情報保護學會論文誌
第14券 第4號, 2004. 8

증권거래시스템에 적합한 위임등록프로토콜의 설계*

이 용 준[a)†‡], 박 세 준[a)], 오 해 석[b)]
숭실대학교[a)], 경원대학교,[b)]

Design of Proxy Registration Protocols for Stock Trading System*

Yong-Joon Lee[a)†‡], Se-Joon Park[a)], Hae-Seok Oh[b)]
Soongsil University[a)], Kyungwon University[b)]

요 약

최근에 권한의 위임을 통한 위임 서명 기법들이 많이 연구되고 있다. 위임서명 기법은 원서명자가 서명 권한을 위임서명자에게 위임하여 위임서명자가 원서명자를 대신해서 서명을 생성하는 것을 말한다. 이러한 위임서명 기법은 위임자의 권한 위임장이 위 변조와 오남용의 위험으로부터 안전하게 보호되어야 한다. 또한 위임서명의 수행을 위해서 원서명자의 위임에 대한 정보가 명확해야 한다. 이러한 위임서명 기법을 사용하기 위해서는 몇 가지의 보안 사항들이 요구된다. 본 논문에서는 원서명자와 위임서명자가 기존의 인증서를 발급받은 환경에서 원서명자가 위임서명자에 대해 검증자를 통하여 위임정보를 등록하는 프로토콜을 제안하고자 한다. 위임내용에 대해 원서명자가 전자서명을 하고 검증자는 이에 대한 내용을 검증한 후 위임서명에 대한 권한, 기간 등의 제약사항을 설정한 후 위임서명자는 위임내용에 대해 고지를 받고 허가된 범위 내에서 위임서명을 하게 된다. 마지막으로 기존의 방법들과의 비교 분석을 통하여 제안하는 위임 등록 프로토콜에 대한 효율성을 제시하고자 한다.

ABSTRACT

Proxy signature scheme based on delegation of warrant is studied in these days. Proxy signature is a signature scheme that the original signer delegates his signing warrant to the proxy signer, and the proxy signer creates a signature on behalf of the original signer. For using this scheme, the security for protecting from the forgeability or misuse is necessary. There are several security requirements for using the proxy signature schemes. In this paper we suggest the proxy-register protocol scheme that original signer registers to the verifier about the proxy related information. In our scheme, verifier verifies the signature that original signer creates about the proxy information and sets the warrant of proxy signer, validity period for proxy signature and some limitation. Finally, we will show the advantages of our suggestion by comparing with the previous proxy signature schemes.

Keywords : *PKI, Proxy Signature, Delegation*

Ⅰ. 서 론

최근 PKI(Public Key Infrastructure)기술의 발전과 국가정책으로 인하여 증권거래시스템에 공인인증이 의무적으로 적용되어 있다. 따라서 증권거래의 사용자는 전자서명을 이용해야만 로그인과 거래가 가능하다[1]. 그러나 현재 PKI가 적용된 증권거래시

접수일 : 2004년 2월 17일 ; 채택일 : 2004년 7월 9일
* 본 논문은 숭실대학교 멀티미디어연구실의 산학연 연구결과로 수행되었음.
† 주저자 ‡ 교신저자 : yjlee@koscom.co.kr

스템으로 위임서명을 하고자 하는 경우에는 개인키와 인증서를 위임자에게 전달하여 사용하고 있다. 증권거래서비스에 대하여 위임자에게 모든 권한을 위임하는 것은 보안상 많은 문제점이 있다. 가장 큰 문제점은 위임자가 원서명자의 서명키로 해당 증권계좌에 대한 권한의 오용을 방지하기 어렵다. 또한 전자서명을 통한 증권거래에 대하여 원서명자와 위임서명자간의 부인방지가 어렵다. 더하여 최근 금융서비스에 대한 상호연동으로 해당 증권거래 뿐아니라 인터넷뱅킹, 쇼핑몰 등에 오용될 위험이 있다. 위임자가 제3자에게 원서명자의 동의 없이 인증서와 비밀키를 알려 줌으로서 위임서명 능력을 가지게 할 수 있으며 무엇보다 개인키 자체의 노출이 늘어남에 따라 안전성에 심각한 문제가 발생한다[2].

위임서명의 문제를 해결하기 위해 위임키생성 방법을 이용하거나 위임권한이 설정된 보증서를 이용하는 방법들이 제안되었다. 그러나 기존의 제안된 위임서명 기법은 현재의 공인인증체계을 변경해야 하기 때문에 적용하는데 어려움이 존재한다.

본 논문에서는 원서명자와 위임서명자가 기존의 인증서를 발급된 환경에서 원서명자가 위임서명자에 대하여 검증자 기반의 위임정보를 등록하는 프로토콜을 제안한다. 위임내용에 대하여 원서명자의 전자서명과 검증자는 이에 해당하는 내용을 검증한 후 위임서명자에 대한 권한, 기간, 제약사항 등을 설정한다. 이후 위임서명자는 위임내용에 대한 고지를 받고 허가된 권한과 범위 내에서 위임서명을 하게 된다.

본 논문은 기존의 공인인증체계를 유지하면서 검증자에게 위임등록과정을 적용하여 증권거래시스템에 적합한 위임서명을 제공한다.

II. 기존연구

2.1 Mambo, Usuda, Okamoto's Scheme

최초로 위임서명에 대한 개념을 소개하였고 3가지의 위임서명 방식을 구분하였다. 위임서명 방식에서 원서명자의 권한을 위임하는 형태에 따라서 완전위임, 부분위임으로 분류하였고 원서명자에 의해 만들어진 보증서를 사용하여 위임서명을 가능하도록 보증위임을 제안하였다[3][8].

2.1.1 완전위임

원서명자가 자신의 개인키를 위임서명자에게 전달하는 방식으로 위임서명자에 의한 서명과 원서명자에 의한 서명은 구분되지 않는다.

