무선 PKI 기반의 가상 식별자를 이용한 인증서 검증

정회원 최 승 권*, 신 정 원**, 신 동 화***, 김 선 철****, 이 병 록*, 조 용 환*

Wireless PKI Based Certificate Verification Using Virtual Identifier

Seung-kwon Choi*, Jung-won Shin**, Dong-hwa Shin***, Sun-chul Kim****
Byong-rok Lee*, Young-hwan Cho* ***Regular Members***

요 약

무선 인터넷 서비스의 꾸준한 증가에 따라 무선환경에서 PKI(Public Key Infrastructure) 서비스는 정보보호 서비스를 제공하기 위해 중요하고 기본적인 기술로 대두되고 있다. 본 논문에서는 CSMP에서 VID를 사용하여 통신의 과부하를 감소시키는 인증 방법을 제시하였다. 이는 보안과 실시간 처리, 기존 인증 방법에 대한 성능을 보장한다. 보안과 실시간에서의 성능은 인증자에 의해 인증 노드를 관리함으로써 보증되며 VID를 통해 데이터 전송량을 감소시킬 수 있었다.

Key Words : PKI, CSMP, VID, RA, WAP

ABSTRACT

In wireless Internet environment that demand of wireless Internet service increase steadily, wireless PKI(Public Key Infrastructure) service is appearing on stage as necessary essential base technology for information protection service offer, In this paper, we propose the method for verification to reduce the communication overload using VID to CSMP made with a goal of the performance guarantee for security and use in a real time and examine the existent certificate verification methods. The performance of security and the use in a real time is guaranteed by managing the note of authentification by the person who verifies and reducing the amount of the data transmission using VID.

Ⅰ. 서 론

인터넷 및 이동통신기술의 발전과 함께 사무실내에서 뿐만 아니라 자동차나 거리, 공항이나 지하철역 등 다양한 환경에서 인터넷에 접속이 가능해지고 있다. 그리고 처음에는 게임, 캐릭터, 벨 소리, 이모티콘 등의 엔터테인먼트가 주류를 이루던 서비스 영역에서 증권, 은행, 지불, 예약 및 경매 등 다양한 서비스의 영역으로 확대되고 있다[1].

정보 유통시 안정성과 신뢰성 확보를 위해 공개키 암호기술을 적용한 인증서 기반의 공개키 기반 구조(PKI : Public Key Infrastructure)가 현재 각종 분야에 가장 보편화되어 있는 방법이다. PKI 구축을 위하여 사용되는 기술 중 인증서 검증 방법은 실제 전자상거래에서 그 거래의 유효성에 관한 것이므로 신중히 처리되어야 한다[2]. 그러나 무선 인터넷의 경우는 일반 PC와는 달리 많은 제약 조건이 따르고 있다. 휴대폰이나 PDA 단말기 내부의 작은

* 충북대학교 전기전자컴퓨터공학부 (yhcho@cbucc.chungbuk,ac.kr), ** (주)엠프론티어 (jungw04@naver.com)
*** (주)다이퀘스트 (talose21th@hotmail.com), **** (주)신명전기공사 (kimsunc@hanmail.net)
논문번호 : KICS2006-02-067, 접수일자 : 2006년 2월 8일, 최종논문접수일자 : 2006년 7월 21일

프로세서들은 메모리 및 장치의 한계 때문에 PC와 유선망의 암호화 및 인증을 사용하는 것은 불가능하다[3].

이에 본 논문에서는 보안성, 실시간성, 성능 보장을 목표로 한 인증서 상태 관리 프로토콜(CSMP: Certificate Status Management Protocol)에서 통신 부하를 줄이기 위해 인증서 관리를 할 때 신상정보를 가상 식별자(VID : Virtual Identifier)를 이용하는 것을 제안하였다. CSMP는 인증서 폐지 처리를 하는 기능과 검증자 등록 처리를 하는 기능으로 구성이 되어 있다. 검증자가 인증서의 상태 검증을 실시간으로 관리하도록 지원함으로써 실시간 응용 분야에서 인증서 상태 검증을 실시간으로 처리하도록 하였다. 또한, 검증자 별로 인증서 상태를 관리하므로 필요한 검증자에서만 인증서를 요청하므로 통신 부하가 분산이 된다. 그리고 가상 식별자를 통해 인증서 상태 요청을 위한 데이터의 크기를 줄이고, 전송속도를 향상시킬 수 있다.

Ⅱ. 무선 PKI 기반의 인증서 검증

무선 인터넷이란 휴대용 무선단말기와 무선 데이터 통신망을 이용해 인터넷에 접속하여 데이터 통신이나 인터넷 서비스를 이용하는 것이라고 정의할 수 있으며, 유선 인터넷과 달리 케이블링이 필요하지 않은 무선 연결 방식이면서, 동시에 한 곳에 고정되어 있지 않고 이동하며 사용할 수 있다는 두 가지 의미를 동시에 가지고 있다고 볼 수 있다.

유선 인터넷 환경과 마찬가지로 인터넷이 안전한 서비스를 제공하기 위해서는 인증, 접근 통제, 기밀성, 부인봉쇄와 같은 보안 서비스를 제공하기 위해 현재 인증서비스의 기반기술로서 가장 주목되고 있는 무선 PKI가 필요하다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용한다. 무선환경에 적합하도록 기능을 최소한 변화시킨 것이 무선 PKI이다. 예를 들어 WAP 게이트웨이를 통한 무선 PKI 서비스에서는 기존의 유선 환경에 사용하는 X.509 인증서에 비해 부피가 작고 간단한 WTLS(Wireless Transport Layer Security) 인증서를 사용한다. 이는 무선 환경에서 사용하는 소용량 단말기에서 암호화 및 인증 업무를 효율적으로 수행할 수 있도록 구성되어 있다.

