실시간 인증서 상태검증의 성능개선

정 재 동† · 오 해 석††

요 약

실물 경제행위가 사이버 공간에서 이루어지게 되고 거래 상대방의 신원확인 문제가 대두되면서 전자서명이 보급되기 시작하였다. 인증서 폐지목록을 이용한 전자서명 검증방안이 실시간 검증에 대한 취약점을 내포하고 있었기 때문에, 온라인 인증서 상태검증이라는 방법이 도입되었다. 이 경우 사이버 거래의 전자서명 검증을 요구하는 모든 트랜잭션 부하가 한 곳의 서버노드에 집중되는 현상을 피할 수 없었다. 현재 국내 금융거래에서는 이 방법을 일부 도입하여 사용하고 있지만 곧 한계를 드러낼 전망이다. 본 논문에서는 실시간 검증을 보장하면서, 인증 검증을 요청하는 노드에서 실시간 인증서의 상태정보를 유지할 수 있는 방안을 제시하였다. 이 방법은 인증서를 폐지할 때 폐지관리 노드가 검증노드에 인증서 상태정보를 실시간으로 업데이트 시켜준다. 이 방법의 특징은 폐지관리 노드가 인증서 사용자들이 이용하는 검증노드의 리스트를 저장한다. 인증서 사용자가 처음으로 한 검증노드를 접속한다면 상위 폐지관리 노드까지 가서 인증서 상태정보를 확인하여야 하며 이 때 폐지관리 노드에 사용하는 검증노드가 저장한다. 그 이후에는 폐지관리 노드에 폐지요청이 발생할 때 그 인증서를 사용하는 모든 검증노드에 실시간으로 폐지정보를 전달한다. 제안한 방식의 장점은 인증서 검증이 검증 요청 노드에서 완료될 수 있어서 검증시간을 단축시킬 수 있다는 점과, 인증서 상태정보에 대한 요청이 폐지관리 노드 한 곳에 집중되는 것을 방지할 수 있다.

Improvement of Performance for Online Certificate Status Validation

Jai Dong Jung† · Hae Seok Oh††

ABSTRACT

According as the real economic activities are carried out in the cyber world and the identity problem of a trade counterpart emerges, digital signature has been diffused. Due to the weakness for real-time validation using the validation method of digital signature, Certificate Revocation List, On-line Certificate Status Protocol was introduced. In this case, every transaction workload requested to verify digital signature is concentrated on a validation server node. Currently this method has been utilized on domestic financial transactions, but sooner or later the limitation will be revealed. In this paper, the validation method will be introduced which not only it can guarantee real-time validation but also the requesting node of certificate validation can maintain real-time certificate status information. This method makes the revocation management node update the certificate status information in real-time to the validation node while revoking certificate. The characteristic of this method is that the revocation management node should memorize the validation nodes which a certificate holder uses. If a certificate holder connects a validation node for the first time, the validation node should request its certificate status information to the above revocation management node and the revocation management node memorizes the validation node at the time. After that, the revocation management node inform the revocation information in real-time to all the validation node registered when a request of revocation happens. The benefits of this method are the fact that we can reduce the validation time because the certificate validation can be completed at the validation node and that we can avoid the concentration of requesting certificate status information to a revocation node.

키워드 : 공개키 기반구조(PKI), 실시간 인증서 상태 검증(Online Certificate Status Validation), 인증서 폐지목록(CRL), 온라인 인증서 상태 프로토콜(OCSP)

1. 서 론

네트워크 상에서 양자간에 정보를 송수신할 때, 직접 상대방과 만나서 정보를 전달하는 것과는 달리 다음과 같은 문제가 발생할 수 있다. 정보를 교환하고 있는 사람이 정확히 누구인지, 전달하는 정보가 정확히 전달되는지, 제3자가 불법적으로 정보를 도청하지는 않는지에 관한 확인과정이 필요하다. 이러한 문제는 일반적으로 인증(authentication)과 암호(Encryption)화의 과정을 거쳐 해결할 수 있다.

인증과 암호화는 신원확인, 데이터의 무결성, 데이터의 기밀성 및 부인방지 기능을 제공한다. 국내에서는 전자서명법을 기반으로한 공인 인증서를 사용하여 법적인 보호 아래 사이버상의 전자적 거래를 수행할 수 있다. 또한 인증서는 개인키분실, 자격상실, 키변경 등의 이유로 폐지가 가능하다. 이런 경우 검증자는 수신한 인증서 상태가 유효한 것인

† 정 회 원 : 한국증권전산 공인인증센터장 보안연구소장
†† 종신회원 : 숭실대학교 정보과학대학 교수
논문접수 : 2002년 12월 20일, 심사완료 : 2003년 6월 25일

지를 확인해야 하는데 이것을 "인증서 유효성 검증"이라고 한다[1].

