한국산학기술학회논문지
Vol. 7, No. 5, pp. 858-865, 2006

VDN을 이용한 실시간 인증서 상태 검증 시스템의 관한 연구

이광형[1*], 김현철[2]

A Study on the Real-Time Certificate Status Verification System Using VDN

Kwang-Hyoung Lee[1*] and Hyun-Chul Kim[2]

요 약 인증기관에 의해 발급된 인증서는 개인키 분실, 자격 상실, 키 변경 등의 여러 사유로 유효기간 이전에 폐지될 수 있다. 이로 인해 해당 거래의 사용되는 인증서에 대한 상태 검증은 반드시 선행되어야 한다. 현재 가장 보편적인 방식은 CRL을 이용하는 방식과 OCSP를 이용하는 방식이 있다. 하지만 CRL 방식은 인증서 상태에 대한 현재성 보장이 어려우며 OCSP방식은 실시간으로 대용량의 메시지를 이용해 상태 검증을 요청하고 검증을 수행함으로서 많은 통신량을 발생시킨다. 본 논문에서는 사용자 신원 정보에 대한 VDN을 생성하여 검증을 요청하고 인증기관은 해당 VDN에 대한 사용자 신원 정보를 찾아 검증을 수행함으로서 인증서 상태에 대한 현재성 보장 및 서버 과부하 그리고 네트워크 과부하를 해결한다. 이 결과로 인증서 상태 검증 수행 속도를 향상시키는 실시간 인증서 상태 검증 시스템을 제안한다. 또한, 기존 방식들과의 비교 실험을 통해 인증서 상태 검증 수행 속도가 향상됨을 확인하였다.

Abstract A certificate that is issued by the certification authority can be revoked within the period of validity by various reasons such as the loss of private key, disqualification or the change in key.Therefore, the certificate status verification must precede prior to use Currently, the CRL or the OCSP methods are used in most cases.But the CRL system can't guarantee the present status of the certificate, and the OCSP generates heavy network traffic by checking or requesting certificate status in real-time using high-capacity messages. In this paper, we propose a system that requests the certificate verification by creating VDN for user identity information. Through this system, the certification authority will be able to guarantee the certificate's status in real-time, and solve the problem of the server and network overload by verifying and finding user identity information from VDN, Based on the results, we propose a real-time certificate status verification system which can improve the speed of the verification. We confirmed the improvement in speed by testing and comparing it with the existing methods.

Key Words : Real-time Certificate Status Verification, VDN, OCSP, CRL

1. 서론

인터넷의 발달 및 보급 확대는 과거 종이문서를 통한 대면 방식 오프라인 비즈니스 환경을 비대면 온라인 전자문서 기반으로 전환시켜 놓았으며 우리 사회 전반의 걸쳐 지식정보화 사회를 빠르게 구축하는 밑거름이 되었다[1]. 하지만 온라인에서의 주요 문서 및 정보의 전송은 불법적인 도청 및 위·변조 그리고 신분 위장 등의 각종 위협에 항상 노출되어 있다. 이러한 위협으로부터 전송되는 정보를 보호하기 위해서는 기밀성, 무결성, 부인방지, 인증등의 기능을 통해 해당 거래에 대한 신뢰성과 안정성을 보장할 수 있는 인증 시스템이 요구된다[2-3].

PKI(Public Key Infrastructure : 공개키 기반구조) 인증서를 이용한 인증 시스템은 공개키 암호화 개념을 이용하여 송수신 데이터를 암호화하고 인증서를 통해 사용자

이 논문은 2005년 서일대학 학술연구비 지원에 의해 연구되었음
[1]서일대학 인터넷정보과
[2]숭실대학교 컴퓨터공학과
*교신저자: 이광형(dreamace@seoil.ac.kr)

를 인증하는 기술로서 디지털서명과 메시지 인증코드를 사용하여 기밀성과 무결성을 보장한다. 또한 별도의 부인방지 프로토콜과 사용자 인증 그리고 메시지 인증을 통해 부인방지 및 인증을 보장한다. 이러한 공개키 기반 구조 인증시스템은 거래가 발생 할 때 마다 해당 거래가 유효한 거래인지 아닌지를 판별하는 유효성 검증 과정을 거쳐야 하는데 이러한 유효성 검증은 전송되는 메시지에 대한 전자서명 검증과 해당 거래의 사용되는 인증서에 대한 인증서 상태 검증으로 구분 된다[2][4][5].

인증기관에 의해 발급된 인증서는 개인키 분실, 자격상실, 키 변경 등의 여러 가지 이유로 폐지 될 수 있다. 이러한 이유로 검증자는 수신한 인증서에 대해 유효한 인증서인지 아닌지 확인하는 인증서 상태 검증 과정을 거쳐야 한다. 특히 이 과정은 인증서의 현재 상태와 인증서의 소유자 및 발행자의 신원을 확인 하는 것으로 전자거래에 있어 가장 중요한 부분이다[2][6][7].

