실시간 인증서 상태확인 기술규격

Online Certificate Status Protocol Specification

v1.21

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

실시간 인증서 상태확인 기술규격
Online Certificate Status Protocol Specification

1. 목적

본 규격은 전자서명인증체계에서 공인인증서비스 이용의 신뢰성 확보를 위한 인증서 유효성 확인 기능을 제공을 위해 필수적으로 요구되는 실시간 인증서 상태 확인 프로토콜(Online Certificate Status Protocol)을 규정한다.

2. 규격의 구성 및 범위

본 규격은 [RFC2560]을 준수하여 전자서명인증체계에서 이용되는 OCSP에 대한 규격을 정의한다.

첫 번째로, OCSP 인증서 발급 및 운영 모델을 명시하며 OCSP 서버와 클라이언트간 메시지 교환을 위한 프로토콜 및 공인인증서 효력정지 및 폐지정보 획득 방법에 대해 정의한다.

두 번째로, OCSP 서비스를 제공하기 위해 필요한 OCSP 서버 및 클라이언트 소프트웨어 요구사항을 명시한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[RFC2560] IETF RFC 2560 (1999), *Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

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

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

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

Authentication Framework

3.2 국내 표준 및 규격

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

[TTAS.KO-12.0001/R1] TTA, TTAS.KO-12.0001/R1, "부가형 전자서명 방식 표준 - 제2부 : 인증서 기반 전자서명 알고리즘", 2002년12월

[TTAS.KO-12.0011/R1] TTAS.KO-12.0011/R1, "해쉬 함수 표준 - 제2부 : 해쉬 암호 알고리즘 표준(HAS-160)", 2000

[KCAC.TS.DSCP] KISA, KCAC.TS.DSCP, *전자서명 인증서 프로파일 기술규격 v1.10,* 2004

[KCAC.TS.CRL] KISA, KCAC.TS.CRL, *전자서명 인증서 효력정지 및 폐지 목록 프로파일 v1.10,* 2004

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) 전자서명인증체계
나) 인증서
다) 공인인증서
라) 공인인증기관
마) 가입자

4.2 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 규격을 위하여 다음과 같은 용어들을 정의한다.

가) CA : Certification Authority, 인증기관
나) DN : Distinguished Name, 식별명칭
다) OCSP : Online Certificate Status Protocol, 실시간 인증서 상태확인 프로토콜

6. OCSP 모델

6.1 OCSP서버용 공인인증서 발급 모델

공인인증기관이 OCSP서버를 운영하고자 하는 경우 OCSP서버를 위한 공인인증서를 발급해야 한다. 본 기술규격에서는 OCSP서버를 위한 공인인증서를 최상위인증기관이 발행한 경우와 최상위인증기관이 발행한 공인인증기관의 공인인증서에 해당하는 공인인증기관의 전자서명 생성키로 발행한 공인인증서만

을 허용한다.

OCSP서버의 전자서명 생성키를 공인인증기관 CA서버의 전자서명 생성키와 동일하게 운영하는 것을 허용하지 않는다.

6.1.1 최상위인증기관이 발급하는 경우

공인인증기관이 OCSP서버를 운영하고자 하는 경우 OCSP서버를 위한 공인인증서를 최상위 인증기관에서 발급해 줄 수 있다. 이 경우 OCSP서버용 공인인증서 발급 모델은 그림 1과 같다.

OCSP 서버용 공인인증서 프로파일은 [KCAC.TS.DSCP]을 준용해야 한다.

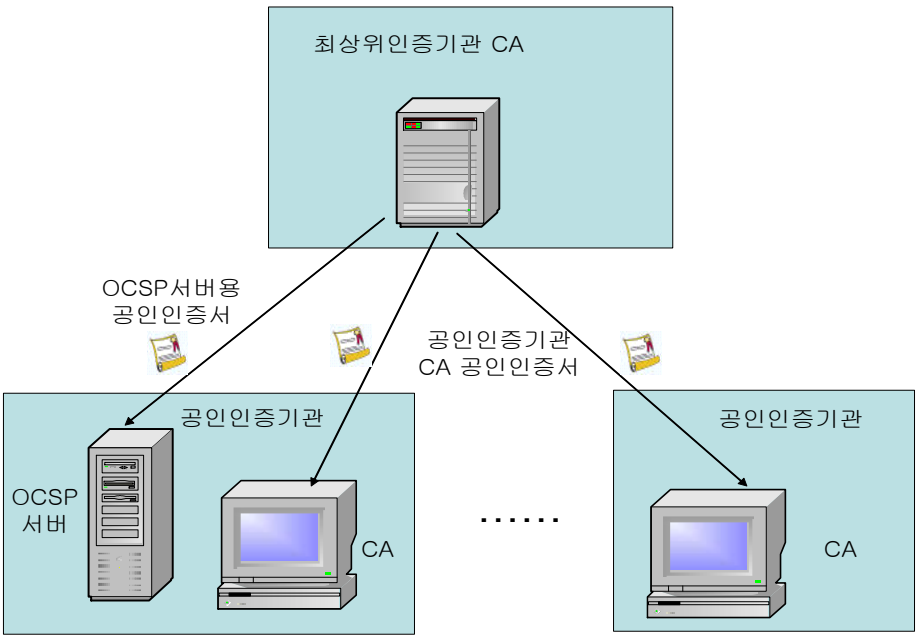

그림 1. 최상위기관이 OCSP서버용 공인인증서를 발급하는 모델.

