위임 인증서 발급 및 관리 시스템 구현

김태성 조상래 진승헌

한국전자통신연구원, 인증기반연구팀

Implementation of Issuing and Managing Proxy Certificate

Taesung Kim Sangrae Cho Seunghun Jin

Electronics and Telecommunications Research Institute

요 약

실생활에서 권한의 위임을 통한 대리서명은 일상적으로 널리 사용되고 있다. 이러한 대리서명을 온라인상에서 사용하기 위해서는 위임자의 권한위임장이 안전하게 유통되어야 하고 대리자의 권한 오남용을 막아야 한다. 이에 따라 IETF의 PKIX 워킹그룹에서는 위임인증서(proxy certificate)를 제안하였다.

본 논문에서는 대리자의 권한의 오남용을 막기위해 위임제한 필드를 제안하였고, 위임 인증서의 서비스 가능성을 보이기 위한 프로토타입을 설계하고 구현하였다

I. 서론

PKI(Public Key Infrastructure)는 공개키인증서를 이용하여 전자상거래에서의 기밀성, 무결성, 인증, 부인봉쇄 기능을 제공하는 정보보호 기반구조이다. 공개키 인증서는 현재 금융권의 정보보호에 주로 적용되고 있으나 점차 다양한 분야의 정보보호 기반으로 그 활용이 확산되고 있는 상황이다.[1]

발급되는 인증서는 전자서명을 통하여 사용자를 인증하는데 사용된다. 실생활에서는 해당 개인이 직접 인감 날인을 통하여 계약을 하는 경우도 있지만 위임장을 통하여 대리인에게 계약에 관한 권한을 위임하는 경우도 있다. 이러한 상황을 인터넷 환경에서 수행하기에는 현재의 공개키 인증서만으로는 해결하기 힘든 문제가 있다. 전자서명은 해당 전자서명을 할 수 있는 비밀키를 해당 개인만이 가지고 있다는 가정에서 시작하는데, 현재 상황에서는 대리 서명을 위해서는 자신의 비밀키와 인증서를 대리인에게 제공하고 비밀키를 암호화한 비밀번호를 알려주어야 한다. 이러한 상황은 많은 보안상의 취약점을 내포하고 있다. 또한 응용서버 또는 검증서버에 대리인을 위임자에 권한으로 부여함으로써 위임을 달성할 수 있지만 위임의 상태와 위임 권한의 변경시 마다 서버의 정책을 재설정해야 하는 어려움과 서명에 의한 분쟁이 있을 경우에 책임의 소재가 불분명해지는 문제가 있다. 이러한 기존 인증서 활용의 한계를 극복하고자 IETF PKIX 워킹그룹에서는 위임 인증서 프로파일을 제안하고 있다. 이는 기존 X.509 인증서의 확장 필드 영역에 위임과 관련된 정보를 제공하여 대리 서명에 활용하고자 하는 것이다.[3]

위임 인증서 프로파일은 위임에 관한 기본적인 정보에 대해서는 기술하고 있을 뿐, 실제 환경에 적용시의 절차나 위임 권한을 제한하는 방법에 대해서는 다루고 있지 못하다. 따라서 본 논문에서는 인증서를 이용한 권한 위임시에 권한의 오남용을 막기 위한 동작 메커니즘을 제안하고 프로토타입을 구현함으로써 권한위임 메커니즘의 가능성을 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 위임 인증서의 정의 및 확장에 대해 설명하고 3장에서는 제안된 위임 제한 언어에 대해 기술한다. 4장에서는 위임 인증서의 프로토타입 구현에 대해 설명하고 5장에서 결론을 맺는다.

II. 위임 인증서

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

1. 인증기관에서 발급한 공개키 인증서나 이미 발급된 위임 인증서에 의해 서명된다.

2. 위임 인증서는 독립적인 별도의 공개키와 비밀키를 가지고 있다. 대리 서명자는 인증기관에 의해 발급된 인증서에 명시된 키와 구분되는 위임 인증서만을 위한 키 쌍을 생성하여야 한다.

