# 실시간 인증서 폐지 정보제공을 위한 메커니즘

김동수*, 박세현*, 송오영*

*중앙대학교, 전자전기공학부

# A study of real time verification mechanism between CA and OCSP

Dong Su Kim*, Se Hyun Park*, Oh Young Song*

*Chung-Ang University, School of Electrical & Electronic Engineering

## 요 약

인터넷 금융거래나 전자 상거래 등에서 인증, 기밀성, 부인방인, 무결성을 제공하기 위한 목적으로 PKI를 사용한다. PKI 시스템에 있어서 공개키 알고리즘의 공개키에 대한 CA 인증의 유효성이 중요하다. 현재 널리 사용되고 있는 CRL를 이용한 인증서의 검증은 CRL의 주기적인 발행으로 인해 인증서 폐지 정보를 실시간으로 인증서 사용자에게 전달할 수 없다는 단점이 있다. 본 논문에서는 CRL를 이용하여 인증서 검증을 하는 OCSP 서버와 CA사이에 인증서 상태정보를 전달하는 메커니즘을 제안함으로서 OCSP를 이용하여 인증서 검증을 하는 인증서 사용자에게 실시간 인증서 검증 서비스를 제공하고자 한다.

## I. 서론

PKI(Public Key Infrastructure)는 비대칭 키 알고리즘을 이용하여 네트워크 상에서 인증, 기밀성, 무결성, 부인방지를 제공하기 위한 기반구조이다. PKI는 CA(Certificate Authority), RA(Registration Authority), 인증서 소유자 이루어져있다. 인증서 소유자는 개인키와 공개키 쌍을 생성하고 이중 공개키를 RA를 통해 CA로부터 인증 받게 된다. CA로부터 인증 받은 공개키는 인증서 형태로 외부에 공개하게 된다. 인증서는 인증서 소유자의 개인키로 생성된 사인값을 검증하거나 인증서 사용자에게 데이터를 암호화 하여 보낼 때 사용된다. 이때 인증서 사용자는 인증서를 사용하기 전에 인증서 자체가 유효한지를 검사하게 된다.[1]

인증서 사용자는 CRL(Certificate Revocation List)을 이용하여 인증서의 유효성 검사한다. CA는 인증서의 내용이 바뀌거나 인증서와 관련된 개인키가 노출 또는 분실되었을 때 해당 인증서 정보를 CRL에 담아 공고함으로서 폐지된 인증서들을 인증서 사용자들에게 알린다. 이때 CRL는 폐지된 인증서가 늘어날수록 크기가 커지게 되고 그에 따른 CRL를 처리하는 CA 및 인증서 사용자의 부하를 줄이기 위해 일정 주기별로 CRL를 발행하게 된다.

인증서 사용자는 OCSP(Online Certificate Status Protocol)를 이용하여 인증서의 유효성을 검사할 수 있다. OCSP는 CRL 사이즈가 커짐에 따라 CRL를 다루는 인증서 사용자의 부하를 줄이고 최신의 인증서 상태정보를 Online으로 확인하기 위해 사용된다.[2] OCSP가 인증서의 상태를 검증하기 위해서는 CA와 인증서 상태 정보 DB를 공유하거나 그 인증서를 발행한 CA로부터 CRL를 가져와 인증서 상태정보를 얻는다.

CRL를 통한 인증서 검증은 다음 CRL이 발행될 때까지 CRL 발행 후 폐지된 인증서의 폐지 정보를 알 수 없다는 것이다. 본 논문에서는 인증서 상태정보를 같은 도메인 내 또는 제휴 CA와 OCSP사이에 인증서 상태 정보를 공유함으로서 도메인내 인증서 사용자에게 인증서의 실시간 상태정보를 제공하는 메커니즘을 제안하고자 한다.

## II. 제안 메커니즘의 필요성

실시간으로 인증서 상태정보를 조회할 수 있는 OCSP는 이러한 문제를 해결하기 위해 표준으로 채택이 되었다.[3] 그러나 OCSP 또한 인증서 상태정보를 알아내기 위해 CRL를 사용하기 때문에 실시간 상태정보를 알아내기 위한 기능을 제대로 수행하지 못하는 문제점이 발생한다.

