전자서명인증체계 시점확인 프로토콜 규격

Time-Stamp Protocol Specification

v1.11

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

전자서명인증체계 시점확인 프로토콜 규격

Time-Stamp Protocol Specification

1. 개 요

본 규격에서는 전자서명법에 따라 구축된 공인전자서명인증체계 시점확인 서비스에서 사용되는 시점확인 프로토콜을 규정한다.

2. 규격의 구성 및 범위

본 규격은 [RFC3161] 국제표준을 준수하여, 공인전자서명인증체계 시점확인 서비스에 사용되는 시점확인 요청·응답 메시지 형식, 시점확인용 인증서 정책 식별자(OID) 등 시점확인 프로토콜을 정의하고 있다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[RFC3161] IETF, RFC3161, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, August 2001

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

3.2 국내 표준 및 규격

해당사항 없음

3.3. 기타

해당사항 없음

4. 정의

본 규격에서 사용하는 용어의 정의는 제4장에서 정한 것을 제외하고는 관련 법령 등이 정하는 바에 의한다.

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) 공인인증서
나) 공인인증기관
다) 가입자

4.2 용어의 정의

해당사항 없음

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 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

해당사항 없음

6. 시점확인 프로토콜 요구사항

공인인증기관이 공인인증서를 기반으로 시점확인서비스를 제공하는 경우 [RFC3161]의 시점확인 요청・응답 메시지 형식, 시점확인용 인증서정책 식별자(OID) 등 시점확인 프로토콜을 준용하여야 한다. 다만, 공인인증기관은 필요한 경우 [RFC3161]과 다른 형식의 시점확인 프로토콜을 추가적으로 제공할 수 있다.

부록 1. 규격 연혁

버전	제・개정일	제・개정내역
v1.00	2007년 4월	・"전자서명인증체계 시점확인 프로토콜 규격"으로 제정
v1.10	2008년 10월	・특정 응용서비스의 시점확인 프로토콜을 추가로 제공할 수 있도록 개정
v1.11	2009년 9월	・공인전자서명인증체계 기술규격 개정에 따라 본문 내용 중 관련 기술규격 참조 변경 사항 개정