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

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.

```
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 }
```

[그림 1] 위임 인증서 확장자 ASN.1 정의

[그림 1]을 참조하면 ProxyCertInfo 확장자는 인증서가 위임 인증서이면 반드시 설정되어야 하며 확장자의 내부 필드인 pC에 True라고 표시를 한다. proxyRestriction 필드는 위임 인증서 사용을 제한하는 내용을 policy 필드에 담으며 이 경우 확장자는 critical로 설정된다. policy는 프로파일에서 정의하고 있지 않고 응용에서 개발하여 사용하여야 한다. 이 필드의 실명은 3장에 자세히 설명되어 있다.

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. 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 받아들일 것인지에 대한 대리인의 의지에 영향을 미치지 않을 것이다. certSubsetHash 필드는 대리인이 받아 드리려고 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

III. 위임 제한(Proxy Restriction)

위임 인증서의 확장자중에 하나인 ProxyCertInfo의 ProxyRestriction은 대리 서명자의 권한을 제한하는 필드이다. 위임자는 이 필드에 인증서의 사용용도, 특정 사용시간, 접근 가능한 서버의 리스트 등을 기록하고 검증자는 대리자의 서명이 이 필드의 권한 내에서 이루어 졌는지 검사한다. IETF의 위임인증서 프로파일은 ProxyRestriction 필드를 정의하고 있지 않다. 따라서, 응용분야 별로 특성에 맞고 응용 시스템간 혼동을 막을 수 있는 ProxyRestriction 필드를 위

