# 시간 정보를 이용한 인증서 상태 검증 정보 제공에 관한 연구

곽 진*, 이승우*, 조석향*, 홍순좌**, 원동호*
*성균관대학교 전기전자 및 컴퓨터공학부
**국가보안기술연구소
e-mail : jkwak@dosan.skku.ac.kr

# A Study on Certificate Status Verification Information Providing using the Time-stamp Information

Jin Kwak*, Seung-Woo Lee*, Seok-Hyang Cho*, Soon-Jwa Hong**, Dong-Ho Won*
*School of Electrical & Computer Eng., Sungkyunkwan University
**National Security Research Institute

요 약

공개키 기반구조의 응용이 네트워크 상의 전자 거래로 확대됨에 따라 통신 상대방의 인증을 위해 인증서의 사용이 증대되었으며, 이 인증서는 사용하기 전에 반드시 검증 과정을 거쳐야 한다. 본 논문에서는 시간정보(Time-stamp Information)를 포함한 인증서 검증 프로토콜을 제안한다. 본 논문에서는 긴 길이의 폐지 정보와 주기적으로 발행되는 특징을 가진 인증서 폐지 목록 등 기존의 인증서 검증 메커니즘들이 가지는 문제점을 분석하고 현재의 인증서 상태에 대한 유효성뿐만 아니라 인증서 검증 결과에 시간 정보를 추가하여 보다 신뢰할 수 있는 인증서의 상태 검증 정보를 제공할 수 있는 프로토콜을 제안한다.

## 1. 서론

최근 인터넷의 급속한 발전과 함께 공개키 기반구조를 이용한 새로운 서비스들이 제공되기 시작하였으며, 이러한 서비스들에서 제공하고 있는 데이터의 기밀성과 통신 상대방의 인증을 위해 공개키 기반구조의 응용이 확대되었다. 특히 전자 거래에서의 공개키 기반구조 응용의 확대로 인증서의 사용과 검증에 대한 중요성이 증가하게 되었다. 공개키 기반구조를 이용한 서비스들은 통신하는 상대방의 공개키에 대한 유효성을 확인하기 위해 인증서를 사용하게 되었으며, 이 인증서는 사용하기 전에 반드시 검증 과정을 거쳐야 한다. 인증서의 검증 과정이란 인증서와 인증 경로상의 인증서들이 사용하고자 하는 시점에서 그 효력이 정지되었거나 폐지되었는지를 검사하는 것이다[1][2].

인증서의 상태를 검증하기 위한 방법으로는 현재 가장 널리 사용되고 있는 인증서 폐지 목록(CRL: Certificate Revocation List) 방식과 Delta-CRL 방식, 인증서 폐지 트리(CRT:Certificate Revocation Tree) 방식, Over-Issued CRL 방식, Indirect CRL 방식, 그리고 온라인 인증서 상태 검증 프로토콜(OCSP:Online Certificate Status Protocol) 방식 등이 있다[3].

본 논문에서는 기존의 인증서 상태 검증 방식이 지니고 있는 문제점을 분석하고 이를 개선하여 현재의 인증서 상태 정보의 유효성을 제공하고 특정 시점에서 사용했던 인증서의 상태에 대해 신뢰할 수 있는 시간정보를 포함한 인증서 상태 검증 정보를 제공하는 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 기존의 인증서 상태 검증 메커니즘에 관한 관련 연구에 대하여 알아본다. 3 장에서는 본 논문의 제안 배경과 제안하는 메시지 형식에 대하여 설명하고, 4 장에서 결론 및 향후 연구 계획에 대하여 언급한다.

## 2. 관련 연구

인증기관(CA:Certification Authority)으로부터 발급된 인증서는, 인증서 내에 포함된 공개키에 대응하는 비밀키가 손상되었거나 노출, 도난, 분실되는 경우에 인증서의 유효기간이 만료되기 전에 폐지 될 수 있다. 또한 이렇게 폐지된 인증서의 상태는 공개키 기반구조 내의 모든 사용자들에게 공지되어 다른 사용자가 해당 인증서를 사용하지 못하도록 해야 한다.

