CSMS와 도메인과의 통신을 이용한 인증서 상태 검증 시스템 구현

이종호*, 이용준, 김현철, 오해석
*숭실대학교 컴퓨터공학과
e-mail:jjongayaho@hotmail.com

Certification Status Verification System Implementation for Communication of Domain with CSMS

Chong-Ho Lee*, Yong-Jun Lee*, Hyun-chul Kim*, Hae-Seok Oh*
*Dept of Computing, Soongsil University

요 약

일반적으로 기존의 도메인으로부터 인증서를 검증하는 방법은 CRL(Certificate Revocation List), OCSP(Online Certificate Status Protocol), Freshest CRL, Delta CRL등이 있으나 CRL 검증 방식에 대해서 여러 단점이 부각 되었다. 현재 CRL 검증 방법에 대해서 효율적으로 검증하기 위한 방안이 OCSP, Delta CRL등이 제시하여 서비스를 하고 있는 실정이다. 그러나 이런 검증 서비스 시스템에도 한계성이 드러나게 되었고 그 단점을 보완하기 위한 검증 시스템을 채택하여 기존의 인증서 검증 서비스보다 효율적이고 안정적인 시스템을 구현하기 위해 CSMS(Certificate Status Management Server)를 제시한다.

CSMS는 OCSP와 같이 실시간으로 검증과 빠른 서비스로 USER에게로의 응답을 위한 서비스를 제공함으로써 전자상거래를 통한 트랜젝션에 적합한 시스템을 위한 것이다.

1. 서론

인터넷 보급이 확산되고 웹을 통한 거래가 활발해지면서 금융권이나 기업간의 거래에 인터넷을 이용하는 업무가 증가하고 있다. 과거의 웹 기반 환경에서의 금융거래는 많은 문제점을 안고 있었다. 그러한 문제점 중 대표적인 것이 위조나 변조 등이며 이를 위해 인증서를 사용하게 되었다. 인증서는 기밀성, 인증 , 무결성, 부인 방지를 제공하게 되는데 일반적으로 사용자의 개인키로 전자서명을 하고 CA(Certificate Authority)에서 사용자의 공개키를 이용해 사용자의 전자 서명을 검증하게 된다.

검증은 인증서의 상태정보에 대하여 하게 되는데 보통 인증서가 유효한지, 폐지되었는지를 검증하게 된다. 또한 공개키로 인해 인증서 소유 여부를 확인하며 개인키 유출이나 분실, 자격 박탈, 키 변경 등으로 인증서 폐지를 할 수가 있다. 폐지를 하였을 경우 공개키의 유효성을 확인하기 위해 인증기관에 조회를 하게 된다. 인증서 검증 표준안인 CRL,

Delta-CRL, Freshest CRL, OCSP가 제안되었는데 OCSP는 인증서 폐지에 관한 검증 보다는 유효성 검증을 목적으로 하고 있다.

본 논문은 2장에서 관련 연구를 통해 기존의 시스템의 검증 구성과 문제점을 제시하고 3장에서 CSMS 시스템의 대략적인 설계와 구현 소스 분석, 4장에서는 제안하는 CSMS 시스템모듈을 테스트 한다. 5장에서는 향후 과제에 대해서 다루고 결론을 맺는다.

2. 관련 연구

유효한 인증서는 일정한 기간동안 효력이 있으며 기간이 만료되면 폐지가 된다. 그러나 인증서가 유효한 기간동안 사용자의 개인키의 유출이나 분실, 인증서 내용 변경 등의 여러 가지 사유에 의해서 폐지가 가능하다. 이러한 경우 대표적인 인증서 상태 검증의 표준으로 CRL을 제안하는데 인증서 폐지 리스트로서 디렉토리에 인증서 정보와 폐지 사유 등의 정보가 저장되어 있다. 그러나 실시간성은 보장되지 않으며 필요하지 않은 정보(모든 사용자의 폐지 리스트)까지 제공함으로서 속도의 저하 등이 문제가 되고 있다. 이러한 CRL의 단점을 보완하기 위하여 여러 표준이 제시되었는데 Delta CRL이나 Freshest CRL, OCSP등이 이에 속한다.