인증서 상태 검증을 수행하는 가장 일반적인 방법은 CRL(Certificate Revocation List : 인증서 폐지 목록)[9-10]을 이용하는 것이다. 이 방법은 인증서 폐지 목록을 검증자 디렉토리에 다운로드 한 후 검증을 수행하는 것으로 인증서 폐지 목록 배포의 주기적 특성(기존 24시간, 현재 12시간)으로 인해 인증서 상태에 대한 현재성을 보장하기 어렵다. 또한 발급되는 인증서 양에 따라 폐지되는 인증서 양이 비례적으로 증가되기 때문에 CRL의 크기가 계속적으로 증가하며 이러한 CRL을 저장하기 위한 대용량의 저장 장치가 필요하다는 문제점이 있다[1][2][8]. 이러한 CRL 방법의 현재성 문제를 해결하기 위한 대안으로 OCSP(Online Certificate Status Protocol : 온라인 인증서 상태 프로토콜)[11-12]를 이용한 실시간 방법이 제시되었다. 하지만 이 방법은 실시간으로 다수의 클라이언트가 대용량의 메시지를 이용해 중앙 서버에게 상태 검증을 요청하고 검증을 수행함으로서 서버 과부하 및 네트워크 과부하가 발생하며 이로 인해 인증서 상태 검증 수행시간이 다소 오래 걸린다는 문제점이 있다. 따라서 실시간 응답시간이 중요시 되는 분야에 적용하기에는 적합하지 않다[1][2][4]. 따라서 본 논문에서는 기존 시스템의 문제점인 인증서 상태의 현재성과 서버 과부하 그리고 네트워크 과부하를 해결하기 위하여 사용자 신원정보에 대한 VDN(Virtual Discernment Number : 가상식별번호)을 생성하여 검증을 요청하고 처리한다. 이에 대한 결과로 인증서 상태 검증 수행속도를 향상시킴으로서 시간적 특성이 중요시되는 분야에 적합한 인증서 상태 검증 방법을 제안하고자 한다.

2. 관련연구

2.1 공개키 기반구조 인증 시스템

공개키 암호 개념은 1976년 Diffie와 Hellman이 발표한 논문 "New Direction in Cryptography"[13]에서 처음 제시 되었으며 공개키와 개인키라는 두 개의 상이한 키 쌍을 이용하여 비밀키 암호 방식이 가지는 키 노출에 따른 키 분배 문제를 해결함과 동시에 송신자의 개인키로 서명된 전자문서를 이용해서 송·수신자의 신원과 송·수신 사실에 대한 무결성과 부인방지를 제공하는 전자서명 응용에 널리 사용된다. 이러한 공개키 암호를 이용하는 PKI 인증 시스템은 합법적인 서명자만이 전자서명을 생성할 수 있는 위조불가(Unforgeable), 서명자가 서명한 사실을 부인할 수 없는 부인방지(Non-Repudiation), 전자서명의 서명자를 불특정 다수가 검증 할 수 있는 신원확인(Authentication), 전자문서의 서명을 다른 전자문서의 서명으로 사용할 수 없는 재사용불가(Not-Reusable) 기능을 통해 해당 거래에 대한 유효성을 보장한다[2][14][15].

2.2 전자서명 검증

전자서명 검증은 서명자가 보낸 전자문서를 검증자가 서명자 이외의 다른 사람에 의해 서명되지 않았음을 확인하는 것으로 서명자는 자신만이 아는 개인키를 이용하여 문서를 전자서명하여 검증을 요청하고 검증자는 서명자의 공개키를 이용해 수신한 전자서명 문서에 대해 검증을 수행하는 과정이다[1][14].

2.3 인증서 상태 검증

2.3.1 CRL을 이용한 상태 검증

인증서 폐지 목록은 RFC2459[10]에 정의되어 있으며 CA(Certification Authority : 인증기관)가 주기적으로 폐지된 모든 인증서의 일련번호, 폐지시간, 폐지이유를 서명한 후 디렉토리에 게시하고 검증자는 이를 다운 받아 검증을 수행하는 방식이다. 인증서 폐지 목록에는 게시시간, 다음 게시시간이 포함되어 있어 검증자는 현재 가지고 있는 인증서 폐지 목록이 최신의 것임을 확인 할 수 있다. 하지만 인증서 폐지 목록은 인증기관에 의해 주기적으로 생성되어 배포되기 때문에 인증서 상태의 대한 현재성을 보장하기 힘들다. 또한 발행되는 인증서의 수가 증가 할수록 폐지되는 인증서의 수 또한 증가함으로서 인증서 폐지 목록의 크기가 지속적으로 증가하며 이를 저장하기 위한 대용량의 저장장치가 필요하다는 문제점이 있다[2][6][7]. 인증서 폐지 목록을 이용한 인증서 상태 검증 절차는 아래 [그림 1]과 같다.