본 장에서는 기존의 인증서 상태 검증 방식 중에서 가장 널리 사용되고 있는 CRL 방식과 Delta-CRL 방식, 그리고 OCSP 에 대해서만 알아보도록 한다.

### 2.1 인증서 폐지 목록(CRL) 방식

CRL 을 이용하는 방식은 현재 가장 널리 사용되고 있는 인증서 상태 검증 방법이다. 이 방식은 사용자가 인증서를 폐지해 줄 것을 요청할 경우 인증기관이 인증서 폐지 목록(Certificate Revocation List)을 생성하여 배포함으로써 다른 사용자의 인증서 사용을 중지시키는 방식으로, 폐지된 인증서의 일련번호와 사유를 포함하여 전자서명 한 후, 디렉토리와 같은 공개된 장소에 게시하고 클라이언트는 이를 다운받아 필요로 하는 인증서를 검색하여 인증서의 상태 정보를 획득하는 방법이다. 이 방식은 인증서의 폐지 여부를 파악할 수 있는 가장 일반적인 방법으로 인증서의 폐지사유가 발생하였을 경우 인증서 폐지 목록에 새롭게 추가하여 주기적으로 발행하게 된다. 그러나 주기적으로 발행되는 특징으로 인해 인증서의 현재 상태를 제공할 수 없으며 CRL 전체를 다운 받아야 하므로 통신부담이 발생하는 문제를 가지고 있다[4][5].

### 2.2 Delta-CRL 방식

Delta-CRL 방식은 CRL 방식의 통신부담과 주기적으로 발행되는 문제를 개선하기 위해 제안된 방식이다. 이 방식은 전체 CRL 을 대상으로 하지 않으며 최근 CRL 이 발행된 시점에서 새로운 CRL 이 발행된 시점까지의 변화된 목록만을 대상으로 한다. CRL 보다 빈번하게 발행되지만 크기가 작기 때문에 통신부담을 줄이고 적절한 시기에 인증서의 상태를 제공할 수 있는 장점이 있지만, Delta-CRL 과 함께 전체 CRL 도 함께 발행해야 하는 문제점을 가지고 있다.[4][5]

### 2.3 온라인 인증서 상태 검증 프로토콜(OCSP)

OCSP 는 인증서의 현재 상태에 대한 정보를 제공하기 위해 제안된 프로토콜이다. 클라이언트와 서버의 형태로 구성되어 있으며, RFC2560 으로 정의되어 있다. 이 프로토콜은 온라인 상에서 서버와 클라이언트간에 수행되는 프로토콜로서 인증서의 효력 정지 및 폐지 상태를 CRL 을 사용하지 않고 확인할 수 있도록 사용자에게 제공하는 프로토콜이다. 클라이언트가 서버에게 원하는 인증서에 대한 정보를 요청하면 서버는 해당 인증서의 상태 정보를 검색하여 전자서명을 한 후, 이를 클라이언트에게 전달해주는 방식이다. OCSP 는 클라이언트가 인증서 상태 정보를 획득 하는 방식이지만 현재 구체적인 동작을 정의하고 있지 않으며 서버와 클라이언트 사이에 교환되는 메시지의 구성과 형태만을 ASN.1(Abstract Syntax Notation One)으로 정의하고 있다[6][7].

## 3. 제안하는 시간 정보를 이용한 인증서 상태 검증 정보 제공 프로토콜

인증서는 사용자들의 공개키 정보와 이름을 바탕으로 하여 인증기관의 비밀키로 서명을 하고, 이러한 과정을 통해 공개키에 대한 무결성을 제공해 준다. 인증서를 사용하거나 서명문을 검증하고자 하는 사용자는 공개키에 대한 인증서의 유효성을 확인한 후 서명문을 검증을 하거나 인증서를 사용하여야 한다.

### 3.1 제안 배경

2 장에서 살펴본 바와 같이 CRL 방식은 인증서의 상태 검증을 위해 널리 사용되고 있지만 인증서를 검증하고자 할 때마다 인증서 폐지 목록 전체를 다운받아야 하고, 인증서 폐지 목록의 크기가 커질수록 다운 받는 시간과 통신량이 증가하는 단점을 가지고 있으며, 시스템에 높은 부하를 주게 된다. 또한 Delta-CRL 방식과 CRT 방식 등도 주기적으로 발행되는 CRL 에 기반을 두고 있기 때문에, CRL 방식이 가지고 있었던 문제점을 완전히 개선하지는 못하였다.

