위임등록 프로토콜을 이용한 대리서명 기법

이용준*, 박세준*, 오해석*
*숭실대학교 대학원 컴퓨터학과
mail:yjlee@koscom.co.kr

Proxy Signature Scheme based on Proxy-Register Protocol

Yong-Jun Lee*, Se-Joon* Park, Hea-Suk Oh*
*Dept. of Computing, Graduate School, Soongsil University

요 약

실생활에서 권한의 위임을 통한 대리 서명 기법들이 최근 많이 연구되고 있다. 대리서명은 원서명자가 그의 서명 권한을 대리서명자에게 위임하여 대리서명자가 원서명자를 대신해서 서명을 생성하는 것을 말한다. 이러한 대리서명을 온라인 상에서 사용하기 위해서는 위임자의 권한 위임장이 위 변조와 오남용의 위험으로부터 안전하게 보호되어야 한다. 또한 대리서명의 수행을 위해서는 원서명자의 위임에 대한 정보가 명확해야 한다. 대리서명의 기본적인 방법은 원서명자가 위임 정보에 대한 서명을 생성하고 이를 위임자에게 전달하여 위임자가 위임키로서 사용하게 하는 것이다. 위임키쌍이 위임 정보에 기반한 원서명자의 서명으로부터 생성되기 때문에 어떠한 검증절차에서도 원서명자의 동의를 확인할 수 있다. 본 논문에서는 원서명자와 대리서명자가 기존의 인증서를 발급 받은 환경에서 원서명자가 대리서명자에 대하여 검증자에게 위임정보를 등록하는 프로토콜을 제안한다. 위임내용에 대해 원서명자가 전자서명을 하고 검증자는 이에 해당하는 내용을 검증한 후 위임서명자에 대한 권한, 기간 등의 제약사항을 설정한다. 이후 위임서명자는 위임내용에 대해 고지를 받고 허가된 범위 내에서 위임 서명을 한다. 마지막으로 본 논문에서는 기존의 방법들과 비교 분석하여 제안하는 위임 등록 프로토콜에 대한 효율성을 제시한다.

1. 서론

기업에서는 많은 일로 인해 필요한 서류에 서명을 하지 못하거나 책임자가 부재중일 경우 온라인 상의 문제로 인해 서명을 할 수 없는 상황이 빈번하게 일어나곤 한다. 조직에게 발급된 인증서는 그 조직에 속한 직원들이 사용하고 있는데 이 경우 권한을 위임하기 위해서는 인증서와 비밀키를 직접 직원에게 위임하여 전자 거래에 서명하도록 하는 방법을 사용하고 있다[1]. 직원들에게 인증서가 가지고 있는 모든 권한을 위임하는 것은 보안상 많은 문제점이 있다. 가장 큰 문제점은 조직의 인증서를 직원에게 대여함으로써 발생할 수 있는 인증서와 비밀키의 오남용을 막기가 힘들다는 것이다. 또한 대리 서명 후 직원의 부인 방지를 막을 수가 없고 위임을 받은 직원이 제삼자에게 원서명자의 동의 없이 인증서와 비밀키를 알려 줌으로서 대리 서명 능력을 가지게 할 수 있다. 그리고 비밀키 자체의 노출이 늘어남에 따라 안전성에 심각한 문제를 야기할 수 있다[2][3].

이러한 문제점을 극복하기 위해 공개키 인증서를 가진 조직이 각 구성원이 위임 받을 수 있는 권한에 대해 규정하고 이를 자신의 공개키로 서명함으로써 인증서를 발급하여 대리 서명을 사용할 수 있다. 대리인은 위임을 받음과 동시에 위임자가 규정한 범위 내에서 제 3자에게 위임자로 인증 받을 수 있다[4]. 특히, 위임자는 대리인의 사내의 지위나 역할을 고려하여 권한을 제한 할 수 있기 때문에 앞에서 언급한 문제들을 해결할 수 있다. 또한 수직적인 권한의 위임뿐만 아니라 수평적인 권한의 위임이 가능한 위임등록 프로토콜을 설계하고자 한다.