PKI 구축을 위해 사용하는 기술로는 인증서 발급, 갱신, 폐지 등을 다루는 인증서 관리 기술과 보안 알고리즘을 이용하여 전자서명의 생성 및 검증, 암호화를 다루는 보안 기술, 그리고 인증서의 유효성 및 현재 상태를 다루는 인증서 검증 기술로 크게 구분할 수 있다[2].

2.1 무선 PKI의 고려사항 및 구성요소

2.1.1 무선 PKI 고려사항

무선 인터넷은 기존의 유선 인터넷과 비교하여 통신 환경에서 몇 가지 차이점은 갖는다. 따라서 무선 인터넷에서의 PKI는 다음과 같은 사항을 고려해야한다. 첫 번째 유선 인터넷과의 연동이다. 초기의 무선 인터넷에서는 제공 서비스가 부족한 상태이므로 유선 인터넷에서 제공되는 서비스를 이용해야 한다. 따라서 무선 인터넷과의 연동 방안을 고려해야 한다. 두 번째로 대역폭의 제한이다. 무선 인터넷은 우선 인터넷에 비해 데이터 전송 속도가 떨어지며, 전송할 수 있는 데이터 량에도 제한이 있다. 따라서 대역폭의 제한을 고려해야 한다. 마지막으로 단말기의 제한이다. 이동단말기는 데스크탑 컴퓨터에 비해 CPU 성능, 메모리 용량, 입출력 장치 제한이 따른다. 따라서 이러한 단말기의 제한을 고려해야 한다[4, 5]

2.1.2 무선 PKI 구성요소

무선 PKI를 구성하는 요소로는, 인증서를 발행하고 효력정지 및 폐지 기능을 수행하는 인증기관, 인증서 등록 및 사용자 신원 확인을 대행하는 등록기관(RA : Registration Authority), 인증서 및 인증서 폐지목록을 저장하는 디렉토리, 그리고 인증서를 신청하고 인증서를 사용하는 사용자로 분류될 수 있으며 그림 1은 무선 PKI 구성도를 보여주고 있으며 각각의 특징은 다음과 같다.

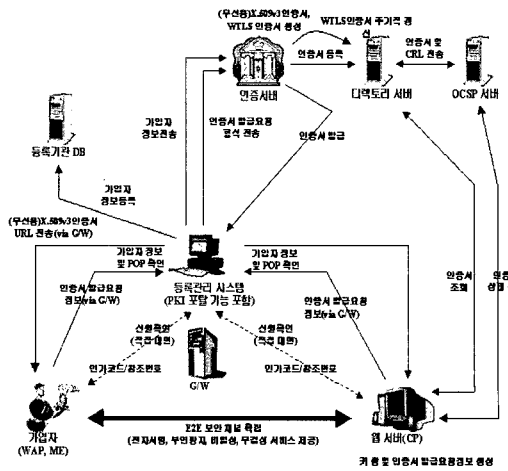

그림 1. 무선 PKI구성도

(1) 인증기관

인증기관은 공개키 기반구조를 구성하는 가장 핵심 객체로 사용자의 공개키 인증서의 발급·효력정지 및 폐지와 등록기관의 요청에 따라 인증서를 발급하는 기능을 수행한다. 또한, 인증서와 인증서 소유자의 정보의 관리, 인증서와 그 소유자의 정보를 관리하는 데이터베이스의 관리, 인증서 효력정지 및 폐지목록, 감시파일의 보관 등의 업무를 수행하는 핵심 기관이다.

(2) 등록기관

등록기관은 인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자 사이에 설치하여, 인증기관을 대신하여 사용자들의 인증서 신청 시 그들의 신분과 소속의 확인, 인증기관에 인증서 요청서 전송, 디렉토리로부터 인증서와 인증서 효력의 정지 및 폐지목록 검색, 인증서 효력정지 및 폐지 요청 등의 기능을 수행한다.

(3) 디렉토리

디렉토리란 인증서와 사용자 관련정보, 상호 인증서 쌍 및 인증서 폐지목록 저장 및 검색 장소로, 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버는 DAP (Directory Access Protocol) 또는 LDAP(Lightweight DAP v2, v3)를 이용하여 X.500 디렉토리 서비스를 제공한다. 인증서와 상호 인증서 쌍은 유효기간이 경과된 후에도 서명검증의 응용을 위해 일정기간 동안 디렉토리에 저장된다.

(4) 사용자

공개키 기반구조내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 말하며, 자신의 비밀키/공개키 쌍을 생성하고 검증, 공개키 인증서의 요청/획득, 전자서명의 생성 및 검증, 특정 사용자의 인증서 획득 및 검증, 자신의 인증서 취소 등의 기능을 수행한다.

(5) 인증서

인증서는 공개키의 합법성을 보증하는데 이용한다. 서명을 확인하는 사람은 인증서의 서명을 확인하여 서명에 위조나 변조가 없다는 사실을 확인한다. 현재 공개키 인증 시스템에서 사용되는 표준은 ITU-T X.509 표준에 의해서 정의된다.

(6) 인증서 효력정지 및 폐지목록

예정된 유효 기간의 만기일이 도래하기 전에 취소된 인증서에 대한 정보를 인증서 효력정지 및 폐지목록이라 한다.

위에서 설명한 무선 PKI를 구성하는 4개의 중추적인 구성 요소 외에 무선 인터넷 사용자를 대신하여 인증서 상태정보와 함께 인증경로에 대한 검증 정보들을 제공하는 OCSP나 무선단말기의 계산 능력 저하로 인한 단점을 보완하기 위하여 사용되는 보안 모듈 등이 무선 인터넷상에서 PKI를 구성하기 위한 부수적인 구성요소이다. 더불어, 무선 PKI는 무선 인터넷상에서 구성되어야 하므로, WAP(Wireless Application Protocol) 방식이나 ME(Mobile Explorer) 방식과 같은 무선 인터넷 접속 기술 또한 중요한 구성 요소이다. 각 접속 기술에 따라 PKI를 구성하는 인증서의 형식, 전송 포맷, 서명 알고리즘, 키 분배 알고리즘 등이 각 방식에 적합하게 변형되어 사용된다.