인증서의 유효성을 검증하기 위한 방법으로는 인증서폐지목록(CRL, Certificate Revocation List)[2]을 이용하는 방법과 실시간 인증서 상태를 조회할 수 있는 온라인 인증서 상태 프로토콜(OCSP, Online Certificate Status Protocol)[3]을 이용하는 방법이 있다. 인증서 폐지목록을 사용하는 경우에는 폐지목록이 갱신되는 주기에 따라 그 사이에 폐지된 인증서에 대하여 실시간으로 상태정보를 전파하지 못하는 단점이 있고, 온라인 인증서 상태 프로토콜을 이용하는 경우 모든 검증 트랜잭션에 대해 하나의 노드에서 응답하여야하는 구조적인 집중화 문제가 잠재되어 있다. 따라서 금융거래와 같이 실시간 응답시간이 중요한 경우 적합하지 않다[4].

본 논문은 인증서를 검증할 때 검증주체가 실시간 인증서 상태정보를 유지하면서 요청에 대한 응답의 집중화 문제를 해결하여 검증속도와 효율을 향상시키고자 한다. 제안하는 알고리즘은 서명자의 인증서 상태정보를 관리하고 폐지정보를 실시간으로 전송한다. 따라서 검증자는 요청한 인증서에 대하여 이미 저장되어 있는 정보를 사용함으로써 검증속도를 개선한다.

본 논문의 구성은 다음과 같다. 2장에서는 인증서 상태검증에 대한 기존방안을 분석하고, 3장에서는 기존 방식의 문제점을 분석한다. 4장에서는 성능이 개선된 실시간 인증서 상태 검증 방안을 제안하고 5장에서는 그에 따른 실험결과를 제시한다. 마지막으로 6장에서는 결론을 맺는다.

2. 기존 인증서 상태검증 방안 분석

인증서는 발급 시점부터 일정기간을 사용할 수 있는데, 이를 유효기간이라 한다. 유효기간내에 개인키분실, 자격상실, 키변경 등의 이유로 인증서를 폐지 할 수 있다. 인증서 소유자는 인증기관인 CA(Certificate Authority)에 인증서 폐지를 요청하며, 인증기관은 검증자에게 인증서 상태정보를 게시한다. 이러한 과정을 통해 폐지된 인증서는 사용이 허가되지 않는다[5].

인증서 상태검증 방법에는 대표적으로 CRL과 OCSP 방식이 제시되었다. CRL은 인증기관에 의해 제시된 인증서 폐지목록으로 디렉토리에 게시한다. 그러나 일정기간을 가지고 게시하기 때문에 실시간의 인증서 상태정보를 제공하지 않는다. 실시간 정보제공을 위해 OCSP 방식이 제안되었다. OCSP 클라이언트가 OCSP 서버에 인증서 검증시 매번 요청하는 방법으로 실시간 정보를 제공한다.

2.1 인증서 폐지 목록(CRL : Certificate Revocation List)

CRL은 인증기관이 게시하는 인증서 폐지 목록으로 검증자는 검증시 해당 인증서의 폐지 여부를 확인한다. (그림 1)에는 X.509 V2의 CRL 프로파일을 기술하였으며, thisUpdate는 게시시점과 nextUpdate는 갱신시점을 명시하고 있다. 유효기간동안 한번 획득된 CRL은 nextUpdate 시점까지 사용하기 때문에 안정된 검증속도가 보장된다. 그러나 CRL은 배치작업으로 게시하기 때문에 실시간 상태조회는 제공하지 않는다[6].

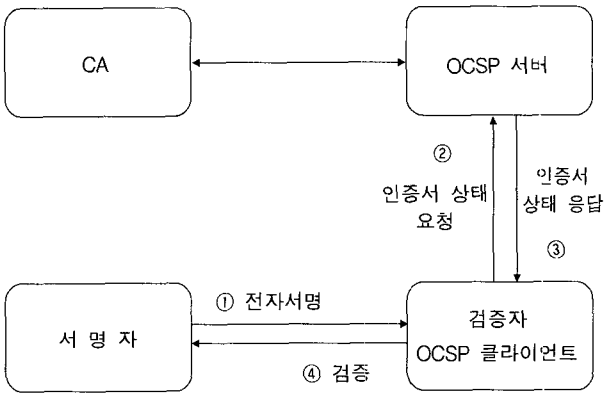
```
CertificateList ::= SEQUENCE
{
        tbsCertList                 인증서 목록,
        signatureAlgorithm          전자서명 알고리즘 식별자,
        signatureValue              전자서명
}

TBSCertList ::= SEQUENCE
{
        version                     버전(OPTIONAL),
        signature                   전자서명 알고리즘 식별자,
        issuer                      발급자,
        thisUpdate                  게시시점,
        nextUpdate                  갱신시점(OPTIONAL),
        revokedCertificates
        {
                userCertificate     인증서 일련번호,
                revocationDate      폐지시점,
                crlEntryExtensions  CRL 엔트리확장(OPTIONAL)
        } OPTIONAL,
        crlExtensions               CRL 확장(OPTIONAL)
}
```

(그림 1) X.509 버전2의 CRL 프로파일

2.2 온라인 인증서 상태 프로토콜(OCSP : Online Certificate Status Protocol)

OCSP는 실시간으로 인증서 상태를 요청하는 OCSP 클라이언트와 응답을 하는 OCSP 서버로 구성된다. (그림 2)는 OCSP의 인증서 상태검증 과정을 나타낸 것이다[7].



