금융거래 서비스 제공자의 향상된 검증속도를 위한 인증서폐지 전송 시스템

이용준[0], 정재동, 오해석
숭실대학교 대학원 컴퓨터학과
{yjlee[0], jjd}@koscom.co.kr, oh@computing.ssu.ac.kr

Certificate Revocation Notice System for Quick Validation Based Financial Transaction Service Provider

Yong-Jun Lee[0], Jea-Dong Jong, Hea-Suk Oh
Dept. of Computing, Graduated School, Soongsil University

요 약

인증서기반의 인터넷뱅킹과 온라인증권거래에서, 금융거래 서비스 제공자는 많은 사용자의 인증서상태 검증이 요구된다. 금융거래 서비스는 사용자 인증서상태를 실시간의 검증이 보장되어야 한다. 인증서 상태 검증을 위해 기존의 CRL(Certificate Revocation List), Delta CRL, Freshest CRL과 실시간 인증서상태 검증을 위하여 OCSP(Online Certificate Status Protocol)의 표준이 제안된 바 있다. 실시간성과 검증속도는 상호 대비되기 때문에 응용프로그램의 특성을 고려하여 인증서상태 검증방법을 채택한다. 본 논문에서는 CRL의 갱신되기 이전의 폐지에 대하여 실시간으로 전송하는 시스템을 설계한다. 제안하는 인증서폐지 전송서버는 서명자의 검증자 리스트를 관리하여 금융거래 사용자가 CA에 폐지를 요청하면 사용자가 이용하는 금융거래 서비스 제공자들에게 실시간으로 폐지를 고지한다. 본 논문은 CRL 생성이후 갱신까지의 인증서 폐지정보를 검증자에게 전송하여 인증서의 실시간 상태정보를 유지하면서 OCSP보다는 검증속도를 향상시켜 금융거래 환경에서 향상된 효율성을 제공한다.

1. 서론

인터넷뱅킹, 온라인주식거래의 발전에 따라 사용자는 금융거래를 컴퓨터 통신망으로 거래와 계약을 하고 있다. 그러나, 사용자와 거래정보에 대한 불법적인 도청, 위조, 변조, 신분위장 등의 위험이 증가하고 있다. 이러한 보안의 위험을 최소화하기 위해 인증서기반의 온라인 금융거래가 선택이 아닌 의무화가 되고 있다[1].

인증서기반의 전자서명은 개인키의 소유자만이 할 수 있으며, 전자서명의 진위여부를 확인하는 절차를 전자서명검증이라고 한다. 전자서명검증은 개인키의 소유자 확인과 개인키에 합치하는 공개키의 획득하여 전자서명값에 대한 확인절차를 수행한다. 개인키 소유자 확인과정은 인증서유효성 검증을 통해서 이루어지게 되는데 인증서는 개인키에 해당하는 공개키를 가지고 있기 때문이다[4]. 그러나 사용자의 개인키 유출, 분실, 자격박탈, 인증서내용의 변경, 키변경 등의 이유로 인증서 폐지가 가능하다. 따라서 검증자는 수신한 인증서상태가 유효한 것인지를 확인해야 하며 이는 인증기관이 폐지된 인증서에 대한 정보를 공개하거나 검증자가 원하는 인증서의 상태를 인증기관에 직접 조회하여 알 수 있다[9].

온라인금융거래는 상대적으로 높은 보안성이 필수적이므로 인증서상태에 대하여 실시간 확인이 요구된다. 또한, 많은 사용자에 대한 검증이 집중되기 때문에 인증서 상태 검증속도가 향상되어야 한다[8].

인증서상태를 검증하는 일반적인 제안은 CRL(Certificate Revocation List)이 있으며, 보다 개선된 인증서상태의 현재성을 제공하기 위하여 Delta-CRL, Freshest CRL이 제안되었다. 또한 실시간 인증서검증을 위해 OCSP(Onlince Certificate Status Protocol)가 표준으로 제안되었다[7]. 본 논문에서는 인터넷뱅킹, 온라인증권거래 환경에서 실시간의 인증서상태 검증과 검증속도를 개선시킨 인증서폐지 전송 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 인증서상태 검증 표준과 문제점을 분석한다. 3장에서는 온라인금융거래의 실시간 인증서폐지 전송 시스템을 제안한다. 4장에서는 기대효과를 제시한다. 5장에서는 결론을 맺는다.