2.1.2 부분위임

원서명자가 위임서명키를 자신의 개인키를 이용하여 생성한다. 부분위임은 위임서명의 암호여부에 따라서 대리인 비보호형 위임서명과 대리인 보호형 위임서명으로 구분된다.

• 대리인 비보호형 위임서명

위임서명자는 원서명자를 대신하여 서명할 수 있지만 위임서명자 이외의 원서명자는 위임서명자를 가장하여 위임서명할 수 있다. 그러나 위임서명자로 지정 받지 않은 제3자는 위임서명을 생성할 수 없다.

• 대리인 보호형 위임서명

위임서명자만이 위임서명이 가능하다. 그러므로 원서명자 또한 정당한 위임서명자를 가장하여 위임서명할 수 없다.

2.1.3 보증위임

원서명자가 자신과 위임자의 정보와 관련된 권한에 대해서 서명하고 검증자는 이 정보를 이용하여 권한을 확인한다. 즉, 원서명자가 위임서명자에게 보증서를 발행함으로서 위임서명을 구현하는 방식이다. 보증서 기반 위임서명과 소지자 기반 위임서명으로 구분된다.

• 보증서 기반 위임서명

지정한 사람을 위임서명자로 선언하는 정보에 원서명자가 전자서명을 통하여 서명한 후 그 서명된 보증서를 이용하여 위임서명을 실행한다.

• 소지자 기반 위임서명

지정한 서명자를 위한 비밀키와 공개키를 생성하고 생성된 공개키에 대하여 원서명자가 보증서를 만들어 지정된 위임서명자에게 전달한다. 이때 생성된 비밀키는 위임서명자에게 비밀리에 전달된다. 이들이 제안한 위임서명 기술의 단점은 다음과 같다.

- 위임되는 권한에 대한 제약이 없으므로 대리인에 의한 오남용이 가능하다.
- 원서명자의 동의 없이 제3자에게 전달하여 위임서명이 가능하고 제3자가 명백한 대리인인지에

대한 결정을 할 수 없다.

2.2 Petersen and Horster's Scheme

Petersen과 Horster는 원서명자가 위임키를 생성하여 위임서명을 하는 방식을 제안하였다. 또한 이들은 위임키쌍을 생성하기 위해 기본키 생성 프로토콜과 보안키 생성 프로토콜을 제안하였다. 기본키 생성 프로토콜은 대리인 비보호형 위임서명으로써 원서명자가 위임키쌍을 생성하여 위임서명자에게 전달하는 것이며 보안키 생성 프로토콜은 대리인 보호형 위임 서명으로서 원서명자와 위임서명자가 함께 위임키를 생성하지만 위임서명자의 개인키를 원서명자가 알 수 없도록 하는 방법이다. 이들이 제안한 위임서명 기술의 단점은 다음과 같다[4].

- 위임되는 권한에 대한 제약이 없으므로 대리인에 의한 오남용이 가능하다.
- 위임서명시 위임자에 대한 정보가 포함되어 있지 않기 때문에 서명을 수행한 후 추후에 부인할 수 있다.

2.3 Kim, Park and Won's Scheme

기존의 방식은 원서명자의 정보에 위임서명자의 신원이나 권한과 같은 정보가 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 위임서명에 포함시켜 위임된 권한의 오남용, 제3자에게로의 서명 권한 전달을 방지하는 방법을 제안하였다. 이 방법은 위임 개인키가 대리인에 의해서만 표현되어질 수 있기 때문에 대리인 보호형 위임서명이다. 이들이 제안한 위임서명 기술의 단점은 위임서명 내에 원서명자와 위임자의 역할이 동일하다는 것이다. 그러므로 이들의 권한이 아주 명백하게 표시되어 있어야 한다. 그렇지 않은 경우에는 이들의 역할이 바뀔 수 있다. 그러므로 검증자는 위임서명이 권한에 표시된 내용과 일치하는지에 대해서 확인해야 한다[5].

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 생성해 주는 신뢰기관의 구축이 필요하기 때문에 ID 기반 서명 기법은 시스템 파라미터와 각 사용자의 개인키를 생성하는 초기화 과정과 이를 이용하여 서명을 생성하고 검증하는 과정으로 구성되어 있다. 이들이 제안한 기법의 단점은 다음과 같다[6].

- 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 상세한 제약이 없다.

Ⅲ. 본 론

3.1 위임서명의 보안 요구 사항

위임서명의 보안 요구사항은 다음과 같이 정의된다[7].

- 검증성

검증자는 위임서명으로부터 위임자의 위임에 대한 동의를 확인할 수 있어야 하며 선택적으로 위임서명자의 신원을 확인할 수 있어야 한다.

- 신원확인성

위임서명으로부터 위임서명자의 신원을 확인할 수 있어야 한다.

- 위조 불가능성

위임자에 의해 지명된 대리인만이 유효한 서명을 생성할 수 있어야 한다. 또한 위임자나 제3자는 대리인을 가장하여 유효한 서명을 생성할 수 없어야 한다.

- 부인 불가능성

위임서명자는 유효한 위임서명의 생성 후 서명한 사실에 대한 부인 거부를 할 수 없어야 한다.

• 오용 방지

위임자가 위임한 권한 범위 내에서 위임서명이 되어야 한다. 즉 위임서명자는 원서명자로부터 위임받은 권한 이외의 목적으로 위임키를 사용할 수 없어야 한다. 즉, 위임서명에 대리인의 권한의 한계를 규정하여 위임서명의 사용에 있어서 명백한 제한을 가하는 영역의 필요성을 제시한다.

• 권한의 제약

위임된 권한 내에서만 위임키를 사용할 수 있어야 한다.

• 양도 불가

위임자가 생성한 위임키는 양도할 수 없어야 한다.

