위임 인증서 기반의 다단계 대리 서명 방식 프로토콜

남기희*, 김중태*, 조영주*, 정일용*

*조선대학교 전자계산학과

A Multi-level Proxy Signature Protocol based on Proxy Certificate

Gi-hee Nam*, Jung-tae Kim*, Yeong-ju Cho*, Il-yong Chung*

*Department of Computer Science, Chosun Univ.

요 약

정보통신사회에서 전자서명은 컴퓨터 및 통신망의 확대로 전자거래, 전자결재 등에 활용되어 점점 더 그 중요성이 확대되고 있다. 대리 서명 방식은 전자서명 방식의 한 응용 분야로써 1996년 Mambo[1,2]에 의하여 최초로 제안이 되었고, Araki[4]에 의하여 다단계 대리 서명 방식으로 확장되었다. 그러나 제안된 다단계 대리 서명 방식의 연구에서는 다단계로 확장 시 원 서명자를 보호하는 문제와 부인 공격에 대하여 취약하다는 문제가 있다. 따라서 본 연구에서는 PKI기반의 위임 인증서 사용으로 서명 검증자의 서명 생성 여부를 원 서명자가 추후 확인 가능하도록 하는 프로토콜을 이용하여 부인봉쇄 및 원 서명자의 보호가 이루어지는 효율적이고 안정적인 다단계 대리 서명 방식을 제안하고자 한다.

I. 서론

대리 서명 방식은 서명자가 대리 서명자에게 자신의 서명 권한을 위임하여 대리 서명자가 원 서명자를 대신하여 서명 생성이 가능하도록 하는 전자서명 응용 기법 중의 하나이다. 이 때, 서명 권한을 위임받은 대리 서명자 역시 또 다른 대리인에게 서명 권한을 위임할 수 있어야 한다. 이러한 대리 서명 방식의 확장된 형태인 다단계 대리 서명 방식은 Araki[4]에 의하여 제안되었다.

다단계 대리 서명 방식은 원 서명자의 위임 부인을 방지하여 대리 서명자를 보호할 수 있어야 하며, 원 서명자에게는 자신이 위임한 서명이 실제로 이루어진 상황을 알 수 있게 하여 원 서명자의 서명에 대해 보호할 수 있어야 한다.

본 논문에서는 Tuecke[7]가 제안한 위임 인증서 개념과 원 서명자가 추후 확인이 가능하도록 하는 프로토콜을 이용하여 위임 부인을 방지하고 원 서명자를 보호할 수 있는 다단계 대리 서명 확장 방식을 제안하였다.

II. 대리 서명에 관한 연구

Mambo[1,2]는 대리 서명 기법을 원 서명자의 서명 권한을 위임하는 형태에 따라 완전 위임, 부분 위임, 보증 위임 방식으로 나누어 제안하였다. 완전 위임 방식은 원 서명자가 대리 서명자에게

다단계 대리 서명의 시나리오는 그림 1과 같다.

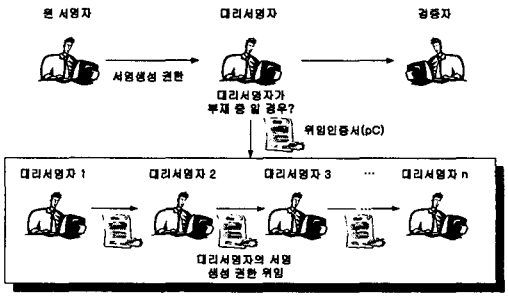

그림 1: 다단계 대리서명 방식의 시나리오

자신의 비밀키를 주는 경우로 대리 서명자의 서명과 원 서명자의 서명이 구분이 되지 않는 방식이다. 부분 위임은 완전 위임 보다 안전한 방식으로 원 서명자가 대리 서명용 비밀키를 자신의 비밀키를 이용하여 생성하는 방식이다 이 때 비밀키는 대리 서명용 비밀키로부터 계산이 불가능하여야 한다. 보증 위임 방식은 원 서명자가 대리 서명자에게 보증서를 발행함으로써 대리 서명을 구현하는 방식이다.

KPW[3]에서는 위의 부분 위임과 보증 위임의 장점만을 취하여 보증 부분 위임 대리 서명 방식을 제안하였다. 보증 부분 위임은 원 서명자가 대리 서명용 비밀키를 자신의 비밀키와 유효기간과 대리서명자와의 관계 등이 언급된 보증서를 이용하여 생성하는 경우를 말한다. 이 때 원 서명자의 비밀키는 대리 서명용 비밀키와 보증서로부터 계산 불가능하여야 한다.

Araki[4]는 Mambo의 대리 서명 방식을 확장하여 다단계 대리 서명 방식을 제안하였다. 제안된 다단계 대리 서명 방식의 문제점은 다음과 같다.

- 원 서명자가 지정한 대리인이 아닌 다른 사람이 원 서명자를 대신하여 서명할 수 있다.
- 원 서명자가 어떤 불법적인 의도에 의해서 위임 부인을 할 경우가 발생할 수 있다.
- 다단계 확장 시 대리 서명자가 또 다른 대리 서명자에게 권한 위임을 하는 과정에서 제3자에 의한 불법적인 변조가 있을 수 있다.
- 원 서명자가 사후 자신의 위임 서명에 대한 결과를 알 수가 없으므로 원 서명자의 보호가 이루어지지 않는다.

