위임 인증서를 이용한 대리 서명 기술

조상래[0] 이정연 진승헌 김태성
한국전자통신연구원 인증기반연구팀
(sangrae[0], ljy63526, jinsh, taesung)@etri.re.kr

Proxy Signature Technology using Proxy Certificate

Sangrae Cho[0] Jung-Yeun Lee Seunghun Jin Taesung Kim
Electronics and Telecommunications Research Institute

요 약

실생활에서 권한의 위임을 통한 대리 서명은 일상적으로 널리 사용되고 있다. 이러한 대리 서명을 온라인 상에서 사용하기 위해서는 위임자의 권한 위임장이 위 변조와 오남용의 위험으로부터 안전하게 보호 되어야 한다. 위임 인증서는 안전한 대리 서명을 효과적으로 달성하기 위해 등장하였으며 현재 여러 가지 응용 서비스가 제안되고 있다. 위임 인증서는 대리 서명자가 대리 서명을 위한 키 쌍을 생성하고 이를 위임자의 이름과 묶어 서명을 한 인증서이다. 위임자는 이 인증서 내에 대리 서명자를 지정할 수 있으며 대리 서명자의 서명 권한을 제한할 수 있다. 본 논문은 이러한 위임 인증서를 이용하여 안전한 대리 서명을 지원할 수 있는 기술을 제안한다.

1. 서 론

한 기업체에게 발급되는 인증서는 여러 응용에 서명 또는 인증을 하는 데 사용된다. 하지만 실제 조직에게 발급된 인증서는 그 조직에 속한 직원들이 사용하고 있는데 이 경우 권한을 위임 하기 위해서는 인증서와 비밀키를 직접 직원에게 위임하여 전자 거래에 서명하도록 하는 방법을 사용하고 있다. 이러한 방법은 직원들에게 인증서가 가지고 있는 모든 권한을 위임하는 의미를 내포하고 있어 보안상 많은 문제점을 가지고 있다.

가장 큰 문제점은 조직의 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 비밀키 자체의 노출이 늘어남에 따라 안전성에 심각한 문제를 야기할 수 있다.

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 있는데 이때 사용되는 인증서를 위임 인증서라고 부른다[5].

위임 인증서의 사용에 있어서 대리인은 위임 인증서를 발급 받음과 동시에 위임자가 규정한 범위 내에서 제 3자에게 위임자로 인증 받을 수 있다. 특히, 위임자는 대리인의 사내의 지위나 역할을 고려하여 권한을 제한 할 수 있기 때문에 앞에서 언급한 문제들을 해결할 수 있다.

이 문서에서는 또한 수직적인 권한의 위임뿐만 아니라 수평적인 권한의 위임이 가능한 위임 인증서를 이용한 방법을 구체적으로 살펴본다.

이 문서의 나머지 부분은 다음과 같은 순서로 정리되어 있다. 먼저 2 장에서는 위임 인증서 정의를 소개하고 3 장에서는 위임 인증서의 사용시 요구 되는 보안 기능에 관하여 언급한다. 4 장에서는 대리 서명 기술의 핵심인 위임 인증서의 사용법 제한과 권한 위임의 제한 기술 등을 알아 보고 5장에서는 결론을 내린다.

2. 위임 인증서의 정의

위임 인증서는 다음과 같은 성질을 가진 X.509 공개키 인증서이다.

1. 인증기관에서 발급한 공개키 인증서나 이미 발급된 위임 인증서에 의해 서명된다. 즉 공개키 인증서를 가진 위임자에 의한 서명 권한 위임과 위임 인증서를 가진 대리 서명자에 의한 또 다른 대리 서명자로의 서명 권한 위임 시 생성된다.
2. 다른 위임 인증서에 서명하는데 사용될 수 있다. 발급된 위임 인증서는 위임자가 정한 대리 서명자의 자격 요건이나 서명 권한 내에서 또 다른 대리 서명자를 정하여 위임 인증서를 발급함으로써 위임이 가능하다.
3. 위임 인증서는 독립적인 별도의 공개키와 비밀키를 가지고 있다. 대리 서명자는 인증기관에 의해 발급된 인증서에 명시된 키와 구분되는 위임 인증서만을 위한 키 쌍을 생성하여야 한다.
4. 위임 인증서는 그 자신만을 위한 실체를 갖지 않는다. 위임 인증서는 이미 인증기관에 의해 발급된 인증서를 가진 실체에게 서명의 권한만을 주기 위해 발급되는 인증서이다. 따라서 PC에 대한 인

증이 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 유효 기간이나 대리 서명자의 자격 요건 등 위임자가 원하는 권한 위임에 대한 제한 조건을 담아서 대리 서명자의 서명 능력을 제한할 수 있다.

