# 법인의 대리서명을 위한 위임 인증서 기술

조상래, 김태성, 진승헌

*한국전자통신연구원 인증기반연구팀

# Proxy Signature for a Corporate using Proxy Certificate Technology

Sangrae Cho Taesung Kim Seunghun Jin

*Certification Infrastructure Research Team, Electronics and Telecommunications Research Institute

## 요 약

법인에서 권한의 위임을 통한 대리 서명은 이미 오프라인에서 널리 사용되고 있다. 이러한 대리 서명을 온라인 상에서 사용하기 위해서는 법인은 위임자에게 위임 인증서를 발급하고 위임자는 그 인증서로 대리서명을 하여 온라인 상에서 업무를 수행할 수 있다. 그러나 이러한 기술을 사용하기 위해서는 위임자의 권한 위임장이 위 변조와 오남용의 위험으로부터 안전하게 보호되어야 한다는 요구 사항이 먼저 만족 되야 하는 필요성이 있다. 위임 인증서는 안전한 대리 서명을 효과적으로 달성하기 위해 등장하였으며 현재 여러 가지 응용 서비스가 제안되고 있다. 본 논문에서는 법인이라는 특수한 환경에서 위임 인증서를 이용하여 안전한 대리서명을 사용할 수 있는 기술과 방법을 제안한다.

## I. 서론

한 법인에게 발급되는 인증서는 여러 응용에 서명 또는 인증을 하는 데 사용된다. 법인의 경우 입찰을 하거나 금융거래 또는 타 법인과의 상거래 등 모든 온라인 상에서의 거래에 서명을 필요로 한다. 그러나 실제 법인에게 발급된 인증서는 그 법인에 속한 직원들이 사용하고 있는데 이 경우 권한을 위임하기 위해서는 인증서와 비밀키를 직접 직원에게 전달하여 전자 거래에 서명하도록 하는 방법을 사용하고 있다. 이러한 방법은 직원들에게 인증서가 가지고 있는 모든 권한을 위임하는 의미를 내포하고 있어 보안상 많은 문제점을 가지고 있다 [1].

이러한 문제점들 중 가장 심각한 것은 법인의 인증서를 직원에게 대여함으로써 발생할 수 있는 인증서와 비밀키의 오남용을 막기가 힘들다 것이다. 또한 대리 서명 후 직원의 부인 방지를 막을 수 없고 해당 직원은 제삼자에게 원 위임자의 동의 없이 인증서와 비밀키를 알려 줌으로서 대리 서명 능력을 갖게 할 수 있다. 그리고 마지막으로 수많은 직원에게 대여되는 비밀키 자체의 노출이 늘어남에 따라 키의 안전성에 심각한 문제가 발생할 수 있다.

최근에는 이러한 문제점을 극복하기 위해 공개키 인증서를 가진 법인이 각 구성원이 위임받을 수 있는 권한에 대해 규정하고 이를 자신의 공개키로 서명함으로써 위임 인증서를 발급하여 대리 서명을 사용할 수 있는 방법에 관한 연구가 활발히 진행되고 있다 [5].

그러나 실제 위임 인증서를 이용하여 대리서명의 권한을 제한하기 위해서는 정책 언어의 연구가 필요하고 위임 추적을 효과적으로 구현할 수 있는 기술이 필요하다. 본 논문에서는 이러한 기술이 어떻게 응용 환경에서 구현되어 적용될 수 있는지에 대하여 간단한 권한을 제한할 수 있는 구조와 위임 추적에 필요한 프로토콜을 제안한다.

이 논문의 구성은 다음과 같다. 먼저 II 장에서는 위임 인증서 정의와 대리서명의 사용 시 요구되는 보안 기능에 관하여 정의하고 대리 서명 기술의 핵심인 위임 인증서의 사용법 제한과 권한 위임의 제한 기술 등을 알아보고 III에서는 실제 위임 인증서를 이용하여 II에서 제시한 보안 요구사항을 만족시키는 메커니즘에 관하여 제안하고 IV에서는 결론을 내린다.

## II. 위임 인증서

## 1. 법인용 위임 인증서의 정의

위임 인증서는 다음과 같은 성질을 가진 X.509 공개키 인증서이다 [5] 그러나 본 논문에서는 법인용 위임 인증서를 위해 실제 위임 인증서의 범위를 재 정의한다.