본 논문에서는 원서명자와 대리서명자가 기존의 인증서를 발급 받은 환경에서 원서명자가 대리서명자에 대하여 검증자에게 위임정보를 등록하는 프로토콜을 제안한다. 위임내용에 대해 원서명자가 전자서명을 하고 검증자는 이에 해당하는 내용을 검증한 후 대리서명자에 대한 권한, 기간, 제약사항 등을 설정한다. 이후 대리서명자는 위임내용에 대해 고지를

받고 허가된 권한과 범위 내에서 위임 서명을 한다.

2. 관련연구

2.1 Mambo, Usuda, Okamoto's Scheme

최초로 대리서명에 대한 개념을 소개하였고 3가지 타입의 위임에 기반하여 대리서명 기술을 구분하였다[1]. 대리 서명 방식에서 원서명자의 서명 권한을 위임하는 형태에 따라서 완전 위임, 부분 위임으로 분류하였고 원서명자에 의해 만들어진 보증서를 사용하여 대리 서명을 실현하는 보증 위임을 제안하였다[5][6].

- 완전 위임 : 원서명자가 자신의 개인키를 위임자에게 주는 것이다. 그러므로 대리 서명자에 의한 서명과 원서명자에 의한 서명은 구분되지 않는다.
- 부분 위임 : 원서명자가 대리서명 비밀키를 자신의 비밀키를 이용하여 생성한다. 부분 위임은 대리서명의 암호화에 따라 대리인 비보호형 대리서명 방식 기법과 대리인 보호형 대리 서명방식 기법으로 구분되며 위임 서명키는 원서명자와 위임자 모두에 의해서 생성된다.
- 보증 위임 : 원서명자가 자신과 위임자의 정보와 관련된 권한에 대해서 서명하고 검증자는 이 정보에 기반하여 권한을 검증한다. 즉, 원서명자가 대리서명자에게 보증서를 발행함으로서 대리 서명을 구현하는 기법이다. 이 기법은 보증서 기반 대리서명 방식 기법과 소지자 기반 대리 서명 방식 기법으로 구분된다[7].

이들이 제안한 대리서명 기술의 단점은 다음과 같다.

- 위임되는 권한에 대한 제약이 없으므로 대리인에 의한 오남용이 가능하다.
- 원서명자의 동의 없이 제 3자에게 전달하여 대리서명이 가능하고 제 3자가 명백한 위임자인지에 대한 결정을 할 수 없다.

2.2 Petersen and Horster's Scheme

Petersen과 Horster는 자체 보증키를 생성하여 대리 서명을 하는 기법을 제안하였다. 또한 이들은 위임키쌍을 생성하기 위해 기본키 생성 프로토콜과 보안키 생성 프로토콜을 제안하였다. 기본키 생성 프로토콜은 대리인 비보호형 대리 서명 기법으로서 원서명자가 위임키쌍을 생성하여 대리서명자에게 전달하는 것이며 보안키 생성 프로토콜은 대리인 보호형 대리 서명 기법으로서 원서명자와 대리서명자가 함께 위임키쌍을 생성하지만 대리서명자의 개인키를 원서명자가 알 수 없도록 하는 방법이다[8][9]. 이들이 제안한 대리서명 기술의 단점은 다음과 같다.

- 대리서명시 위임자에 대한 어떠한 정보도 포함되어 있지 않기 때문에 서명을 수행한 후 추후에 부인할 수 있다.
- 위임자가 위임키를 CA에 자신의 키쌍처럼 등록하여 자신의 목적을 위하여 사용할 수 있으며 추후 부인할 수 있다.
- 원서명자는 위임자의 동의없이 위임자의 ID를 가지고 위임키쌍을 생성하여 CA에 등록하고 자신의 키처럼 사용할 수 있으며 추후 부인할 수 있다.

2.3 Kim, Park and Won's Scheme

위에서 소개한 방법에서는 원서명자의 정보에 대리서명자의 신원이나 권한과 같은 어떠한 정보도 포함되어 있지 않기 때문에 권한의 오남용과 같은 문제들이 발생할 수 있다. 이와 같은 문제들을 해결하기 위해 Kim, Park and Won은 Schnorr 서명 기법을 이용하고 대리인과 위임되는 권한에 대한 정보를 대리서명에 포함시켜 위임된 권한의 오남용, 제 3자에게로의 서명 권한 전달을 방지하는 방법을 제안하였다[6]. 이 방법은 위임 개인키가 대리인에 의해서만 표현되어질 수 있기 때문에 대리인 보호형 대리서명 기법이다. 이들이 제안한 대리서명 기술의 단점은 대리서명 내에 원서명자와 위임자의 역할이 동일하다는 것이다. 그러므로 이들의 권한이 아주 명백하게 표시되어 있어야 한다. 그렇지 않은 경우에는 이들의 역할이 바뀔 수 있다. 그러므로 검증자는 대리서명이 권한에 표시된 내용과 일치하는지에 대해서 체크해야 한다.