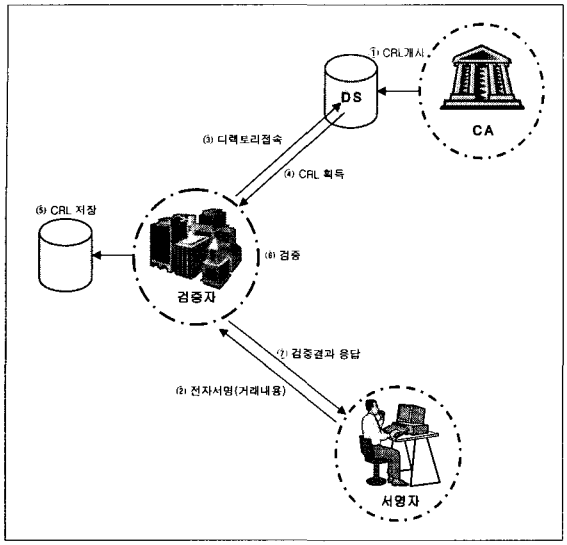

그림 1. CRL 기반의 인증서 상태 검증 방식

① 인증기관은 폐지된 인증서 목록에 대하여 전자 서명 한 후 디렉토리에 게시한다.
② 검증자는 인증기관 디렉토리에 접속한다.
③ 검증자는 디렉토리에서 인증서 폐지 목록을 획득한다.
④ 검증자는 자신의 디렉토리에 인증서 폐지 목록을 저장한다.
⑤ 서명자는 전자서명 메시지와 인증서를 검증자에게 전송하여 검증을 요청한다.
⑥ 검증자는 자신의 디렉토리에서 검증 요청받은 인증서 정보가 있는지를 확인한 후 전자서명 메시지에 대한 검증을 수행한다.
⑦ 검증자는 서명자에게 검증 결과를 전송한다.

2.3.2 OCSP를 이용한 상태 검증

OCSP는 1999년 6월 'X.509 Public Key Infrastructure Online Certificate Status Protocol' OCSP 버전 1.0 발표되었으며 현재는 2001년 3월 드래프트 형태로 발표된 OCSP 버전 2.0이 사용되고 있다[2]. 이러한 OCSP는 거래내용이 중요하여 실시간 인증서 상태 확인이 요구되는 증권이나 은행과 같은 금융거래에 주로 사용되며 CRL 방식에 현재성 문제를 해결한다. 이러한 OCSP 기법은 이용자와 서버간의 요청과 응답 메시지에 상호 전자서명을 통해 보안과 인증서 상태에 대한 실시간성을 보장한다. 그러나 검증자와 CA간의 검증 요청과 응답 정보 즉 OCSP 요청 메시지와 OCSP 응답 메시지가 담고 있는 불필요한 정보로 인해 검증자와 CA간의 통신 하는데 있어서 네트워크 과부하가 발생할 수 있으며 또한 실시간으로 다수의 클라이언트가 중앙 서버에게 상태 검증을 요청하고 검증을 수행함으로서 서버 과부하를 발생시킬 수 있다[1][2][6][7]. [그림 2]는 OCSP를 이용한 인증서 상태 검증 절차를 보여주고 있다.

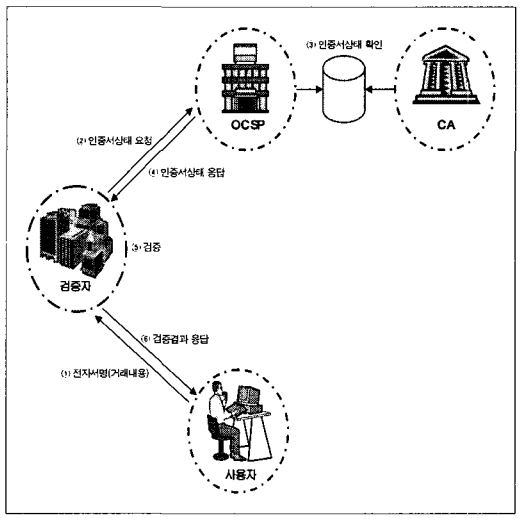

그림 2. OCSP 기반의 인증서 상태 검증 방식

① 서명자는 전자서명 메시지와 인증서를 검증자에게 전송하여 검증을 요청한다.
② 검증자는 요청받은 인증서를 OCSP 서버에 전송해 인증서 상태를 요청한다.
③ OCSP 서버는 인증기관의 디렉토리를 검색한다.
④ OCSP 서버는 인증서 상태 결과를 검증자에게 전송한다.
⑤ 검증자는 인증서 상태 응답을 확인한 후 전자서명에 대한 검증을 수행한다.
⑥ 검증자는 서명자에게 검증결과를 응답한다.