Ⅲ. 가상 식별자를 이용한 인증서 검증

3.1 인증서 상태 관리 프로토콜

실시간 응용 분야에서는 인증서를 검증할 때 보안성과 성능을 보장하면서 항상 CA의 인증서 상태 정보와 동일한 정보를 이용해야 한다. 그런데 기존의 인증서 상태 검증 방법으로는 성능에 문제가 있다. 인증서 상태 관리 프로토콜(CSMP : Certificate Status Management Protocol)은 보안성, 실시간성, 성능 3요소를 모두 보장한다[2].

3.1.1 인증서 상태 관리 프로토콜 구성

- 인증기관 : 서명자에게 인증서의 발급을 담당
- 서명자 : 인증서를 발급 받아 온라인서비스를 이용하는 고객
- 검증자 : 검증자는 온라인서비스의 서버로써, 서명자의 전자서명에 대하여 검증을 수행한다. 검증시 인증서 상태에 대한 검증을 CSMC에 요청하여 처리한다.
- 인증서 상태 관리 서버(CSMS : Certificate Status Management Server) : CA에서 관리하는 인증서들의 상태 정보를 CSMC에 제공하는 서버로써 이용자가 상태정보를 조회한 적이 있는 검증자들을 Verifier Lists에 이용자별로 관리한다.

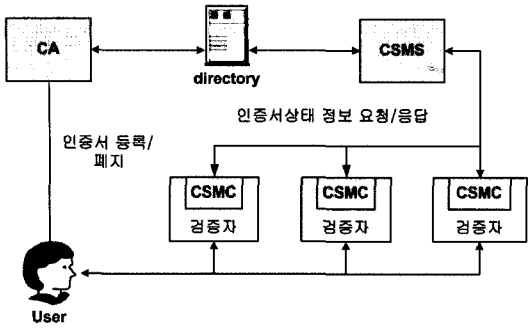

그림 2. CSMP의 구성요소

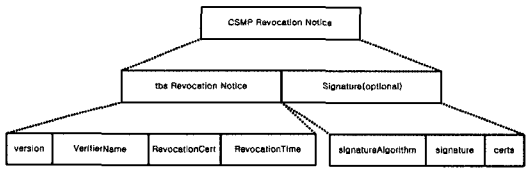

그림 3. CSMP Revocation Notice 구조도

- 인증서 상태 관리 클라이언트(CSMC : Certificate Status Management Client) : 검증자에게 이용자의 인증서 상태 정보를 제공하며 검증자가 인증서 상태 검증 처리를 효율적으로 수행할 수 있도록 지원한다.

그림 2는 CSMP의 인증서 상태 검증 방식의 구성요소이다.

3.1.2 인증서 상태 관리 프로토콜

(1) CSMP_Revocation : 인증서 폐지처리

CA의 인증서가 폐지될 때 CSMS가 검증자에 분산되어 있는 인증서 상태 정보를 갱신하는 프로토콜로서 인증서의 폐지는 CA에서 비롯되는 트랜잭션이기 때문에 CA의 정보가 갱신될 때 검증자에 분산되어 있는 인증서 상태 정보들을 실시간으로 동기화 시켜야 한다. 인증서 상태 정보가 분산되어 유지되는 것을 가능하게 함으로써 CA 또는 CSMS에 트랜잭션이 집중되는 것을 방지하고 검증자가 인증서 상태 정보를 스스로 검증을 가능하게 한다.

가. CSMP_Revocation_Notice

CSMS는 폐지된 인증서 정보를 CSMC에 전송한다. CSMP Revocation Notice 구조는 그림 3과 같다.

나. CSMP_Revocation_Confirm

CSMS의 폐지정보에 대한 승인에 대해 CSMC가 전송한다. 그림 4는 CSMP Revocation Confirm 구조이다.

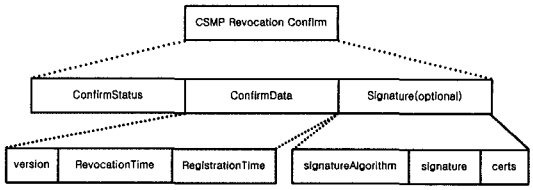

그림 4. CSMP Revocation Confirm 구조도

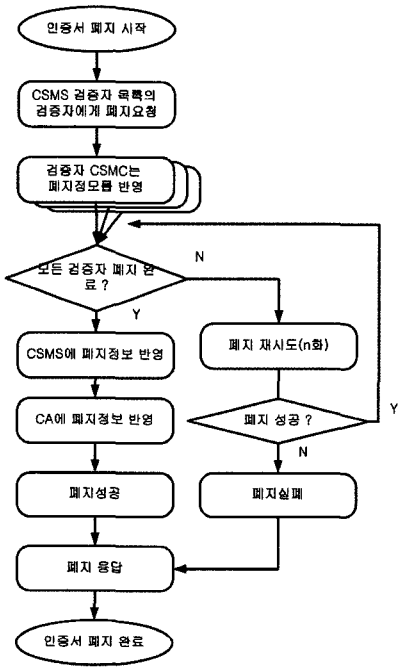

그림 5. 인증서 폐지 절차

이용자가 본인의 인증서에 대하여 CSMS에게 폐지를 신청한다. CSMS는 해당 인증서의 등록된 검증자 목록(RVL : Registration Verification List)을 조회하고 검증자가 존재하면 폐지정보를 전송한다. RVL의 검증자 목록에 등록된 모든 검증자로부터 전송확인을 받아야 폐지가 등록된다. 그림 5는 인증서 폐지 절차를 나타낸다.