(그림 2) OCSP의 인증서 상태검증

① 서명자가 전자서명을 생성하여 검증자에게 전송한다.
② 검증자는 전송된 인증서의 유효성을 위해 OCSP 서버에 인증서 상태정보를 요청하게 된다. 이때 OCSP 클라이언트는 OCSP 서버로부터 응답이 올 때까지 요청한 인증서 검증을 대기한다.
③ 인증서 상태를 요청 받은 OCSP 서버는 인증서 상태정보를 조회하여 OCSP 클라이언트인 검증자에게 응답한다.
④ 응답된 인증서 상태가 유효하면 거래성공을 폐지일 경우는 거래실패를 고지한다.

실시간 인증서 상태에 대한 요청이 OCSP 서버에 집중되기 때문에 네트워크에 부하로 응답이 늦어지게 된다. OCSP 클라이언트는 동일한 인증서를 검증시점마다 상태요청을 해야 하므로 성능을 저하시키게 된다.

3. 기존방식의 문제점

기존의 패스워드 방식의 온라인 서비스는 보안기능이 제공되지 않는다. 그러나, 고부가가치의 온라인 서비스는 높은 수준의 보안이 요구된다. 대표적으로 인터넷뱅킹, 증권거래 시스템, 전자입찰은 인증서를 이용하고 있다[8].

인증서 기반의 온라인 서비스는 다음과 같은 기능을 가진다. 디면에 의한 신원확인을 받기 때문에 신뢰성이 보장된다. 서비스 정보에 대한 전자서명으로 사용자와 서비스 제공자간의 통신구간에서 변조되지 않았다는 무결성이 검증된다. 서비스 제공자는 사용자의 전자서명 데이터를 보관하여 부인방지가 가능하다[9].

이러한 기능을 보장받기 위해서는 사용자는 본인의 개인키를 관리해야 하는 의무가 있다. 그러나 개인키분실, 자격상실, 키변경 등의 이유로 인증서의 폐지가 가능하다. 이런 경우 검증자는 수신한 인증서 상태가 유효한 것인지를 확인해야 한다[10]. 기존방식으로 인증서 폐지목록인 CRL[11]과 실시간 인증서 상태를 제공하는 OCSP가 제안되었다[12].

고부가가치의 온라인 서비스는 실시간의 인증서 상태가 제공되지 않는다면 거래 쌍방의 분쟁 가능성이 존재한다. 이러한 이유로 CRL은 고부가가치의 온라인 서비스에 적합하지 않다. 따라서 OCSP가 실시간 인증서 상태의 제공이 가능하다[13-15].

인터넷뱅킹, 증권거래 시스템, 전자입찰은 한정된 시점에 거래가 되어야 한다. 또한 상대적으로 서버에 집중된 서비스를 제공하고 있다. OCSP는 검증시마다 인증서상태를 요청하기 때문에 통신부하와 병목의 문제점을 가지고 있다. 따라서 통신량이 집중된 온라인 서비스에는 적합하지 않다[16]. 최근 공인 인증서의 상호연동을 위한 인증기관간 OCSP의 통신을 해야하기 때문에 통신부하의 문제점은 해결이 되어야 한다[17].

4. 제안하는 인증서 상태검증 방안

인터넷뱅킹, 증권거래 시스템을 제공하는 온라인 서비스는 거래정보의 전송이 안전해야 한다. 따라서 거래정보에 대한 전자서명을 검증할 때도 높은 수준의 보안성이 요구되기 때문에 실시간의 인증서 상태 확인이 필요하다. 기존의 실시간 검증 방식의 OCSP는 인증서 상태의 요청과 응답 과정에서 집중화로 인하여 지연이 되기 때문에 속도를 저하시킨다.

본 논문은 실시간 검증과 성능의 개선을 위한 인증서 상태검증 방식을 제안한다. 제안하는 CSMC(Certificate Status Management Client)는 온라인 서비스를 이용하는 사용자의 인증서 정보를 등록하고 관리한다. CSMS(Certificate Status Management Server)는 인증서 폐지를 담당하고 폐지된 정보를 각각의 CSMC에게 전송한다. 본 장에서는 제안한 실시간 방식의 알고리즘과 효용성을 제시한다.

4.1 구성요소

제안하는 인증서 상태검증 방식의 구성요소를 정의한다.

- 인증기관(CA : Certificate Authority)

서명자에게 인증서의 발급을 담당한다. 또한 인증서와 관련된 정보를 게시하고 상태정보를 제공한다.

- 서명자(Signer)

인증서를 발급 받아 온라인 서비스를 이용하는 고객을 의미한다.