2.3.3 기존 인증서 상태 검증 방식의 장단점

오프라인 방식의 CRL은 폐지정보에 대하여 인증기관이 전자서명을 하고 검증자는 CRL을 검증함으로써 보안이 제공된다. 검증자가 획득한 후 로컬에 저장되면 CRL이 재갱신되기 전까지 사용함으로써 적합한 성능을 제공한다. 그러나 CRL은 일정기간에 인증기관에 의해 생성되기 때문에 실시간으로 인증서 상태 확인을 제공하지 못한다. 실시간 응용 분야에서는 실시간으로 인증서 상태가 제공되지 않는다면 거래 쌍방의 분쟁 가능성이 존재하게 된다. 이러한 이유로 CRL은 실시간 응용 분야에 적합하지 않다. 인증서 발행 수량의 증가에 따라 폐지되는

인증서의 수량도 증가한다. 따라서 CRL방법을 이용하게 되면 폐지된 인증서의 정보를 담고 있는 CRL의 크기 또한 지속적으로 증가하게 되는 단점이 있다.

온라인으로 처리하는 OCSP는 이용자와 서버간의 요청과 응답 메시지에 상호 전자서명을 이용한 보안과 인증서상태 확인에 대하여 실시간이 보장한다. 그러나 OCSP Request와 OCSP Response는 검증자와 CA가 통신하기에 데이터의가 큰 문제가 있기 때문에 통신부하로 인하여 성능이 보장되지 않는다. 따라서 통신량이 집중된 클라이언트-서버 환경에서 이용되기에 부담이 크다.

3. 제안하는 시스템

3.1 제안하는 시스템 전체구조

국내 공인 인증체계에서는 대면확인을 거쳐 높은 수준의 보안을 유지하고 있다. 이를 위해 사용자는 인증서 등록과정에서 개인은 주민번호, 법인은 법인번호를 인증기관에게 전송해야 한다. 이에 따라 인증기관은 사용자에 대한 신원정보와 인증서상태 정보를 보유하고 있다. 또한 인터넷뱅킹, 증권거래시스템, 전자상거래 등의 온라인서비스를 사용하기 위해서 사용자는 가입의 절차를 통해 아이디와 패스워드를 부여받아야 한다. 이러한 가입과정에서 사용자의 신원정보가 서비스제공자에게 제공하도록 되어 있다.

온라인서비스 사용자는 특정거래에 대해 전자서명을 수행하여 서비스제공자에게 전송한다. 서비스제공자는 다수의 사용자가 전송한 전자서명을 검증해야 한다. 이때 인증서상태 확인을 수행하는 과정에서 기존의 CRL 방법을 실시간 응용 분야에 적용할 경우 거래 쌍방의 분쟁 가능성이 발생하며 이를 해결한 OCSP는 검증 요청 및 응답의 불 필요한 정보를 포함하고 있기 때문에 메지지의 크기가 커지며 이로 인해 통신부하과 발생 성능을 보장할 수 없다. 본 논문에서는 사용자의 신원정보의 대하여 해쉬를 이용하여 VDN을 생성하고 이를 통해 검증을 요청하고 인증기관과 서비스제공자가 보유하고 있는 사용자 신원정보를 통해 검증을 수행함으로써 실시간 인증서 상태 프로토콜과 같은 실시간을 보장하고 통신부하를 감소시킨다. 이에 대한 결과로 인증서 상태 검증 수행 시간을 향상 시키는 실시간 인증서 상태 검증 메커니즘을 제안한다. [그림 3]은 본 논문에서 제안하는 시스템 구조를 보여주고 있다.

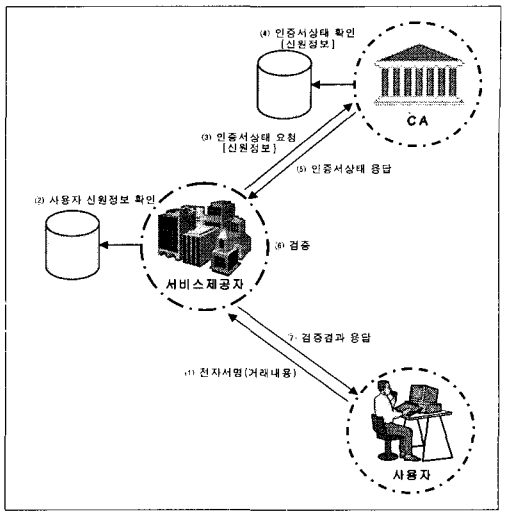

그림 3. 제안하는 인증서 상태 검증 시스템 구조

① 사용자는 온라인서비스에 접속하여 특정 전자거래에 본인의 개인키로 전자서명을 수행한 후 서비스제공자에게 전송한다.