(2) CSMP_Registration: 검증자 등록 처리

신규 이용자의 인증서의 정보는 등록된 인증서 목록(RCL : Registration Certificate List)에 없기 때문에 검증자는 CSMC를 통하여 CSMS에 신규 고객의 인증서 상태 정보를 요청한다. CSMS는 CA에 문의하여 신규 고객의 인증서 상태 정보를 획득한다. 만약 인증서 상태 정보가 없으면 해당 이용자는 CA가 인증서를 발행한 이용자가 아님을 CSMC를 통하여 검증기관에 통보한다. 인증서 상태 정보가 획득되면 CSMS는 RVL에 인증서 상태 정보와

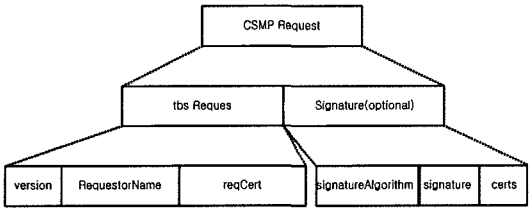

그림 6. CSMP Registration Request 구조도

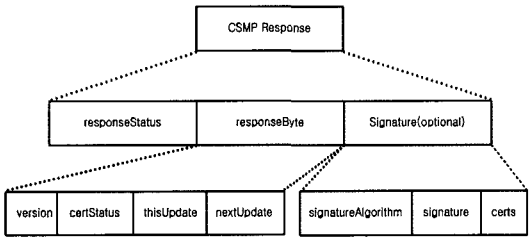

그림 7. CSMP Registration Response 구조도

인증서 상태 정보를 요청한 검증자를 기록하고, CSMC를 통하여 RCL에 인증서 상태 정보를 기록하여 검증자의 인증서 상태 검증 처리가 가능하도록 한다.

가. CSMP_Registration_Request

해당 인증서의 상태를 요청하기 때문에 구조가 간단한 것이 특징이 있다. 그림 6는 CSMP Registration Request 구조이다.

나. CSMP_Registration_Response

certStatus : 특정 인증서의 상태를 나타내며 "good", "revoked", 그리고 "unknown"으로 나타낸다. 그림 7은 CSMP Registration Response 구조이다.

"good"은 [0]으로 표시하면 긍정적인 응답으로 인증서 상태가 취소되지 않았음을 나타낸다.

"revoked"는 [1]로 표시하며 인증서의 상태가 영구적 또는 일시적으로 취소되었음을 나타낸다.

"unknown"은 [2]로 표시하며 인증서의 최소 여부에 대하여 응답자가 알지 못할 경우를 나타낸다.

검증자는 이용자의 인증서 상태를 CSMC에 요청한다. 두가지 검증하는 방법이 제시되어 있는데 첫 번째는 최초로 이용자가 검증자에게 접속하였을 때 CSMS에 인증서 상태를 요청하여 정보를 서명자의 검증자 목록에 등록 한 후에 인증서 상태에 응답한다. 두 번째는 검증자 목록에 등록된 경우로 CSMC에서 인증서 상태 정보를 바로 응답한다. 그림 8은 인증서 상태 검증 및 검증자 등록 처리를 나타낸 것이다.

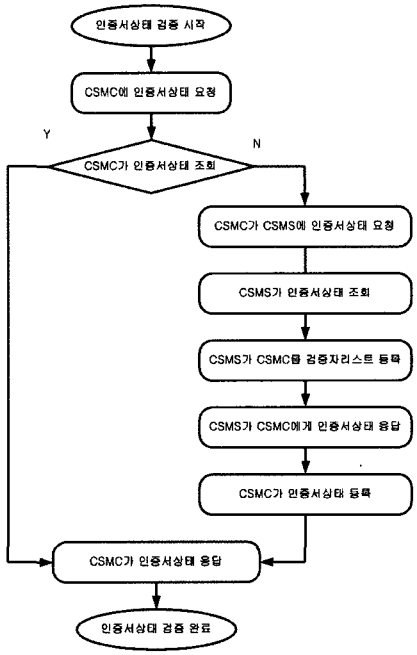

그림 8. 인증서 상태 검증 및 검증자 등록 절차

3.2 RVL과 RCL의 가상 식별자

CSMP를 지원하는 이용자 목록으로 RVL은 등록 검증자 목록으로 이용자별, 폐지정보, 검증자 명세를 나타내며 CSMS가 관리하여 이 목록을 이용하여 인증서 폐지 전달을 효율적으로 관리함으로써 인증서 폐지 시 이 목록에 등록된 기관들에게만 폐지 정보를 전달한다. RCL은 등록된 인증서 목록으로 이용자별, 인증서 상태를 나타내며 이용자가 최초로 검증자인 기관을 이용할 때 유효한 인증서를 보유하고 있으며 RCL에 등록한다. 검증자는 RCL만 이용하여 검증이 가능하다.

CSMP가 금융거래에서 이용할 수 있도록 하는 실시간성은 CSMS의 RVL과 CSMC의 RCL의 실시간 동기화에 의해서 보장이 된다. 만약 동기화 처리에 의한 부하가 발생하면 금융거래 자체를 지연시키는 등 문제가 발생한다.

RVL에 등록된 검증자 수가 늘어나면 CSMP의 처리 속도 중 인증서 폐지 처리가 늘어난다. 그래서 데이터의 전송량을 줄여 동기화에 걸리는 시간을 줄이기 위해 RVL과 RCL의 사용자의 정보를 가상 식별자로 표시한다.

VID는 인증서를 발급할 때 인증기관이 가지고 있는 신원정보와 사용자가 서비스제공자에 회원가입하면서 등록하는 신원정보가 일치 한다는 점에 착안을 하였다.