- 검증자(Verifier)

검증자는 온라인 서비스의 서버로써, 서명자의 전자서명에 대하여 검증을 수행한다. 검증시 인증서 상태에 대한 검증을 CSMC에 요청하여 처리한다.

- 인증서 상태관리 서버(CSMS)

인증서 상태를 관리하며 CSMC의 요청에 응답한다. 서명자의 검증자 리스트를 관리하여 폐지시점에 해당 인증서에 등록한 CSMC에게 실시간으로 상태를 전송한다.

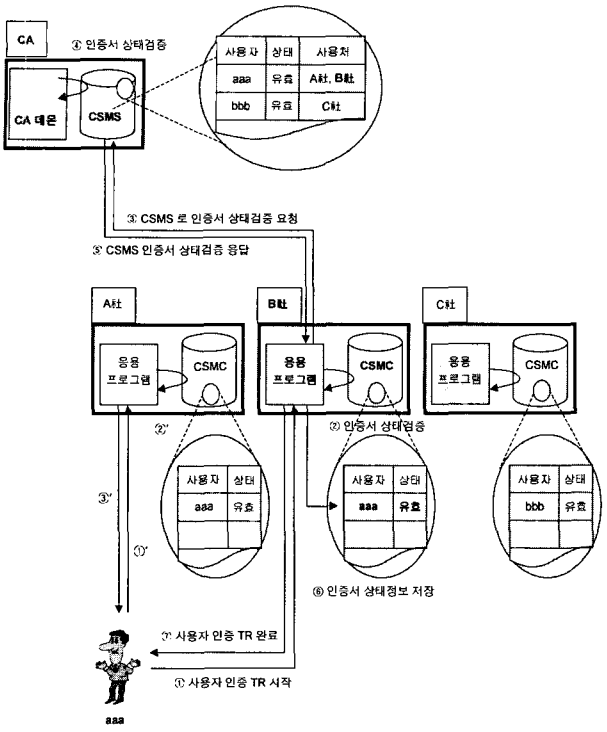
- 인증서 상태관리 클라이언트(CSMC)

온라인 서비스의 사용자에 대한 인증서 상태를 관리하여 검증시 상태정보를 제공한다.

4.2 인증서 상태검증의 시나리오

(그림 3)은 제안하는 실시간 인증서 상태검증의 시나리오를 나타낸 것이다. 본 논문의 검증자는 온라인 서비스를 제공

하는 서버이며, 서명자는 온라인 서비스의 고객을 의미한다.



(그림 3) 실시간 인증서 상태검증 시나리오
(최초 및 등록후 두 경우)

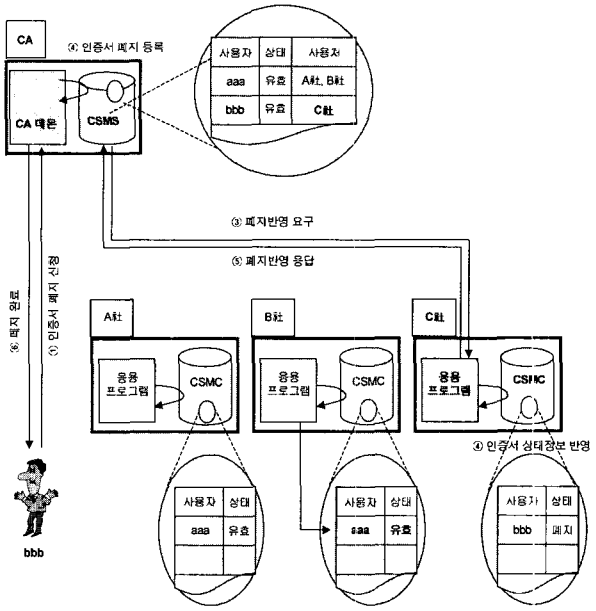
최초로 인증 트랜잭션을 시작하는 경우 인증서 상태검증 시나리오는 다음과 같다.

① 서명자 aaa는 B社에 인증 트랜잭션을 시작한다.
② aaa의 인증서 상태정보가 CSMC에 있는지 확인하고 있으면 인증서 상태정보를 반환한다.
③ 사용자 인증서 상태정보가 없으면 CSMS로 인증서 상태정보를 요청한다.
④ CSMS의 경우 CA와 인증서 상태정보를 공유 또는 동기화를 유지하므로, 인증서 상태정보를 반환한다.
⑤ CSMC로부터 요청된 사용자의 인증서 상태정보를 응답한다.
⑥ CSMC는 해당 사용자의 인증서 상태정보를 저장한다.
⑦ CSMC는 사용자에게 인증 트랜잭션완료 정보를 응답한다.

응용 서비스에서 사용자 등록이 된 경우 인증서 상태검증 시나리오는 다음과 같다.

①′ 서명자 aaa는 A社에 인증 트랜잭션을 시작한다.
②′ CSMC는 사용자의 상태정보를 반환한다.
③′ CSMC는 사용자에게 인증 트랜잭션완료 정보를 응답한다.