본 논문에서는 인증서의 사용자들이 시간 정보를 이용하여 인증서 상태 검증 정보를 획득할 수 있는 프로토콜을 제안한다.

### 3.2 제안하는 프로토콜

본 논문에서 제안하는 시간 정보를 이용한 인증서 상태 정보 제공 프로토콜은 인증서의 현재 상태를 문의하는 요구 메시지와 이에 대한 검증 결과를 포함한 응답 메시지로 구성되어 있다.

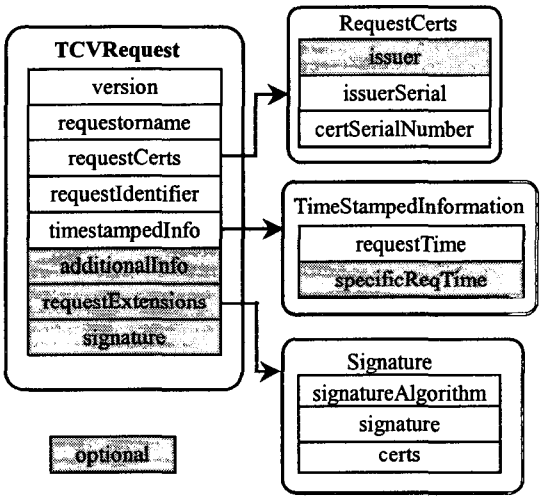
요구 메시지는 인증서를 사용하고자 하는 사용자(요구자)가 인증서 상태 검증 서버(응답자)에게 문의하는 메시지이며, 응답 메시지는 인증서의 상태 검증 결과에 시간정보를 포함하여 사용자에게 제공하는 메시지이다. 요구 메시지에는 시간 정보를 포함할 수 있는 필드를 정의하고 상태 검증을 요청하는 시간과 특정 시간에서의 인증서 상태 검증을 요구하는 필드로 구성되어 있으며, 응답 메시지에는 요청을 받은 시간과 사용자가 요구한 인증서의 상태를 검증한 시간, 응답 메시지를 전송한 시간을 포함하는 필드를 포함하고 있다. 이러한 시간정보를 포함한 필드를 이용하여 사용자는 자신이 원하는 특정 시간에서의 인증서 상태를 획득할 수 있으며 응답 메시지에 포함된 시간정보를 바탕으로 인증서의 유효성 여부에 대한 분쟁일 발생하였을 경우 분쟁 해결을 위해 사용할 수 있다. 응답자 또한 응답 메시지에 포함되어 있는 시간정보

를 이용하여 사용자가 신뢰할 수 있는 인증서 상태 검증 정보를 제공할 수 있다.

### 3.2.1 요구 메시지

사용자는 자신이 확인하고자 하는 인증서의 상태를 서버에게 문의하고 서버가 보내주는 응답 메시지를 확인하여 인증서의 유효성을 확인 할 수 있다. 이 메시지는 자신이 필요로 하는 정보만을 요구하게 되므로 통신 부담을 줄일 수 있다.

사용자가 인증서의 상태를 요구하는 메시지의 구조는 [그림 1]과 같으며, 사용자가 상태 확인을 요청하는 인증서의 정보와 시간 정보를 포함하는 구조로 이루어져 있으며, 요구자의 서명을 포함하고 있다.




[그림 1] 요구 메시지의 구조

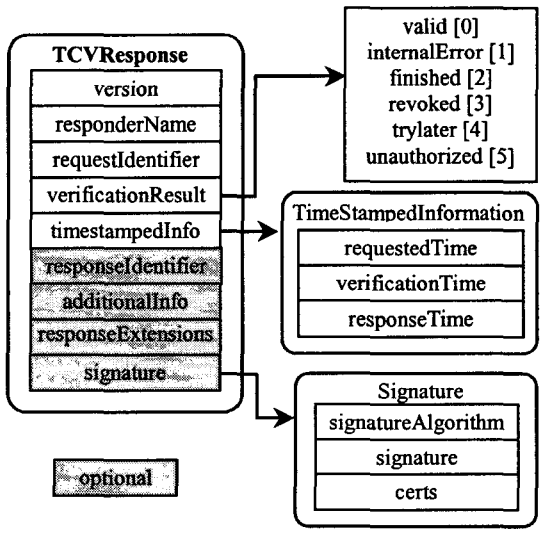
요구 메시지를 구성하는 각 필드들의 내용은 다음과 같다.

