전자위임장 기반 전자거래 활성화 방안

A Method on Promotion of e-Transaction based on e-Proxies

서 문 석*
대불대학교*

Seo moon-seog*n
Daebul Univ.*

요약

원 서명자를 대신해 거래 관련 제 3자가 서명을 수행하는 대리서명의 실행이 필요한 경우 원 서명자의 서명 위임 사실을 증명하는 위임장이 요구되어진다. 위임장을 전자 거래에 적용하기 위해서는 전자위임장에 관한 표준 프로파일 정의, 전자위임장의 배포 및 검증 방법에 대한 처리 기준이 마련되어야 하며 이를 기반으로 하는 사무 처리 모델이 제시되어야 한다. 이러한 전자위임장 기반구조상에서 다양한 유형의 온/오프라인 거래에 전자위임장을 적용함으로써 전자거래의 활성화에 기여할 수 있을 것으로 판단된다.

I. 서론

위임장은 위임자가 수임자에 대하여 법률행위나 사무처리를 위임한다는 뜻을 기재한 서면을 말한다. 이를 전자적으로 정의한 전자위임장을 다양한 분야의 사무 처리 환경에 적용함으로써 거래 활성화에 기여할 수 있을 것으로 판단된다. 전자위임장을 거래에 적용하기 위해서는 사무 처리의 신뢰성을 높일 수 있도록 전자 위임장의 프로파일 정의, 배포 방법 및 검증 방법이 표준화되어야 한다. 이러한 전자 위임장의 적용 메커니즘은 기존 공개키 기반구조와 유사한 면이 있어 이를 적용한 전자위임장 기반 구조의 정의가 가능하다. 전자위임장 기반 구조 하에서 다양한 온/오프라인 사무 처리 환경에 전자위임장을 적용한 거래 모델을 제시함으로써 안전하고 효율적인 처리가 가능하여 거래 활성화가 용이할 것으로 판단된다.

Ⅱ. 본론

전자위임장 기반구조의 모델인 공개키 기반구조에 대해 살펴보고 새로운 전자위임장 기반구조를 정의하여 이를 토대로 한 전자위임장 적용 처리 모델에 대해 기술한다.

1. 공개키 기반 구조(PKI)

PKI는 공개키 암호시스템과 공개키에 대한 인증서를 기반으로 보안서비스를 제공하는 정보보호 기반구조이다. 보안서비스 중 인증서비스의 기반 기술로는 현재 사실상의 표준으로 받아들여지고 있는 ITU-T의 X.509가 있으며 X.509를 이용한 PKI 시스템 구성은 공인인증기관, 인증서, 인증서 폐지목록 및 이를 배포하기 위해 저장하는 저장소 등으로 구성된다. PKI는 개방형 네트워크에서 안전한 서비스가 이루어질 수 있도록 통신정보의 비밀성, 인증, 무결성 및 부인방지 등의 기본적인 보안서비스를 가장 효과적으로 제공하는 기반 구조이다[1]. 공개키 암호기술의 문제점은 공개키의 가용성을 훼손하는 경우에 발생 하는데 공개키의 가용성이란 어느 누구든지 다른 사용자의 공개키가 필요한 경우에 이를 사용할 수 있는 서비스이다. 공개키가 위·변조되지 않았음을 보장하는 문제 즉, 공개키의 무결성을 보장하기 위해 공개키 대신 공개키와 그 공개키의 소유자를 강하게 연결하여 주는 인증서(Certificate)를 공개하고 인증서는 신뢰할 수 있는 제3자인 인증기관이 자신의 개인키로 서명하여 공개키를 인증하는 시스템을 PKI 시스템이라 한다. 이는 공개키 암호기술이 안전하게 적용될 수 있는 기반구조로써 공개키와 그 소유자를 연결해 주는 인증서, 키와 인증서를 안전하게 관리해주는 서비스 그리고 인증서의 유효성 여부를 확인할 수 있는 구조라고 정의 할 수 있다.

2. 전자위임장 기반 구조

전자위임장이 거래에 활용되기 위해서는 전자위임장 프로파일, 전자위임장의 생성 및 배포, 검증 방법에 대한 정의 및 표준화를 수행하고 이를 준용하는 시스템을 구축 운영함으로써 실세계에 적용이 가능하다. 이러한 전자위임장 기반구조 관련 내용에 대해 설명한다.

2.1 전자위임장 프로파일

거래에서 원 서명자의 위임사실에 대한 위변조 등의 진정성 문제를 해결하기 위해 전자위임장 내에 포함되어져야 하는 정보는 다음과 같다[3].

· 버전 : 위임장 정의 프로파일 버전번호.

