위임 인증서를 이용한 권한 위임 메커니즘 설계

진 승 헌[†]·조 상 래[††]·김 태 성[††]·류 재 철[†††]

요 약

실생활에서 권한의 위임을 통한 대리 서명은 일상적으로 널리 사용되고 있다. 이러한 대리 서명을 인터넷상에서 사용하기 위해서는 권한 위임한 내용이 안전하게 전달되어야 한다. 이러한 목적으로 현재 IETF에서는 위임 인증서를 제안하고 있다[5]. 그러나 인터넷상에서의 안전한 대리 서명을 위해서는 대리자가 발급받은 위임 인증서를 가지고 권한을 오남용 하지 않도록 하는 것도 필요하다. 본 논문에서는 위임 인증서를 이용하여 권한의 오남용을 막기 위한 정책제한 필드를 제안하고 안전하게 권한위임 정보를 관리할 수 있는 권한 위임 메커니즘을 설계하였다. 또한 프로토타입 구현을 통하여 위임 인증서를 이용한 대리서명 서비스의 가능성을 보였다.

Design of Privilege Delegation Mechanism using Proxy Certificate

Seunghun Jin[†] · Sangrae Cho[††] · Tae-sung Kim[††] · Jae-cheol Ryou[†††]

ABSTRACT

In real life, we frequently use the proxy signature by delegating one's own privileges. It is necessary to distribute the data related to privilege delegation securely in order to use such a proxy signature in the Internet. However, in order to use the secure proxy signature, we need to have some mechanism to prevent a proxy signer from misusing his delegated privilege with an issued proxy certificate. In this paper, we have proposed a policy restriction field to prevent the misuse of privileges by applying proxy certificate and a privilege delegation mechanism to manage information with related to privilege delegation. In addition, we have implemented the prototype to demonstrate the possible proxy signature service using proxy certificate.

키워드 : PKI(Public Key Infrastructure), Proxy Certificate, 인증서(Certificate), 위임(Delegation)

1. 서 론

PKI(Public Key Infrastructure)는 공개키 인증서를 이용하여 전자상거래에서의 기밀성, 무결성, 인증, 부인봉쇄 기능을 제공하는 정보보호 기반구조이다. 선진국에서는 PKI를 기반으로 전자상거래의 안전성을 확보하려는 연구가 많이 진행되었으며 전자상거래의 정보보호 기반구조로 활용되고 있다[4]. 국내에서도 1999년 7월 전자서명법이 발효되어 PKI를 이용한 정보보호를 위해 법적인 토대가 마련되었으며 2000년 국가공인 PKI 운용 기관인 공인인증기관이 지정되었고 현재 많은 정보보호 산업체들이 PKI에 대한 연구개발을 진행하고 있다. PKI는 현재 금융권의 정보보호에 주로 적용되고 있으나 점차 다양한 분야의 정보보호 기반으로 그 활용이 확산되고 있는 상황이다.

특히 기존에 실생활에서 수행되는 업무나 절차를 인터넷 환경으로 옮겨올 때 발생할 수 있는 보안적인 문제점을 해결하기 위하여 많은 검토가 이루어지고 있다.

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. 이러한 기존 인증서 활용의 한계를 극복하고자 [5]에서는 위임 인증서

† 정 회 원 : 한국전자통신연구원 인증기반연구팀장
†† 정 회 원 : 한국전자통신연구원 정보보호연구본부 인증기반연구팀
††† 종신회원 : 충남대학교 정보통신공학부 교수
논문접수 : 2003년 7월 22일, 심사완료 : 2003년 9월 22일

프로파일을 제안하고 있다. 이는 기존 X.509 인증서의 확장 필드 영역에 위임과 관련된 정보를 제공하여 대리 서명에 활용하고자 하는 것이다. 그러나 이는 위임에 관한 기본적인 정보에 대해서만 기술하고 있을 뿐, 실제 환경에 적용시의 절차나 발생가능한 문제점에 대해서는 다루고 있지 못하다. 그러므로 본 논문에서는 인증서를 이용한 권한 위임과 대리서명 시에 권한의 오남용을 막고 안전한 거래를 하기 위한 위임 인증서의 확장필드의 사용법과 위임 추적 메커니즘을 제안한다. 또한 프로토타입을 구현함으로써 권한 위임 메커니즘의 가능성을 보인다.