법인용 위임 인증서는 인증기관에서 발급한 공개키 인증서에 의해 서명되어 발급된다. 즉 공개키 인증서를 가진 법인에 의한 대리서명 권한 위임이 이루어진다. 법인의 경우에는 위임자가 발급된 위임 인증서로 위임자가 정한 대리 서명자의 자격 요건이나 서명 권한 내에서 또 다른 대리 서명자를 정하여 위임 인증서를 발급하는 것을 제한한다. 위임 인증서는 독립적인 별도의 공개키와 비밀키를 가지고 있다. 대리 서명자는 인증기관에 의해 발급된 인증서에 명시된 키와 구분되는 위임 인증서만을 위한 키 쌍을 생성하여야 한다. 위임 인증서는 그 자신만을 위한 실체를 갖지 않는다. 위임 인증서는 이미 인증기관에 의해 발급된 인증서를 가진 실체에게 서명의 권한만을 주기 위해 발급되는 인증서이다. 따라서 위임 인증서에 대한 인증이 끝난 후에는 대리 서명자는 그에게 주어진 권한 내에서 위임자의 역할을 하는데 한정하여 사용된다.

이와 같은 위임 인증서는 대리 서명자에 대한 여러 가지 정보를 담은 문서에 위임자가 서명을 함으로서 발급된다. 대리 서명자의 정보를 담은 부분에 위임 인증서의 사용 용도나 대리 서명자의 자격 요건 등 위임자가 원하는 권한 위임에 대한 제한 조건을 담아서 대리 서명자의 서명 능력을 제한할 수 있다.

## 2. 대리서명의 보안 요구 사항

위임 인증서는 아래에 소개되는 다음과 같은 보안 요구 사항을 만족시키도록 설계되어야 한다.

강한 위조방지는 법인에 의해 지명된 대리인만이 유효한 서명을 생성할 수 있어야 한다. 또한 법인이나 제 3자는 대리인을 가장하여 유효한 서명을 생성할 수 없어야 한다.

검증가능성 및 확인은 서명 검증자는 대리 서명으로부터 위임자의 서명 권한 위임에 대한 동의를 확인할 수 있어야 하며 선택적으로 대리 서명자의 신원을 확인할 수 있어야 한다.

강한 부인방지는 대리 서명자는 유효한 대리 서명의 생성 후 서명한 사실에 대한 부인 거부를 할 수 없어야 한다.

오남용 방지는 위임자가 발급한 위임 인증서는 위임자가 정한 인증서의 사용 범위 내에서 사용되어야 한다.

첫 번째와 세 번째의 보안 요구사항을 만족시키기 위해서는 각 위임 인증서마다 새로운 공개키와 개인키 쌍이 생성되어야 한다. 새로운 키 쌍을 생성하지 않고 단순한 권한의 위임만을 사용하였을 경우 대리인의 공개키 인증서에 명시된 키의 사용 목적에 대한 서술이 모든 서명에 명시되어야 하는 불편함이 있다. 또한 이미 서명된 임의의 문서에 대하여 위임자의 동의 없이 위임 인

```
EtriPolicyLanguage ::= SEQUENCE {
    period          [0] EtriPeriod OPTIONAL,
    usage           [1] EtriUsage OPTIONAL,
    targetApplication   [2] GeneralNames OPTIONAL
}

EtriPeriod ::= SEQUENCE {
    notBefore INTEGER (0..MAX),
    notAfter  INTEGER (0..MAX)
}

EtriUsage ::= SEQUENCE OF IA5String
```

그림 1 정책 구조 정의

증서를 발급하여 위임자를 대리인으로 만들이 버리는 경우가 발생할 수 있다.

두 번째 보안 요구 사항은 위임 인증서 내에 위임자의 서명의 필요성을 지적하는 부분이다. 법인의 경우 대리 서명자의 신원 확인은 필수 보안 요구 사항이 된다.

네 번째 보안 요구 사항은 위임 인증서 내에 대리인의 권한의 한계를 규정하여 위임 인증서의 사용에 있어서 명백한 제한을 가하는 영역의 필요성을 제시한다. 사실상 이 영역의 활용이 위임 인증서를 이용한 응용 서비스 개발의 출발선이 된다.

## 3. 위임 인증서의 확장자

기존 공개키 인증서에 없고 위임 인증서에만 사용하는 확장자는 ProxyCertInfo와 DelegationTracing 확장자가 있다. 전자는 인증서가 위임 인증서인지를 확인시키고 그것의 사용에 발급자가 어떠한 제한을 설정했는지를 보여주는 확장자이며 후자는 위임 인증서를 발급 받은 대리 서명자에 대한 정보와 특별한 경우에는 위임 인증서의 사용자가 위임 인증서를 발급 받는데 동의하였다는 증거로도 사용된다. 이 두 확장자의 내용이 위임 인증서의 대부분의 특징을 규정하며 앞에서 언급한 보안 요구사항을 만족시킨다.