2.1 기존의 제안된 시스템 분석

1. CRL(Certificate Revocation List)은 CA(certificate authority)에 의해 작성되는데 인증서를 발급하고 취소할 경우 취소한 증명들의 정보가 저장되어 있다. CRL에는 폐지 정보로서 인증서 폐지 일자, 폐지 사유, 기타 인증서 정보등이 기재되어 있는데 폐지 갱신 기간이 24시간의 갭이 있기 때문에 실질적으로 금융 거래 등에서 요구할 수밖에 없는 도메인에게 실시간으로 정보를 전달할 수 없다는 단점과 CRL이 증가할 경우 검증 속도의 저하를 초래 한다.

2. OCSP(Online Certificate Status Protocol)은 제안하는 CSMS와 거의 비슷한 기능을 수행하는데 인증서 검증을 요청할 시 CA로부터 인증서 상태를 응답 받는다. 좀더 구체적으로 살펴보면 그림 1과 같이 설명할 수 있다.

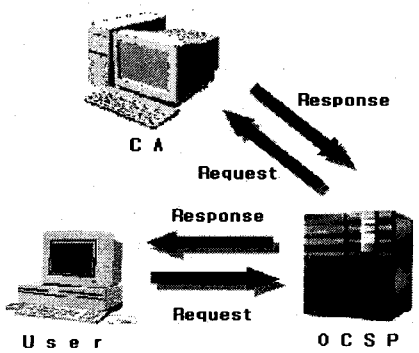

그림 1 OCSP 구성도

사용자는 클라이언트에 트랜잭션을 시작하게 되면 클라이언트는 사용자의 인증서 상태를 확인 하기 위하여 OCSP 서버에게로 인증서 상태 검증 요청을 시작한다. OCSP는 사용자의 정보를 가지고 CA에게로 인증서 상태 검증을 요청한다. CA로부터 응답 메시지가 올 때까지 대기하고 있으며 응답 메시지가 오면 다시 클라이언트에게로 정보를 전송해 준다. OCSP는 기존 CRL등의 현재성 문제나 실시간성 문제를 극복하였으나 속도의 문제, 즉 상태 정보를 제공하기까지 CA를 거쳐야 하고 또한 응답시까지 대기 상태로 있어야 하기 때문에 속도의 문제점이 남아 있다.

3. CSMS 시스템 설계 및 구현

본 논문에서 제안하는 CSMS는 폐지 정보에 관한 검증을 통해 인증서 상태를 실시간으로 도메인에 제공한다. 각각의 도메인(예: 금융서비스)은 인증서 상태 정보를 실시간으로 전송 받음으로서 도메인 자체 폐지리스트에 저장하여 이후 사용자가 인증서 검증을 요청할 경우 도메인 내부에서 효율적인 인증서 상태 정보를 전달할 수 있다. 이는 CRL의 주기적인 갱신으로 인한 실시간 검증이 이루어지지 않는 단점과 OCSP와 같은 CA로의 검증 단계까지 거치지 않게 되어 속도의 효율성을 보장할 수 있게 된다.

CSMS는 기존의 시스템에서의 단점을 보완하기 위해 자체 저장소(Data Base)와 도메인과의 실시간 통신을 중점으로 설계하고 구현한다.

CSMS 시스템의 모듈의 구성을 보면 아래 그림과 설명할 수 있다.

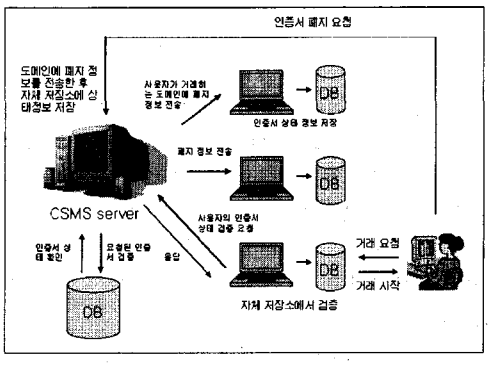

그림 2. CSMS 시스템 모듈 구성

그림 2는 사용자가 인증서 발급을 끝마친 상황에서 도메인과의 거래를 하기 위한 단계이다. 사용자

는 도메인에게 거래를 요청하게 되면 도메인 내부 저장소에서 사용자의 인증서 상태 검증을 하게 된다. 도메인에 사용자의 인증서 정보가 없을 경우 CSMS로 사용자의 인증서 상태 정보 검증을 요청하게 된다. CSMS는 도메인의 요청대로 사용자의 인증서 상태 검증을 하게 되는데 이전에 도메인의 정보와 사용자의 정보를 받게 된다. 요청 접수가 완료되면 CSMS 저장소에 사용자의 인증 상태를 검증한다. CSMS는 디렉토리 저장 방식이 아닌 Data Base화 하였으며 도메인측에서 검증 요청이 있으면 Data Base로 접근하도록 설정이 되어 있다. Data Base에는 인증서 정보의 현재 상태를 저장한다. 그리고 요청하는 정보만을 추출하여 도메인에게로 응답메시지를 전송하며 도메인은 사용자의 인증서 상태 정보를 가지고 거래를 시작하게 된다.