본 논문의 구성은 다음과 같다. 위임 인증서의 정의와 위임 인증서의 사용 시 요구되는 보안 기능에 대해서 2장에서 기술하고, 3장에서는 본 논문에서 제시하는 권한 위임 메커니즘에 대해 기술한다. 4장은 위임 인증서 사용 시 요구되는 위임 추적 프로토콜에 대해서 정의하고 안전성 분석을 기술하고 5장에서는 본 논문에서 제안하는 방법을 구현한 프로토타입을 보여준다. 그리고 마지막으로 결론과 향후계획에 대해 기술한다.

2. 위임 인증서

2.1 위임 인증서의 정의

위임 인증서의 기본적인 구조는 X.509 공개키 인증서와 동일하다[4]. X.509 공개키 인증서는 사용자의 이름과 공개키를 제 삼의 신뢰기관이 전자서명하여 발급한 일종의 전자 신분증과 같다. 이러한 인증서에는 일련번호, 사용자의 이름, 유효기간 및 사용자의 공개키가 있고 이것을 비밀키로 전자서명한 서명이 추가된다. 그리고 인증서 정책, 사용용도, 인증기관 표시 정보 등을 표시하기 위해서 추가적으로 인증서에는 확장필드가 사용되는데 위임 인증서도 이러한 확장필드의 활용을 통해 정의된다.

위임 인증서는 X.509 공개키 인증서와는 달리 다음과 같은 특성을 가진다.

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 시에 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 위임 인증서에 대한 인증이 끝난 후에는 대리 서명자는 그에게 주어진 권한 내에서 위임자의 역할을 하는데 한정하여 사용된다.

이와 같은 위임 인증서는 대리서명자에 대한 여러 가지 정보를 담은 문서에 위임자가 서명을 함으로써 발급된다. 대리 서명자의 정보를 담은 부분에 위임 인증서의 유효 기간이나 대리 서명자의 자격 요건 등 위임자가 원하는 권한 위임에 대한 제한조건을 담아서 대리 서명자의 서명 권한을 제한할 수 있다.

현재 발급되어 사용되고 있는 공개키 인증서 내에 소유주의 권한을 삽입하는 것이 활발히 논의되었으나 이 방법의 사용은 다음과 같은 문제점이 있는 것으로 파악되고 있다.

① 권한에 대한 정보의 유효 기간과 공개키의 유효 기간이 서로 다르다는 것이다. 일반적으로 권한에 대한 정보의 유효기간이 공개키의 유효 기간보다 짧아서 공개키의 유효기간을 단축시키는 단점이 있다.

② 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.

2.2 위임 인증서의 보안 요구 사항

위임 인증서는 다음과 같은 보안 요구 사항을 만족시키도록 설계되어야 한다.

2.2.1 강한 위조 방지

위임자에 의해 지명된 대리인만이 유효한 서명을 생성할 수 있어야 한다. 또한 위임자나 제 3자는 대리인을 가장하여 유효한 서명을 생성할 수 없어야 한다.

2.2.2 검증가능성 및 확인

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

2.2.3 부인 방지

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

2.2.4 오남용 방지

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 키쌍을 생성하지 않고 단순한 권한 위임만을 사용하였을 경우에는 대리인이 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 위임자 서명의 필요성을 의미하고 있다. 다단계의 위임이 이루어지면 대리 서명자의 신원 확인은 필수 보안 요구 사항이 된다.