위의 경우에서와 같이 최초로 인증서 상태검증을 하는 경우에는 실시간 인증서 검증 프로토콜과 유사하게 응답하나, 인증서 상태정보가 CSMC에 등록된 이후에는 응용 서비스를 공급하는 해당 도메인 내부에서 인증서 검증을 완료할 수 있게된다.



(그림 4) 인증서 폐지 시나리오

인증서 폐지 및 실시간 폐지정보 전송 시나리오는 (그림 4)와 같다.

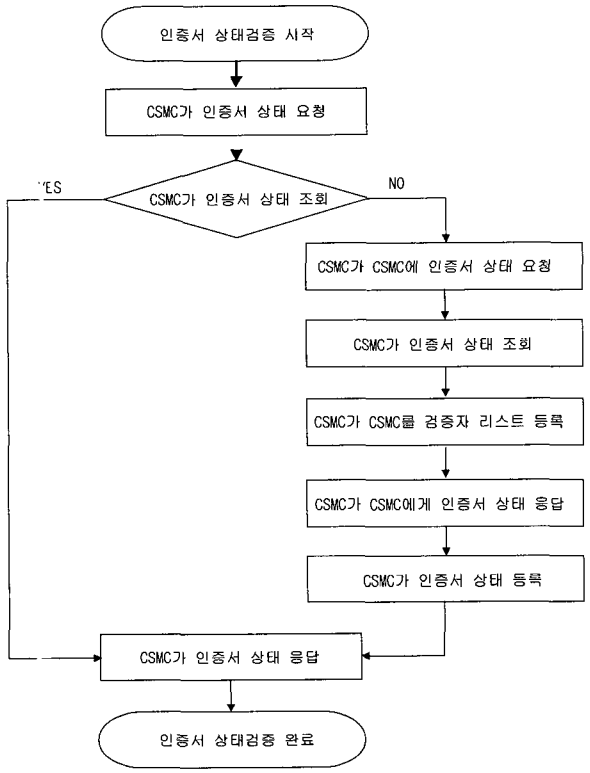
① 사용자 bbb는 인증서 폐지를 신청한다.
② CSMS는 인증서 폐지처리를 완료하고 상태정보를 저장한다.
③ CSMS는 사용자 bbb가 등록된 모든 사용처로 폐지반영을 요구한다. (그림 4)에서는 등록된 사용처가 C社이기 때문에 C社에만 전송하는 것을 볼 수 있다.
④ 전송된 해당 사용자의 인증서 상태정보를 CSMC에 반영한다.
⑤ CSMC에 반영이 완료되면 CSMS로 응답 메시지를 한다.
⑥ CSMS는 사용자에게 폐지완료 메시지를 응답한다.

이 때 CSMS는 등록된 모든 사용처에서 폐지반영 응답을 수신하고서 폐지를 완료하기 때문에 폐지정보에 대한 무결성을 보장받을 수 있다.

4.3 인증서 상태검증 알고리즘

(그림 5)에 인증서 상태검증 알고리즘을 도식화하였다. 검증자는 서명자의 인증서 상태를 CSMC에 요청한다. CSMC

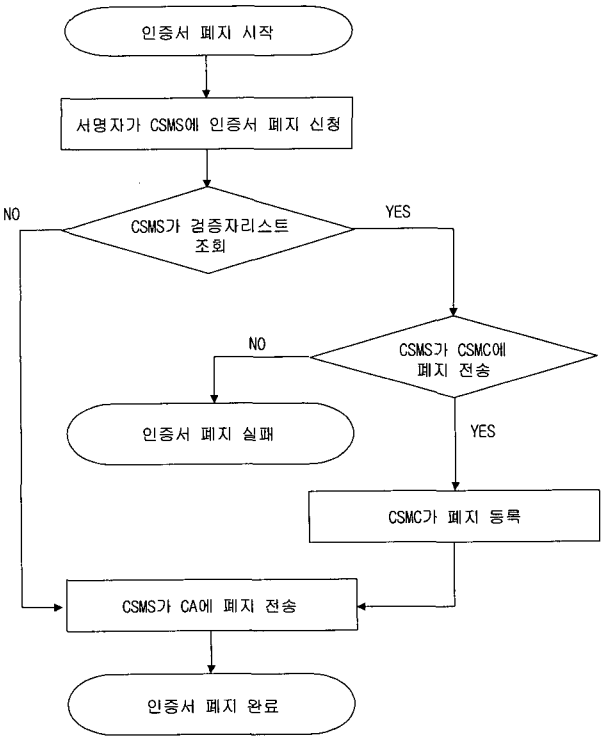
는 해당 인증서를 조회하고 정보가 없으면 새로운 서명자이므로 CSMS에 상태를 요청한다. CSMS는 요청한 CSMC의 정보와 서명자의 검증자 리스트에 등록한 후에 인증서 상태를 응답하고, CSMC는 응답된 인증서 상태를 등록하고 검증한다. 따라서 본 논문이 제안하는 알고리즘은 온라인 서비스의 새로운 고객의 인증서 상태정보를 등록하기 위하여 최초 1회는 CSMS에 조회하는 과정이 필요하다. 이후 동일한 인증서 상태에 대한 요청에 대하여 CSMC는 등록된 정보로 검증함으로써 검증속도를 개선한다.