3.2 위임서명 기술의 분류

본 절에서는 위임서명 기술의 분류에 대해서 알아본다. 우선 부인방지 기법에 따라서 strong 위임서명과 weak 위임서명으로 분류할 수 있다[8].

• Strong 위임서명

위임자와 원서명자의 서명을 표현하는 기법으로서 위임자가 위임서명을 수행한 후 부인할 수 없다. 위임키쌍은 다른 목적으로 사용될 수 없다.

• Weak 위임서명

원서명자의 서명만을 표현하는 기법으로서 부인방지를 제공하지 못한다. 이러한 단점을 가지고 있는 이유로 분산환경에서는 사용할 수 없다.

원서명자는 특정한 위임자를 명시하지 않고 위임서명의 조건만을 명시하여 일정한 위임서명자 집합을 만들 수 있다. 이러한 위임자에 대한 임명방법에 따라서 designated 위임서명과 non-designated 위임서명으로 구분한다.

• designated 위임서명

원서명자가 위임자를 명시하는 기법으로서 위임자의 신원에 대한 정보가 위임키를 포함하는 보증서에 포함되어 있다.

• non-designated 위임서명

원서명자가 위임자를 명시하지 않는 기법으로서 원서명자의 서명 파라미터를 알고 있으면 누구든지 위임키를 생성할 수 있다. 생성 후 보증서의 정보와 일치하면 원서명자를 대신하여 위임서명을 할 수 있다.

마지막으로 원서명자가 스스로 위임키쌍을 생성하여 위임서명에 사용하는 기법으로서 이 경우 원서명자와 위임서명자가 동일인이 된다.

• 자체 위임서명 기법

원서명자가 스스로 권한에 대한 정보를 포함한 위임키쌍을 생성하여 자신의 새로운 키쌍으로 사용한다. 이 기법은 키의 갱신 목적으로도 사용될 수 있다.

3.3 제안하는 위임등록프로토콜

국내에서는 공인인증기관을 중심으로 공개키 기반 구조를 발전시켰으며 온라인 금융거래에 전자서명의 거래가 이루어지고 있다. 인증서 기반의 금융서비스를 제공하는 대표적인 시스템은 인터넷뱅킹, 증권거래시스템, 전자상거래, 전자결제 등이 있다. 특히 증권거래시스템의 경우, 투자자와 펀드메니저간에는 위임서명이 필요하지만 현재는 투자자의 개인키를 펀드메니저에게 위탁하고 있다. 현재의 위임방식은 개인키를 위탁함으로서 보안기능을 제공하지 못한다. 또한, 온라인 금융서비스는 거래당사자간의 권리와 의무에 대하여 상호동의 또는 상호계약이 동의되었다는 것을 의미한다. 또한 거래내용이 민감한 사안이기 때문에 거래당사자간의 분쟁 가능성이 존재한다. 따라서 검증자는 위임서명자의 신원확인과 상세한 권한을 설정함으로서 분쟁의 위험을 최소화해야 한다. 제안하는 위임등록 기법은 원서명자와 위임서명자가 인증서를 발급 받은 환경에서 원서명자가 위임서명자에 대하여 검증자에게 등록하는 방식을 제안한다. 위임내용에 대해 원서명자가 전자서명을 하고 검증자는 이에 해당하는 내용을 검증한 후 위임서명자에 대한 권한, 기간, 제약사항을 저장한다. 이후 위임서명자는 위임내용에 대해 고지를 받고 허가된 범위 내에서 위임 서명을 하게 된다.

3.3.1 구성요소

본 논문에서 제안하는 위임등록 기법은 PKI 표준에서 제안하는 구성요소를 기반으로 하며 〔그림 1〕에 기술한다[9].

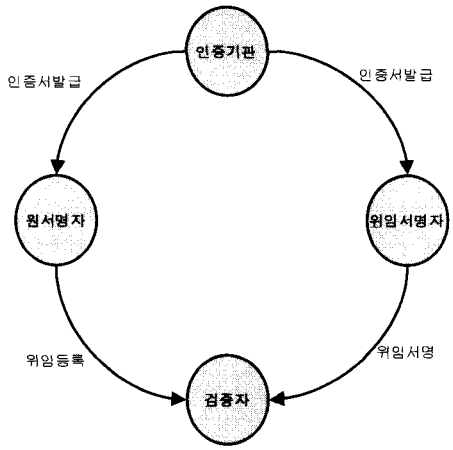


그림 1. 제안하는 PKI의 구성요소

· 인증기관

원서명자와 위임서명자의 인증서 발급을 담당하며 인증서와 관련된 정보를 게시하고 상태정보를 제공한다.

· 원서명자

인증서를 발급받아 서비스를 이용하는 사용자로서 위임서명자에게 위임권한, 시간, 제약사항에 관한 자세한 사항을 정의하고 위임할 수 있다.

· 위임서명자

원서명자의 권한 중 전부 혹은 일부를 위임받아 본인의 인증서를 통해 관련 서비스에 원서명자를 대신하여 전자서명을 수행할 수 있다.

· 검증자

온라인 서비스의 서버로서 원서명자에게 위임 등록을 할 수 있도록 하는 기능을 제공하고 원서명자가 정의한 권한을 위임서명자가 위임하여 수행할 수 있도록 처리한다.

3.3.2 위임 등록 프로토콜

제안한 프로토콜을 기술하기 위한 용어정의는 다음과 같다.

- $Ailce$: 원서명자
- Bob : 위임서명자
- HTS : 검증자
- S_{Alice} : $Alice$의 개인키
- M : 원문
- $sS_{Alice}(M)$: 원문 M을 $Alice$의 개인키로 수행한 전자서명
- f : 전자서명의 목적을 명시하는 플래그
- P : 위임내용
- L : 제약사항
- R : 전송결과
- $T\ start$: 위임시작시간
- T_{end} : 위임종료시간
- $T_{registration}$: 위임등록시간
- $T\ notice$: 전송고지시간
- $T_{confirm}$: 전송확인시간
- T_{sign} : 위임서명생성시간
- $T_{revocation}$: 폐지요청시간
- $reason$: 폐지사유

위임등록 프로토콜은 4가지 토큰으로 구성이 된다. 그 구성도는 [그림 2]와 같다.