네 번째 보안 요구 사항은 위임 인증서 내에 대리인의 권한 한계를 규정하여 위임 인증서의 사용에 있어서 대리자가 제한된 권한만을 사용하게 하여 위임 인증서가 가질 수 있는 역기능을 최소화 한다.

2.3 위임 인증서의 확장자

(그림 1)은 기존 공개키 인증서에는 없고 위임 인증서에만 사용하는 확장자인 ProxyCertInfo와 DelegationTracing의 ASN.1 구조를 보여준다. 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 인증서인 경우 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 확인시 대리 서명이 이 필드가 제한하고 있는 내용의 범위 내에서 이루어 졌는지 확인하여 유효성을 판단할 수 있게 한다. 이러한 ProxyCert Info의 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 분석하여 대리인의 서명이 정책에서 정의하고 있는 범위 내에서 사용됐는지 확인한다.

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

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

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

ProxyGroup ::= SEQUENCE {
    proxyGroupName          OCTET STRING,
    proxyGroupAttached      BOOLEAN DEFAILT 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

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. 일반 기업 환경에서 사용하는 경우에 이 확장자에는 대리인이 자신의 인증서에

대응하는 비밀키를 사용하여 서명한 값과 이것을 검증자가 검증할 때 필요한 정보를 함께 담고 있어 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 위임자의 권한 위임에 대한 동의 여부와 위임자의 신원을 확인함으로써 검증가능성의 항목을 만족한다.

3. 권한 위임 메커니즘 제안

본 장에서는 권한 위임에 대한 메커니즘을 제안한다.

3.1 위임 인증서 발급 절차

위임 인증서의 발급은 2장에서 기술한 위임 인증서가 갖추어야 할 성질에 맞추어 아래와 같은 발급절차를 따른다.

① 대리 서명자는 대리 서명에 사용할 공개키와 개인키를 생성하여 이중 공개키에 대한 위임 인증서 발급을 위임자에게 요구한다.

② 위임자는 대리 서명키와 대리 서명자의 서명 권한을 포함한 위임 인증서의 내용을 정리한 문서에 자신의 개인키를 이용하여 서명함으로써 위임 인증서를 발급한다.

③ 대리 서명자는 위임자의 공개키 인증서를 이용하여 위임 인증서의 서명을 검증하고 유효성이 확인된 후 자신의 개인키를 이용하여 자신의 서명을 첨부한다.

위의 발급 절차는 위임자가 End Entity인 경우이다. 위임 인증서를 가진 대리 서명자가 위임자로서 새로운 대리 서명자를 정하여 서명 권한을 다시 위임할 수 있으며 그때의 발급 절차도 역시 위와 동일하다.

3.2 정책 구조 정의

ProxyCertInfo 확장자는 기본적으로 위임 인증서의 정책을 담기 위한 구조에 불과하다. 실제 권한 위임에 관한 정책을 사용하기 위해서는 다양한 정책을 표현할 수 있는 일정한 규칙에 의한 자연어로 정의된 정책 언어가 사용되는 것이 일반적이다. 이러한 자연어의 성격을 갖는 정책을 시스템에 표현하기 위해서는 일반적으로 별도의 언어를 정의하여 서로 다른 응용들간에도 정책을 이해하고 적용하는 것이 일반적인 방법이다. 그러나 정책을 위한 언어를 별도로 개발하는 것은 많은 시간의 연구가 필요하여 본 논문에서는 프로토타입을 구현하여 권한을 제한하는 방법을 보여주기 위하여 간단한 정책을 ASN.1으로 정의하여 실제 사용 예를 보여준다.