2.4 Delos, Quisquater's Scheme

Oliver Delos와 Jean-Jacques Quisquater는 서명하는 횟수를 제한할 수 있는 ID 기반 서명 기법과 제한된 서명 횟수의 일부분을 대리인이 수행할 수 있는 방법을 제안하였다. ID 기반 인증 모델에서는 각 사용자의 ID에 대응하는 개인키를 생성해주는 신뢰기관의 구축이 필요하기 때문에 ID 기반 서명 기법은 시스템 파라미터와 각 사용자의 개인키를 생성하는 초기화 과정과 이를 이용하여 서명을 생성하고 검증하는 과정으로 구성되어 있다[1][10].
이들이 제안한 기법의 단점은 다음과 같다.

- ID 기반 인증 모델에서의 서명 기법임에도 불구하고 유효성 확인을 위해 원서명자나 신뢰기관이 제공하는 인증서를 사용해야 한다.
- 시스템이 각 사용자의 개인키를 알고 있다는 것과 서명자의 공개키에 대한 신뢰기관의 인증서를 받아야 한다.
- 단순한 횟수의 제한을 제외하고 권한의 사용에 대한 아무런 제약이 없다.

3. 제안하는 위임등록 프로토콜

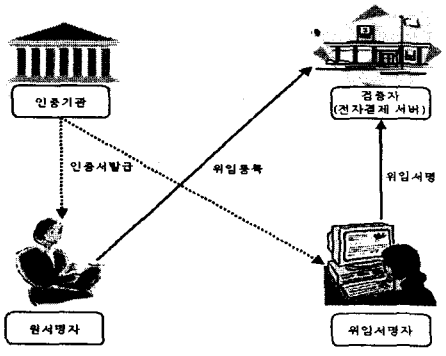
공개키기반 구조의 발전과 함께 인터넷뱅킹, 증권거래시스템, 전자결제의 온라인서비스에 인증기술이 적용되어 전자서명을 이용한 로그인과 거래가 보편화되었

다. 그러나 원서명자의 부재와 권한위임에 대해 많은 연구가 진행되었으나 현실적인 공개키기반 구조를 반영하지 못하고 있다. 제안하는 위임 등록 프로토콜은 PKI 기반의 구성요소를 준용하며 원서명자와 대리서명자가 기존의 인증서를 발급 받은 환경에서 원서명자가 대리서명자에 대하여 검증자에게 위임정보를 등록하는 프로토콜을 제안한다. 위임내용에 대해 원서명자가 전자서명을 하고 검증자는 이에 해당하는 내용을 검증한 후 대리서명자에 대한 권한, 기간, 제약사항을 설정한다. 이후 대리서명자는 위임내용에 대해 고지를 받고 허가된 범위 내에서 위임 서명을 한다. 본 장에서는 제안하는 위임 등록 프로토콜에 대한 효용성을 제시한다.

3.1 구성요소

본 논문에서 제안하는 위임등록 프로토콜을 이용한 대리서명 방식의 구성요소는 [그림 1]과 같다.

- 인증기관 (CA : Certificate Authority)
  원서명자와 대리서명자에게 인증서의 발급을 담당한다. 또한 인증서와 관련된 정보를 게시하고 상태정보를 제공한다.
- 원서명자(Original Signer)
  인증서를 발급 받아 온라인서비스를 이용하는 사용자로써 대리서명자에게 위임범위, 시간, 제약사항을 정의하여 위임할 수 있다.
- 대리서명자(Proxy Signer)
  원서명자의 권한 중 전부 또는 일부를 위임 받아 본인의 인증서를 통해 온라인서비스에 원서명자를 대신하여 전자서명을 수행한다.
- 검증자(Verifier)
  검증자는 온라인서비스의 서버로써, 원서명자에게 위임 등록을 제공하고 원서명자가 정의한 권한을 대리서명자가 위임하여 수행할 수 있게 처리한다.