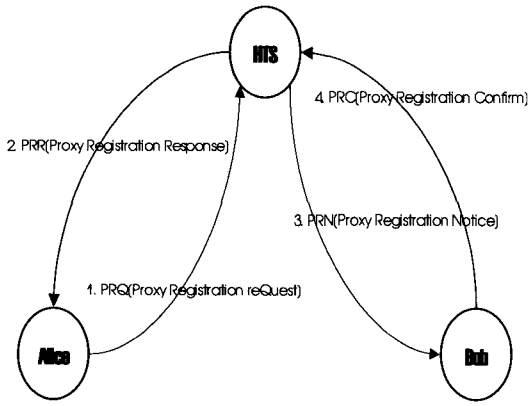


그림 2. 위임 등록 프로토콜의 구성도

· PRQ: $PRQ = sS_{Alice}(f_{PRQ}, HTS, Bob, P, L, Tstart, T_{end})$이며 위임등록요청(*Proxy Registration reQuest*)을 나타낸다.

· PRR: $PRR = sS_{HTS}(f_{PRR}, Alice, T_{registration}, PRQ)$이며 위임등록응답(*Proxy Registration Response*)을 나타낸다.

· PRN: $PRN = sS_{HTS}(f_{PRN}, HTS, Bob, P, L, T\ start, T_{end}, T\ notice, PRQ)$이며

위임등록고지(*Proxy Registration Notice*)를 나타낸다.

- *PRC*: $PRC = sS_{Bob}$ (f_{PRC}, *HTS*, *R*, $T_{confirm}$)이며 위임등록확인(*Proxy Registration Conform*)을 나타낸다. 위임등록확인할 때, 위임서명자가 위임에 대하여 승인(Accept)와 거절(Reject)에 대하여 결과(Result)에 명시한다.

위임등록 프로토콜은 다음과 같은 순서로 진행한다. 프로토콜이 완료되면 투자가 *Alice*는 펀드매니저 *Bob*에게 *HTS*의 거래에 대하여 위임기간동안 제약사항 내에서 위임을 제공한다.

① *Alice* → *HTS* : f_{PRQ}, *HTS*, *B*, *P*, *L*, *T start*, T_{end}, *PRQ*

② *HTS* → *Alice* : f_{PRR}, *Alice*, $T_{registration}$, *PRQ*, *PRR*

③ *HTS* → *Bob* : f_{PRN}, *HTS*, *Bob*, *P*, *L*, *T start*, T_{end}, *T notice*, *PRQ*, *PRN*

④ *Bob* → *HTS* : f_{PRC}, *HTS*, *R*, $T_{confirm}$, *PRC*

① 원서명자 *Alice*는 검증자 *HTS*에 위임서명자 *Bob*에 대하여 위임등록을 요청한다. 이때 *Alice*는 플래그 f_{PRQ}, 위임서명자 *Bob*, 위임내용 *P*, 제약사항 *L*, 위임시작시점 *T start*, 위임종료시점 T_{end}에 대하여 개인키로 서명하여 전송한다. 검증자인 증권거래서비스 *HTS*는 *Alice*로부터 전송받은 위임등록에 대한 검증을 수행한다. *Alice*의 위임등록이 유효하면 *HTS*의 데이터베이스에 상세하게 세분화된 위임권한을 설정한다.

② 검증자는 원서명자의 위임 등록 요청에 대하여 검증과 등록 결과를 응답한다. 검증자 *HTS*는 플래그 f_{PRR}, 원서명자 *Alice*, 위임등록시간 $T_{registration}$, 위임등록요청 *PRQ*를 전자서명하여 원서명자 *A*에게 위임등록요청에 대한 응답한다. *PRQ*를 포함하는 것은 추후에 *Alice*의 위임등록요청에 대한 부인방지를 위해 추가해야 한다.

③ 검증자는 위임서명자에게 원서명자의 위임내용을 고지해야 한다. *HTS*가 플래그 f_{PRN}, 위임서명자 *Bob*, 위임내용 *P*, 제약사항 *L*, 위임시작시간 *T start*, 위임종료시간 T_{end}, 전송고지시간 *T notice*, 위임등록요청 *PRQ*를 전자서명하여 *Bob*에게 고지한다.

④ 위임서명자 *Bob*은 *HTS*로부터 고지된 *Alice*의 위임내용에 대해 인지하였다는 것을 확인한다. 위임서명자 *Bob*이 플래그 f_{PRC}, 검증자 *HTS*, 전송결과 *R*, 전송확인시간 $T_{confirm}$을 전자서명하여 *HTS*에게 응답한다. 이때 위임서명자는 *Alice*의 권한 설정에 대하여 결과(*Result*)에 대하여 승인(*Accept*)과 거절(*Reject*)을 명시해야하며, 이 결과에 대하여 *HTS*는 권한을 설정한다.

3.3.3 위임 서명 프로토콜

위임서명 프로토콜은 2가지 토큰으로 구성이 된다. 그 구성도는 [그림 3]에서 기술한다. 제안하는 위임서명의 특징은 *HTS*에서 *Alice*를 대신할 위임서명자인 *Bob*을 등록시킴으로 *Bob*은 이후에 별도의 보증서 없이도 위임서명을 가능하도록 설계하였다. *Alice*는 *HTS*에게 위임권한을 설정하여 위임등록을 하면, *HTS*는 *Alice*의 권한에 대하여 *Bob*이 수행할 수 있다는 것을 데이터베이스에 설정한다. 이후 *Bob*의 위임서명에 대하여 *HTS*는 해당 권한을 수행할 수 있는지 데이터베이스에 조회를 통해 검증하기 때문에 별도의 보증서 또는 정보가 요구되지 않는다.

