한다.

9.2 인증서 경로 구축

가입자 소프트웨어는 인증서 경로 구축시 동일키와 동일DN으로 갱신된 인증기관 인증서를 구분하여 올바른 경로를 구축해야 한다. 즉, 동일키와 동일DN으로 공인인증기관 인증서가 갱신된 경우, 갱신전 발급된 사용자 인증서는 갱신전 공인인증서를 발급자 인증서로 인식하여 인증 경로를 구축해야 한다.

이를 위하여 가입자 소프트웨어는 인증서 경로 구축시 인증서의 발급자 공개키 식별자(Authority Key Identifier) 확장필드에 포함된 키 식별자, 발급자 인증서 DN, 발급자 인증서 일련번호를 모두 사용하여 동일키·동일DN으로 발급된 인증서를 구분할 수 있는 방법을 제공해야 한다.

인증서 경로 구축 및 검증과 관련된 자세한 사항은 [KCAC.TS.CERTVAL]를 준용해야 한다.

부록 1. 규격의 연혁

버전	제・개정일	제・개정내역
v1.00	2004년 6월	“전자서명인증체계 공인인증서 갱신 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