(그림 2)를 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 target Application으로 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.

```
EtriPolicyLanguage ::= SEQUENCE {
    period              [0] EtriPeriodOPTIONAL,
    usage               [0] EtriUsageOPTIONAL,
    targetApplication   [2] GeneralNamesOPTIONAL.
}

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

EtriUsage ::= SEQUENCE OF IA5String
```

(그림 2) 정책 구조 정의

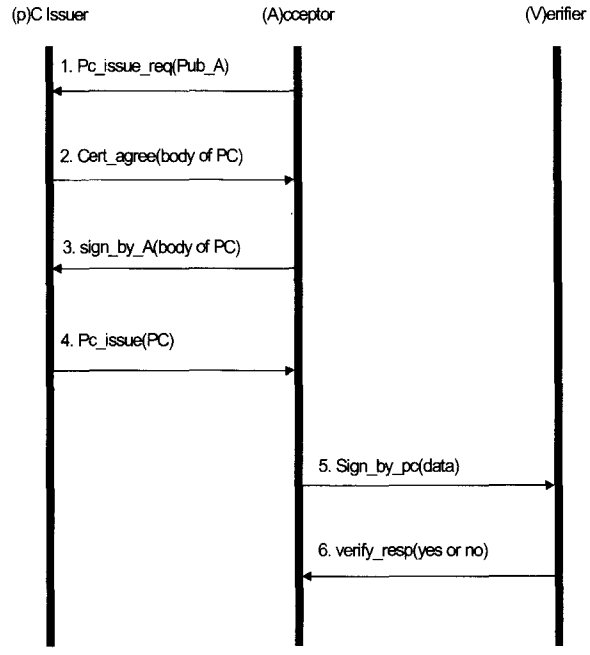
4. 위임 추적 메커니즘

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

4.1 위임 추적 프로토콜 개요

(그림 3)에서 A는 위임자 P에게 자신의 위임 인증서용으로 생성한 공개키를 보내서 발급 신청을 한다. P는 위임 인증서의 본체를 서명하기 전에 A에게 보내서 발급할 위임 인증서의 내용에 대해 A의 동의를 구한다. A는 동의하면 자신의 일반 인증서의 개인키로 본체를 서명하고 P에게 자

신의 인증서와 같이 보낸다. P는 A의 인증서를 검증하여 A의 신원을 확인하고 보내온 서명을 인증서로 확인하여 A가 위임 인증서 발급에 동의하였음을 확인하고 A에게 위임 인증서를 발급한다.



(그림 3) 위임 추적을 위한 프로토콜

A는 발급 받은 위임 인증서로 데이터를 서명하여 V에게 전달하면 V는 위임 인증서를 검증하고 또한 위임 인증서 내의 A가 서명한 부분을 검증하여 A만이 사용 가능한 위임 인증서라는 것을 확인하고 또한 A가 위임 인증서를 발급 받는데 동의한 동일한 사람이라는 것을 확인하고 마지막으로 권한 제한을 확인한 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.

4.2 위임 추적 프로토콜 정의

본 절에서는 위임 추적 프로토콜에 대한 정의를 한다. 다음은 정의에 사용하는 기본적인 기호의 설명이다.

- Xpub : Entity X의 공개키
- Xpri : Entity X의 비밀키
- Xcert : Entity X의 공개키 인증서
- S-Xpri[ ] : X의 비밀키로 전자서명 생성
- V-Xpub[ ] : X의 공개키로 전자서명 검증
- H[ ] : 해쉬함수
- || : concatenation
- PI : PC Issuer 위임인증서 발급자, 원서명자
- A : 대리 서명자
- V : 검증자
- DP : 대리서명에 대한 권한 위임 내용
- Xi : X에 대한 정보

다음은 (그림 3)에 표기된 프로토콜을 다음과 같이 구성하여 단계별로 진행한다.

[1 단계] - PCpub, PCpri
A는 위임 인증서(PC)용 키쌍을 생성한다.

[2 단계] A → PI : pc_issue_req(PCpub)
A는 원서명자 PI에게 자신의 위임 인증서용으로 생성한 공개키를 보내서 발급 신청을 한다.