김소진[5]에서는 위의 문제점을 해결하기 위해서 대리 서명자와 유효기간을 지정한 보증 위임 대리 서명 방식의 확장에 대해서 제안하였다. 이 제안 방식에서는 보증서 보관에 대한 문제점이 발생할 수 있다.

III. 위임 인증서

위임 인증서는 대리 서명자가 대리 서명을 위한 키 쌍을 생성하고 이를 위임자의 이름과 묶어 서명을 한 인증서이다[7]. 다단계 대리 서명 시 다단계의 위임이 이루어지면 대리 서명자의 신원 확인은 필수적인 보안 요소가 되며, 위임 인증서 내에 대리인의 권한의 한계를 규정하여 위임 인증서의 사용에 명백한 제한을 가하는 요소가 필요하다.

이와 같은 위임 인증서는 대리 서명자에 대한 여러 가지 정보를 담은 문서에 위임자가 서명을 함으로써 발급된다. 대리 서명자의 정보를 담은 부분에 위임 인증서의 유효기간이나 대리서명자의 자격 요건 등 위임자가 원하는 권한 위임에 대한 제한 조건을 담아서 대리 서명자의 서명 능력을 제한할 수 있다[6]. 실생활에서 권한의 위임은 자주 일어나고 있으며 이를 위해서 대리 서명도 앞으로 반드시 필요한 정보 보호 서비스 중 하나가 될 것이다.

위임인증서의 구조는 그림 2와 같다[7].

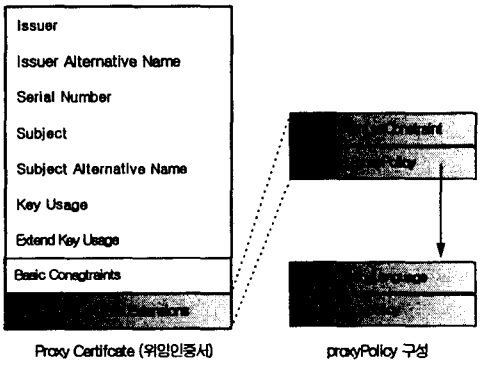

그림 2: Proxy Certificate 구성

위임 인증서의 확장영역의 ASN.1의 표기는 아래 표 1과 같다.

표 1: 위임 인증서 확장자 ASN.1 정의

```
ProxyCertInfo ::= SEQUENCE {
        pCPathLenConstraint     INTEGER
        (0..MAX) OPTIONAL,
        proxyPolicy             ProxyPolicy
        }

ProxyPolicy ::= SEQUENCE {
        policyLanguage      OBJECT
        IDENTIFIER,
        policy              OCTET STRING
        OPTIONAL
        }
```

IV. 제안 방식

본 논문에서는 Tuecke가 제안한 위임 인증서에 원 서명자의 정보를 추가적으로 삽입하여 위임 인증서를 재구성함으로써 원 서명자가 추후 확인이 가능하도록 하는 프로토콜을 설계하여 위임 부인을 방지하고 원 서명자 및 대리 서명자를 동시에 보호할 수 있는 다단계 대리 서명 방식을 제안하였다.

본 논문에서 제안하는 프로토콜 표기법은 표 2와 같다.

표 2: 프로토콜 표기법

표기법	
p, q	$q \mid p-1$ 을 만족하는 큰 소수
g	위수가 q인 Z_p상의 원소
x_i	각 대리자의 비밀키
y_i	각 대리자의 공개키
h	해쉬함수
pC	위임 인증서(proxy certificate)
$SIG_{u_i}(\ )$	U_i가 수행하는 전자서명
$Ver(Sig_{u_i}(\ ))$	U_i의 서명에 대한 검증

1. 대리 서명용 키 생성

원 서명자 U_0는 아래와 같이 대리 서명용 키를 생성하여 대리 서명자 U_1에게 전송한다.

1) U_0는 난수 $k_0 \in Z_{p-1}$을 선택한 후

$K_0 \equiv g^{k_0} \pmod{p}$를 계산한다.

2) U_0는 자신의 서명정보와 대리 서명자의 정보가 포함된 위임 인증서 pC_0와 K_0을 가지고 $e_0 \equiv h(pC_0, K_0) \pmod{q}$을 계산한다.

3) U_0는 대리 서명용 키

$s_0 \equiv x_0 e_0 + k_0 \pmod{q}$를 계산한다.

4) U_0는 s_0, e_0, pC_0를 안전한 채널을 통해 U_1에게 전송한다.

i번째 대리 서명자 $U_i\ (i>0)$가 다른 대리 서명자 U_{i+1}에게 원 서명자 U_0의 서명 생성 능력을 위임하고자 한다면 다음 단계를 수행한다.

1) U_i는 난수 $k_i \in Z_{p-1}$를 선택한 후

$K_i \equiv g^{k_i} \pmod{p}$를 계산한다.