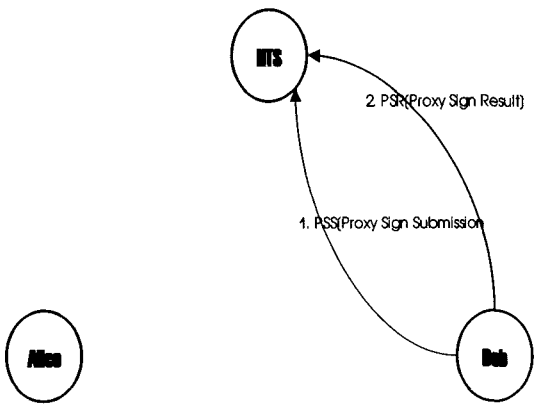


그림 3. 위임 서명 프로토콜의 구성도

- *PSS*: $PSS = sS_{Bob}$ (f_{PSS}, *HTS*, *M*, T_{sign}, *PRN*)이며 위임서명제출(*Proxy*

Sign Submission)을 나타낸다.

- *PSR* : $PSR = sS_{HTS}(f_{PSR}, Bob, R)$이며 위임서명결과(*Proxy Sign Result*)를 나타낸다.

위임서명 프로토콜은 다음과 같은 순서로 진행한다. 펀드매니저 *Bob*은 투자자 *Alice*를 대신하여 *HTS*의 서비스에 위임내용에 따르는 전자서명을 수행한다.

① $Bob \rightarrow HTS$: f_{PSS}, *HTS*, *M*, T_{sign},, *PRN*, *PSS*

② $HTS \rightarrow Bob$: f_{PSR}, *Bob*, *R*, *PSR*

① 위임서명자는 원서명자를 대신하여 검증자의 서비스에 전자서명을 수행한다. Bob은 Alice를 대신하여 플래그 f_{PSS}, 검증자 HTS, 원문 M, 위임서명시간 T_{sign}에 대하여 전자서명을 수행한다. Bob의 위임서명이 유효하면 HTS의 데이터베이스에 설정된 위임권한을 확인한다. 이때 위임내용 P, 제약사항 L에 위배되는지 검증한 후 위임서명시간 T_{sign}가 위임시작시간 T start와 위임종료시간 T_{end}의 범위내에 있어야 위임서명이 유효하게 된다.

② 검증자는 위임서명자에게 위임서명에 대한 결과를 전달한다. *HTS*는 플래그 f_{PSR}, 위임서명자 *Bob*, 위임서명결과 *R*을 전자서명하여 전송한다. 이때 *R*의 결과로써 위임서명의 유효여부를 확인할 수 있다.

3.3.4 위임 폐지 프로토콜

등록 폐지 프로토콜은 4가지 토큰으로 구성이 된다. 그 구성도는 [그림 4]에서 나타내었다.

- *RRQ*: $RRQ = sS_{Alice}(f_{RRQ}, HTS, reason, T_{revocation}, PRQ)$이며 등록폐지요청(*Registration Revocation reQuest*)을 나타낸다.
- *RRR*: $RRR = sS_{HTS}(f_{RRR}, Alice, R)$이며 등록폐지응답(*Registration Revocation Response*)을 나타낸다.
- *RRN*: $RRN = sS_{HTS}(f_{RRN}, Bob, T$ *notice*)이며 등록폐지고지(*Registration Revocation Notice*)를 나타낸다.
- *RRC*: $RRC = sS_{Bob}(f_{RRC}, HTS, T_{confirm})$이며 등록폐지확인(*Registration Revocation Confirm*)을 나타낸다.

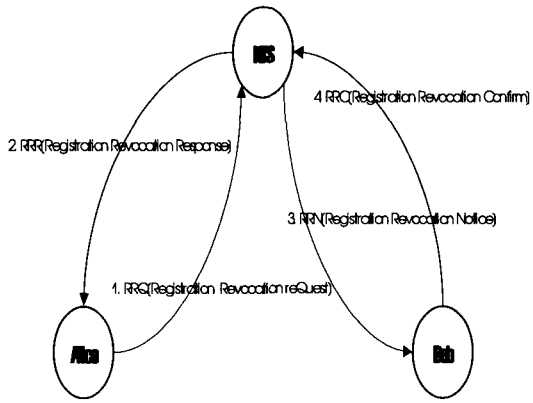


그림 4. 위임 폐지 프로토콜의 구성도

등록폐지 프로토콜은 다음과 같이 수행한다. 투자자 *Alice*는 펀드매니저 *Bob*에 대한 권한을 폐지해야 할 경우 *HTS*에 위임폐지요청을 통해 안전성을 확보할 수 있다.

① $Alice \rightarrow HTS$: f_{RRQ}, *HTS*, *reason*, $T_{revocation}$, *PRQ*, *RRQ*

② $HTS \rightarrow Alice$: f_{RRR}, *Alice*, *R*, *RRR*

③ $HTS \rightarrow Bob$: f_{RRN}, *HTS*, *Bob*, $T_{revocation}$, T *notice*, *RRQ*, *PRN*

④ $Bob \rightarrow HTS$: f_{PRC}, *HTS*, *R*, $T_{confirm}$, *PRC*

① 원서명자는 위임서명자에 대하여 위임권한을 폐지할 수 있다. *Alice*는 플래그 f_{RRQ}, 검증자 *HTS*, 폐지사유 *reason*, 폐지요청시간 $T_{revocation}$, PRQ에 대하여 전자서명을 수행한다. *Alice*가 *HTS*에게 설정한 권한이 무엇인지를 명시하기 위해 *PRQ*를 포함하여 전송한다. *HTS*가 위임등록에 대하여 폐지요청을 반영하면 *Bob*은 *Alice*가 설정한 권한내에서의 위임을 실시간으로 상실한다. *Bob*이 *HTS*에 전송하는 위임서명 메시지의 *PRN*을 통하여 위임자인 원서명자가 *Alice*임을 확인할 수 있다. 또