3.2.1 검증자의 수행 절차

앞에 살펴본 검증자 등록 처리에서처럼 신규 이용자의 인증서의 정보는 RCL에 없기 때문에 검증자는 CSMC를 통하여 CSMS에 신규 고객의 인증서 상태 정보를 요청한다. CSMS는 CA에 문의하여 신규 고객의 인증서 상태 정보를 획득한다.

서비스 제공자는 전자서명을 한 후에 사용자의 신상정보를 찾아내고, 난수 L을 생성한다. 난수 L은 NIST(National Institute of Standards and Technology : 미국 국립표준기술원)의 FIPS PUB 140-2의 테스트를 통과한, 160비트 이상의 안전한 난수를 사용한다. 서비스 제공자는 난수 L과 사용자의 신원정보 SSN을 해쉬하여 가상 식별자 VID을 생성한다.

$$L \text{ Generation} \quad (3\text{-}1)$$

$$VID = h(SSN,L) \quad (3\text{-}2)$$

위 식에서 L은 난수, SSN은 신원정보, h( )는 해쉬함수, VID은 가상 식별자이다. 다음으로 생성된 식별번호 VID을 인증기관의 공개키로 암호화를 수행하여 EVID을 생성한다. 이렇게 암호화를 하는 이유는 통신구간에서 VID과 난수 L의 기밀성을 보장하기 때문이다.

$$EVID=EPK\text{-}CA(VID,L) \quad (3\text{-}3)$$

여기서 PK는 공개키, E( )는 암호화 함수, EVID은 암호화된 가상 식별자이다. 다음으로 암호화된 EVID을 인증기관에 인증서 상태 요청을 한다.

3.2.2 인증자의 수행 절차

인증서 상태 검증을 요청을 받은 인증기관은 EVID을 개인키로 복호화를 수행한다. 복호화를 수행하면 가상 식별자 VID과 난수 L을 획득하게 된다.

$$VID, L=D\ SK\text{-}CA\ (EVID) \quad (3\text{-}4)$$

여기서 SK는 개인키, D( )는 복호화 함수이다.

다음으로 인증기관의 데이터베이스에서 신원정보를 찾아내고, 복호화를 획득한 난수 L과 해쉬함수를 수행하면 가상 식별자 VID1을 생성하게 된다.

$$VID1 = h(SSN2, L) \quad (3\text{-}5)$$

$$VID1 = VID \quad (3\text{-}6)$$

해쉬함수를 수행하여 나온 VID1과 VID을 비교하여 일치하면, 인증서 상태 정보를 획득할 수 있다.

인증서 상태 정보가 획득되면 VID을 인증서에

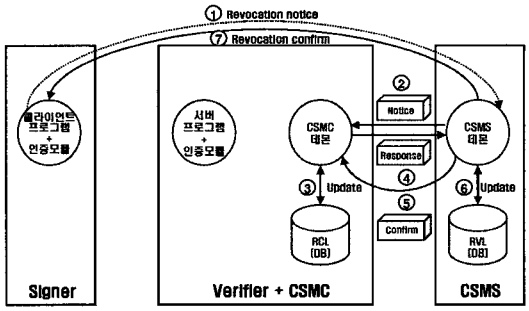

그림 9. 폐지처리 과정

저장하고 CSMS는 사용자 정보를 VID으로 하여 RVL에 인증서 상태 정보와 인증서 상태 정보를 요청한 검증자를 기록하고, CSMC를 통하여 RCL에 인증서 상태 정보를 기록하여 검증자의 인증서 상태 검증 처리가 가능하도록 한다.

VID을 이용하여 데이터의 전송량을 줄여 속도를 높이고 등록된 검증자에 대해서는 암호화를 거치지 않고 CSMC에서 상태 검증을 처리한다[6].

3.3. 가상 식별자를 이용한 인증서 상태 검증

CSMP는 기존의 PKI 기본 구성요소에 CSMS와 CSMC를 추가하였는데 사용자 정보를 가상 식별자를 이용하여 표시한다. CSMS는 인증서 폐지 처리가 주된 기능이고, CSMC는 RVL에 검증자를 등록하는 기능이 주된 기능이다.

3.3.1 CSMS 기능

CSMS는 인증서의 폐지 처리를 주로 수행하며, 인증서 폐지 신청 처리와 인증서 폐지 완료 처리로 구분된다. 인증서 폐지 처리는 CSMP_Revocation_Notice를 이용하고, 인증서 폐지 완료 처리는 CSMP_Revocation_Confirm을 이용한다. CSMC는 RCL에 폐지 정보가 반영되면 CSMS에 폐지 완료 처리를 전송한다. 그림 9는 폐지처리 과정이다.

① 인증서 소유자가 CA에 인증서 폐지를 신청하면 가상 식별자로 RVL을 확인하여 폐지 정보를 전달할 검증자 목록을 확보한다.
② CSMC에 대칭키로 암호화된 CSMP_Revocation_Notice의 프로파일과 전자서명을 전달한다.
③ RCL의 인증서 상태 정보 변경한다.
④ 폐지 완료 정보 전달 준비한다.
⑤ CSMP_Revocation_Confirm의 암호화 결과와 전자서명을 함께 전달한다.
⑥ RVL의 인증서 상태 정보 변경한다.

⑦ 인증서의 소유자에게 폐지 처리가 완료되었음을 통보한다.

3.3.2 CSMC 기능

CSMC의 주 기능은 인증서 상태 검증과 검증자 등록처리이다.

신규인증서를 소유한 최초 거래 이용자 경우에는 RVL의 검증자 목록에 등록되어 있지 않다. 따라서 금융기관인 검증자와 이용자가 최초의 거래를 할 때 검증자 등록을 하여야 한다. RVL에 등록된 경우에는 검증자는 난수 L과 사용자의 신원정보 SSN을 해쉬하여 가상 식별자 VID을 생성한다. 검증자는 CSMC의 조회를 통해 VID이 동일한 값을 가진 RCL에 등록된 인증서 상태정보를 사용한다. 그림 10은 인증서 상태 검증과 검증자 등록처리 과정이다.