- ***version*** : 요구 메시지의 버전을 나타내며 default 값인 0 으로 표시되어 있다.
- ***requestorName*** : 인증서 상태 확인을 요구하는 사용자의 이름을 나타낸다.
- ***requestCerts*** : 사용자가 상태 확인을 요청하는 인증서의 정보를 포함하고 있으며 인증서의 발급자를 나타내는 issuer, 발급자와 인증서의 식별 번호를 나타내는 issuerSerial 과 certSerialNumber 로 구성되어 있다.
- ***requestIdentifier*** : 요구 메시지의 식별자를 나타내는 정보이다.
- ***timestampedInfo*** : 사용자가 요구 메시지를 전송한 시간과 메시지를 작성한 시간 정보를 나타내는 필드이다. 요구 메시지에 서명을 하고 전송한 시간 정보를 나타내는 requestTime 필드와 특정 시간에서의 인증서 상태 검증을 요구하는 specificReqTime 으로 구성되어 있다.
- ***additionalInfo*** : 요구 메시지의 부가적인 정보를 포함할 수 있는 필드로서 선택사항으로 처리되는 부분이다. 이 필드에는 상태 확인을 요구하는 인증서와 시간 정보를 포함하는 데이터에 대한 부가적인 정보 등을 포함할 수 있다.
- ***requestExtensions*** : 요구 메시지의 확장 영역을 나타내는 필드이다.
- ***signature*** : 인증서 상태 확인을 요구하는 사용자의 서명을 나타내는 필드로서, 서명에 사용된 알고리즘을 나타내는 signatureAlgorithm 과 서명값을 나타내는 signature, 사용자의 서명 검증용 공개키에 대한 인증서를 나타내는 certs 로 구성되어 있다.

### 3.2.2 응답 메시지

서버가 검색한 인증서의 상태 결과를 요청한 사용자에게 전송하는 메시지이다. 응답 메시지에는 현재의 인증서 상태와 시간 정보를 포함하여 사용자에게 제공되며, 일정한 응답 시간을 보장하여 요구와 응답 사이의 실시간 특성을 제공한다.

응답자가 사용자에게 전송하는 응답 메시지의 구조는 [그림 2]와 같으며 사용자가 요청한 인증서에 대한 상태 검증 결과와 응답자의 서명 등을 포함하고 있다.




[그림 2] 응답 메시지의 구조

응답 메시지를 구성하는 각 필드들의 내용은 다음과 같다.

- ***version*** : 응답 메시지의 버전을 나타내며 default 값인 0 으로 표시되어 있다.
- ***responderName*** : 인증서 상태 검증 결과를 사용자에게 제공하는 응답자의 이름을 나타낸다.
- ***requestIdentifier*** : 요구 메시지에 포함되어 있는 식별자와 같은 정보이다.
- ***verificationResult*** : 인증서 상태 검증 결과를 포함

하고 있는 필드로서, 인증서가 유효함을 나타내는 valid, 응답 서버가 내부적인 오류 상태임을 나타내는 internalError, 인증서의 유효기간이 경과했음을 나타내는 finished, 인증서에 대한 폐지 사유가 발생하여 폐지되었음을 나타내는 revoked, 응답 서버가 일시적으로 응답할 수 없는 상태를 나타내는 trylater, 인증서 상태 검증을 요구한 사용자가 인가되지 않았음을 나타내는 unauthorized 로 구성되어 있다.