한 증권거래시 다수의 사용자가 위임할 경우가 있다. 다수의 원서명자가 *HTS*에게 *Bob*을 위임서명자로 등록하면 *HTS*가 *PRN'*를 가지고 있는 경우 *Bob*은 *HTS*에 보내는 위임서명 메시지에 *PRN'*를 추가하여 보냄으로써 *Alice*가 아닌 다른 원서명자에 대한 위임서명임을 *HTS*에게 표시할 수 있다. 따라서 *Bob*은 자신의 전자서명생성키를 원서명자 마다 별도로 가지고 있을 필요 없이 하나의 전자서명생성키를 이용하여 다수의 원서명자에 대해 위임서명이 가능하다.

② 검증자는 원서명자의 등록폐지요청에 대해 응답해야 한다. *HTS*는 플래그 f_{RRR}, 원서명자 *Alice*, 전송결과 *R*에 대해 전자서명을 수행한다. 등록폐지응답을 확보한 *Alice*는 *HTS*에게 폐지신청에 대해 부인방지기능을 가진다.

③ 검증자는 위임서명자에 대하여 위임권한이 폐지되었다는 사실을 고지해야 한다. *HTS*는 플래그 f_{RRN}, 검증자 *HTS*, 위임서명자 *Bob*, 폐지요청시간 $T_{revocation}$, 전송고지시간 T *notice*, 등록폐지요청 *RRQ*을 전자서명한다. *Bob*은 *HTS*에게 전송한 등록폐지고지를 통해 위임권한이 상실되었음을 확인한다.

④ 위임서명자는 등록폐지고지에 대하여 검증자에게 응답해야 한다. *Bob*은 플래그 f_{RRC}, 검증자 *HTS*, 전송결과 *R*, 전송확인시간 $T_{confirm}$,에 대하여 전자서명을 수행한다. *Bob*이 전송한 등록폐지확인을 통해 *HTS*는 프로토콜이 종료되었음을 확인한다.

V. 실험 및 고찰

실험환경은 펜티엄IV 1.6GHz, 256M SDRAM 메모리, Windows 2000 서버 사용하였으며 데이터베이스로 MS-SQL을 사용하였다. 서버 클라이언트 프로그램은 Visual C 언어로 구현하였다. 인증모듈은 국내 공인인증기관이 제공하는 클라이언트와 서버 라이브러리로 적용하였고 전자서명 알고리즘은 RSA, 해쉬함수는 SHA-1, 대칭키 알고리즘은 국내 알고리즘인 SEED로 구현하였다. 실험의 시나리오는 증권거래시스템 환경을 가정하고 기존의 공인인증체계의 인증서를 기반으로 하여 실험하였다.

〔그림 5〕는 증권거래 환경에서 서비스 제공자인 검증자 기반으로 등록하기 때문에 위임자가 조건과 제약에 대하여 상세한 기술이 가능한 것을 나타낸다.

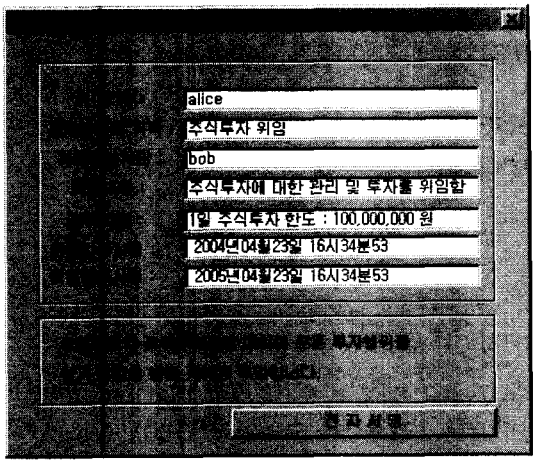


그림 5. 위임서명자에 대한 위임정보 입력창

〔그림 6〕은 원서명자가 입력한 위임내용에 대하여 공인인증기관의 개인키로 전자서명을 수행한 위임등록 토큰을 보여준다.

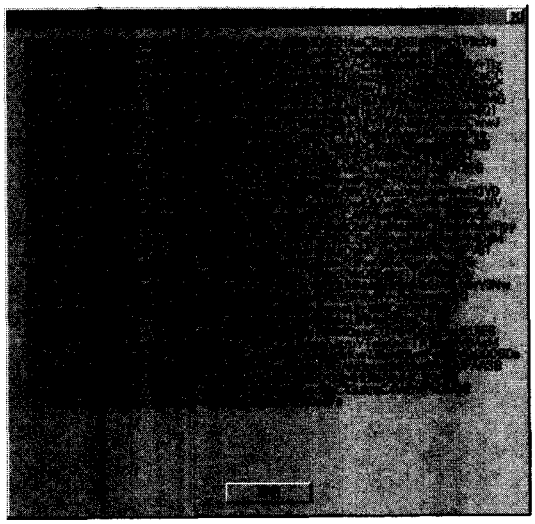


그림 6. 원서명자의 위임등록 토큰

〔그림 7〕은 증권거래 서비스를 제공하는 검증자가 위임등록토큰을 검증한 후 서버에 권한 설정을 하는 과정을 나타낸다.