요청을 위해 필요한 정보는 사용자의 인증서 번호(Serial Number)와 도메인명(SignerDN) 등이며 응답을 위한 메시지로서 인증서 번호와 상태 정보(Status)만을 전송하게 된다.

사용자가 폐지 신청을 하였을 경우 CSMS에게 폐지 요청을 하게 된다. 폐지 요청을 받으면 CSMS는 사용자의 상태정보를 저장소에 저장하기 전에 사용자가 등록되어 있는 도메인에게 먼저 폐지 전송을 한다. 도메인으로부터 완료 메시지를 받게 되면 CSMS는 사용자의 폐지 정보를 저장소에 저장하게 된다. 사용자가 폐지 요청시 CSMS는 인증서 정보(예 : 인증서 번호, DN, 유효기간, 폐지사유 등등)를 받게 되고 도메인에 전송시에는 사용자 인증서 번호와 DN, 폐지사유, 상태 정보 등을 전송하게 된다.

3.1 CSMS 시스템 모듈 프로그램 분석

CSMS 시스템 모듈은 크게 두가지의 수행과정이 있다. 도메인과의 요청, 응답을 할 수 있는 과정과 사용자의 폐지 요청 시 정보를 받아 처리하고 도메인에게 폐지 정보를 전송하는 과정인데 처음 검증 요청 대기중의 상태에 있다가 사용자나 도메인의 요청을 받아서 수행할 수 있다.

3.1.1 도메인 요청에 CSMS의 시스템 수행

사용자와 도메인간의 통신을 위한 요청 및 응답 서비스를 구현하기 위하여 두개의 구조체 변수를 선언하였다. request_info 구조체는 도메인의 요청 서비스를 받기 위한 구조체 변수로 선언하였는데 도메인은 사용자의 정보를 자체 저장소에서 검증한 후 해당 정보가 없을 경우 사용자의 인증서 정보인 인증서 번호, DN(Domain Name), 원문과 전자 서명값을 저장하여 검증 요청을 하게 된다. 구조체 변수에 선언한 변수로는 UserSerial, UserDN, LogValue, Signature가 있는데 이 변수에 인증서 정보를 저장한다.

CSMS에서 요청 정보를 받고 도메인의 검증 형식과 마찬가지로 인증서 정보 검증을 시작한다. 인증서 정보를 검증하면서 CSMS Data Base에 저장되어 있는 인증서 정보 테이블에 접근하게 된다. Data Base내에 있는 사용자의 인증서 정보를 검색하고 도메인에게로 전송할 정보들을 추출하게 된다(사용자 정보, 인증서 상태값 등등). DataBase에 있는 값을 추출하기 위해서 제공되는 API인 Row구조체 변수를 호출하면서 사용자 정보를 각각 저장한다.추출한 정보는 응답 메시지 변수에 저장하고 요청 도메인에 정보를 전송한다. 응답 메시지인 response_info 구조체를 사용하는데 여기에는 UserSerial, Status, RevocReason의 변수가 선언되어 있다. UserSerial은 인증서 번호, Status는 인증서 상태값(VALID, REVOC)을 포함하고 RevocReason은 폐지 사유 등을 저장하게 된다. 일반적으로 인증서의 상태 정보를 요청하는 것이기 때문에 유효한 인증서일 경우에는 UserSerial과 Status, 그리고 인증서 정보(유효기간, 서명키, 공개키 등등)를 전송하게 된다. 인증서 정보는 CA프로그램에 구조체로 정의되어 있다. 도메인은 사용자의 정보를 받고 자체 저장소에 업데이트 시킨 후 이후에 사용자가 거래 요청을 할 경우 CSMS나 CA등에 정보 요청을 하지 않아도 검증을 할 수가 있게 된다.

