위임등록을 통한 효율적인 대리 서명방식

박 세 준, 이 용 준, 오 해 석

Efficient Proxy Signature Technology using Proxy-Register

Se-Joon Park, Yong-Jun Lee, Hae-Suk Oh,

요 약

대리서명은 원서명자가 자신의 서명 권한을 대리 서명자에게 위임하여 대리 서명자가 원서명자를 대신해서 서명을 생성하는 것을 말한다. 대리서명은 원서명자가 위임 정보에 대한 서명을 생성하고 이를 위임자에게 전달하여 위임자가 위임키로서 사용하게 하는 것이다. 본 논문에서는 원서명자와 대리서명자가 기존의 인증서를 발급 받은 환경에서 원서명자가 대리서명자에 대하여 검증자에게 위임정보를 등록하는 프로토콜을 제안한다. 위임내용에 대해 원서명자가 디지털 서명을 하고 검증자는 이에 해당하는 내용을 검증한 후 위임서명자에 대한 권한, 기간 등의 제약사항을 설정하고 허가된 범위 내에서 위임 서명을 한다.

key Words : proxy-register protocol; proxy signature; unforgeability; undeniability.

ABSTRACT

Proxy signature is the signature that an original signer delegates his signing capability to a proxy signer and the proxy signer creates a signature on behalf of the original signer. The basic methodology of proxy signature is that the original signer creates a signature on delegation information and gives it secretly to the proxy signer, and the proxy signer uses it as a proxy private key or uses it to generate a proxy private key. In this paper, we suggest the proxy-register protocol that the original signer register to the verifier about the proxy related information, and verifier sets the warrant of proxy signer, validity period for proxy signature and some limitation.

(주) 씨큐리콥 (atprince@empal.com), 경원대학교 IT부총장 (oh@kyungwon.ac.kr)
논문번호 : 030463-1017, 접수일자 : 2003년 10월 17일

Ⅰ. 서 론

대리인에게 서명의 권한을 위임하는 기법이 최근에 많이 연구되고 있다. 담당자가 부재중이거나 휴가중일 경우 혹은 대리인에게 위임을 필요로 하는 경우와 온라인 상의 문제로 인해 서명을 할 수 없는 상황과 같은 경우에 대리서명이 필요하게 된다.

대리 서명은 원 서명자가 자신의 서명 능력을 대리인에게 위임하는 서명 기법으로서 대리 서명자는 원 서명자를 대신하여 서명을 하게 된다. 대리 서명의 기본적인 원리는 원서명자가 대리 서명자의 ID나 혹은 어떠한 권한에 대한 정보를 포함하는 서명을 생성하고 이를 대리 서명자에게 넘겨주게 되면 대리 서명자는 대리 서명 개인키로 사용하거나 혹은 대리 서명 개인키를 생성시키기 위해 사용하게 된다[9]. 원서명자의 서명으로부터 생성된 대리 서명키는 임의의 검증자에 의해서 원 서명자의 동의사항 등을 확인할 수 있다.

그러나 현실적으로 위임과 관련하여 많은 보안상의 문제점들이 지적되고 있다. 가장 큰 문제점은 인증서를 직원에게 발급함으로서 발생하는 인증서와 비밀키의 오남용에 대한 처리가 힘들다는 것이다[8]. 또한 대리 서명이 이루어진 이후에 대리인의 부인 방지를 막을 수가 없고 위임을 받은 대리인이 제삼자에게 원서명자의 동의 없이 인증서와 비밀키를 유출함으로서 제삼자는 대리 서명 능력을 가지게 할 수 있으며 비밀키 자체의 노출이 늘어남에 따라 보안상의 심각한 문제가 발생할 수 있다[12].