② 전송된 전자서명의 사용자에 대하여 서비스제공자가 보유한 데이터베이스의 신원을 확인한다.

③ 신원확인을 통해 적법한 사용자 여부를 확인한 후 인증기관에 신원확인을 전송하여 인증서 상태를 요청한다.

④ 인증기관은 자신의 데이터베이스에서 요청받은 사용자의 신원정보가 존재하는지 확인한다.

⑤ 인증기관은 해당 사용자의 인증서 상태를 서비스제공자에게 응답한다.

⑥ 서비스제공자는 응답 받은 인증서 상태가 유효인지를 확인한 후 전자서명 검증을 수행한다.

⑦ 서비스제공자는 사용자에게 전자서명 검증결과를 응답한다.

3.2 인증서 상태 검증 프로세스

[표 1]은 제안하는 시스템에서 사용하는 약어의 대한 정의를 보여주고 있으며 [그림 4]는 본 논문에서 제안하는 인증서 상태 검증 프로세스를 보여주고 있다. 본 논문에서 제안하는 시스템의 인증서 상태 검증 프로세스는 총 20단계의 걸쳐 수행되며 수행 절차에 대한 세부적인 과정은 다음과 같다.

1. 검증자는 인증기관과의 통신을 식별하기 위한 라벨 L을 생성한다.

$$Create\ Lable\ L \qquad (1)$$

2. 검증자와 인증기관과의 인증서 상태 요청과 응답시의 사용할 대칭키 K를 생성한다.

$$Create\ Lable\ K \tag{2}$$

3. 검증자는 생성한 라벨 L과 대칭키 K를 CA의 공개키 CAK로 암호화한 값 전자봉투 EK를 CA에 전달한다. 전자봉투EK는 라벨 L에 대한 대칭키 K를 제3자가 열람하지 못하게 함으로써 완전한 Key 교환이 목적이다.

$$EK = E_{CAK}(K,L) \tag{3}$$

4. 검증자는 CA에게 생성된 전자봉투 EK를 전송한다.
5. 서명자는 거래내용 M에 대하여 자신의 개인키 Ak로 전자서명을 수행한다.

$$S = S_{Ak}(M) \tag{4}$$

6. 서명자는 전자서명 S를 검증자에게 요청한다.
7. 검증자는 전송된 S에 해당하는 사용자 신원 정보 UIN1을 자신의 데이터베이스에서 획득한다.
8. 검증자는 사용자 신원 정보 UIN1과 통신식별 L을 해쉬하여 가상 식별 번호 VDN1을 생성한다. 해쉬함수는 일방향 특성으로 인해 신원정보에 대한 보안성이 우수하며 또한 검증자와 CA간의 통신 데이터를 해쉬의 길이로 감소시킨다.

$$VDN1 = H(UIN1, L) \tag{5}$$

9. 검증자는 가상 식별 번호 VDN1에 대하여 대칭키 K로 암호화한 정보 EVDN1을 생성한다.

$$EVDN1 = E_K(VDN_1) \tag{6}$$

10. 검증자는 EVDN1을 CA에게 전송한다.
11. CA는 전송된 EVDN1을 소유하고 있는 키 K로 복호화하여 VDN1을 획득한다.

$$VDN1 = D_K(EVDN1) \tag{7}$$

12. CA는 인증서등록과정에서 보유하고 있는 사용자의 UIN2를 데이터베이스에서 획득한다.
13. CA는 보유하고 있는 신원정보 UIN2와 통신식별 L을 해쉬하여 무결성 비교를 위한 VDN2를 생성한다.

$$VDN2 = H(UIN2, L) \tag{8}$$

14. CA는 VDN1과 VDN2를 비교하여 사용자의 신원정보에 대한 무결성을 검증한다.
15. CA는 무결성을 확인한 후 VDN2에 해당하는 인증서상태 CS를 데이터베이스에서 획득한다.
16. CA는 인증서상태 CS와 통신식별 L을 대칭키 K로 암호화한 결과값 ECS를 생성한다.

$$ECS = E_K(CS, L) \tag{9}$$

17. CA는 ECS를 검증자에게 전송한다.
18. 검증자는 전송받은 ECS를 대칭키 K로 복호화하여 CS와 L을 획득하고 확인한다.

$$CS, L = D_K(ECS) \tag{10}$$

19. 검증자는 인증서상태 CS가 유효하면 거래내용에 대한 전자서명을 검증한다.
20. 서명자는 검증자가 응답한 R에 대해 확인한다.