먼저 현재 발급되어 사용되고 있는 공개키 인증서(PKC) 내에 소유주의 권한을 삽입하는 것이 활발히 논의 되었으나 이 방법의 사용은 다음과 같은 문제점이 있는 것으로 파악 되고 있다.

- 권한에 대한 정보의 유효 기간과 공개키의 유효 기간이 서로 다르다는 것이다. 일반적으로 권한에 대한 정보의 유효 기간이 공개키의 그것보다 짧아서 공개키의 유효 기간을 단축시키는 단점이 있다.
- 공개키 인증서의 발급자는 일반적으로 각 소유주의 사내 또는 공동체에서 가지는 권한을 직접 담당하지 않기 때문에 공개키 인증서 발급 당시에 권한의 명시는 여러 가지 부작용을 낳을 수 있다.

3. 위임 인증서의 보안 요구 사항

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

1. Strong unforgeability
   위임자에 의해 지명된 대리인만이 유효한 서명을 생성할 수 있어야 한다. 또한 위임자나 제 3자는 대리인을 가장하여 유효한 서명을 생성할 수 없어야 한다.
2. Verifiability
   검증자는 대리 서명으로부터 위임자의 서명 권한 위임에 대한 동의를 확인할 수 있어야 하며 선택적으로 대리 서명자의 신원을 확인할 수 있어야 한다.
3. Strong undeniability
   대리 서명자는 유효한 대리 서명의 생성 후 서명한 사실에 대한 부인 거부를 할 수 없어야 한다.
4. Prevention of misuse
   위임자가 발급한 위임 인증서는 위임자가 정한 인증서의 사용 범위 내에서 사용되어야 한다.

첫 번째와 세 번째의 보안 요구사항을 만족시키기 위해서는 각 위임 인증서 마다 새로운 공개키와 개인키 쌍이 생성 되어야 한다. 새로운 키 쌍을 생성하지 않고 단순한 권한의 위임 만을 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 인증서를 발급하여 위임자를 대리인으로 만들어 버리는 경우가 발생할 수 있다.

두 번째 보안 요구 사항은 위임 인증서 내에 위임자의 서명의 필요성을 지적하는 부분이다. 다단계의 위임이 이루어 지면 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.

4. 위임 인증서 확장자

기존 공개키 인증서에 없고 위임 인증서에만 사용하는 확장자는 ProxyCertInfo와 DelegationTracing 확장자가 있다. 전자는 인증서가 위임 인증서 인지를 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 동의 하였다는 증거로도 사용된다. 이 두 확장자의 내용이 위임 인증서의 대부분의 특징을 규정하며 앞에서 언급한 보안 요구사항을 만족시킨다.

표 1을 참조 하면 ProxyCertInfo 확장자는 인증서가 위임 인증서이면 반드시 설정 되어야 하며 확장자의 내부 필드인 pC에 True라고 표시를 한다. proxyRestriction 필드는 위임 인증서 사용을 제한하는 내용을 policy 필드에 담으며 이 경우 확장자는 critical로 설정된다. policy 필드는 위임 인증서의 사용 용도, 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 있다. 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 proxyRestriction 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 인증서 이어야 하며, 위임 인증서에 따라 이 확장자는 없을 수 있지만 발급자가 위임 인증서인 경우에는 반드시 이 확장자를 가지고 있어야 한다. 이 확장자에서는 대리인이 자신의 인증서의 공개키에 대응하는 비밀키를 사용하여 서명한 값과 이것을 검증자가 검증할 때 필요한 정보를 함께 담고 있다. 이 정보는 위임 인증서를 추적하는데 사용된다. X.509DelegationTrace의 구조는 두 개의 필드로 구성되어 있다. 하나는 agreedCertInfo 필드로 발급되는 위임 인증서의 내용을 해쉬한 값을 포함하고 있고 다른 하나는 acceptorInfo 필드로 agreedCertInfo 필드에 대한 대리인의 서명과 서명을 검증하는데 사용되는 정보를 포함한다. agreedCertInfo 필드는 대리인이 발급 받고자 하는 위임 인증서를 묘사하는데 사용되며 다음과 같은 두 개의 필드로 구성되어 있다.