이러한 문제점을 극복하기 위해 공개키 인증서를 가진 대리인이 위임받는 권한에 대해 규정하여 이를 자신의 공개키로 서명함으로서 대리 서명을 할 수 있다. 대리인은 위임을 받음과 동시에 위임자가 규정한 범위 내에서 대리서명이 가능하며 위임자는 대리인의 지위나 역할을 고려하여 적절한 권한을 위임할 수 있기 때문에 앞에서 제기된 문제들을 해결할 수 있다. 이러한 권한의 위임이 가능하도록 하는 위임등록 기법을 설계하고자 한다.

본 논문에서는 원서명자와 대리 서명자가 기존의 인증서를 가지고 원서명자가 대리 서명자에 대하여 검증자에게 위임정보를 등록하는 위임 등록 기법을 제안한다. 위임내용에 대한 전자서명을 원서명자가 시행하고 검증자는 이에 해당하는 내용을 검증한 이후에 대리 서명자에 대한 권한, 기간, 제약사항 등을 설정하게 되며 대리 서명자는 이러한 내용을 기반으로 하여 허가된 권한과 범위 내에서 위임 서명을 하게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 대리서명 기법과 보안요구 사항에 대해서 알아보고 3장에서는 제안하는 대리서명 기법을 설계하고 4장에서는 실험 평가값을 통한 비교 분석을 하며 5장에서는 결론을 맺는다.

Ⅱ. 기존 대리서명 기법

1. Mambo, Usuda, Okamoto's Scheme

MUO 기법에서는 3가지 타입의 위임에 기반하여 대리서명 기술을 구분하였다. 대리 서명 방식에서 원서명자의 서명 권한을 위임하는 형태에 따라서 완전 위임, 부분 위임으로 분류하였고 원서명자에 의해 만들어진 인증서를 사용하여 대리 서명을 실현하는 보증 위임을 제안하였다[2][11].

완전 위임은 원서명자가 자신의 개인키를 대리인에게 주는 방법으로서 대리 서명자에 의한 서명과 원서명자에 의한 서명이 구분되지 않는다. 부분 위임은 원서명자가 대리서명 비밀키를 자신의 비밀키를 이용하여 생성하는 방법으로서 대리서명의 암호화에 따라 대리 서명자가 원서명자를 대신하여 서명할 수 있는 대리인 비보호형 대리서명 방식 기법과 정당한 대리 서명자만이 대리서명이 가능한 대리인 보호형 대리 서명방식 기법으로 구분되며 위임 서명키는 원서명자와 위임자 모두에 의해서 생성된다. 보증 위임은 원서명자가 자신과 대리 서명자의 정보와 관련된 권한에 대해서 서명하고 검증자는 이 정보에 기반하여 권한을 검증하는 방법을 말하며 지정한 사람을 대리 서명자로 선언하는 서류에 원서명자가 디지털 서명을 통하여 서명한 후 그 서명된 인증서를 이용하여 대리 서명을 실행하는 인증서 기반 대리 서명 방식 기법과 지정한 서명자를 위한 비밀키와 공개키를 생성하고 생성된 공개키에 대하여 원서명자

가 인증서를 만들어 지정된 대리 서명자에게 전달하는 소지자 기반 대리 서명 방식 기법으로 구분된다.

이들이 제안한 대리서명 기법은 위임되는 권한에 대한 제약이 없으므로 대리 서명자에 의한 오남용이 가능하다는 점과 원서명자의 동의 없이 제 3자에게 전달하여 대리서명이 가능하고 제 3자가 명백한 위임자인지에 대한 결정을 할 수 없다는 단점이 있다.