2. 관련연구

인증서는 유효기간이 있으며, 그 기간동안에 해당 인증서에 대한 유효성을 입증한다. 그러나 사용자의 개인키 유출, 분실, 자격박탈, 인증서내용 변경, 키변경 등 여러 사유에 의해 유효기간 내에 폐지가 가능하다. 이런 경우 인증서의 폐지 사실을 인증기관이 검증자에게 공지해야 한다. 본 장에서는 기존의 인증서상태 검증에 대하여 실시간과 검증속도를 비교하고 문제점을 제시한다[10].

2.1 CRL

인증서폐지 여부를 확인하는 일반적인 방법으로 인증기관 CA(Certificate Authority)가 인증서의 폐지목록을 디렉토리에 게시하는 방법이다. 검증자는 인증서 검증시 CRL을 CA의 디렉토리에서 수신하여 해당 인증서가 목록에 포함되어 있는지 여부를 판단한다. CRL은 CA가 주기적으로 갱신하기 때문에 실시간 인증서상태 검증이 제공되지 않는다. 그러나 검증자가 CRL을 획득하면 갱신이전까지는 로컬에서 CRL을 검색하기 때문에 빠른 검증속도가 보장된다[5].

2.2 Delta-CRL

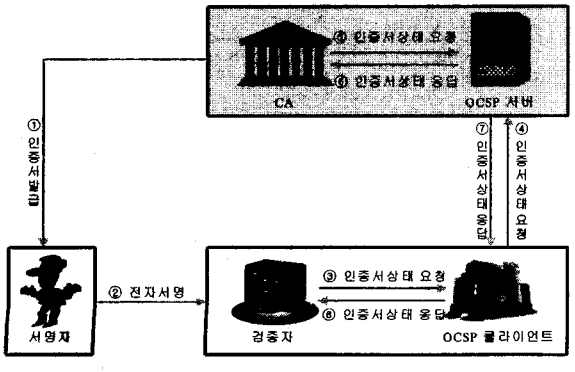
CRL 갱신기간 이전의 폐지목록을 공지하기 위한 방법으로 Delta-CRL이 제안되었다. Delta-CRL은 CRL이 생성된 때부터 다음 생성까지의 폐지된 목록만을 생성한다. 따라서 사용자는 전체 CRL을 받거나 처리할 필요없이 최초 CRL을 받은 후 변경된 Delta-CRL을 추가하게 된다. Delta-CRL은 CRL의 갱신되기 이전의 폐지목록을 제공하기 때문에 현재성에 있어 개선이 되었으나, Delta-CRL 자체의 갱신 시간에 영향을 받기 때문에 실시간 검증은 제공하지 못한다[6].

2.3 Freshest CRL

Freshest CRL은 검증자의 특성을 고려하여 Delta-CRL의 갱신시간을 다르게 제공한다. 높은 현재성을 요구하는 검증자와 상대적으로 낮은 현재성을 가지는 검증자에게 갱신기간이 다른 Delta-CRL을 제공한다. Freshest CRL은 검증자에게 다른 현재성을 제공하지만 실시간의 정보는 제공하지 못한다[2].

2.4 OCSP

OCSP는 실시간 인증서상태 정보를 제공해 준다. (그림 1)에서 기술하듯이, 서명자의 전자서명을 검증시점에 검증자의 OCSP 클라이언트가 OCSP 서버에게 해당 인증서의 상태 정보를 요청한다. 요청을 받은 OCSP 서버는 CA와의 요청을 통해 실시간의 인증서상태 정보를 전송해 준다. OCSP 클라이언트는 OCSP 서버로부터 응답이을 때까지 요청한 인증서 상태의 확인을 대기시킨다[3].