2) U_i는 $e_i \equiv h(pC_0 \| pC_1 \| \ldots \| pC_i, K_i)$

$\pmod{q}$를 계산한다.

이 때 이전에 받은 $pC_0, pC_1, \ldots, pC_{i-1}$의 내용과 pC_i를 연결하여 해쉬함수를 적용한다.

3) U_i는 대리 서명 생성 키

$s_i \equiv s_{i-1} + x_i e_i + k_i \pmod{q}$를 계산한다.

4) U_i는 $s_i, (e_0, e_1, \ldots, e_i), (pC_0, pC_1, \ldots pC_i)$를 U_{i+1}에게 전송한다.

2. 대리 서명용 키 검증

대리 서명자 U_i는 U_{i-1}에게 받은 정보와 U_{i-1}의 공개키 y_{i-1}와 대리 서명용 공개키를 이용하여 다음과 같이 대리 서명용 키를 검증한다.

1) $e_{i-1}' \equiv h(pC_0 \| pC_1 \| \ldots \| pC_{i-1}, K_{i-1})$를 계산한 후 e_{i-1}과 같은지 확인한다.

2) 위 식이 성립하면

$g^{s_{i-1}} \equiv y_0^{e_0} y_1^{e_1} \ldots y_{i-1}^{e_{i-1}} K_0 K_1 \ldots K_{i-1}$

$\pmod{p}$를 확인한다.

위 식이 검증되면, U_i는 U_0의 대리 서명용 키 s_i, r_i를 생성할 수 있다. 여기에서 r_i는 서명키이고, s_i는 다른 대리인에게 보내는 대리 서명용 키이다.

$r_i \equiv s_{i-1} + e_{i-1} x_i \pmod{q}$

3. 서명 생성 및 검증

U_i는 일반적인 서명 방식을 이용하여 $SIG_{U_i}(m, r_i)$대리 서명을 생성할 수 있다. 또한 이 서명을 받은 검증자도 다음 식과 대리 서명 공개키를 검증할 수 있다.

$$R_i \equiv g^{r_i} \pmod{p}$$

$$\equiv y_0^{e_0} y_1^{e_1} \cdots y_{i-1}^{e_{i-1}} K_0 K_1 \cdots K_{i-1} \pmod{p}$$

그리고 $Ver(Sig_{U_i}(m, r_i), R_i)$을 이용하여 대리 서명을 검증할 수 있다.

4. 원 서명자 대리 서명 확인

최종 대리 서명자는 위임 인증서의 원 서명자 정보를 이용하여 원 서명자에게 대리 서명한 정보를 보냄으로서 원 서명자가 추후 서명 결과에 대한 정보를 확인할 수 있다.

V. 결론

본 논문에서는 위임 인증서를 이용한 다단계 대리 서명 방식을 제시하여 원 서명자의 위임 부인을 봉쇄함으로써 원 서명자 및 대리 서명자를 보호할 수 있는 프로토콜을 제안하였다.

김소진[5]에서 제시된 보증서를 이용한 방식은 공개기관의 인증서 방식의 표준을 따르지 않으므로 부인 방지 및 정보 보호 등의 책임을 사설기관이 져야 하며 다단계로 확장시 보증서 보관에 대한 문제점들이 발생할 수 있다. 위임인증서를 이용한 다단계 대리서명 방식은 이러한 발생 가능한 문제점 등을 해결하여, 보다 강력한 위임 부인봉쇄가 가능하게 된다.

또한, 위임 인증서에 원 서명자 정보를 추가하여 구성함으로써 원 서명자가 사후 자신이 위임했던 서명에 대한 정보 확인이 가능하게 된다. 이를 통해 원 서명자의 서명에 대한 보호 및 대리 서명자의 보호가 가능하게 된다.

참고문헌

[1] M.Mambo, K.Usuda, and E.Okamoto, "Proxy signature : Delegation of the power to sign message", IEICE Transaction on Fundamentals, vol.E79-A, no.9, pp.1338~1354, 1996.

[2] M.Mambo, K.Usuda, and E.Okamoto, "Proxy signature for delegating signing operation", Proc. Third ACM Conf. on Computer and Communications Security, pp.48~57, 1996.

[3] S.J. Kim, S.J. Park and D.H. Won, "Proxy signatures, revisited", Proc. of ICICS'97, LNCS 1334, pp.223~232, 1997.

[4] Shunsuke Araki and Kyoki Imamura, "An application of Mambo-Usuda-Okamoto Proxy Signature Schemes", Proc. of ISITA, 2000.

[5] 김소진, 이명희, 최재귀, 박지환, "대리 서명 방식의 확장에 관한 연구", 한국멀티미디어학회 춘계발표논문지, 제5권, 제1호, pp.844~848, 2002.5.

[6] 조상래, 이정연, 진승헌, 김태성, "위임 인증서를 이용한 대리 서명 기술", 한국정보과학회추계발표논문지, 제29권, 제2호, pp.676~678, 2002.10.

[7] S.Tuecke, D.Engert, I.Foster, "Internet X.509 Public Key Infrastructure Proxy Certification Profile", Internet Draft draft-ietf-pkix-05.txt, Feb.2003.