2. Pertersen and Horster's Scheme

PH 기법에서는 자체 보증키를 생성하여 대리 서명을 하는 기법을 제안하였다[2][7]. 또한 이들은 위임키쌍을 생성하기 위해 기본키 생성 프로토콜과 보안키 생성 프로토콜을 제안하였다. 기본키 생성 프로토콜은 대리인 비보호형 대리 서명 기법으로서 원서명자가 위임키쌍을 생성하여 대리 서명자에게 전달하는 것이며 보안키 생성 프로토콜은 대리인 보호형 대리 서명 기법으로서 원서명자와 대리 서명자가 함께 위임키쌍을 생성하지만 대리 서명자의 개인키를 원서명자가 알 수 없도록 하는 방법이다. 이들이 제안한 대리서명 기법은 대리서명시 위임자에 대한 어떠한 정보도 포함되어 있지 않기 때문에 서명을 수행한 후 추후에 부인할 수 있고 위임자가 위임키를 CA에 자신의 키쌍처럼 등록하여 자신의 목적을 위하여 사용할 수 있으며 원서명자는 위임자의 동의없이 위임자의 ID를 가지고 위임키쌍을 생성하여 CA에 등록하고 자신의 키처럼 사용할 수 있다는 단점이 있다.

3. Kim, Park and Won's Scheme

MUO 혹은 PH 기법에서는 원서명자의 정보에 대리 서명자의 신원이나 권한과 같은 어떠한 정보도 포함되어 있지 않기 때문에 권한의 오남용과 같은 문제들이 발생할 수 있다. 이와 같은 문제들을 해결하기 위해 KPW 기법에서는 Schnorr 서명 기법을 이용하고 대리인과 위임되는 권한에 대한 정보를 대리서명에 포함시켜 위임된 권한의 오남용, 제 3자에게로의 서명 권한 전달을 방지하는 방법을 제안하였다[6].

KPW 기법에서는 위임 개인키가 대리인에 의해서만 표현되어질 수 있기 때문에 대리인 보호형 대리서명 기법이다[3][16]. 이들이 제안한 대리서명 기법은 대리서명 내에 원서명자와 위임자의 역할이 동일하다는 단점이 있다. 그러므로 권한에 대한 내용이 아주 명백하게 표시되어 있어야 하며 그렇지 않은 경우에는 이들의 역할이 바뀔 수 있기 때문에 검증자는 대리서명의 권한에 표시된 내용과 일치하는지에 대해서 체크해야 한다.

4. Delos, Quisquater's Scheme

DQ 기법에서는 서명하는 횟수를 제한할 수 있는 ID 기반 서명 기법과 제한된 서명 횟수의 일부분을 대리인이 수행할 수 있는 방법을 제안하였다[14][15]. 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. 이들이 제안한 대리서명 기법은 ID 기반 인증 모델에서의 서명 기법임에도 불구하고 유효성 확인을 위해 원서명자나 신뢰기관이 제공하는 인증서를 사용해야 하며 시스템이 각 사용자의 개인키를 알고 있고 단순한 횟수의 제한을 제외하고는 권한의 사용에 대한 아무런 제약이 없다는 단점이 있다.

Ⅲ. 제안 위임 등록 기법의 설계 및 구현

국내에서는 공인인증기관을 중심으로 공개키 기반구조를 발전시켰으며 다수의 온라인 금융거래에 전자서명의 거래가 이루어지고 있다. 인증서 기반의 금융서비스를 제공하는 대표적인 시스템은 인터넷뱅킹, 증권거래시스템, 전자상거래, 전자결제 등이 있다. 특히 증권거래시스템과 같은 경우에는 투자자와 펀드매니저간에는 위임서명이 필요하지만 현재 어플리케이션에서는 투자자의 개인키를 펀드매니저에게 위탁하고 있다. 현재의 위임방식은 개인키 전체를 위탁함으로서 보안기능을 제공하지 못하고 있으며 현실적인 공개키기반 구조를 반영하지 못하고 있다. 온라인 금융서비스는 거래당사자간의 권리와 의무에 대하여 상호동의 또는 상호계약이 정의되었다는 것을 의미한다. 또한 거래내용이 직접금융이기 때문에 거래당사자간의 분쟁 가능성이 존재한다. 따라서 검증자는 위임

서명자의 신원확인과 상세한 권한을 설정함으로서 분쟁의 위험을 최소화할 수 있다. 제안하는 위임등록 기법은 원서명자와 대리 서명자가 인증서를 발급 받은 환경에서 원서명자가 대리 서명자에 대하여 검증자에게 위임정보를 등록하는 기법을 제안한다. 위임내용에 대해 원서명자가 전자서명을 하고 검증자는 이에 해당하는 내용을 검증한 후 대리 서명자에 대한 권한, 기간, 제약사항을 저장한다. 이후 대리 서명자는 위임내용에 대해 고지를 받고 허가된 범위 내에서 위임 서명을 하게된다.