ignoredExtentions은 OID들의 목록으로, 이 목록 안에 있는 OID를 가진 필드의 값은 대리인이 그 인증서를 받아 들일 것인지에 대한 대리인의 의지에 영향을 미치지 않을 것이다. certSubsetHash 필드는 대리인이 받아드리려고 하는 인증서의 TSBCertificate 구조에 대한

해쉬 값이다.

이 필드를 검증할 때 먼저 certSubsetHash 값을 생성할 때와 동일한 TSBCertificate 구조를 만들어 내는 것이 선행되어야 한다. x509AcceptorInfo 필드는 대리인이 자신의 인증서의 공개키에 대응하는 비밀키를 사용하여 agreedCertInfo 값에 서명한 값과 이것을 검증자가 검증할 때 필요한 정보를 함께 담고 있다

```
ProxyCertInfo ::= SEQUENCE {
    version                 INTEGER (0..MAX),
    pC                      BOOLEAN DEFAULT TRUE,
    pCPathLenConstraint     INTEGER (0..MAX) OPTIONAL,
    proxyRestriction        ProxyRestriction OPTIONAL,
    proxyGroup              ProxyGroup OPTIONAL,
    issuerCertSignature     Signature OPTIONAL }

ProxyRestriction ::= SEQUENCE {
    policyLanguage          OBJECT IDENTIFIER,
    policy                  OCTET STRING }

Signature ::= SEQUENCE {
    signatureAlgorithm      AlgorithmIdentifier,
    SignatureValue          BIT STRING }

ProxyGroup :: = SEQUENCE {
    proxyGroupName          OCTET STRING,
    proxyGroupAttached      BOOLEAN DEFAULT TRUE };

DelegationTrace ::= CHOICE {
    x509                    [0]  X509DelegationTrace }

X509DelegationTrace ::= SEQUENCE {
    agreedCertInfo          AgreedCertInfo,
    x509AcceptorInfo        X509AcceptorInfo }

AgreedCertInfo ::= SEQUENCE {
    ignoredExtensions       SEQUENCE OF OBJECT IDENTIFIER,
    certSubsetHash          Hash }

X509AcceptorInfo ::= SEQUENCE {
    acceptorSig             Signature,
    acceptorName            Name,
    acceptorAltName         GeneralName OPTIONAL,
    acceptorCertHash        Signature }

Signature ::= SEQUENCE {
    signatureAlgorithm      AlgorithmIdentifier,
    signatureValue          BIT STRING }
```

표 1. 위임 인증서 확장자 ASN.1 정의

5. 결 론

전자 상거래에서의 대리 서명 기술은 위임 인증서를 사용하여 보다 안전하게 제공할 수 있고 이러한 기술은 전자 입찰과 인터넷 금융 서비스 같은 여러 가지 응용 환경에 적용될 수 있다. 위임 인증서의 활용은 대리 서명 권한을 제한 하는 기술에 그 기반을 두고 있다. 권한 제한 기술은 기본 적으로 정책을 시스템이 이해할 수 있는 언어를 정의하여 사용하는 것이 효율적이며 간단하게는 임의의 특정한 구조체를 정의하여 사용하기도 한다.

향후 연구 방향은 위임 인증서의 전자 상거래에서의 응용 방안에 관하여 중점적으로 연구를 하는 것이다. 위임 인증서의 적용은 실제 환경의 보안 요구사항을 분석하여 이루어지며 정의된 요구사항을 어떻게 만족 시킬 수 있는지 아키텍처를 정의하여 보여줄 수 있다. 위임 인증서에 사용하는 권한 제한 언어 기술에 관한 연구를 병행할 예정이다.

5 참고 문헌

[1]. Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997.

[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.