다음 그림 1는 기존의 CA와 OCSP사이의 인증서 폐지 정보공유 구조를 보여준다.

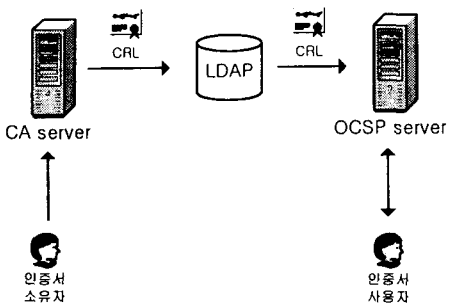


그림 1 기존 인증서폐지정보 공유 메커니즘

PKI표준에서 제시하는 PKI 구조는 주기적인 CRL의 발행과 그 주기에 의한 OCSP의 CRL의 조회에 의해 OCSP는 인증서 폐지정보를 획득한다. 이로 인해 CA 서버에서는 일정기간(주기 동안)동안 CRL발행에 대한 부하를 제거할 수 있고 OCSP 서버에서도 주기 동안 CRL를 읽어오지 않음으로서 네트워크를 통해 CRL를 읽어오고 이를 처리하는 데 필요한 부하를 제거할 수 있다.[4] 그러나 주기적인 CRL발생 메커니즘은 실시간 인증서 상태정보를 제공하지 못하는 문제가 있다. 이를 해결하기 위해 인증서 소유자에 의해 인증서 폐지 요청이 발생하면 CA는 인증서를 폐지하고 이에 대한 정보를 OCSP에게 보냄으로서 CA와 OCSP간의 인증서 상태정보를 동기화 할 것을 제안한다.

## III. 제안 메커니즘의 구조

그림 2는 본 논문에서 제안한 인증서폐지메시지를 이용한 인증서 폐지정보 공유 구조를 보여준다. 인증서 소유자가 인증서폐지 요청서를 CA에 보내면 CA는 이를 CA의 DB에 기록하고 그 정보를 OCSP에게 바로 알려준다. OCSP는 이 정보를 받아서 OCSP의 인증서 폐지정보 DB에 기록하게 된다.

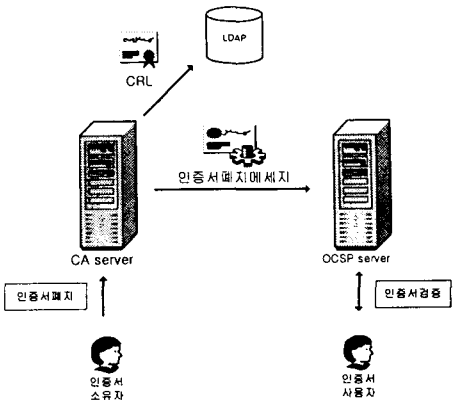


그림 2 본 논문에서 제안한 구조

이를 통해 CA와 OCSP 간에 인증서 폐지정보를 동일하게 유지시킴으로서 실시간 인증서 폐지정보 서비스를 인증서 사용자에게 제공하게 된다.

CA서버는 메시지 내용에 각 메시지의 일련번호를 부여하여 OCSP가 중간에 수신하지 못한 메시지가 있는지 체크 할 수 있도록 하고 Nonce를 부여하여 OCSP가 reply에 같은 값을 삽입하여 보냄으로써 중간에 제 3자가 메시지를 중간에 가로채고 replay attack을 통해 CA가 그 사실 모르도록 하는 것을 방지 한다.

또한 OCSP는 메시지를 수신하면 이를 처리하고 이에 대한 응답메시지를 CA서버에게 보낸다. 응답메시지를 통해 메시지 수신이 성공적이었는지 에러가 발생했는지를 알려주고 에러의 원인을 기록한다. CA서버에서는 reply에 기록된 에러를 체크하고 그 따라 에러를 수정할 수 있도록 한다.