① 사용자는 전자서명된 거래를 검증자에게 전송한다.
② 검증자는 가상 식별자를 생성하여 검증자는 CSMC를 조회하고 사용자의 인증서 상태가 등록되어 있는지 확인한다.
③ 사용자의 인증서 상태가 CSMC의 RCL에 등록되어 있는지 응답한다.
④ RCL을 확인하여 최초의 거래자인 경우 CSMP_Registration_Request의 프로파일을 인증서 폐지 처리 방법과 동일한 방법으로 전자서명과 대칭키암호화를 통하여 메시지인 증처리를 수행한다.
⑤ 메세지 인증 처리가 완성된 CSMP_Registration_Request의 프로파일을 CSMS에게 전달한다.
⑥ 최초 거래자의 인증서가 유효한지 CA에 확인한다. 이때 유효하지 않으면 에러 처리를 한다. RVL에 인증서 상태 정보와 검증자 목록에 정보를 등록한다. CSMP_Registration_Re-sponse의 프로파일을 메시지인증 처리한다.
⑦ CSMC에 CSMP_Registration_Response의 프로파일을 메시지인증 처리한 결과를 전달한다.

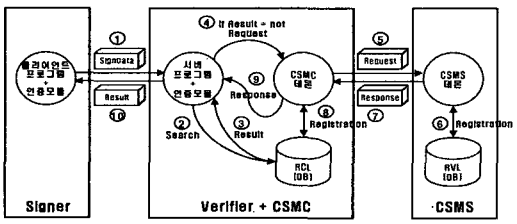

그림 10. 인증서 상태 검증과 검증자 등록처리 과정

⑧ 메시지인증 처리된 CSMP_Registration_Response의 프로파일을 회복처리하여 정보를 획득한다. RCL의 인증서 상태 정보를 등록한다.
⑨ 검증자에게 인증서 상태 정보를 전달한다.
⑩ 사용자에게 인증서 상태 정보를 알린다.

Ⅳ. 실험 및 결과 분석

본 장에서는 검증자의 실시간 인증서 상태 검증을 위한 CSMP에서 RVL, RCL의 사용자 정보를 가상 식별자를 이용한 검증 기법에 대해 구현한다. 또한 기존의 인증서 검증 기법과 검증시간을 비교하고 인증서 폐지 처리 시간과 전송되는 데이터량을 알아본다.

4.1 실험

실험은 Intel Pentium Ⅳ 2GHz, 메모리는 512MByte의 PC 환경에서 Visual C++ 언어를 이용하여 검증자 수를 50개, 총 발행 유효 인증서 4백개, 폐지율 10%, CRL크기 100Mb, 전자서명한 값은 128Byte이고 OCSP 패킷의 크기는 2KByte의 환경으로 실험을 하였다.

4.2 결과 분석

모든 검증자에게 인증서 상태 정보를 제공하는 것이 이상적이나 부하가 부담이 된다. 따라서 필요한 검증자에게만 제공하는 검증 방법을 제안하였다. 그리고 인증서 상태 검증에서 가장 많이 쓰이는 CRL방법과 OCSP방법, SCVP 방법을 제안한 방법과 비교하였다.

첫 번째 실험은 원문의 데이터의 크기를 변화시키면서 가상 식별자를 생성하여 CSMC에 해당 인증서가 존재하지 않아 CSMS에 조회한 경우와 CSMC에 해당 인증서 상태를 보유하여 즉시 검증했을 때의 속도를 분석하였다.

최초등록인 경우는 CSMS에 요청하여 인증서 정보를 등록하기 때문에 OCSP와 동일한 성능을 보여주지만, CSMC에 등록된 경우는 검증속도를 비교할 때 CRL보다 항상된 결과를 보임으로써 제안한 방식이 성능을 개성시켰다는 결과가 도출되었다. 또한 원문의 크기가 커짐으로 CRL, OCSP, 제안한 CSMS의 검증속도가 다소 증가했으나 결과에 영향이 없음을 보여준다. 따라서 실시간 검증을 제공하는 OCSP와 비교하면 상태 정보 등록 후 성능이 개선된 결과를 나타낸다.