3.1.2 사용자 폐지 요청 시 CSMS의 시스템 수행

사용자가 폐지 요청을 하거나 인증서의 유효기간이 만료되어 폐지가 될 경우 CSMS는 CA로부터 폐지 정보를 받는다. CSMS의 특징중 하나가 실시간 처리이기 때문에 폐지가 되면 바로 처리를 해야 한다. CSMS 시스템은 CA프로그램 내부에 CSMS 서버가 존재하기 때문에 도메인의 인증서 상태 검증이나 폐지 요청 등을 처리할 수가 있다. 사용자의 인증서 폐지가 되면 CRL에 디렉토리로 정보가 저장되는데 이때 CSMS 모듈이 수행하여 따로 생성한 자체 저장소에도 저장하게 된다. 저장소는 Data Base로 구축하였으며 DB에 저장되기 이전에 사용자의 폐지정보를 곧바로 사용자가 거래하는 도메인에 전

송하게 된다. 도메인은 이미 사용자의 정보를 갖고 있기 때문에 인증서 번호와 상태, 사용자 DN, 폐지 사유 등의 정보만으로 처리할 수 있게 된다. 정보를 전송하고 도메인으로부터 응답 메시지를 받는다. CSMS 내부에 폐지정보를 저장한다.

4. CSMS 시스템 실험

CSMS시스템은 Linux에서 도메인의 검증 요청과 폐지등록에 대한 시뮬레이션을 수행 하였다.

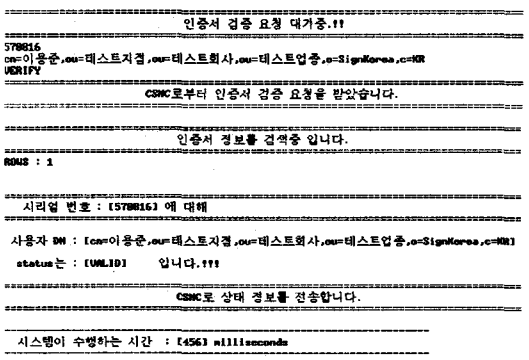

그림 3 사용자 폐지 요청 처리

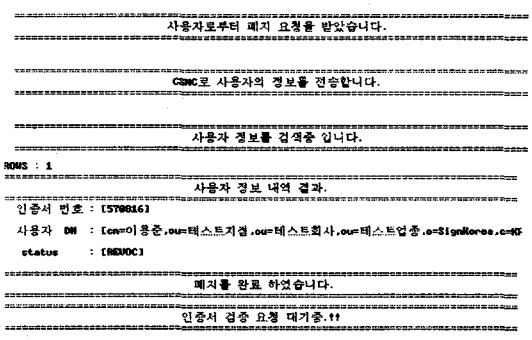

그림 4. 도메인 검증 요청 처리

그림 3은 도메인으로부터 사용자의 인증서에 대한 검증을 요청을 받아 CSMS의 Data Base에서 정보를 추출하게 된다. 추출한 정보를 다시 도메인에게 응답 메시지로 전송을 하게 된다.

그림 4는 사용자로부터 폐지 요청이 있고 Data Base에서의 갱신을 처리하기 전에 먼저 도메인(CSMC)에게 정보를 전송한다. 검증 수행 후 정보를 전송하는 시간과의 속도를 고려하였다.

5. 결론 및 향후 과제

인터넷을 이용한 금융거래가 확산되면서 속도와 실시간성이 보장되는 시스템을 요구한다.

특히 이 두 가지 같은 경우 제대로 수행이 되지 못한다면 불법적인 거래등의 영향이 미칠 수 있다. 본 논문에서는 이러한 실시간성과 속도를 중심으로 구현함으로서 불법적인 행위를 예방할 수 있고 정확한 정보를 전송할 수 있게 한다.

또한 제안하는 시스템인 CSMS는 기존 시스템인 OCSP의 실시간 전송이 되는 점은 더욱 부각 시키고 속도 저하의 단점을 보완함으로서 검증의 융통성 있고 효율적인 인증서 정보를 교환하는데 있다. 금융 거래의 필수적인 조건이라고 할 수 있는 정보 전송의 속도, 실시간의 정보 전송 등은 앞으로도 계속적인 발전을 이루어야 할 것이다.

향후 연구 방안으로는 CSMS와 도메인과의 정보 교환에 있어서 인증서의 몇 가지 정보를 통해 기존의 검증과정을 수행함으로서 검증 속도의 향상을 위한 연구가 필요하다.

참고 문헌

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

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

[3] Patrick McDaniel & Sugih Jamin. "Windowed Certificate Revocation", IEEE Infocom, 2000.

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

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