ProxyCertInfo 확장자는 인증서가 위임 인증서이면 반드시 설정되어야 한다. 이 확장자 내의 proxyRestriction 필드는 위임 인증서 사용을 제한하는 내용을 policy라는 필드에 담으며 이 경우 확장자는 critical로 설정된다. policy 필드는 위임 인증서의 사용용도, 또는 특정 사용 가능 시간 등을 설정하여 서명 확인 시 대리 서명이 이 필드가 제한하고 있는 내용의 범위 내에서 대리 서명이 이루어 졌는지 확인하여 유효성을 판단할 수

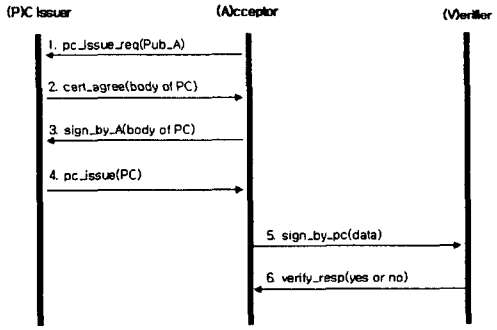


그림 2 위임 추적을 위한 프로토콜

있다. 이러한 ProxyCertInfo의 기능은 위임 인증서의 오남용을 방지하는 것이 주목적이다. 서명자와 검증자는 policyLanguage가 정하는 원칙에 따라 policy 필드를 해석하여 적용하기 때문에 policy 필드에는 반드시 정형화된 언어로 표현된 명확한 정책을 사용해야 응용 시스템간의 혼동을 막을 수 있다. 서명 검증자는 proxyRestriction을 이용하여 대리인이 대리인으로서 서명한 전자 서명들에 대하여 정당성을 검증한다. 검증자는 이 필드 안에 있는 정책을 분석하고 대리인의 서명이 정책에서 정의하고 있는 범위 내에서 사용됐는지 확인한다.

X.509DelegationTrace 확장자를 가지고 있는 인증서는 반드시 위임 인증서이어야 하며, 위임 인증서에 따라 이 확장자는 없을 수 있지만 발급자가 위임 인증서인 경우에는 반드시 이 확장자를 가지고 있어야 한다. 법인의 경우에는 이 확장자에 대리인이 자신의 인증서에 대응하는 비밀키를 사용하여 서명한 값과 이것을 검증자가 검증할 때 필요한 정보를 함께 담고 있다. 이 정보는 위임 인증서를 추적하는데 사용된다. 이 확장자는 위임 인증서를 발급 받을 때 사용한 인증서의 소유주만이 대리 서명을 해야 검증자가 서명을 검증할 수 있는 기능을 부여함으로써 강한 위조방지와 부인 방지 보안 요구 사항을 만족시키고 있고 또한 검증자가 위임자가 권한의 위임에 대한 동의 여부와 위임자의 신원을 확인함으로써 검증 가능성의 항목을 만족한다.

## Ⅲ. 정책과 위임 추적 메커니즘

### 1. 정책 구조 정의

정책은 일반적으로 구조화되고 정형화된 형태도 있지만 대부분의 경우에는 일정한 규칙에 의한 자연어로 정의가 되는 것이 일반적이다. 이러한 자연어의 성격을 갖는 정책을 시스템에 표현하기 위해서는 일반적으로 별도의 언어를 정의하여 사용하여 서로 다른 응용들 간에도 정책을 이해하고 적용하는 것이 일반적인 방법이다. 그러나 정책을 위한 언어를 별도로 개발하는 것은 많은 시간의 연구가 필요하고 본 프로젝트 연구 초기 단계에 있어서 프로토타입을 구현하여 권한을 제한하는 방법을 보여주기 위하여 간단한 정책을 ASN.1으로 정의하여 실제 사용 예를 보여준다.