[3 단계] PI → A : DP
PI는 위임인증서의 본체를 서명하기 전에 발급할 인증서의 내용에 대해 A에게 전송하여 A의 동의를 구한다.

[4 단계] A → PI : S-Apri[H[DP]], Acert
A는 동의하면 자신의 개인키(Apri)로 위임내용(DP)을 서명하고 자신의 인증서(Acert)와 같이 보낸다.

[5 단계] *verify acceptor_certificate and signature of DP* :
Acert = {Ai, Apub, S-CApri [H [Ai || Apub]}
H[Ai || Apub] == V-CApub [S-CApri[H[Ai || Apub]]
H[DP] == V-Apub [S-Apri [H [DP]]]

generate proxy_certificate :
PCcert = {Ai, DP, PCpub, S-PIpri[H[Ai || DP || PCpub]}
PI → A : PCcert

PI는 A의 공개키 인증서를 검증하여 A의 신원을 확인하고 보내온 서명을 공개키 인증서로 확인하여 A가 위임 인증서 발급에 동의하였음을 확인하고 A에게 위임 인증서를 발급한다.

[6 단계] *sign message and send it to V* :
S-PCpri [M]
A → V : S-PCpri [M], PCcert, Acert
verify proxy_certificate :
H [Ai || DP || PCpub] == V-PIpub [S-PIpri [H [Ai || DP || PCpub]]
confirm privilege restriction : delegation_policy
verify message :
H [M] == V-PCpub [S-PCpri [M]]

A는 PC용 개인키로 메시지(M)를 서명하여 V에 전달하면 V는 위임 인증서를 검증하고, 또한 위임 인증서내의 A가 서명한 부분을 검증하여 A만이 사용 가능한 위임 인증서라는 것을 확인하고 A가 위임 인증서를 받는데 동의한 동일한 사람이라는 것을 확인하고 마지막으로 권한 제한을 확인한 다음에 결과를 A에게 보내준다. 이 프로토콜은 V가 A만이 위임 인증서를 이용하여 서명하였다는 위조 방지의 가능성을 배제 시켜주고 거래가 성립된 후에도 A가 부인하는 것을 방지하여 준다.

4.3 제안된 프로토콜의 안전성 분석

본 절에서는 본 논문에서 제안한 위임인증서 기반 대리서명 방법을 2.2에서 언급한 위임 인증서가 갖추어야 할 보안요구사항에 대하여 서명의 위임자와 대리서명자의 서명권한 위임 시나리오를 통해 안전성을 분석한다.

① 강한 위조 방지 : 지명된 대리인만이 유효한 대리서명을 생성할 수 있어야 한다. 즉, 원서명자와 제 3자는 유효한 지명된 대리인을 가장하여 유효한 대리서명을 생성할 수 없어야 한다.
- [1 단계]에서 대리인이 위임 인증서를 위한 키쌍을 생성하고, 위임 인증서의 private key를 유출하지 않으므로 위임 인증서로 유효한 서명은 대리인만이 할 수 있다.

② 검증 가능성 : 대리서명으로부터 검증자는 권한위임에 대한 원서명자의 위임사실과, 대리서명자의 위임동의를 확인할 수 있어야 한다.
- [6 단계]에서 위임인증서의 위임 내용의 서명을 원서명자와 대리서명자의 공개키로 검증하여, 원서명자와 대리서명자의 위임사실과 위임동의를 확인할 수 있다.

③ 강한 부인 방지 : 한번 유효한 대리서명이 생성되면 대리서명자는 자신의 대리서명 생성에 대한 사실을 부인할 수 없어야 한다.
- [6 단계]에서 위임내용 검증 및 메시지 검증을 통하여 대리서명자의 서명을 검증하고, 위임인증서의 위임내용(DP)의 서명을 검증하여 위임인증서 발급에 대한 동의를 확인 할 수 있으므로 부인방지가 가능하다.