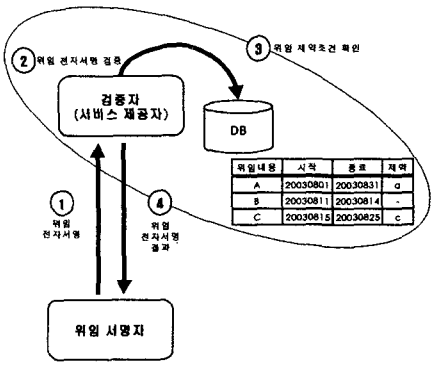


[그림 1] 시스템 구성 요소

4.2 위임 등록 프로토콜의 시나리오

[그림 2]는 제안하는 위임 등록 프로토콜의 시나리오를 나타낸 것이다. 본 논문의 검증자는 온라인서비스를 제공하는 서버이며, 원서명자와 대리서명자는 온라인서비스의 사용자를 의미한다. 원서명자는 대리서명자에게 안전한 방법으로 위임권한, 기간, 제약사항을 위임등록프로토콜을 사용하여 정의할 수 있다. 위임 등록 프로토콜은 다음과 같이 구성되어 있다.

(1) 원서명자는 검증자인 서비스제공자의 서버에 접속하여 대리서명자에 대하여 위임 등록을 요청한다. 이때 원서명자가 등록하는 내용은 위임내용, 위임시작시점, 위임종료시점, 위임에 대한 제약사항에 대하여 상세하게 명시한 후 원서명자의 개인키로 서명하여 전송한다.
(2) 검증자는 원서명자로부터 전송받은 위임등록에 대한 검증을 수행한다. 원서명자의 인증서의 유효성과 위임내용의 전자서명의 검증 후 결과를 반영한다.
(3) 위임정보의 전자서명 검증이 정상적이면 위임내용, 위임시작시점, 위임종료시점, 제약사항에 대하여 데이터베이스에 등록하여 대리서명자의 권한을 설정한다.
(4) 검증자는 원서명자의 위임 등록 요청에 대하여 검증과 등록 결과를 응답한다.
(5) 대리서명자가 검증자의 서비스를 제공받기 위해 로그인을 한 경우 원서명자가 대리서명자에게 위임한 내용에 대해 고지를 한다.
(6) 대리서명자는 검증자의 서비스를 통해 제공받은 원서명자의 위임내용에 대해 인지하였다는 것을 확인한다.



[그림 2] 위임 전자서명 및 검증 시나리오

[그림 3]은 제안하는 위임 전자서명의 시나리오를 나타낸 것이다. 대리서명자는 원서명자로 위임받은 권한을 인지한 후, 원서명자를 대신하여 전자서명을 수행한다. 이때 검증자는 위임 등록된 위임내용, 위임기간, 제약사항을 확인함으로써 전부 또는 제한적인 위임을 가능하게 한다. 대리서명자의 전자서명과 검증은 다음의 구성과 같다.

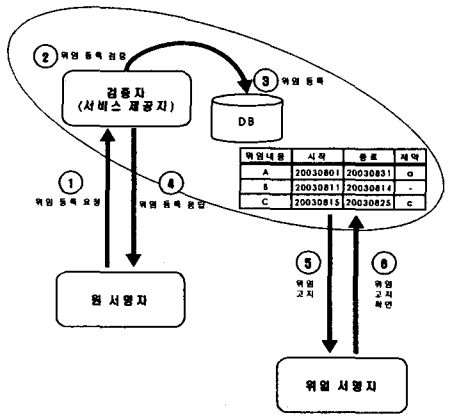
(1) 대리서명자는 원서명자를 대신하여 대리서명자의

개인키로 전자서명을 수행한다. 이러한 서비스는 증권거래시스템, 전자결제와 같이 전부 또는 부분적인 권한을 위임할 수 있는 서비스에 적합하다. 특히 다수의 그룹이 전자서명을 수행할 경우를 고려한다.

(2) 검증자는 대리서명자의 전자서명을 검증한다. 우선적으로 대리서명자의 인증서를 검증한 후 위임 전자서명에 대해 검증을 수행한다.