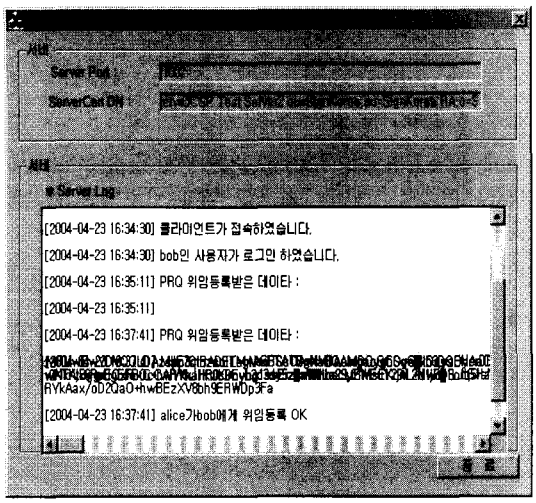


그림 7. 검증자의 위임등록검증 과정

〔표 1〕은 제안하는 위임등록 프로토콜의 실험데이터를 보여준다. 실험은 위임등록과정과 위임서명과정으로 측정하였으며, 처리량, 처리속도, 입력데이터와 출력데이터 크기를 나타내었다. 측정횟수는 측정횟수 1,000번 수행 평균값을 나타내며 명시된 단위는 〔ms〕는 Milliseconds(10^{-3}초)를 나타낸다.

표 1. 위임등록 프로토콜 실험 데이터

기 능	초당 처리량	1회 처리시간	입력데이터	출력데이터
위임 등록	33.93 [KB/sec]	29.46 [ms]	98 Byte (위임내용)	1,442 Byte (위임등록)
위임 등록 검증	22.90 [KB/sec]	43.65 [ms]	1,442 Byte (위임등록)	98 Byte (위임등록검증)
위임 서명	128.45 [KB/sec]	7.78 [ms]	32 Byte (원문)	1,384 Byte (위임서명)
위임 서명 검증	58.91 [KB/sec]	16.97 [ms]	1,384 Byte (위임서명)	32 Byte (검증)

〔표 2〕는 제안하는 위임 서명기법과 기존의 위임 서명 기법을 비교한 것이다. 위임서명의 보안 요구사항들을 기준으로 MUO(Mambo, Usuda, Okamoto), PH(Petersen, Horster), KPW(Kim, Park, Won), DQ(Delos, Quisquater)의 기법들과 제안하는 PRP(Proxy Registration Protocol)를 비교 분석하였다.

표 2. 기존 방법과의 비교 분석

비교항목	MUO	PH	KPW	DQ	PRP
검증성	○	○	○	○	○
신원확인성	○	○	○	○	○
위조불가능성	○	×	○	×	○
부인 불가능성	○	×	○	×	○
권한의 제약	×	×	△	△	○
오용방지	×	×	△	△	○
위임키/보증서 생성여부	필요	필요	필요	필요	불필요

MUO방식은 원서명자가 보증서을 생성하여 위임서명자에게 전달하고 위임서명자는 위임키를 생성하여 위임서명을 수행한다. 검증자는 보증서와 위임서명을 검증하는 과정에서 위임여부에 대한 검증성과 위임서명자의 신원확인성이 확보된다. 보증서와 위임키가 매칭되기 때문에 위조불가능성과 부인불가능성이 보장이 된다. 그러나 위임장에는 위임서명자만을 지정했기 때문에 권한의 제약이 되지 않으며 대리인에 의한 오남용이 가능하다. 원서명자는 보증서를 생성해야 하며 위임서명자는 위임키를 생성해야 하는 부담이 있다.

PH방식은 원서명자가 위임개인키와 공개키를 생성하여 원서명자에게 전달하여 위임서명을 수행한다. 검증자는 위임서명에 대한 검증을 통해 검증성과 신원확인성을 보장된다. 그러나 위임서명자는 원서명자의 동의없이 타인에게 양도가 가능한 문제점이 있다. 따라서 위조불가능성과 부인불가능성은 보장되지 않는다. 권한의 제약도 명시되지 않기 때문에 오용방지가 불가하다. 원서명자는 위임키를 생성해야 하는 부담이 있다.

KPW방식은 원서명자가 위임제약을 포함하는 보증서를 생성하고 위임서명자는 위임키를 생성하여 위임서명을 수행한다. 검증자는 보증서와 위임서명을 검증하는 과정에서 검증성과 신원확인이 가능하다. 보증서와 위임키가 매칭되기 때문에 위조불가능성과 부인불가능성이 보장이 된다. 보증서의 내용에 부분적인 권한제약이 명시되어 있기에 권한제약과 오용방지가 가능하다. 그러나 원서명자는 보증서를 생성해야 하며 위임서명자는 위임키를 생성해야 하는 부담이 있다.

DQ방식은 사용자의 ID에 대응하는 개인키를 생

성하여 위임횟수를 제한하여 수행한다. 검증자는 위임서명자의 위임서명을 검증하는 과정에서 검증성, 신원확인이 가능하다. 그러나 사용자의 ID도용에 의한 위조가능성이 존재하기 때문에 부인방지가 제공되지 않는다. 부분적인기 하지만 위임서명에 대하여 횟수로써 권한의 제약과 오용방지가 가능하다. 각 사용자에게 개인키를 생성하는 부담과 횟수를 제안하기 위해 인증서버에 횟수사용을 전송해야 하는 부담이 있다.