1. 구성 요소

본 논문에서 제안하는 위임등록 기법을 이용한 대리서명 기법의 구성요소는 다음과 같다.

1) 인증기관
   원서명자와 대리 서명자의 인증서 발급을 담당하며 인증서와 관련된 정보를 게시하고 상태정보를 제공한다.
2) 원서명자
   인증서를 발급받아 서비스를 이용하는 사용자로서 대리 서명자에게 위임권한, 시간, 제약사항에 관한 자세한 사항을 정의하고 위임할 수 있다.
3) 대리 서명자
   원서명자의 권한 중 전부 혹은 일부를 위임받아 본인의 인증서를 통해 관련 서비스에 원서명자를 대신하여 전자서명을 수행할 수 있다.
4) 검증자
   온라인 서비스의 서버로서 원서명자에게 위임 등록을 할 수 있도록 하는 기능을 제공하고 원서명자가 정의한 권한을 대리 서명자가 위임하여 수행할 수 있도록 처리한다.

그림 1 은 제안하는 시스템의 구성 요소를 도식화하였다. 인증기관은 기존의 공개키 기반 구조와 같이 원서명자와 위임서명자에게 인증서를 발급한다. 원서명자는 검증자로 대변되는 서비스에 위임등록 기법을 이용하여 등록한다. 검증자의 등록이 완료되면 원서명자는 위임서명자에게 권한위임을 고지하고, 이후 상세하게 설정된 내용에 따라서 위임서명이 가능하게 된다. 기존의 인증서를 이용한 권한 위임에서는 원서명자가 모든 권한과 함께 개인키와 전자서명 비밀번호를 위임서명자에게 전달하는 문제가 있었다. 이러한 문제는 개인키의 복사로 인해 위임서명자의 신원확인이 불가능하며 상호 연동이 적용된 다른 서비스를 사용함으로서 분쟁의 소지가 있었다. 그러나 제안한 방식은 검증자 측면에서 위임서명자의 권한을 설정함으로서 위임서명자에게 개인키를 복사하지 않으며 상세하며 보안이 강화된 위임을 제공한다.

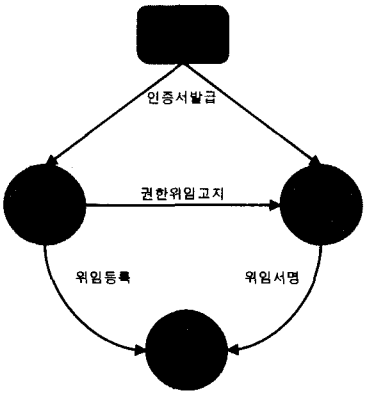


그림 1. 구성 요소

2. 위임등록 기법 시나리오

그림 2 는 제안하는 위임 등록 기법의 시나리오를 나타낸 것이다. 본 논문의 검증자는 온라인서비스를 제공하는 서버이며, 원서명자와 대리 서명자는 온라인서비스의 사용자를 의미한다. 원서명자는 대리 서명자에게 안전한 방법으로 위임권한, 기간, 제약사항을 위임등록기법을 사용하여 정의할 수 있다. 위임등록 기법은 다음과 같이 구성되어 있다.