OCSP가 실시간 인증서 상태 정보를 제공하기 위해 CA와 인증서 상태정보DB를 공유하는 경우 다음과 같은 문제점이 발생할 수 있다. 먼저 여러 CA가 하나의 OCSP와 각각의 CA DB를 공유하는 경우 OCSP가 제 3의 악의적인 공격자에게 공격당할 경우 연관된 모든 CA의 DB가 위험에 노출될 수 있다. 또한 하나의 CA가 여러 OCSP와 상태 정보를 공유할 경우 가장 취약한 OCSP를 통해 해커에게 CA를 노출시킬 위험이 있다.

본 논문에서는 CA의 인증서 상태 정보 DB를 직접 공유하지 않고도 OCSP를 통해 실시간 인증서 상태정보를 인증서 사용자에게 서비스 할 수 있는 장점이 있다.

## IV.제안 메시지 구조

### 1. 인증서폐지정보메시지

다음은 CA 서버에서 OCSP서버로 보내는 인증서폐지메시지의 내용이다.

```
RevokedCertMsg ::= SEQUENCE {
        revokedcertificates     RevokedCertificates
        signatureAlgorithm      AlgorithmIdentifier,
        signatureValue          BIT STRING }
```

□ signatureAlgorithm 필드는 메시지를 서명하기 위해 CA가 사용하는 암호 알고리즘의 식별자를 포함한다.
□ signaureValue 필드는 ASN.1 DER로 인코딩된 revokedcertificates에 기반을 두어 계산된 디지털 서명값을 가진다. ASN.1 DER 인코딩된 revokedcertificates은 서명함수의 입력 값으로 이용된다. 이 서명값은 ASN.1의 BIT STRING으로 인코딩 되어 RevokeCertMsg의 서명 필드에 포함된다.
□ revokedceritificate field는 폐지된 인증서에 대한 정보를 포함하고 그 구조는 다음과 같다.

```
RevokedCertificates ::= SEQUENCE {
    serialNumber          INTEGER,
    issuer                Name,
    userCertificate       CertificateSerialNumber,
    revocationDate        Time,
    nonce                 Nonce
    crlEntryExtensions    Extensions OPTIONAL
}
```

□ serialNumber는 인증서폐지정보메시지의 일련번호를 포함한다. 이를 통해 인증서폐지정보메시지가 누락되지 않고 OCSP로 전달이 되었는지 확인을 하기 위해 사용된다.
□ issuer 필드는 메시지를 보낸 CA의 이름정보를 기록한다. 인증서 폐지 메시지가 두 곳 이상에서 보내질 때 이를 이용하여 메시지의 출처를 구분하고 적절한 서명 검증용 공개키로 메시지를 검증하게 된다.
□ userCertificate에 폐지된 인증서의 일련번호를 기록한다. issuer의 필드에 기록된 CA의 인증서 일련번호를 통해 인증서 자체를 전송할 때에 비해 메시지의 크기를 줄일 수 있다.
□ revocationDate에 인증서가 폐지된 날짜를 기록한다.
□ nonce 메시지에 random하게 생성된 값을 넣어 응답의 nonce값과 비교하여 replay attack을 방지한다.
□ crlEntryExtensions
  ◦ Reason code : 인증서의 폐지의 원인을 정의.
  ◦ Hold instruction code : 정지상태에 놓인 인증서를 만났을 때의 동작을 지시하는 등록된 지시 식별자.
  ◦ Invalid date : 개인키가 노출되거나 인증서가 무효하게 된 날짜 등을 옵션으로 기록하고 이에 대해 사인을 하게 된다.