표 1. 프로토콜 정의

- Signer :서명자(사용자)
- Verifier : 검증자(서비스 제공자)
- CA : 인증기관
- L : 검증자와 CA간의 통신 식별을 위한 통신 식별자
- K : 대칭키
- M : 원문, 거래내용
- S : 원문 M에 대한 전자서명
- CAK : CA의 공개키 K
- CAk : CA의 개인키 K
- Ak : 서명자 A의 개인키 K
- EK(Enveloped Key) : 대칭키 k에 대한 전자봉투
- UIN(User Identification Number) : 사용자 신원 정보
- UIN1(User Security Number 1) : 검증자가 보유하고 있는 신원정보
- UIN2(User Security Number 2) : 인증기관이 보유하고 있는 신원정보
- VDN(Virtual Discernment Number) : 가상 식별 정보
- VDN1(Virtual Discernment Numbe 1) : 검증자가 생성한 가상 식별 정보
- VDN1(Virtual Discernment Numbe 1) : 인증기관이 생성한 가상 식별 정보
- EVDN(Encrypted Virtual Discernment Number) : 암호화된 가상 식별 정보
- CS(Certificate Status) : 인증서상태 ECS(Encrypted Certificate Status) : 암호화된 인증서상태
- R(Result) : 통신결과 H( ) : 일방향성의 해쉬함수
- Ek( )(Encrypt) : 대칭키 k를 이용한 암호화 함수 Dk( )(Decrypt) : 대칭키 k를 이용한 복호화 함수
- EX( )(Envelop) : X의 공개키를 이용한 비 대칭키 암호화 함수
- DX( )(Develop) : X의 개인키를 이용한 비 대칭키 복호화 함수
- SX( )(Sign) : X의 개인키를 이용한 전자서명 함수
- VX( )(Verify) : X의 공개키를 이용한 검증 함수

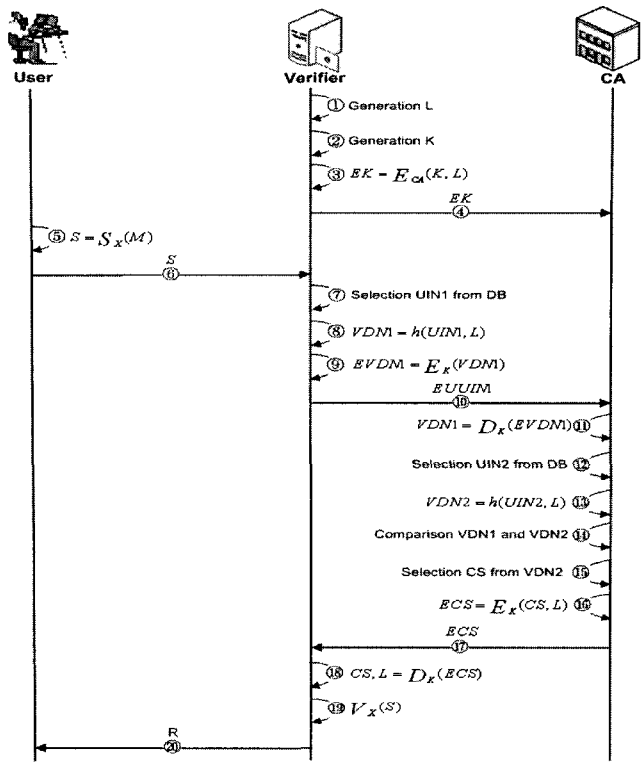

그림 5. 제안하는 인증서 상태 검증 프로세스

4. 실험 및 비교 분석

4.1 실험환경

본 논문에서 제안 하는 인증서 상태 검증 시스템은 서버와 클라이언트로 구성된다. 인증서 상태 검증서버의 하드웨어 구성요소는 Compaq EVO W8000, CPU : Intel Xeon 2GHz, RAM : 2048M, HDD : 36GB SCSI를 사용하였다. 또한 클라이언트의 하드웨어 구성요소는 CPU : Pentium Ⅳ 2.4MHz, RAM 1024M, HDD : 60GB를 사용했다. 시스템 소프트웨어는 서버의 운영체제로 리눅스를 사용하였으며 데이터베이스는 MY-SQL을 사용하였다. 클라이언트의 개발환경은 Visual C++6.0과 ActiveX, SSL을 이용하였다. 본 논문에서의 주요 실험 요소는 기존의 CRL방법과 OCSP방법 그리고 제안하는 방법 사이에 검증 요청을 하는 수에 따라 어떻게 인증서 상태 검증 처리 속도가 차이가 있는가에 중점을 두고 실험을 하였다. 또한 실험의 범위는 각각의 방식에 대해 검증자수를 최대 200명으로 하여, 총 600회에 걸쳐 실험을 하였다. 또한 각각의 실험에서 사용한 인증서는 세 가지 기법 모두 국내 공인 인증기관에서 발급한 인증서를 사용하였다. 아래 [그림 5]는 본 논문에서 제안하는 시스템의 실험 화면을 보여주고 있다.