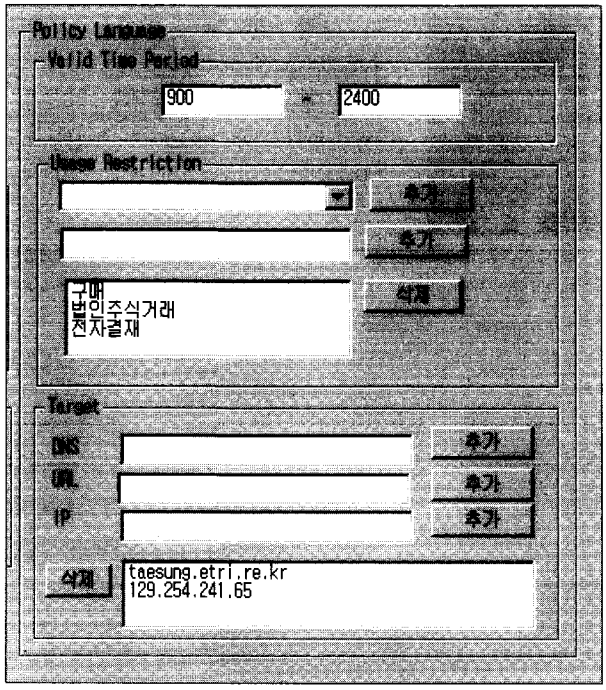
④ 오남용 방지 : 대리인은 자신에게 위임된 권한 내에서 대리서명을 생성해야 한다.
- 먼저 대리인에 의한 서명 권한의 오남용에 대하여 고려해 보면, 본 논문에서 제안한 권한위임제한 정책의 내용을 위임 인증서에 포함시킴으로써 대리인의 오남용을 막을 수 있다.

5. 위임 인증서 프로토타입

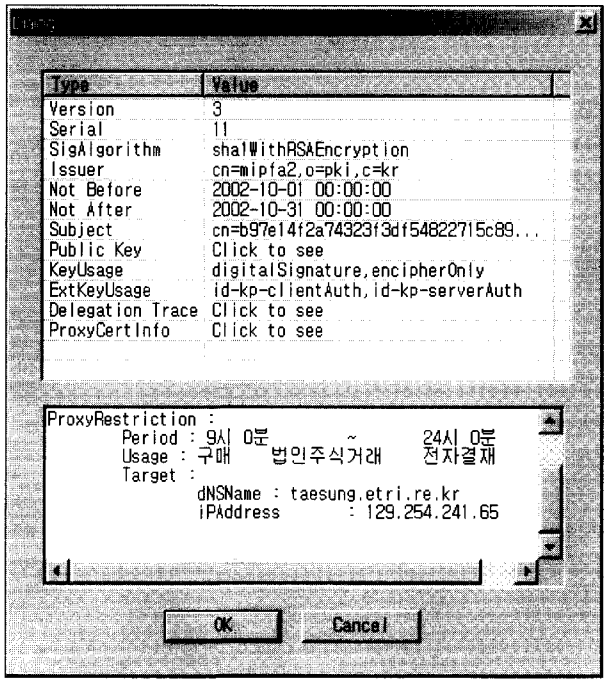
본 절에서는 위임 인증서의 서비스 가능성을 보이기 위한 프로토타입의 설계 및 구현에 대해 기술한다. 프로토타입은 위임 인증서의 발급, 대리 서명의 검증, 위임 제한의 검증 등에 초점을 맞추어 구현되었다. 프로토타입은 위임인증서 발급자, 위임인증서 대리서명자 그리고 검증자로 구성된다. 발급자는 유효기간, 발급자, 키 사용용도, 위임제한 등의 정책을 설정하고 위임 인증서를 발급하며 발급된 위임인증서를 데이터베이스에 보관한다. 대리자는 인증서 발급을 요청하고, 요청했으나 아직 인증서가 발급되지 않은 키쌍과 발급된 인증서를 보관하며, 발급된 위임인증서로 대리서명을 수행한다. 검증자는 발급자의 인증서를 이용해 위임인증서의 서명을 확인하고 위임 인증서 내의 위임 제한을 검증한다. 다음은 위임 인증서 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 3단계는 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, 위임 인증서를 포함하는 인증서 경로를 검증하고, 위임 인증서로 서명된 메시지를 검증한다. 또한 위임인증서에 있는 위임 제한을 조사하여 위임인증서의 사용이 적절한지 검사한다.