1) 응답메시지

```
RevokedCertRep ::= SEQUENCE {
   revokedresponse      RevokedResponse,
   signaureAlgorithm    AlgorithmIdentifier,
   signaureValue        BIT STRING
}
```

□ signaureAlgorithm 필드는 응답메시지를 서명하기 위한 서명 알고리즘의 정보를 포함한다.
□ signatureValue는 인증서폐지 정보메시지와 마찬가지로 revokedresponse의 서명값을 포함한다.
□ revokedresponse는 메시지수신에 대한 상태정보를 포함한다. 메시지구조는 다음과 같다.

```
RevokedResponse ::= SEQUENCE {
    serialNumber      INTEGER,
    issuer            Name,
    nonce             Nonce
    status            Status
}
```

□ serialNumber는 인증서폐지정보메시지의 일련번호를 포함하여 CA서버가 정상적인 응답메시지인가를 확인할 수 있도록 한다.
□ issuer는 CA 서버가 여러 OCSP서버로 메시지를 보낼 때 OCSP서버를 구분할 수 있도록 응답메시지 발행자 이름 정보를 포함한다.
□ status는 OCSP서버가 인증서폐지 정보메시지를 처리하고 그 결과를 기록한다.

```
Status ::= SEQUENCE {
 success BOOL,
 FailureInfo ::= BITSTRING{
        badAlg (0)
        badIssuer(1)
        badSerial(2)
        } OPTIONAL
}
```

## V. 본 논문에서 제안하는 OCSP의 내부구조

그림 3는 이 논문에서 제안한 메커니즘을 적용한 OCSP의 내부구조를 보여준다. OCSP는 같은 도메인내의 CA서버로부터 인증서가 폐지 될 때마다 메시지를 받게 된다. 이를 인증서 폐지정보 메시지 decoder를 통해 DB에 저장하게 된다.

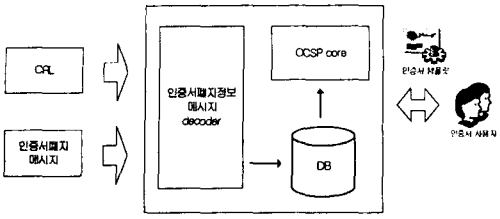


그림 3 OCSP 내부구조

OCSP는 인증서 사용자가 도메인 외부에서 받은 인증서의 상태정보를 요청할 때 인증서의 CRL Distribution Point에 담긴 위치 정보를 이용하여 CRL를 구해 상태검증을 하게 된다. 그러나 그림 3과 같이 인증서 사용자가 도메인 내의 인증서 폐지정보를 공유하는 CA로부터 발급 받은 인증서의 상태정보를 요청할 때는 해당 CA의 인증서 상태 정보 DB에서 바로 인증서 상태정보를 구해서 인증서 상태 정보 서비스를 할 수 있게 된다.

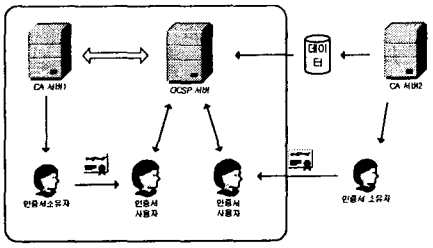

그림 4 전체 OCSP서비스 구조

## VI. 결론

데이터의 암호화나 사용자의 인증을 위해 PKI를 사용할 때 가장 중요한 점이 인증서의 유효성 여부이다. 이러한 인증서의 유효성을 CRL를 통해 검증한다면 현재 CRL의 발생시점과 다음 CRL의 발행 시점사이에 발생하는 인증서 폐지 정보는 사용자에게 전달되지 못한다. 본 논문에서 제안한 CA와 OCSP간에 인증서폐지 정보 메시지를 이용한 정보공유방식을 사용하면 OCSP는 CA와 동일한 인증서 상태 정보 DB를 공유 하게 됨으로서 실시간 인증서 폐지 정보를 제공할 수 있게 된다. 그러므로 이러한 메커니즘을 적용한 OCSP를 사용하는 인증서 사용자는 인증서에 대한 신뢰도를 높일 수 있다.

## 참고문헌

[1] R. Housley, W. Ford, W. Polk, and D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, 2002

[2] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, RFC 2560, 1999

[3] Russ Housley and Tim Polk, Planning for PKI, Wiley Computing Publishing, 2001

[4] Andrew Hash and William Duane and Celia Joseph and Derek Brink, PKI:Implementating and Managing E-Security, McGraw-Hill, 2001