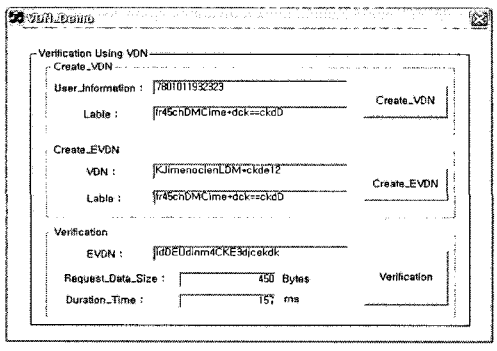

그림 6. 제안하는 시스템 실험화면

4.2 실험결과 및 비교 분석

[그림 6]은 기존의 CRL기법, OCSP기법 그리고 본 논문에서 제안하는 기법에 대해 실험한 결과를 그래프 형식으로 보여주고 있다. [그림 7]의 가운데 추세선은 CRL

을 이용한 방식의 실험결과로 인증서 상태 목록을 검증 서버에 받아 인증서 상태 검증을 수행하기 때문에 인증서 상태 검증 속도가 OCSP기법보다 빠름을 확인한다. 가장 상단의 추세선은 OCSP를 이용한 방식의 실험결과로 비교 실험한 다른 기법에 비해 수행시간이 오래 소요됨을 확인 할 수 있다. 마지막으로 가장 하단에 추세선은 본 논문에서 제안하는 기법으로 불 필요한 정보를 제거하고 사용자의 신원정보에 대한 VDN을 이용하여 인증서 상태 요청 및 검증을 수행하기에 다른 기법에 비해 검증 수행 시간이 적게 소요됨을 확인 할 수 있다.

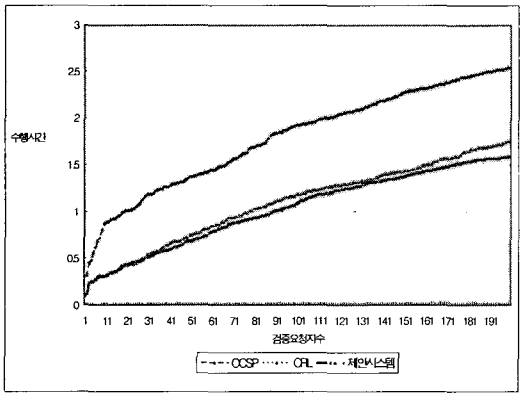

그림 7. 실험 결과

위에 [그림 7]의 실험결과를 토대로 본 논문에서 실험한 인증서 상태 검증 기법과 기존의 인증서 상태 검증 기법간의 비교 분석한 결과는 [표 2]와 같다. [표 2]에서의 비교 분석 항목은 실시간성, 데이터크기, 통신과부하, 수행시간에 대하여 비교 분석하였으며, 비교분석한 결과를 토대로 각각의 방식이 적용되기에 적합한 분야를 제시하였다.

표 3. 비교분석

평가 항목 / 비교 대상	실시간 유/무	데이터 크기	통신 과부하	수행 시간	비고
CRL	offline	high	low	고속	전자결제, 의료정보시스템
OCSP	online	medium	high	저속	인터넷뱅킹, 전자상거래
제안방식	online	low	low	고속	증권거래, 전자입찰

CRL방식은 실시간성 측면에서 offline이며 데이터크기 측면에서는 인증서 폐지 목록이 계속하여 증가하기 때문에 데이터 크기가 high이다. 하지만 새로운 CRL을 다운 받기 전까지 자신의 디렉토리에서 검증을 수행하기 때문에 통신 과부하는 낮으며 이에 대한 결과로 수행속도는 고속으로 분류할 수 있다. 따라서 CRL방식은 실시간 처리가 중요시 되지 않고 인증서를 소유하고 있는 소유자의 이직이 빈번하지 않은 전자결제나 의료정보시스템에 적합한 방식이다. OCSP방식은 실시간 측면에서 Online을 보장하며 요청과 응답의 토큰 안정성이 보장된다. 또한 CRL방식에 비해 데이터 크기가 적기 때문에 중간으로 분류할 수 있다. 하지만 실시간으로 인증서 상태를 확인하기 때문에 통신과부하가 높으며 이로 인해 수행시간 항목을 저속으로 분류할 수 있다. 따라서 OCSP방식은 시간적 특성 보다는 안정성이 요구되는 인터넷뱅킹, 전자상거래등의 금융거래 분야에 적합하다. 본 논문에서 제안하는 방식은 실시간 측면에서 Online을 보장하며, 사용자 신원 정보에 대한 VDN을 생성하여 사용함으로써 데이터크기 및 네트워크 과부하가 적다. 따라서 본 논문에서 제안하는 방식은 시간적 특성이 중요시되는 증권거래, 전자입찰의 금융거래의 적합한 방식이다.