그림 1을 참조하면 권한을 제한하기 위해서 세 개의 정책 필드를 정의하고 있다. 첫 번째는 period로 위임 인증서로 대리서명을 했을 때 응용 서버에서 서명한 데이터를 정해진 시간 안에 받았을 때만 유효한 것으로 인정한다. 응용 서버는 정책 구조를 검증할 때 서버의 현재 시간이 period에서 정의하고 있는 시간 내에 있는지를 확인하여 대리인의 위임 인증서 사용 시간을 제한한다. 두 번째 usage는 대리서명의 용도를 설정하는 것으로 인감증명서의 용도와 같은 역할을 한다. 예를 들면 usage에 입찰용이면 응용 서버가 입찰을 받는 서버일 경우에만 사용할 수가 있다. 이 경우에는 응용 서버의 검증 모듈에 입찰용 위임 인증서만을 수용한다는 정보가 설정되어야 한다. 마지막 세 번째는 targetApplication으로 위임 인증서가 사용 될 수 있는 응용 서버를 제한할 수 있다. 이 정책은 같은 용도이지만 정해진 서버에서만 사용할 수 있게 하여 위임 인증서의 범위를 제한한다.

향후에 정책언어는 보다 정교하게 XML과 같은 국제적으로 인정하고 호환성을 갖는 표준을 이용하여 정의하여 상호호환성을 높일 수 있다.

### 2. 위임 추적 메커니즘

위임 인증서에서 위임자가 대리인에게 권한을 위임하기 위해서는 위조 방지 및 부인 방지를 보장해주는 방법이 필요한데 이장에서는 위임 추적 메커니즘을 이용하여 위임 인증서 어떻게 이러한 것을 보장해 주는지 알아본다.

그림 2에서 A는 위임자 P에게 자신의 위임 인증서용으로 생성한 공개키를 보내서 발급 신청을 한다. P는 위임 인증서의 본체를 서명하기 전에 A에 보내서 발급할 위임 인증서의 내용에 대해 A의 동의를 구한다. A는 동의하면 자신의 일반 인증서의 개인키로 본체를 서명하고 P에게 자신의 인증서와 같이 보낸다. P는 A의 인증서를 검증하여 A의 신원을 확인하고 보내온 서명을 인증서로 확인하여 A가 위임 인증서 발급에 동의하였음을 확인하고 A에게 위임 인증서를 발급한다.

A는 발급 받은 위임 인증서로 데이터를 서명하여 V에 전달하면 V는 위임 인증서를 검증하고 또한 위임 인증서 내의 A가 서명한 부분을 검증하여 A만이 사용이 가능한 위임 인증서라는 것을 확인하고 또한 A가 위임 인증서를 발급 받는데 동의한 동일한 사람이라는 것을 확인하고 마지막

으로 권한 제한을 확인 다음 A에게 결과를 보내준다. 이 프로토콜은 V가 A만이 위임 인증서를 사용하여 서명하였다는 즉 위조 방지의 가능성을 배제 시켜주고 거래가 성립된 후에도 A가 부인하는 것을 방지하여 준다.

## Ⅳ. 결 론

법인이 전자 상거래에서 기존의 인증서를 이용하여 대리 서명 기술을 안전하게 사용하기 위해서는 무엇보다도 대리인의 서명 권한을 명확하게 정의하고 시스템 적으로 제한할 수 있는 기술이 필요하다. 이러한 기술의 뒷받침 없이 대리서명을 사용한다는 것은 보안상의 많은 문제점을 발생시킨다. 본 논문에서는 [5] 에서 제안한 위임 인증서 프로파일을 이용하여 효율적인 대리서명의 권한 제한을 사용하는 방법과 위임 추적 프로토콜을 제안하여 실제 응용에서 어떻게 위임 인증서가 사용될 수 있는 지를 제시한다.

향후에는 권한을 보다 효율적으로 제한할 수 있는 정책언어의 연구를 통하여 대리서명을 활성화시킬 수 있는 방향을 모색하고 이러한 연구를 바탕으로 시스템을 구현하는 것이 이 프로젝트의 목적이다.

## 참고문헌

[1]. L. Pearlman, V. Welch, I. Foster, C. Kesselman, S. Tuecke., A Community Authorization Service for Group Collaboration. Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

[2]. Butler, R., D. Engert, I. Foster, C. Kesselman, and S. Tuecke, "A National-Scale Authentication Infrastructure," IEEE Computer, vol. 33, pp. 60-66, 2000.

[3]. Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization," Internet Draft draft-ietf-pkix-ac509prof-06.txt, January 2001.

[4]. Housley, R., W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," Internet Draft draft-ietf-pkik-new-part1-12.txt (update to RFC 2459), January 2002.

[5]. S. Tuecke, D. Engert, I. Foster, " Internet X.509 Public Key Infrastructure Proxy Certificate Profile" Internet Draft draft-ietf-pkix-proxy-02.txt, August 2002.