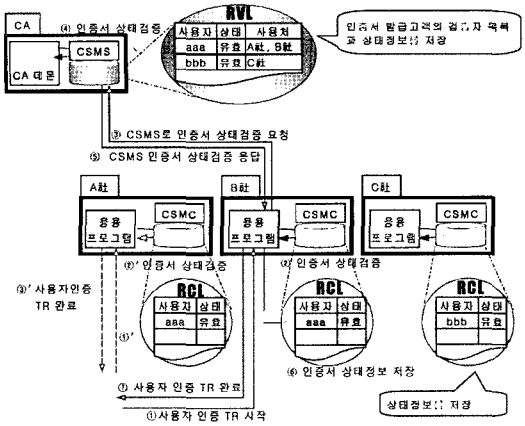

그림 11. 검증자 등록 및 상태 요청 수행 과정

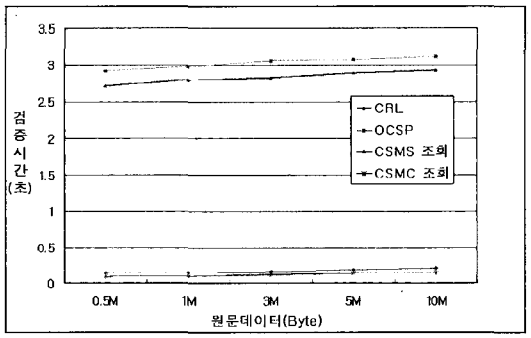

그림 12. 인증서 상태 검증의 검증시간

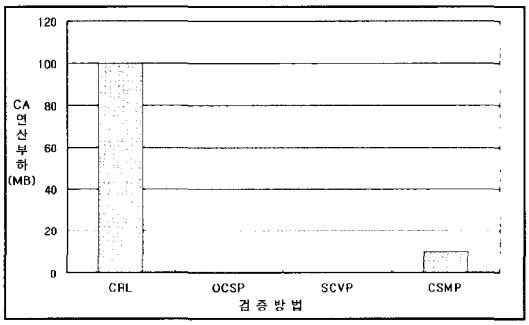

그림 13. CA의 연산 부하

두 번째 실험은 암호화작업에 따른 부하치를 비교하여 본다

그림 13을 보면 CRL은 폐지목록을 갱신할 때 매번 동일한 절차에 따라 전저서명 되어야만 한다. 하루에 한번 인증서 폐지목록을 갱신한다고 하면 CA의 부하는 100MByte이고 OCSP와 SCVP는 암호연산을 거치지 않으므로 0이며 CSMP는 가상 식별자를 만들기 위해 암호화 작업을 위한 작은 연산부하가 생기는 것을 알 수 있다.

그림 14는 CA에서 디렉토리, OCSP, SCVP, CSMS의

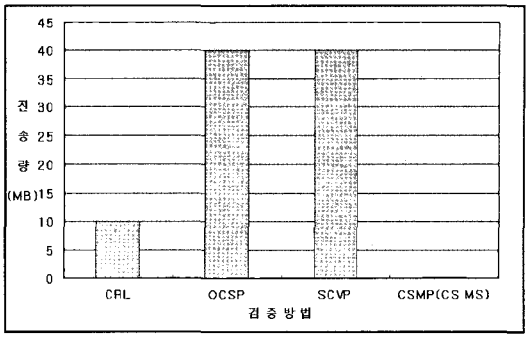

그림 14. CA에서 디렉토리, OCSP, SCVP, CSMS의 전송량

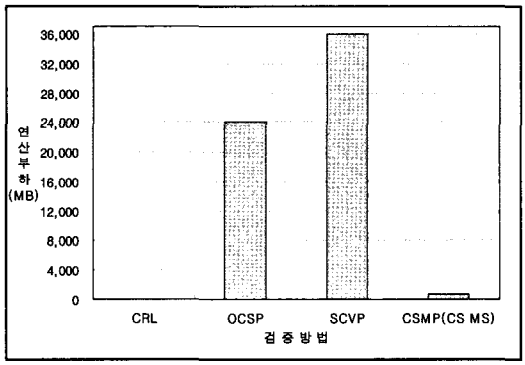

그림 15. 디렉토리, OCSP, SCVP, CSMS의 연산부하

전송량을 비교한 것이다. CSMP의 경우에는 CSMS로 전송량이다. CA와 CSMS사이의 통신량은 두 가지로 표현되는데, 첫 이용자가 인증서를 폐지할 때, 이용자가 이용하였던 검증자들에게 전달하는 인증서 폐지정보와 이용자가 최초로 검증을 이용할 경우 CSMS에 인증서 상태 정보를 요청하는 경우이다. 여기서는 인증서 폐지 요청 시 전송량이다. 이용자가 검증자의 50개 싸이트에 등록을 한 경우의 값이다.

그림 15는 디렉토리, OCSP, SCVP, CSMC의 연산부하로 CRL 같은 경우에는 디렉토리에서 암호연산이 없기 때문에 0이고, 검증자가 요구하는 인증서 상태 정보에 대하여 응답하기 위한 OCSP와 SCVP의 연산부하는 높은 편이며 CSMS는 인증서 폐지시 CA의 인증서 상태 정보와 검증자의 인증서 상태 정보를 동기화 시키는데 필요한 부하이다. 가상 식별자를 이용하기 때문에 데이터의 전송량이 작아 CSMS의 연산부하가 다른 방법들에 비해 작다.

그림 16을 보면 그림15의 설명에서도 말했듯이 다른 방법에 비해 CSMP의 전송량이 작은데 이는 가상 식별자와 인증서 상태 정보가 변경되는 내용만 전송이 되기 때문이다.

그림 17은 검증자의 연산부하로 응답에 대한 해쉬

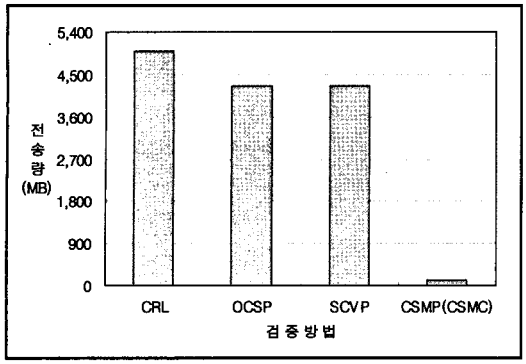

그림 16. 디렉토리, OCSP, SCVP, CSMC에서 검증자에게 전송량

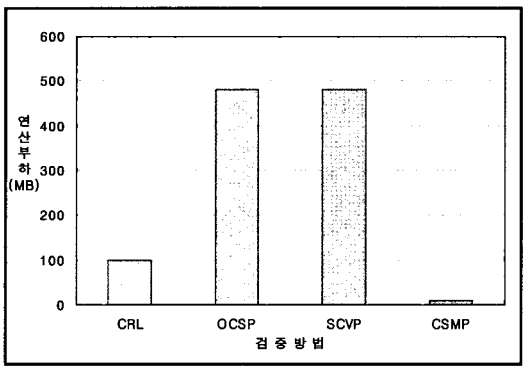

그림 17. 검증자의 연산부하

연산과 전자서명 값을 검증하기 위한 연산 부하들이다.

이와 같은 결과들을 볼 때 CSMP에 가상식별자를 이용함으로써 CA와 검증자에게 연산 부하는 생기지만 데이터의 전송량과 연산부하가 CRL, OCSP, SCVP보다 적고 또한 검증 시간이 향상되는 것을 볼 수 있다.