- ***timestampedInfo*** : 응답자가 응답 메시지를 전송한 시간과 메시지를 작성한 시간 정보를 나타내는 필드이다. 응답 서버가 요구 메시지를 수신한 시간 정보를 나타내는 requestedTime, 인증서 상태 검증 과정을 마친 시간 정보를 나타내는 verificationTime, 응답 메시지에 서명하고 전송한 시간을 나타내는 responseTime 으로 구성되어 있다.
- ***responseIdentifier*** : 응답 메시지의 식별자를 나타내는 정보이다.
- ***additionalInfo*** : 응답 메시지의 부가적인 정보를 포함할 수 있는 필드로서 선택 사항으로 처리되는 부분이다. 이 필드에는 인증서 상태 검증 결과에 대한 사유 등을 포함할 수 있다.
- ***responseExtensions*** : 응답 메시지의 확장 영역을 나타내는 필드이다.
- ***signature*** : 인증서 상태 검증 결과를 제공하는 응답자의 서명을 나타내는 필드로서, 서명에 사용된 알고리즘을 나타내는 signatureAlgorithm 과 서명값을 나타내는 signature, 응답자의 서명 검증용 공개키에 대한 인증서를 나타내는 certs 로 구성되어 있다.

요구 메시지와 응답 메시지는 시간정보를 이용하여 인증서 상태 검증 정보 제공 프로토콜로서 CRL 을 기반으로 하는 기존의 인증서 상태 검증 메커니즘들이 가지고 있던 시간차(time gap) 문제를 해결할 수 있으며, 각각의 메시지에 포함되어 있는 timestampedInfo 필드를 이용하여 시점확인 기능을 제공할 수 있다. 요구 메시지에는 사용자가 메시지를 생성한 시간과 특정 시간에서의 인증서 상태 검증을 요청할 수 있도록 구성되어 있으며 현재의 인증서 상태 검증을 요구할 시에는 specificReqTime 을 사용하지 않고 메시지를 전송하게 된다. 응답 메시지에는 요구 메시지를 전송받은 시간과 인증서 상태 검증을 수행한 시간, 요구 메시지를 전송한 시간을 나타내는 필드를 포함하고 있으며, 인증서 상태 검증 수행 과정에서 오류가 발생하였을 경우에는 오류 발생에 대한 시간 정보를 제공하게 된다. 또한 요구와 응답메시지에 포함되어 있는 부가정보 지원 필드(additionalInfo)와 확장 영역(request & response Extensions) 필드를 이용하여 사용되는 환경과 정책 등에 대한 정보를 제공할 수 있다.

## 4. 결론 및 향후 연구계획

본 논문에서는 실시간 인증서 상태 검증 프로토콜의 특성뿐만 아니라, 요구와 응답 메시지에 포함된 데이터들에 대한 시간 정보를 포함하여 제공함으로써 인증서 상태 검증 결과에 대한 보다 높은 신뢰성을 제공한다. 제안하는 프로토콜은 제공되는 시간 정보를 바탕으로 인증서 상태 검증 결과에 대한 부인 방지 기능 또한 제공할 수 있으며, 전자 거래의 응용에서 거래 사실에 대한 부인방지 기능을 수행할 수 있다.

현재 실시간 인증서 상태 검증 메커니즘들이 계속해서 연구, 발표되고 있지만 실제 시스템에서 적용하기에는 완전하지 못한 문제점을 가지고 있다. 그러므로 본 논문에서 제안하는 프로토콜을 실제 시스템에 적용하기 위해서는 사용자와 서버, 서버와 인증기관 사이의 관계에 대한 명확한 규명과 각 구성 요소들의 요구 사항에 대한 철저한 분석 등에 대한 연구가 더 많이 진행되어야 할 것이다.

## 참고문헌

[1] ISO/IEC 9594-8. "Information thechnology Open System Interconnection The Directory : Authentication Frame Work", X.509, 1997

[2] R. Housley, W. Ford, W. Polk and D. Splo. "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, Jan. 1999

[3] N. Naor and K. Nissim. "Certificate Revocation and Certificate Update", In Proceeding of the 7th USENIX Security Symposium, 1998

[4] J. Willemson. "Certificate Revocation Paradigms", Technical Report, Cybernetica. 1998

[5] M. Just, S. Llotd, H. Meijer, "Certificate Revocation Performance Simulations, 2000

[6] M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams. "Internet X.509 Public key Infrastructure On-line Certificate Status Protocol-OCSP", RFC2560, 1999

[7] ISO/IEC 88240-1. "Information Technology-Abstract Syntax Notation One (ASN.1) : Specification of Basic Notation, 1997