프로토타입을 법인주식거래 응용을 가정하여 살펴본다. (그림 4)은 발급자의 정책 설정에서 위임 제한 부분을 보인 것이다. 발급될 인증서는 9 : 00부터 24 : 00 사이에 사용할 수 있고 구매, 법인주식거래, 전자결재의 용도로 사용해야 하며 Target에 열거된 서버에서만 사용해야 한다. (그림 5)는 위임 제한 정책에 맞게 발급된 위임 인증서를 보여준다.



(그림 4) 위임 인증서 발급자의 정책 설정



(그림 5) 위임 인증서 보기

6. 결론 및 향후과제

본 논문에서는 권한 위임의 한계를 명확히 기술하여 위임 인증서의 오남용을 막을 수 있는 위임 인증서 정책 구조를 제안하였고 위임 인증서를 이용하여 대리서명 서비스를 할 수 있는 권한 위임 메커니즘을 설계하였다. 또한 위임 인증서의 발급 및 대리서명에 대한 위임 추적을 가능하게 하는 프로토콜을 제안하고 프로토타입을 구현하여 위임 인증서를 이용한 권한 위임과 대리서명의 가능성을 보였다.

향후 과제로는 본 논문에서 제안한 인증서의 확장성과 융통성을 높일 수 있도록 권한 제한 언어를 연구하는 것이고 제안된 메커니즘이 실제 환경에 쓰이기 위한 위임 인증서 관리 프로토콜에 대해 연구하는 것이다.

참 고 문 헌

[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.

진 승 헌

e-mail : jinsh@etri.re.kr

1993년 숭실대학교 전자계산학과

1995년 숭실대학교 전자계산학과 석사

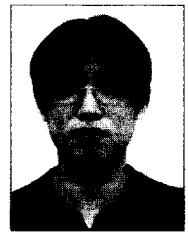
2003년 충남대학교 컴퓨터과학과 박사수료

1994년~1996년 (주)대우통신 종합연구소 연구원

1996년~1999년 (주)삼성전자 통신연구소 전임연구원

1999년~현재 한국전자통신연구원 인증기반연구팀장

관심분야 : 정보보호(인증/인가/프라이버시)



조 상 래

e-mail : sangrae@etri.re.kr

1996년 Imperial College of Science, Technology and Medicine, 전산과(학사)

1997년 Royal Holloway, University of London, 정보보호(석사)

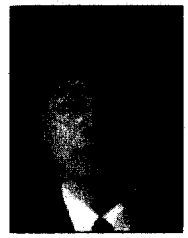
1997년~1999년 LG 종합기술원 연구원

1999년~한국전자통신연구원 정보보호연구본부 인증기반연구팀

관심분야 : PKI, 접근제어(RBAC), 프라이버시 보호 기술

김 태 성

e-mail : taesung@etri.re.kr
1999년 동국대학교 전자계산공학과 공학사
2001년 동국대학교 컴퓨터공학과 공학 석사
2001년~현재 한국전자통신연구원 정보보호연구본부 인증기반연구팀
관심분야 : 정보보호



류 재 철

e-mail : icryou@home.cnu.ac.kr
1985년 한양대학교 산업공학과
1988년 Iowa State University 전산학 석사
1990년 Northwestern University 전산학 박사
1991년~현재 충남대학교 정보통신공학부 교수
관심분야 : 인터넷보안