V. 결 론

본 논문에서는 실시간 인증서 상태 검증을 위해 현재 인증서 상태를 확인하는 방법으로 CRL방법과 OCSP방법이 가장 대표적으로 이용되고 있으나 구조적 한계 때문에 실시간 응용 분야에 충분한 역할을 하고 있지 못하고 있는 단점을 보안하고자 CSMP에서 이용자의 신상정보를 가상 식별자를 이용하여 데이터 전송량을 줄이고 보안성, 실시간성, 성능을 확보하는 방법을 제안하였다..

기존의 CRL방법은 폐지목록이 커질수록 네트워크 통신에 부담이 되기도 하지만 CRL을 검증자가 획득한 후 CRL의 갱신시점까지 상태 정보를 재사용할 수 있다. 따라서 검증자 관점에서는 동일한 상태 정보요청을 하지 않고 보유하고 있는 정보를 요청함으로써 검증부하를 현저히 줄일 수 있다.

하지만 폐지목록에 변동이 있을 시엔 실시간성을 보장하지 못하고 있다. OSCP방법은 다수의 이용자 환경에서 연속된 요청에 대해 병목현상이 발생할 수 있으므로 실시간 처리에 지연이 생길 수 있다. 이런 단점을 보안하고자 필요한 검증자에게만 인증서의 상태를 제공하여 부하를 줄이고 실시간으로 인증서 상태 정보를 제공할 수 있는 CSMP가 제안되었었다. 이에 필요한 정보의 전송을 최대한 줄이고 보안성을 높이고자 신상정보를 해쉬함수와 난수를 통하여 가상 식별자를 생성하여 인증 상태 정보 획득 시간도 단축을 하였다.

보안성은 CSMP의 프로파일을 송수신할 때 프로파일에 대한 전자서명을 우선 실행하고 대칭키로 암호화하여 그 결과물을 송수신하는 통신 방법을 이용하여 검증하였다. 실시간성은 폐지정보를 실시간으로 전송하여 CA의 인증서 상태 정보, CSMS의 RVL 그리고 CSMC의 RCL을 실시간으로 완벽히 동기화 시키는 방법으로 검증하였다. 성능은 가상 식별자를 만들기 위해 CA에 검증자에게 연산 부하가 생기기는 하지만 전송되는 데이터량의 비교를 통하여 CSMP가 CRL방법과 OCSP방법, SCVP방법 보다 우수한 것을 증명하였다. 또한 검증 시간의 단축과 전송 데이터량의 감소는 무선 인터넷의 속도를 고려하면 무선단말기를 이용하여 금융거래나 전자상거래를 하는 사용자에게 편의를 제공할 수 있다.

앞으로 사용자와 검증자수가 많아지면서 폐지목록과 인증서 상태 변경이 증가하고 동기화에 걸리는 시간이 늘어나게 된다. 그러면 금융거래 같은 지연이 발생하므로 동기화 시간을 단축시킬 수 있는 연구가 필요할 것이다.

참 고 문 헌

[1] 이종후, 서인석, 윤혁중, 류재철, "무선랜 환경에서의 PKI 구축", *정보보호학회지*, 제 13권, 제 1호, pp.77-91, 2003. 2.

[2] 정재동, "실시간 동기화를 위한 인증서 상태 관리 프로토콜", *숭실대학교 석사학위논문*, 2004. 2.

[3] D. Critchlow, N. Zhang, "Security enhanced accountable anonymous PKI certificates for mobile e-commerce", *Computer networks*, Vol.45 No.4,

pp.483-503, 2004. 3.
[4] 무선 PKI(Public key Infrastructure)기술기준(안), *한국정보보호센터*.
[5] J. Dankers, R. Schaffelhofer, T. Garefalakis, T. Wright, "PKI in mobile systems". *IEE TELECOMMUNICATION SERIES*, Vol.51 No.2, pp.11-32, 2004.
[6] P. MacKenzie, R. Swaminathan, Secure Network Authentication with Password Identification, *Submission to IEEE* P1363a, July, 1999.

최 승 권 (Seung-kwon Choi) 정회원

2001년 8월 충북대학교 컴퓨터공학과 대학원졸업(공학박사)
현재 충북대학교 초빙교수
<관심분야> 멀티미디어 콘텐츠, 게임디자인, 유비쿼터스 네트워킹

신 정 원 (Jung-won Shin) 정회원

2006년 2월 충북대학교 컴퓨터공학과 대학원 졸업(공학석사)
현재 (주) 엠프론티어
<관심분야> 멀티미디어 통신, 무선통신, Wibro, Home network

신 동 화 (Dong-hwa Shin) 정회원

2005년 2월 충북대학교 컴퓨터공학과 박사
현재 (주)다이퀘스트 기술 영업팀 근무
현재 중국 'saywo.com' 사이트 한국기술고문
현재 충북대학교 컴퓨터공학과 강사
<관심분야> 검색엔진, 포탈

김 선 철 (Sun-Chul Kim) 정회원

현재 신명전기공사 대표이사
<관심분야> 멀티미디어 통신, 유비쿼터스 네트워킹, RFID, 무선통신

이 병 록 (Byong-rok Lee) 정회원

2005년 2월~현재 충북 대학교 겸임교수
현재 (주) 유비컴테크놀러지 연구소장
<관심분야> 유비쿼터스 네트워킹, 멀티미디어 통신, 무대제어 설비, 의용공학, 영상처리

조 용 환 (Young-hwan Cho) 종신회원

1989년 2월 고려대학교 대학원 (이학박사)
1982년 3월~현재 충북 대학교 전기전자컴퓨터공학부 교수
<관심분야> 유비쿼터스 네트워킹, 멀티미디어 통신, 정보통신 정책, 멀티미디어 콘텐츠