제안한 PRP는 기존의 인증서를 사용하기 때문에 위임서명자의 검증성과 신원확인이 가능하다. 공인인증서는 개인신원정보와 공개키에 대하여 제3의 신뢰기관에서 발급 받은 것이기 때문에 위조가 불가능하다. 원서명자가 검증자에게 전송한 위임등록과정을 통해 지명된 위임서명자만이 위임서명이 가능하기 때문에 부인 불가능성을 제공한다. 제안하는 방식이 기존보다 상세한 조건설정이 가능하다는 것은 권한을 제어해야할 책임은 서비스를 제공하는 검증자에게 있다. 그런데, 검증자는 서비스를 제공하기 때문에 서비스 본래의 제약사항 뿐 아니라 원서명자가 서비스 받을 수 있는 한계의 정보를 보유하고 있다. 따라서 검증자와 원서명자가 자신의 권한 한도 내에서 위임을 설정하기 때문에 보다 상세한 권한의 제약이 위임이 가능한 것이다. 또한 기존의 방식에서는 *Alice*가 실제 1,000만원의 잔고가 있으나 *Bob*에게 2,000만원에 대한 위임이 가능하지만, 제안하는 방식은 서비스제공자가 이미 *Alice*의 잔고가 1,000만원이라는 사실을 인지하기 때문에 권한의 범위내에서 위임이 가능하게 되어 오용방지가 가능하다. 본 논문은 서비스제공자인 *HTS*에서 *Alice*를 대신할 위임서명자인 *Bob*을 등록시킴으로 *Bob*은 이후에 별도의 보증서 없이도 위임서명을 가능하도록 설계하였다. *Alice*는 *HTS*에게 위임권한을 설정하여 위임등록을 하면, *HTS*는 *Alice*의 권한에 대하여 *Bob*이 수행할 수 있다는 것을 데이터베이스에 설정한다. 이후 *Bob*의 위임서명에 대하여 *HTS*는 해당 권한을 수행할 수 있는지 데이터베이스에 조회를 통해 검증하기 때문에 별도의 위임키 또는 보증서 정보가 요구되지 않는다.

Ⅵ. 결 론

현재 증권거래시스템은 권한위임 기능의 요구가 증가되고 있으며, 사용자는 개인키를 위임자에게 전달하고 있는 문제점이 있다. 이러한 권한위임방식은 보안의 위험과 원서명자와 위임서명자의 부인방지에 대하여 분쟁의 소지가 있다. 또한 기존 위임서명방식은 공인인증체계 기반의 증권거래시스템의 요구사항을 만족시키지 못한다.

제안하는 위임등록프로토콜은 위임서명의 보안 요구사항을 만족시키며, 위임을 위한 추가적인 키생성과 보증서가 필요하지 않는다. 따라서 기존의 공인인증체계를 준용하기 때문에 추가적인 개발 없이, 현재의 증권거래시스템에 적합한 위임서명을 제공한다.

향후 연구과제로써는 원서명자와 위임서명자의 관계가 1:1, 1:N, N:1, N:N으로 구분하여 실제 증권거래를 반영할 수 있도록 제안한 프로토콜의 확장 모델에 대한 연구가 필요하다.

참 고 문 헌

[1] 양덕기, "사이버 증권거래와 전자서명 인증서비스 체계", 한국정보보호학회 정보보호학회지, 제9권 제3호, pp. 28-43, 1999.

[2] 이대기, 김희선, 조영섭, 진승헌, 정교일, 조현숙, "국내·외 전자서명 및 인증제도 동향 분석", 한국정보보호학회 정보보호학회지, 제11권 제4호, pp. 27-44, 2001.

[3] M. Mambo, K. Usuda, and E. Okarnoto, "Proxy signatures: Delegation of the power to sign messages", IEICE Trans. Fundamentals, Vol.E79-4, No.9, pp. 1338-1353, Sep. 1996.

[4] H. Petersen and P. Horster, "Self-certified keys-concepts and applications", Proc. of Communications and Multimedia Security'97, pp. 102-116, 1997.

[5] S. Kim, S. Park, and D. Won, "Proxy signatures, revisited", Proc. of ICICS'97, International Conference of Information and Communications Security, LNCS 1334, Springer-Verlag, pp. 223-232, 1997.

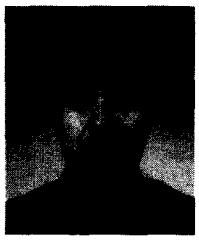
[6] O. Delos and J. J.Quisquater, "An Identity-Based Signature Scheme with Bounded Life-Span", Advances in Cryptology, Proceedings of CRYPTO, 1994.

[7] B. Lee and K. Kim, "Strong Proxy Signatures", IEICE Trans. Fundamentals, Vol.E82, No.1, 1999.

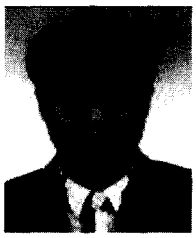
[8] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its applications", Proc. of SCIS2001, PP. 603-608, 2001.

[9] Housley et al, "RFC2459, Internet X.509 Publick Key Infrastructure Certificate and CRL Profile", IETF, 1999.

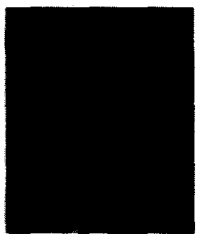
〈著者紹介〉



이 용 준 (Yong-Joon Lee) 정회원
1999년 : 강남대학교 전자계산학과 졸업
2001년 : 숭실대학교 컴퓨터학과 석사
2004년 : 숭실대학교 컴퓨터학과 박사수료
〈관심분야〉 정보보호, 암호학, 유무선 PKI



박 세 준 (Se-Joon Park) 정회원
1996년 : 숭실대학교 수학과 졸업
1998년 : 숭실대학교 대학원 컴퓨터학과
2001년 : 숭실대학교 컴퓨터학과 박사수료
2001년~2002년 : (주)삼보컴퓨터 통신사업부
2002년~현재 : (주)노스텍 R&D 센터
〈관심분야〉 멀티미디어, 컴퓨터통신, 정보보호, 암호학, 유무선 PKI



오 해 석 (Hae-Seok Oh) 정회원
1975년 : 서울대학교 응용수학과 졸업
1981년 : 서울대학교 계산통계학과 석사
1989년 : 서울대학교 계산통계학과 박사
1976년~1982년 : 태평양화학(주), (주)삼호 전산실
1990년~1991년 : 일본 동경대학교 객원교수
1997년~1999년 : 숭실대학교 부총장
2000년~2001년 : 스탠포드대학교 객원교수
1982년~2003년 : 숭실대학교 정보과학대학 교수
2003년~현재 : 경원대학교 소프트웨어대학 교수
〈관심분야〉 정보보호, 멀티미디어, 데이터베이스, 영상처리