6.1.2 공인인증기관이 발급하는 경우

OCSP서버를 위한 공인인증서를 공인인증기관이 직접 발행하여 사용할 수도 있다. 이 경우 OCSP서버용 공인인증서 발급 모델은 그림 2와 같다.

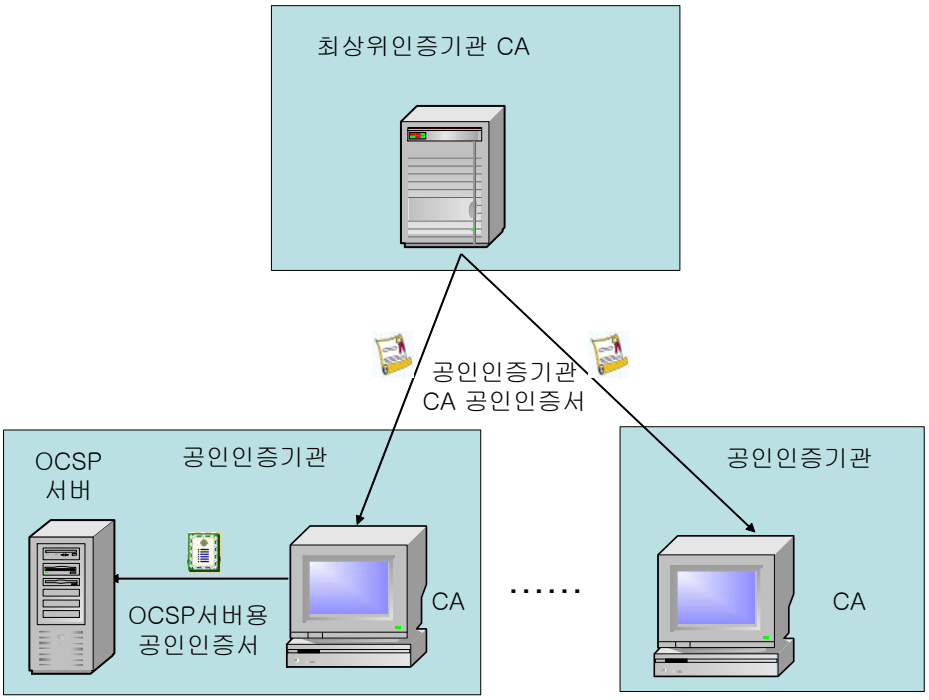

그림 2. 공인인증기관이 OCSP서버용 인증서를 발급하는 모델.

공인인증기관이 OCSP서버용 인증서로 shortlived 인증서를 발행할 경우 OCSP서버용 인증서 프로파일을 준수해야 하며 유효기간은 CRL 갱신주기에 비해 충분히 짧은 유효기간을 가져야 한다. 이용자는 OCSP서버용 인증서가 shortlived 인증서로 사용될 경우라도 CRL이외의 확장필드에 대한 검증은 반드시 수행해야 한다.

OCSP 서버용 shortlived 인증서 프로파일은 [KCAC.TS.DSCP]을 준용해야 한다.

6.2 OCSP서버 운영 모델

공인인증기관이 OCSP서버를 운영하기 위한 모델은 그림 3과 같다.