(3) 검증자인 서비스제공자는 위임서명의 검증이 정상적이라도 이미 위임등록 프로토콜을 통해 데이터베이스에 등록된 위임내용, 위임기간, 제약사항에 대해 확인을 한다. 따라서 대리서명자는 원서명자가 정의한 권한 내에서 전자서명을 수행할 수 있다.

(4) 위임서명 검증이 정상적이고 위임권한이 확인되면 검증자는 해당하는 결과를 대리서명자에게 응답한다.



[그림 3] 위임 등록 프로토콜의 시나리오

<표 1>은 제안하는 방식과 기존 방법을 비교 평가하였다.

<표 1> 제안하는 방식과 기존 방법과의 비교 평가

	MUO	PH	KPW	DQ	SNPS	PRP
검증성	○	○	○	○	○	○
위조불가능성	○	×	○	×	○	○
신원확인성	○	○	○	○	○	○
부인 불가능성	○	×	○	○	○	○
오용방지	×	×	○	×	○	○
권한의 제약	×	×	△	×	△	○
양도불가	×	△	○	△	○	○
적합성 확인	×	×	×	×	○	○
Strong	×	×	○	×	○	○
Non-designate	×	×	×	×	○	○
위임인증서 및 키 생성여부	필요	필요	필요	필요	필요	필요 없음

대리서명의 보안 요구사항들을 기준으로 MUO(Mambo, Usuda, Okamoto), PH(Petersen, Horster), KPW(Kim, Park, Won), DQ(Delos, Quisquater)의 기법들과 PRP(ProxyRegister Protocol)를 비교 분석하였고 SNPS(Strong Nondesignate Proxy Signature) 대리서명 기술과도 비교 분석하였다.

4. 결론

대리서명은 사용자가 자신의 서명 권한을 위임할 필요가 있을 경우 유용하게 사용될 수 있는 기술이다. 그러나 인터넷과 같은 분산환경에서 원서명자나 위임자를 신뢰하기는 매우 어려운 문제이다.

본 논문에서는 기존 대리 서명의 보안 요구사항을 만족하는 위임 등록 프로토콜을 설계하고 구현하였다. 제안한 기법은 대리서명의 보안 요구사항을 모두 만족하며 기존의 방법보다 강력하다. 또한 기존의 인증서를 사용하기 때문에 위임을 위한 인증서를 따로 생성할 필요가 없으며 이에 따른 위임키쌍을 생성할 필요가 없으므로 처리 속도가 빠르다. 제안한 방법은 기존 방법의 문제점을 해결하였고 제안된 위임 등록 프로토콜의 적용은 실제 환경의 보안 요구사항을 분석하여 이루어지며 정의된 요구사항에 맞는 구조를 제공해줄 수 있다.

제안된 기법을 사용하여 전자 상거래에서의 대리서명 기법은 보다 안전하게 제공할 수 있고 이러한 기술은 전자 입찰과 인터넷 금융 서비스 같은 여러 가지 응용 환경에 적용될 수 있다.

참고문헌

[1] B. Lee, H. Kim, K. Kim, "Strong Proxy Signature and its Applications" Proc. of SCIS 2001.

[2] H.M. Sun, "Design of time-stamped proxy signature with traceable receivers," Proc. of IEE Computers and Digital Techniques, Vol. 147, No. 6, 2000.

[3] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign message," IEICE Trans. Fundamentals, Vol. E79-A, No. 9, 1996

[4] M. Bellare and S. Miner, "A forward-Secure digital signature scheme," Crypto'99, 1999.

[5] Housley, R., W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Internet Draft, January 2002.

[6] M.Abe, T. Okamoto, "Provably secure partially blind suignatures", In Advances in Cyyptologt Crypto'2000.

[7] M.Mambo, K.Usuda, and E.Okamoto, "Proxy signatures: Delegation of the power to sign messages" In IEICE Trans. Fundamentals, Vol.E79-A, No.9, Sep 1996.

[8] H.Petersen and P.Horster,"Self-certified keys Concepts and Applications", In Proc. Communications and Multimedia Security'97, 1997

[9] D.Chaum, "Blind signatures for untraceable payments", Advances in Cryptology: Crypto'82, Prenum Publishing Corporation, 1982.

[10] P.Horster, M.Michels, H.Petersen "Hidden signature schemes based on the discrete logarithm problem and related concepts", Proc. of Communications and Multimedia Security'95, Chapman&Hall, 1995.