(그림 5) 인증서 상태검증 알고리즘

4.4 인증서 폐지 알고리즘

본 논문의 인증서 상태검증 알고리즘으로 속도는 개선이 되지만 실시간의 폐지정보는 반영이 되지 않는다. 따라서 검증자에게 실시간의 폐지정보를 전송하는 알고리즘이 요구된다. (그림 6)에 인증서 폐지 알고리즘을 명시하였다. 서명자가 본인의 인증서에 대하여 CSMS에 폐지를 신청한다. CSMS는 해당 인증서의 검증자 리스트를 조회하고 검증자가 존재하면 폐지정보를 전송한다. 본 논문이 제안하는 폐지정보에 대한 무결성 제공을 위해 검증자 리스트에 등록된 모든 검증자로부터 전송확인을 받아야 폐지가 등록된다. 따라서 서명자의 인증서가 폐지가 완료한 후 온라인 서비스에 전자서명을 전송할 경우, 검증자에게 실시간으로 폐지정보가 전송되었기 때문에 해당 인증서는 사용할 수 없다.



(그림 6) 인증서 폐지 알고리즘

5. 실험 및 실험 결과

본 실험은 제안한 실시간 인증서 상태 검증 알고리즘에 대하여 원문의 크기를 변화를 주면서 검증을 수행하였다. 분석된 데이터로 기존의 CRL과 OCSP와의 성능을 비교평가 한다.

5.1 실험 환경

실험 환경은 시스템 하드웨어로 펜티엄 Ⅲ 800MHz, 시스템 메모리 256M SDRAM으로, 운영체제는 REDHAT 7.0 리눅스이며 MY-SQL 4.0.9를 데이터베이스로 하였다. 개발 언어는 C프로그램으로 gcc로 컴파일하였다.

5.2 실험결과

본 논문은 인증서 상태검증 속도와 폐지 전송속도에 대한 두 가지 실험으로 구분하여 실시하였다.

첫 번째 실험에서는 원문의 데이터의 크기를 변화시키면서 CSMC에 해당 인증서 상태가 존재하지 않아 CSMS에 조회한 경우와 CSMC에 해당 인증서 상태를 보유하여 즉시 검증했을 때의 속도를 분석한다. <표 1>은 실험결과를 나타낸 것이다. 제안하는 알고리즘은 금융거래에 있어 적합한 모델이기 때문에 금융거래에 있어 일반적인 통신량이 10M 내외임을 감안하여 실험을 하였다. 실험 데이터의 크기를 0.5M~10M의 범위에서 5단계로 증가시키면서 CRL, OCSP, 제안

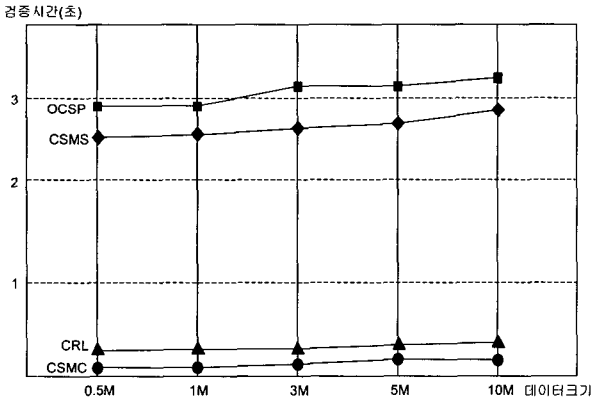
한 CSMS의 3가지에 메커니즘에 대하여 100회를 수행한 평균값이다. 실험형태는 두 가지로 분류하는데 최초등록과, 등록이후로 검증속도를 평가하도록 실험하였다.

〈표 1〉 인증서상태 검증속도 실험결과

(단위 : 초)

비교항목 \ 원문데이터		0.5M	1M	3M	5M	10M
CRL		0.14	0.15	0.16	0.19	0.21
OCSP		2.92	2.98	3.06	3.08	3.12
제안방식	CSMS 조회 (최초 등록)	2.60	2.68	2.71	2.77	2.81
	CSMC 조회 (등록 이후)	0.08	0.09	0.11	0.13	0.14

본 실험결과의 분석은 (그림 7)에서 기술한 것과 같다. 최초등록인 경우는 CSMS에 요청하여 인증서 정보를 등록하기 때문에 OCSP와 동일한 성능을 보여주지만, CSMC에 등록된 경우는 검증속도를 비교할 때 CRL보다 향상된 결과를 보임으로써 제안하는 방식이 성능을 개선시켰다는 결과가 도출되었다. 또한 원문의 크기가 커짐으로 CRL, OCSP, 제안한 CSMS가 다소 검증속도가 증가했으나 결과에 영향이 없음을 보여준다. 따라서 실시간 검증을 제공하는 OCSP와 비교하면 상태정보 등록 후 성능이 개선된 결과를 나타낸다.