5. 결 론

인증서 상태 검증은 공개키 기반구조 인증 시스템의 주요 요소로서 인증서의 현재 상태와 인증서의 소유자 및 발행자의 신원을 확인하는 과정으로 전자거래에 있어 가장 중요한 부분이다. 가장 보편적인 상태 검증 방법으로 CRL방식이 있지만 인증서 상태에 대한 현재성을 보장할 수 없다는 문제점이 있다. 이와 같은 CRL방식의 문제점을 해결하기 위해 OCSP방식이 제기되었다. 하지만 네트워크 과부하 및 서버 과부하로 인해 인증서 상태 검증 수행속도가 다소 오래 소요되는 문제가 발생한다. 본 논문에서는 이러한 기존 방식의 문제점을 해결하기 위하여 사용자 신원정보에 대한 가상 식별자 정보 즉 VDN을 생성하여 인증서 상태 검증을 요청하고 수행함으로써 네트워크 과부하 및 서버 과부하를 해결한다. 또한 이에 대한 결과로 인증서 상태 검증 수행속도가 향상됨을 실험을 통해 확인할 수 있었다. 향후 본 연구를 토대로 대규모 사용자가 동시에 접속하여 검증을 요청하고 처리하는 시스템에 적용하기 위한 계속적인 연구의 필요성이 요구된다.

참고문헌

[1] 장홍종, 이성은, 이정현, " DARC 기반에서의 실시간 인증서 유효성 검증에 관한 연구", 한국정보처리학회 논문지(C), 8(5), pp. 0517 - 0524, 2001

[2] 김현철, 안재명, 이용준, 오해석 " 축약 서명 기반의 실시간 인증서 상태 검증 기법", 한국정보처리학회 논문지(C), VOL. 12-C NO. 02 pp. 0301 - 0308, 2005

[3] 권태경, 강명호, 김승주, 서정욱, 진승헌, "정보보호표준개론", 한국정보통신기술협회, pp 10-12, 2002

[4] 최연희, 박미옥, 전문석 "CA를 인증 경로 처리 작업에 참여시키는 새로운 인증서 검증 방안", 한국정보처리학회 논문지(C), VOL. 11 NO. 01 pp. 0021 - 0030, 2004

[5] 칼리슬 아담스, 스티브 로이드 공저 | 장기식 역, "보안을 위한 효율적인 기법 PKI", pp 51-67, 2003

[6] 정재동, 오해석, "실시간 인증서 상태 검증의 성능개선", 한국정보처리학회 논문지 (C), VOL. 10 NO. 04 pp. 0433 - 0440, 2003

[7] 정재동, "CSMP 기반의 실시간 인증서 상태검증의 성능개선", 숭실대학교 박사학위 논문, pp 30-55, 2003

[8] Ray Hunt, "PKI and Digital Certification Infrastructure," Proceeding of the 9th IEEE International Conference on Networks, 2001.

[9] RFC 3080, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", 2002

[10] RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 1999

[11] RFC 2560, "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol(OCSP)", 2001

[12] draft-ietf-pkix-ocspv2-ext-01, "x.509 Internet Public key Infrastructure Online Certificate Status Protocol Version2", 2002

[13] W. Diffie and M.E Hellman. "New Direction in Cryptography" IEEE Transactions on Information Theory, IT-22(6) : 644-654, 1976

[14] 김영수, 신승중, "식별정보를 이용한 보안서버시스템의 전자서명 모델 및 응용", 한국정보처리학회 논문지 (C), 제12-C권 제2호, pp169-174, 2005

[15] 장혜진, "pki 기반의 보안 다중 에이전트 엔진", 한국산학기술학회논문지, 1229-8832, 제3권4호, pp.319-324, 2002

이 광 형(Kwang-Hyoung Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 (공학사)
- 2002년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터공학과(공학박사)
- 2005년 3월 ~ 현재 : 서일대학 인터넷정보과 전임강사

<관심분야>
멀티미디어 검색, 멀티미디어 보안, RF-ID응용. 홈네트워킹

김 현 철(Hyun-Chul Kim) **[정회원]**

- 2003년 2월 : 인재대학교 정보컴퓨터학부 (학사)
- 2005년 2월 : 경원대학교 전자계산학과 (석사)
- 2006년 3월 ~ 현재 : 숭실대학교 컴퓨터 공학과 박사과정

<관심분야>
PKI, Home-Network 보안, OFDM