1) 원서명자 Alice는 검증자인 서비스제공자의 서버에 접속하여 대리 서명자 Bob에 대하여 위임 등록을 요청한다. 이때 원서명자 Alice가 등록하는 내용은 위임내용, 위임시작시점, 위임종료시점, 위임에 대한 제약사항에 대하여 상세하게 명시한 후 Alice의 개인키로 서명하여 전송한다.
2) 검증자인 증권거래서버 HTS는 Alice로 부터 전송받은 위임등록에 대한 검증을 수행한다. Alice의 인증서의 유효성과 위임내용의

전자서명의 검증 후 결과를 반영한다.

3) 위임정보의 전자서명 검증이 정상적이면 위임내용, 위임시작시점, 위임종료시점, 제약사항에 대하여 데이터베이스에 등록하여 대리 서명자인 Bob의 권한을 설정한다.
4) HTS는 원서명자의 위임 등록 요청에 대하여 검증과 등록 결과를 응답한다.
5) 대리 서명자 Bob이 HTS 서비스를 제공받기 위해 로그인을 한 경우 Alice가 Bob에게 위임한 내용에 대해 고지를 한다.
6) 대리 서명자 Bob은 HTS 서비스를 통해 제공받은 Alice의 **위임내용**에 대해 인지하였다는 것을 확인한다.

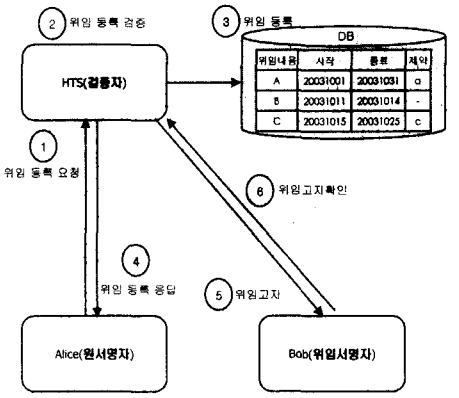


그림 2. 위임등록 및 검증 시나리오

그림 3 은 제안한 위임등록 기법에 대한 구현 내용을 표기한 것이다. 원서명자가 대리 서명자의 집합을 설정해서 등록을 요청하는 과정을 나타내고 있으며 원서명자의 개인키로 전자서명을 수행하는 과정을 표현하였다. 또한 검증자가 원서명자의 위임등록 전자서명을 검증한 후 데이터베이스에 등록하고 그 결과를 나타내는 과정을 보여주고 있다.

그림 4 는 제안하는 위임서명의 시나리오를 나타낸 것이다. 대리 서명자 Bob은 원서명자인 Alice로부터 위임받은 권한을 인지한 후, Alice를 대신하여 전자서명을 수행한다. 이때 검증자인 HTS는 위임 등록된 위임내용, 위임기간, 제약사항을 확인함으로서 전부 또는 제한적인 위임을 가능하게 한다. Bob의 전자서명과 검증은 다음의 구성과 같다.

```
int Proxy_Registration() {
 string proxy_content; /* 위임내용 */
 string from_time; /* 위임시작시간 */
 string to_time; /* 위임종료시간 */
 string limit; /* 위임제약 */
 string proxy_information;      /* 위임정보 */
 string proxy_registration;/* 위임등록서명 */
 /* 위임정보 취합 */
 proxy_information = proxy_content +
                     from_time +
                     to_time + limit;
 /* 위임정보에 원서명자의 전자서명 수행 */
 proxy_registration =
 get_signed_data(proxy_information);
 /* 위임등록서명을 검증자에게 전송 */
 send_proxy_registration(proxy_registration);
 /* 검증자 위임등록서명 검증 */
 result =
 verify_proxy_registration(proxy_registration);
 if (result == ok ) {
 /* 위임정보 데이터베이스에 저장 */
 save_proxy_registration_to_db(proxy_content,
  from_time, to_time, proxy_registration); }
 else {
 /* 에러처리 */
 notice_error(); } }
```