한 정형화된 언어를 개발해야 한다.

```
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 2] 위임 제한 필드의 ASN.1 정의

본 논문에서는 다양한 응용에서 일반적으로 적용 가능한 ProxyRestriction을 위한 언어를 개발했고 [그림 2]는 이 언어의 ASN.1 표현이다. EtriPolicyLanguage의 period는 하루 중에 대리자가 서명을 할 수 있는 시간이다. 예를 들어 notBefore가 0900이고 notAfter가 1800이면 서명 가능 시간은 오전 9시부터 오후 6시까지 이다. Usage는 전자경매, 전자입찰 , 전자 결재 등 하나 또는 그 이상의 인증서의 사용 용도를 적시하는 필드이다. Target은 위임 인증서를 이용해 접근 가능한 서버의 리스트를 나타내는 필드로서 서버는 URL, DNS, IP등의 하나로 표현할 수 있다.

EtriPolicyLanguage가 실제 응용에서 사용하기 위해서는 특정 응용의 요구에 맞게 수정이 불가피하며 확장성, 유연성, 가독성이 뛰어나고 여러 플랫폼에 많은 파서가 있는 XML도 좋은 후보라 하겠다.

IV. 위임 인증서 프로토타입

본 절에서는 위임 인증서의 서비스 가능성을 보이기 위한 프로토타입의 설계 및 구현에 대해 기술한다. 프로토타입은 위임 인증서의 발급, 대리 서명의 검증, 위임 제한의 검증 등에 초점을 맞추어 구현되었다. 프로토타입은 위임인증서 발급자, 위임인증서 대리서명자 그리고 검증자로 구성된다. 발급자는 유효기간, 발급자, 키 사용용도, 위임제한 등의 정책을 설정하고 위임인증서를 발급하며 발급된 위임인증서를 데이터베이스에 보관한다. 대리자는 인증서 발급을 요청하고, 요청했으나 아직 인증서가 발급되지 않은 키쌍과 발급된 인증서를 보관하며, 발급된 위임인증서로 대리서명을 수행한다. 검증자는 발급자의 인증서를 이용해 위임인증서의 서명을 확인하고 위임인증서 내의 위임 제한을 검증한다. 다음은 위임인증서 발급, 대리서명, 검증의 절차를 나타낸 것이다.

1. 대리자는 위임 인증서를 위한 키 쌍을 생성하고 인증서 발급 요청에 공개키를 포함하여 발급자에게 전송한다.

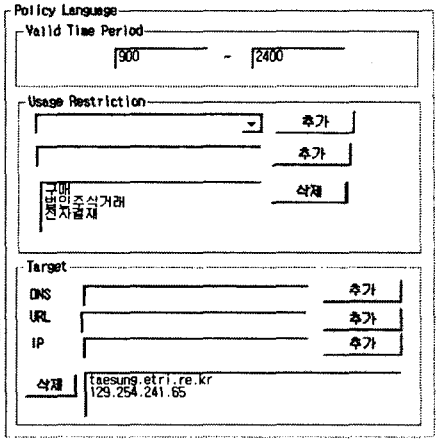
2. 발급자는 정책설정에 맞게 TBSCertificate를 구성한 후 이를 인코딩하여 대리자에게 보낸다.

3. 대리자는 자신의 개인키로 TBSCertificate를 서명하여 응답한다. 2와 3 단계는 위임인증서에 DelegationTrace가 있을 경우에만 수행하는 선택적 단계이다.

4. 발급자는 자신의 개인키로 서명하여 위임인증서를 발급한다.

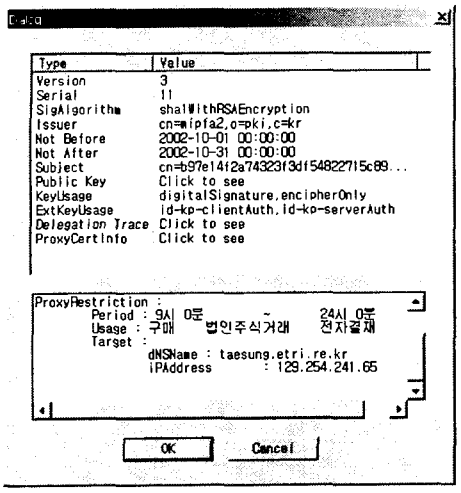
5. 대리자는 위임인증서의 개인키로 메시지를 서명하고 이를 위임인증서와 함께 검증자에게 전송한다.

6. 검증자는 CA 인증서, 발급자 인증서, 위임인증서를 포함하는 인증서 경로를 검증하고, 위임인증서로 서명된 메시지를 검증한다. 또한 위임인증서에 있는 위임 제한을 조사하여 위임인증서의 사용이 적절한지 검사한다.

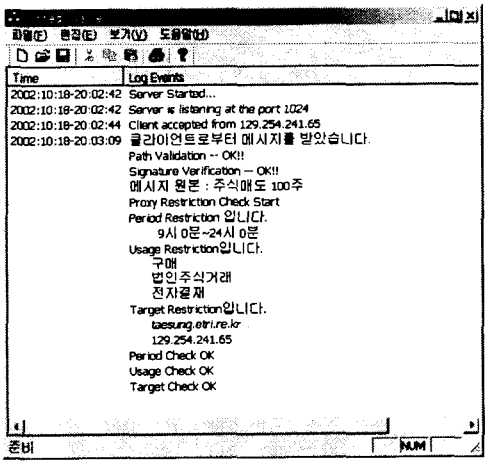


[그림 3] 위임 인증서 발급자의 정책 설정

프로토타입을 법인주식거래 응용을 가정하여 살펴본다. [그림 3]는 발급자의 정책 설정에서 위임 제한 부분을 보인 것이다. 발급될 인증서는 6:00부터 24:00 사이에 사용할 수 있고 구매, 법인주식거래, 전자결재의 용도로 사용해야 하며 Target에 열거된 서버에서만 사용해야 한다. [그림 4]는 정책에 맞게 발급된 위임 인증서를 보인 것이다. [그림 5]는 주소가 129.254.241.65이고 법인주식거래 서버에 대리인이 위임 인증서로 주식거래 내용을 서명하여 서버에 보냈을 때 보여지는 로그이다.



[그림 4] 위임 인증서 보기



[그림 5] 검증자의 로그

V. 결론

본 논문은 전자상거래에서 대리서명이 가능토록 하는 위임 인증서를 설명하였고, 위임 인증서의 위임 제한의 언어를 제안하였으며 또한 위임 인증서 발급 및 검증을 보여주는 프로토타입을 설계하고 구현하였다.

향후 응용 서비스를 위한 보다 유연하고 세부적인 위임 제한 언어의 개발이 필요하고 위임인증서 발급을 위한 완벽한 프로토콜의 개발과 실제 응용의 적용이 필요하다.

참고문헌

[1] 이정현, 진승헌, 정교일 "국내외 PKI 구축 및 시장 동향" 주간기술동향 1008 호, 한국전자통신연구원

[2] 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.

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