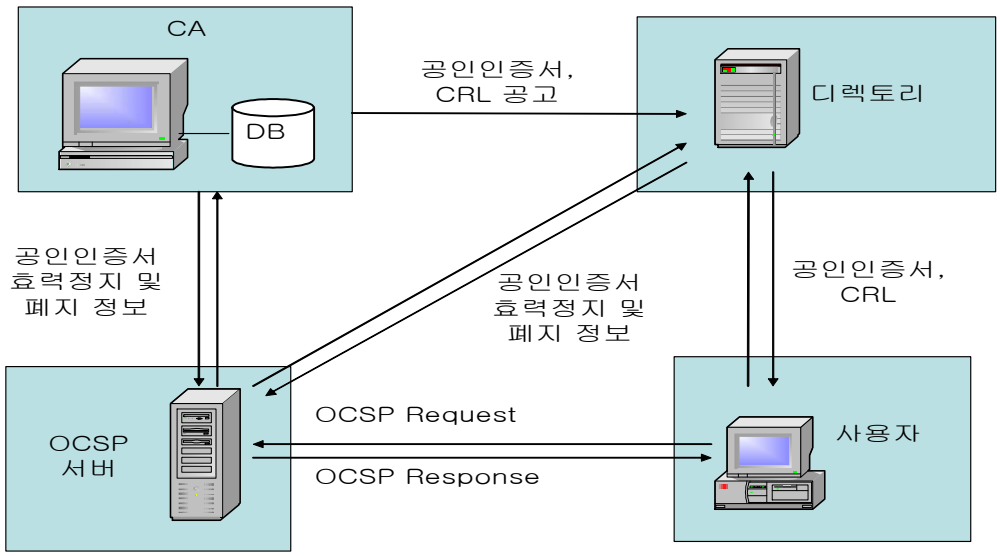

그림 3. OCSP서버 운영 모델.

OCSP서버는 이용자가 원하는 공인인증서 상태 조회 요청이 있을 경우 해당 공인인증서의 상태 정보를 이용자에게 응답하여 준다. OCSP서버는 해당 공인증서의 상태정보를 조회하기 위해 CA에서 제공되는 최신의 효력정지 및 폐지 정보를 획득·관리해야 한다.

OCSP서버와 이용자간의 상태 조회 요청 및 그 응답과 관련된 기술기준은 7.1절에 기술되어 있으며 OCSP서버가 최신의 효력정지 및 폐지 정보를 획득하기위해 필요한 사항들은 7.2절에 기술되어 있다.

7. 구성요소간 기준

7.1 OCSP서버와 클라이언트

OCSP서버는 적법한 클라이언트가 원하는 공인인증서의 상태를 조회할 수 있도록 한다. 이를 위해 OCSP서버와 클라이언트간의 메시지 교환을 위한 프로토콜은 [RFC2560]을 준용해야 한다.

공인인증서 상태 조회를 위한 요청 메시지와 응답메시지 전송을 위한 프로토콜은 HTTP를 사용해야 한다.

클라이언트가 OCSP서버 공인인증서를 획득하기 위하여 응답 메시지에 OCSP서버의 공인인증서를 포함하여 보내야한다.

OCSP 요청 및 응답은 재연 공격(replay attack)에 대처할 수 있도록 난수(Nonce)를 requestExtensions 및 responseExtensions에 반드시 사용해야 한다.

이용자가 요청한 인증서의 상태조회 결과가 폐기인 경우 이용자가 인증서의 폐지사유를 명확히 알 수 있도록 응답 메시지의 revocationReason 필드를 반드시 사용해야 한다.

7.2 OCSP서버의 공인인증서 효력정지 및 폐지정보 획득

OCSP서버가 공인인증서의 상태를 제공하기 위해서 공인인증서 효력정지 및 폐지정보를 획득·관리해야 한다. 이를 위해서 OCSP서버는 CA가 제공하는 최신의 공인인증서 효력정지 및 폐지정보를 획득해야 한다.

OCSP서버가 공인인증기관 내에 존재하여 CA서버 혹은 디렉토리 시스템으로부터 공인인증서 효력정지 및 폐지정보를 획득하는 경우 다음의 사항을 만족해야 한다.

- o OCSP서버가 클라이언트에게 제공하는 공인인증서 효력정지 및 폐지정보는 CA가 제공하는 최신 공인인증서 상태 정보가 모두 반영되어 있어야 한다.

- o OCSP서버가 공인인증서 효력정지 및 폐지정보 획득을 위해 CA서버에 접근하는 경우 CA서버는 OCSP서버에 대한 접근통제 기능을 가져야 한다.

- o CA서버가 공인인증서 효력정지 및 폐지정보를 제공하기 위해 OCSP서버에 접근하는 경우 OCSP서버는 CA서버에 대한 접근통제 기능을 가져야 한다.

- o OCSP서버에 제공된 공인인증서 효력정지 및 폐지정보에 대한 무결성을 보장할 수 있어야 한다.

부록 1. 규격 연혁

버전	제·개정일	제·개정내역
v1.00	2002년 6월	·"실시간 인증서 상태확인 기술규격"으로 제정
v1.10	2004년 5월	·전체적인 문서 형식 및 구성을 전자서명인증관리체계 규격 문서양식에 맞게 개정 ·OCSP관련 공인인증서 프로파일 내용 삭제(인증서 프로파일 기술규격에서 확인가능) ·OCSP서버 및 클라이언트 요구사항 삭제(정보통신부 고시 제2003-53호 참조) ·부록 1. 규격 연혁 추가
v1.20	2008년 10월	·관련 국내 표준 및 규격 갱신 내용 반영 ·법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.21	2009년 9월	·공인전자서명인증체계 기술규격 개정에 따라 본문 내용 중 관련 기술규격 참조 변경 사항 개정