(그림 1) OCSP 구성도

OCSP는 실시간 인증서상태 정보를 제공함으로써 기존의 CRL, Delta-CRL, Freshest CRL의 현재성 문제점을 해결하였다. 그러나 OCSP와 CA와의 인증서 상태 조회 때문에 검증속도의 성능에 저하를 가져온다. 따라서 빠른 검증 속도가 요구되는 금융거래에서는 부담이 되고 있다[8].

3. 제안하는 인증서폐지 전송 서버

본 논문의 인증서폐지 전송 서버는 인증서상태의 실시간성과 신속한 검증속도가 요구되는 인터넷뱅킹, 온라인증권거래의 금융거래환경을 위해 제안한다.

3.1 제안하는 온라인금융거래의 PKI 구성요소

온라인금융거래에서의 PKI(Public Key Infrastructure) 구성요소는 다음과 같이 기술한다.

- 인증기관 (Certificate Authority)

서명자에게 인증서의 발급을 담당한다. 인증서의 상태가 폐지된 인증서 목록으로 CRL을 생성한다. CRL 갱신이전에 대하여 인증서폐지 전송서버에게 폐지정보를 제공한다.

- 인증서폐지 전송서버(Certificate Revocation Notice Server)

CA가 제공한 폐지 정보에 대하여 서명자의 검증자리스트를 관리하여 실시간으로 전송한다.

- 서명자(Signer)

실질적으로 인증서를 발급 받아 전자서명을 수행하는 금융거래 서비스 사용자로 정의한다.

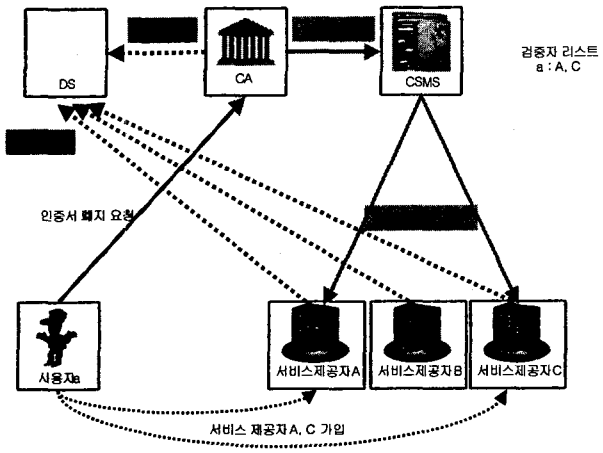
- 검증자(Verifier)

금융 서비스 제공자로써 사용자의 전자서명에 대하여 검증을 수행한다. 이때 기본적인 폐지정보는 CRL로 검증하고, CRL 갱신이전의 폐지정보는 인증서폐지 전송서버를 통해 전송 받는다.

3.2 인증서폐지 전송 서버의 기능

제안하는 시스템은 PKI기반의 표준을 준용하여 CRL과 갱신이전의 폐지정보에 대해서는 인증서폐지 전송서버가 검증자에게 정보를 제공한다. 사용자가 금융거래 제공자에게 가입을 요청하면 서비스 제공자는 일회성으로 CRNS에게 사용자의 검증자 리스트에 등록을 하고 상태조회를 한다. 이 사용자가 CA에 폐지를 요청하면 CA는 폐지 정보를 CRNS에게 전송한다. CRL 갱신이전의 폐지 정보를 전송받은 CRNS는 해당 인증서의 검증자 리스트를 검색하여 전용선으로 금융거래 제공자에게 실시간으로 전송한다. 금융거래 서비스 제공자는 CRNS에게 전송받은 CRL 갱신이전의 폐지리스트를 우선적으로 검색한 후, CRL을 검색한다. CRL과 제안하는 CRNS를 병행하여 인증서상태 조회를 할 경우 실시간 상태조회와 해당 검증자의 로컬에서 폐지리스트를 관리하기 때문에 검증속도가 개선된다.

제안하는 인증서폐지 전송방식은 (그림 2)에 기술하고 있다.