(그림 7) 인증서 상태검증의 실험결과 분석

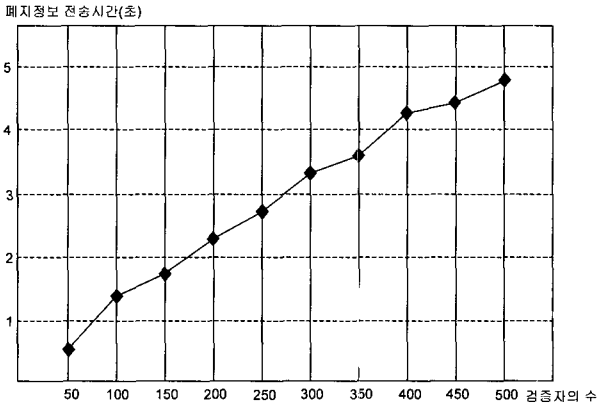
두 번째 실험에서는 검증자 리스트의 수를 50~500까지 10단계로 증가시키면서 폐지 전송속도를 측정하였다. <표 2>은 실험결과를 나타낸 것이다. 제안한 CSMS가 검증자 리스트의 수에 따른 결과를 100회 수행한 평균값이다.

〈표 2〉 인증서 폐지 전송 속도 실험 결과

(단위 : 초)

검증자수	50	100	150	200	250	300	350	400	450	500
폐지 전송시간	0.53	1.37	1.86	2.28	2.84	3.27	3.55	4.12	4.31	4.72

(그림 8)은 인증서 폐지 전송 속도의 실험결과를 나타낸다. 실험결과를 분석해 보면 검증자수가 적을수록 전송량이 감소하기 때문에 효율적이지만, 300개가 넘으면 OCSP보다 성능이 저하되는 결과를 나타낸다. 따라서 제안한 검증 방안은 검증자 리스트의 수가 300개 이내일 경우 폐지전송 속도에 대한 효율성을 가진다.



(그림 8) 인증서 폐지 전송속도의 실험 결과 분석

5.3 개선 효과

제안하는 실시간 인증서 상태검증 방식에 대하여 실험 결과에 기초하여 개선 효과를 제시한다.

5.3.1 성 능

검증속도 측면에서 다른 방식에 비교하여 개선된 실험 결과를 나타내었다. CRL의 경우 1회 획득된 폐지목록에 대하여 갱신전까지 검증하기 때문에 안정된 성능이 보장된다. 그러나 OCSP는 요청과 응답과정에서 네트워크의 부하로 인하여 보장이 어렵다. 제안한 검증방안은 서명자의 인증서정보를 관리함으로써 CRL과 같은 성능이 보장이 되었다.

5.3.2 실시간성

인증서 상태정보가 실시간으로 반영 여부를 나타낸다. CRL은 배치를 통해 폐지목록을 게시하기 때문에 실시간이 보장되지 않는다. OCSP는 실시간을 보장하기 위해 제안된 프로토콜이다. 제안한 검증방안은 폐지정보를 검증자 리스트를 통해 전송함으로써 OCSP와 같은 실시간 상태조회가 가능하다.

5.3.3 무결성

인증서 상태검증 알고리즘은 인증기관의 인증서 상태정보와 검증자의 정보간에 무결성이 보장되어야 한다. 제안하는 방식의 무결성보장 방법은 사용자가 폐지를 신청하였을 때, 사용자가 거래하는 모든 검증자 리스트에 폐지정보가 전송이 되어야 폐지에 대한 승인을 하도록 제안하였습니다.

따라서 사용자가 폐지 확인을 받았다는 것은 이미 금융 서비스를 제공하는 서버에 반영이 되었기 때문에 해당 인증서로 거래시 실패를 응답 받게 된다. 따라서 제안한 인증서 폐지 전송 알고리즘은 인증기관의 인증서 상태정보와 검증자가 보유한 상태정보에 대한 무결성을 보장하게 된다.

<표 3>은 제안한 인증서 상태 확인 알고리즘과 기존 알고리즘을 비교한 기대효과를 나타낸다. 비교항목인 성능, 실시간성, 무결성의 기능으로써, 금융 네트워크에서 필수적으로 제공되어야 한다. 성능에 대한 평가는 실험결과의 평균을 명시한 것으로 CRL, CSMS는 적합하지만 OCSP는 부적합한 결과를 나타내었다. 실시간성은 국내 공인 인증기관은 CRL을 12시간을 주기로 발급하고 있으며, OCSP에 대해서는 응답시간의 유효한 시간이 60초로 되어 있다. 제안한 알고리즘은 10초의 타임을 설정하고 있다. 따라서 OCSP, CSMS는 실시간성이 적합하지만, CRL은 부적합한 결과가 도출되었다. 무결성 항목은 3가지 방식 모두 암호화 채널을 사용하기 때문에 적합한 특성을 가지고 있다.