그림 3. 위임등록 기법

1) Bob은 Alice를 대신하여 자신의 개인키로 전자서명을 수행한다. 이러한 서비스는 증권거래시스템, 전자결제와 같이 부분적인 권한과 시간의 제약으로 위임할 수 있는 서비스에 적합하다.
2) HTS는 Bob의 전자서명을 검증한다. 우선적으로 Bob의 인증서를 검증한 후 위임서명에 대해 검증을 수행한다.
3) HTS는 위임서명의 검증이 정상적이라도 위임등록 기법을 통해 데이터베이스에 등록된 위임내용, 위임기간, 제약사항에 대해 확인을 한다. 즉, Bob은 Alice가 정의한 권한내에서 전자서명을 수행할 수 있다.
4) 위임서명 검증이 정상적이고 위임권한이 확인되면 HTS는 해당하는 결과를 Bob에게 응답한다.

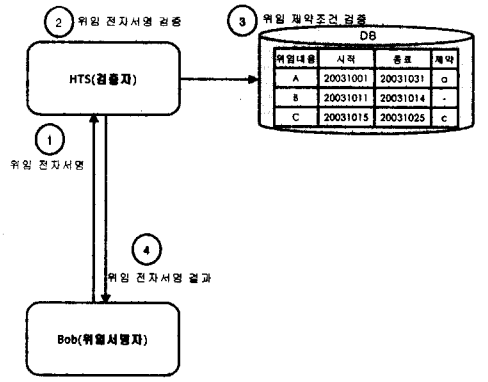


그림 4. 위임서명 및 검증 시나리오

```
int Proxy_Sign() {
 string proxy_content; /* 위임내용 */
 string from_time; /* 위임시작시간 */
 string to_time; /* 위임종료시간 */
 string limit; /* 위임제약 */
 string proxy_sign; /* 위임서명 */
 /* 위임자의 전자서명 수행 */
 proxy_sign =
 get_signed_data(proxy_sign_plaintext);
 /* 위임서명을 검증자에게 전송 */
send_proxy_sign(proxy_sign);
 /* 검증자 위임서명 검증 */
 result = verify_proxy_sign(proxy_sign);
 if (result == ok ) {
 /* 위임정보 데이터베이스에서 획득 */
 retrive_proxy_registration_from_db();
 /* 위임내용 검증 */
 if ( proxy_content == nok )
      notice_error();
 /* 위임시작시간 검증 */
 if ( from_time == nok )
    notice_error();
 /* 위임종료시간 검증 */
 if ( to_time == nok )
   notice_error();
 /* 위임제약 검증 */
 if ( limit == nok )
   notice_error(); }
 else {
   /* 에러처리 */
   notice_error() } }
```

그림 5. 위임서명 및 검증기법

그림 5 는 위임서명과 검증에 대한 구현내용을 표기하였다. 대리 서명자가 위임서명을 하면 검증자는 전자서명 검증을 수행한 후에 데이터베이스에 설정된 위임내용을 추가로 검증하여 위임서명의 진위여부를 판단한다.

Ⅳ. 실험 및 평가

1. 실험 환경

실험환경은 펜티엄 IV 1.6GHz 시스템, 256M SDRAM 메모리, Windows 2000 Server를 사용하였으며 데이터베이스로 MY-SQL 4.0.9를 사용하였다. JAVA 및 JSP 프로그램 언어로 개발하였으며 JSP 컴파일러는 Tomcat V4를 이용하였다. 인증모듈은 국내 공인인증기관이 제공하는 클라이언트와 서버툴킷을 적용하였고 디지털 서명 알고리즘은 RSA 1024bit, 해쉬함수는 SHA-1으로 국제 표준을 준용하였으며 대칭키 알고리즘은 국내 금융기관에서 준용하는 SEED로 구현하였다.