(그림 2) 제안하는 인증서상태 검증

3.3 검증자 리스트 관리

사용자는 온라인 금융서비스를 이용하기 위해 서비스 가입을 요청한다. 서비스 제공자는 해당 사용자의 인증서상태를 CRNS에 조회한다. 이때 서비스 제공자는 해당 사용자의 검증자 리스트에 등록되며 폐지 요청시 실시간으로 폐지 정보를 전송받는다. 검증자 리스트를 관리함으로써 실제 검증을 해야하는 서비스 제공자에게만 한정하여 폐지정보의 전송이 가능하다.

4. 기대효과

CRL을 이용한 인증서폐지 상태 검증은 한번 획득하면 CRL 갱신 전까지 로컬에서 참조하기 때문에 검증속도에 있어 우수하다. 그러나 CRL 갱신이전의 폐지정보에 대하여 전송이 불가능하기 때문에 실시간성이 보장되지 않았다. 본 논문은 실시간성을 보장하기 위하여 CRL 갱신이전의 폐지정보를 인증서폐지 전송서버를 통해 해당인증서의 서비스 제공자에게만 실시간으로 폐지 정보를 전송한다.

본 논문의 인증서폐지 전송방식은 OCSP와 동일한 현재성 확보함과 동시에 인증서 검증속도를 개선시킨 결과를 나타낸다. 인터넷뱅킹, 온라인증권거래의 실시간 상태조회와 검증의 신속성이 요구되는 온라인금융거래 시스템에서 적합한 인증서 상태 검증시스템으로 제안한다.

제안하는 시스템은 <표 1>과 같이 기존의 표준과 비교하여 실시간성, 검증속도, 전송내용에 있어 개선시키는 기대효과를 나타낸다.

<표 1> 제안하는 방식과 표준과의 비교 평가

	CRL	Delta CRL	Freshest CRL	OCSP	CRNS
실시간성	보장안됨	보완	보완	보장	보장
검증속도	고속	고속	고속	저속	고속
전송내용	전체 폐지목록	부분 폐지목록	부분 폐지목록	해당 인증서	해당 인증서

5. 결론

최근 온라인금융거래 시스템이 발전함으로써 다양한 인증서상태를 검증하는 표준이 제안되었다. CRL은 갱신이전에 1회 획득하여 빠른 검증속도가 보장하였으나 실시간 조회는 제공하지 않는다. Delta-CRL, Freshest CRL은 실시간을 보완하였으나 완전한 실시간을 제공하지 않는다. OCSP는 실시간성을 확보하였으나 모든 전자서명 검증시점에 CA에게 인증서상태를 요청함으로써 CA를 포함하여 전체적인 검증속도를 저하시키는 문제점을 가지고 있다. 따라서 기존의 인증서상태 검증 표준은 온라인금융거래의 특성을 고려하지 않았다.

제안하는 인증서상태 검증 방안은 CRL 갱신이전의 폐지정보를 해당 인증서의 서비스 제공자에게만 전송하여 OCSP와 동일한 실시간 상태정보를 보장하고 통신의 부하를 감소시킨다. 또한 기존의 CRL과 병행하여 검증속도를 OCSP보다 개선시킨다.

따라서 인터넷뱅킹, 온라인증권거래의 온라인금융거래 환경에 적합한 결과를 제공한다. 향구 연구 방안으로는 사용자의 검증자 리스트에게 전송 과정중 장애가 발생하여 검증자에게 폐지 정보가 반영되지 않는 문제점에 대하여 연구가 진행되어야 한다. 이와함께 인증기관 상호연동을 반영하여, 각 인증기관과의 인증서상태 검증으로 확장하는 연구의 필요성이 요구된다.

참고문헌

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

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

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

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

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

[6] David A. Cooper "A More Efficient Use of Delta-CRLs" IEEE Symposium on Security and Privacy, 2000.

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

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

[9] Albert Levi & M. Ufuk Caglayan. "An Efficient, Dynamic and Trust Preserving Public Key Infrastructure", IEEE, 2000.

[10] Andre Arnes, Svein J. Knapskog. "Selecting Revocation Solutions for PKI", NORSEC 2000, Sep 25.