〈표 3〉 제안한 인증서 상태 확인 알고리즘의 기대효과

메커니즘 / 비교항목	CRL		OCSP		CSMS	
	시 간	평 가	시 간	평 가	시 간	평 가
성 능	0.68초	○	3.03초	△	0.11초	◎
실시간성	12시간	×	60초	○	10초	◎
무 결 성	-	○	-	○	-	○

※ ◎ 우수, ○ : 양호, △ : 보통, × : 부적합

6. 결 론

인증서는 개인키분실, 자격상실, 키변경 등의 이유로 폐지가 가능하기 때문에 검증자는 수신한 인증서 상태를 확인해야 한다. 실시간 인증서 상태를 제공을 위하여 OCSP가 제안되었다. 그러나 OCSP는 검증시마다 인증서 상태를 요청하기 때문에 통신부하와 병목의 문제점을 가지고 있다. 따라서 실시간이 보장되지만 통신량이 집중된 온라인 서비스에는 적합하지 않다.

본 논문은 실시간 인증서 상태를 보장하면서 성능을 개선시키고자 하였다. 제안하는 알고리즘은 서명자의 인증서 상태 정보를 관리하며 폐지정보를 실시간으로 전송한다. 따라서 검증자는 요청한 인증서에 대하여 이미 저장되어 있는 정보를 사용함으로써 검증 속도를 개선한다. 본 논문은 실험을 기초하여 성능, 실시간성, 무결성에 대하여 기존 방안을 개선시킨 결과를 나타내었다.

본 연구의 향후연구는 폐지정보 전송에서 검증자의 수에 따른 효율성을 분석하고자 한다. 이와 함께 상태조회와 폐지전송 구간의 프로토콜의 보안에 대해 연구가 요구된다.

참 고 문 헌

[1] Ray Hunt. "PKI and Digital Certification Infrastructure," IEEE, 2001.

[2] RFC2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, 1999

[3] RFC2560, Internet X.509 Public Key Infrastructure Online Certificate Status Protocol(OCSP), 2001.

[4] Barbara Fox & Brian LaMacchia, "Online Certificate Status Checking in Financial Transaction : The Case for Re-issuance," financial Cryptography, 1999.

[5] Irene Gassko, Peter S. Gemmell and Philip Mackenzie, "Efficient and Fresh Certification," PKC 2000.

[6] draft-ietf-pkix-ldap-crl-schema-00, Internet X.509 Public Key Infrastructure LDAP Schema for X.509 CRLs, 2003.

[7] draft-ietf-pkix-ocspv2-ext-01, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, version 2, 2002.

[8] Ray Hunt, "Technological Infrastructure for PKI and Digital Certification," 2001.

[9] Vishwa Prasad & Sreenivasa Potakamuri & Michael Ahern, "Scalable Policy Driven and General Purpose Public Key Infrastructure(PKI)," IEEE, 2000.

[10] Eugenio Faldella & Marco Prandini, "A Novel Approach to On-Line Status Authentication of Public-Key Certificates," IEEE, 2000.

[11] RFC3080, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2002.

[12] draft-ietf-pkix-cvp-02, Certificate Validation Protocol, 2003.

[13] Jan Camenisch and Anna Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," 2002.

[14] Jan Camenisch and Anna Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," 2001.

[15] Jan Camenisch and Anna Lysyanskaya, "A signature scheme with efficient protocols," Security in Communication Networks, Amalfi, Italy, 2002.

[16] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," Proceedings of the IEEE Symposium on Security and Privacy, 1996.

[17] Andre Arnes, Svein J. Knapskog, "Selecting Revocation Solutions for PKI," NORSEC 2000, Sep., 2000.

정 재 동

e-mail : jjd@koscom.co.kr

1983년 연세대학교 수학과(이학사)

1994년 연세대학교 산업대학원(공학석사)

1996년 정보통신기술사 취득(47회)

2002년 숭실대학교 컴퓨터공학과 (공학박사 수료)

1983년~현재 한국증권전산 공인인증센터장 보안연구소장

관심분야 : 정보보호, 암호학, 유무선 PKI

오 해 석

e-mail : oh@computing.soongsil.ac.kr

1975년 서울대학교 응용수학과(이학사)

1981년 서울대학교 계산통계학과(이학석사)

1989년 서울대학교 계산통계학과(이학박사)

1976년~1982년 태평양화학(주), (주)삼호 전산실

1990년~1991년 일본 동경대학교 객원교수

1997년~1999년 숭실대학교 부총장

2000년~2001년 스탠포드대학교 객원교수

1982년~현재 숭실대학교 정보과학대학 교수

관심분야 : 정보보호, 멀티미디어, 데이터베이스, 영상처리