2. 실험 평가

본 논문에서 제안하는 기법은 RSA 전자서명 알고리즘을 이용하였다. RSA 알고리즘에서 원서명자 A는 충분히 큰 소수 p_A, q_A를 선택하고 $n_A = p_A \cdot q_A$를 계산한다. 그리고 $\varphi(n_A) = (p_A - 1)(q_A - 1)$과 서로소인 e_A를 선택하여 $e_A \cdot d_A \equiv 1 \bmod \varphi(n_A)$를 만족하는 d_A를 구하고 e_A를 공개키로서 d_A를 비밀키로서 보관한다. e_A, n_A는 전자서명 검증을 위한 공개 정보이고 d_A는 비밀서명 생성 정보이다. 원문 M은 서명할 수 있는 크기로 일방향 해쉬함수를 이용하여 $H = h(M)$과 같이 압축된다. 압축된 서명문 H에 대한 서명 $S \equiv H^{d_A} \bmod n_A$를 계산하게 된다. 위임등록 원문 M은 대리 서명자의 인증서 DN, 위임내용 C, 위임기간 T, 위임제약 L의 내용을 포함하고 있다. 원서명자 A가 서명한 원문 S에 대해 검증자 B가 검증하여 그 결과가 정상적이면 데이터베이스에 M을 토큰한 위임정보를 저장하게 된다.

기존의 위임서명 권한에서 제어할 수 있는 제약보다 상세한 조건이 가능하며 원서명자가

대리 서명자의 인증서 DN을 지정하였기 때문에 위조가 불가능하게 된다. 그리고 원서명자가 대리 서명자의 DN을 명시하였기 때문에 양도가 불가하게 되며 원서명자가 대리 서명자의 권한에 대해 상세하게 명시하였기 때문에 오용방지가 가능하다. 또한 별도의 대리 서명자의 위임키쌍을 생성하지 않기 때문에 효율적인 결과를 얻을 수 있다. 또한 대리서명 수행시에 인증서를 통해 대리 서명자의 신원을 확인할 수 있기 때문에 검증성이 보장되며 대리 서명자의 인증서는 기존의 발급된 인증서를 적용하기 때문에 신원성이 보장된다. 대리 서명자 C가 수행한 전자서명에 대해 제약조건을 비교함으로서 적합성이 확인되며 검증자 B가 대리 서명자 C의 전자서명을 보유할 경우 부인방지가 가능하다.

표 1 은 제안하는 위임등록 프로토콜의 실험 데이터를 보여준다. 측정횟수는 측정횟수 10,000번 수행 평균값을 나타내며 명시된 단위는 [ms] : Milliseconds(10^{-3}초), [μs] : Microseconds(10^{-6}초)를 나타낸다. RSA의 암호강도는 공인인증기관에서 적용하고 있는 RSA 1024bit 알고리즘으로 적용하였다.

표 1. 위임등록 프로토콜 실험 데이터

기능		초당 처리량	1회 처리시간
위임등록	Sign 1024bit	58.91	16.97
	Verify 1024bit	128.45	7.78
대리서명	Sign 1024bit	33.93	29.46
	Verify 1024bit	22.90	43.65

표 2 는 제안하는 대리 서명기법과 기존의 대리 서명기법을 비교한 것이다. 대리서명의 보안 요구사항들을 기준으로 MUO(Mambo, Usuda, Okamoto), PH(Petersen, Horster), KPW(Kim, Park, Won), DQ(Delos, Quisquater)의 기법들과 제안하는 PR(Proxy-Register)를 비교 분석하였다.

표 2. 기존 방법과의 비교 분석

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

V. 결 론

대리서명은 자신의 서명 권한을 위임할 필요가 있을 경우에 유용하게 사용될 수 있는 기술이다. 그러나 서명의 권한을 위임하는 것은 위험한 일이고 분산환경에서는 원서명자, 대리 서명자, 대리서명 기법간의 신뢰에 관한 사항이 해결해야할 사항으로 남아 있다.

본 논문에서는 기존 대리 서명의 보안 요구사항을 만족하는 위임 등록 기법을 제안하였다. 제안한 기법은 대리서명의 보안 요구사항을 모두 만족시키며 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 해결하였으며 제안된 위임등록 기법의 적용은 실제 환경의 보안 요구사항을 분석하여 이루어진다. 또한 정의된 요구사항과 시스템 구조에 맞는 구조와 전자상거래를 통한 안전한 대리서명 기법을 제공할 수 있다.

참 고 문 헌

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

[2] 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.

[3] M.Abe, T. Okamoto, "Provably secure

partially blind suignatures", *In Advances in Cyyptologt Crypto'*2000.

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

[5] L.Yi, G.Bai and G.Xiao, "Proxy multi-signature scheme: A new type of proxy signature scheme", *Electronics Letters*, Vol.36, No.6, 2000.

[6] K.Shum and Victor K. Wei, "A strong proxy signatures scheme with proxy signer privacy protection", *Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies*: Infrastructure for Collaborative Enterprises, 2002.

[7] D.Chaum and H.van Antwerpen, "Undeniable signatures", *Advances in Cryptology-CRYPTO'89 Proceedings*, Springer-Verlag, 1990.

[8] D.Pointcheval and J. Stern, "Security proofs for signatures", *In Advances in Cryptology: Eurocrypt'96*, Springer, 1996.

[9] V.Varadharajan, P. Allen, and S. Black, "An analysis of the proxy problem in distributed systems." *Proc. IEEE Computer Sociery Symp.* on Research in Security and Privacy, 1991.

[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.

[11] 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.

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

[13] M.Cerecedo, T.Matsumoto, and H.Imai, "Efficient and secure multiparty generation of digital signatures based on discrete logarithms," *IEICE Trans. Fundamentals*, 1993.

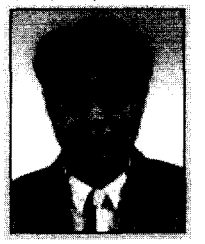
[14] B.C, Neuman, "Proxy-based authorization and accounting for distributed systems," *Proc. 13th International Conference on Distributed Computing Systems*, 1993.

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

[16] J.Cha and J. Cheon, "An Identity-based Signature from Gap Diffie-Hellman Groups," *Springer-Verlag, Advances in Cryptology*, Proceedings of PKC, 2003.

[17] N.Lee, T.Hwang, and C.Wang, "On Zhang's Nonrepudiable Proxy Signature Scheme", *in Proceedings of ACISP'98-Australasian Conference on Information Security and Privacy*, Vol. 1438 of Lecture Notes in Computer Science, 1998.

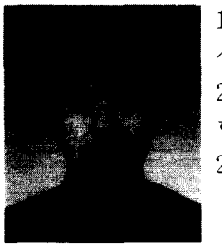
박 세 준(Se-Joon Park) 정회원



1996년 2월 : 숭실대학교 수학과 학사
1998년 2월 : 숭실대학교 컴퓨터학과 석사
2001년 2월: 숭실대학교 컴퓨터학과 박사과정 수료

<관심분야> 멀티미디어, 암호학, 유무선 PKI

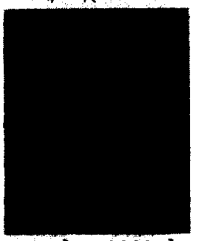
이 용 준(Yong-Jun Lee) 정회원



1999년 : 강남대학교 전자계산학과 졸업
2001년 : 숭실대학교 컴퓨터학과 석사
2001년 ~현재 : 숭실대학교 컴퓨터학과 박사과정

<주관심분야> 정보보호, 암호학, 유무선 PKI

오 해 석(Hae-Suk Oh) 정회원



1975년 2월 : 서울대학교 응용수학과 학사
1981년 2월 : 서울대학교 계산통계학과 석사
1989년 2월: 서울대학교 계산 통계학과 박사
1982년 ~ 2003년 : 숭실대학교 정보과학대학 교수
2003년 ~ : 경원대학교 IT 부총장

<관심분야> 멀티미디어, 데이터베이스, 영상처리, 정보보호, 유무선 PKI