· 일련번호 : 위임장의 일련번호.
· 위임장 발급자 : 위임장을 발행한 발급기관으로 위임장에 대한 서명자.
· 유효기간 : 위임장의 유효기간으로 특별한 단서가 없는 한 대리서명의 유효기간과 일치.
· 위임 공개키 : 대리서명의 검증에 이용하는 공개키로 이 공개키에 대응하는 개인키로 대리서명을 생성하고 검증자는 대리서명의 검증에 이 공개키를 사용.
· 키 사용 : 공개키가 사용되는 목적 명시.
· 서명 : 위임장 발급자가 위임장의 정당성을 입증하는 서명생성.
· 위임장에서 추가로 정의되어져야 하는 항목들로 확장 필드 영역에 정의되어져야 하는 항목들은 다음과 같다.
· 대리서명자 : 위임장을 활용하여 대리서명을 생성할 수 있는 대리서명자의 식별 값.
· 위임기간 : 공개키의 유효기간과는 별도로 대리서명의 위임기간을 별도로 명시.
· 권한의 제한 : 위임장을 적용하여 대리서명 가능한 업무범위 등 권한의 제한을 설정.

2.2 전자위임장 생성 및 배포

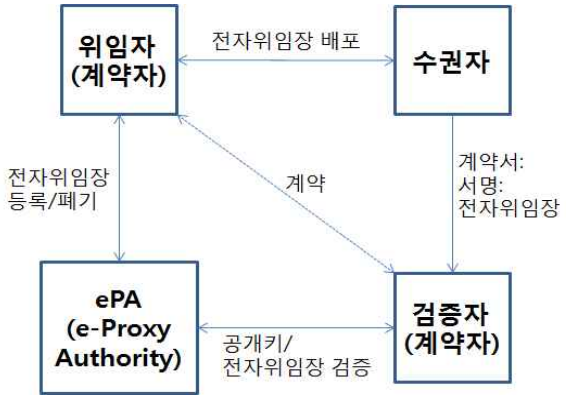
전자위임장은 원 서명자가 자신의 정보와 위임관련 시실을 설정하고 대리서명자로부터 대리서명자의 공개키를 확보하여 검증한 후 대리서명자의 공개키가 정당하면 이를 위임 공개키로 설정하여 자신의 개인키로 전자 서명하여 전자 위임장을 생성하고 이를 전자위임장 공증기관(ePA)에 등록하고 ePA의 배포목록을 통해 서명 검증자 및 대리서명자 등 참가자에게 배포한다[4]. 원 서명자는 대리서명자에게 직접 전자위임장의 전달이 가능하다.

2.3 전자위임장 검증

대리서명자 및 대리서명 검증자는 업무 처리 시 전자위임장의 검증이 필요한 시점에서 위임장에 서명한 원 서명자의 전자서명을 검증하여 전자위임장의 정당성을 검증한다. 전자위임장의 정당성 검증을 위해서는 기존 PKI 시스템에서 실시간 인증서 상태 검증에 사용하는 OCSP(Online Certificate Status Protocol)의 기능을 확대하여 전자위임장 실시간 검증에 적용하는 것도 가능하다[2]. 전자위임장의 정당성이 확인된 후에 전자위임장으로부터 위임 공개키를 획득하여 거래 전자서명의 검증에 이용한다. 위임 공개키는 대리서명자의 공개키로 대리서명자의 공개키도 기존 PKI 환경 하에서의 공개키 검증과 동일한 방법으로 검증이 가능하다.

3. 전자위임장 유통 모델

온/오프라인 계약업무에서 활용될 수 있는 전자위임장의 유통 모델은 [그림 1]과 같다.



▶▶그림 1. 전자위임장 기반 계약처리

Ⅲ. 결론

본 논문에서는 공개키 기반구조를 활용하여 위임장을 전자적으로 정의한 전자위임장의 프로파일을 제시하였으며 또한 전자위임장의 배포 방법 및 검증 방법을 제시하였다. 다양한 분야의 거래에 전자위임장을 적용하기 위해서는 이를 표준으로 정의하고 운영하는 기반구조의 구축이 필요하며 이를 토대로 거래에 적용함으로써 거래의 신뢰성을 높일 수 있고 활성화에 기여할 수 있을 것으로 판단된다.

▌참 고 문 헌▐

[1] W. Stallings, *Cryptography and Network Security (3rd Ed),* Prentice Hall, 2003.
[2] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, RFC2560, 1999.
[3] 서문석, 장필식, 최출헌, "RSA 문제와 위임장에 기반한 안전한 대리서명 기법", 한국콘텐츠학회논문지, 제1권, 제11호, pp.43-49, 2011.
[4] 김소진, 이명희, 최재귀, 박지환, "대리서명방식의 확장에 관한 연구", 한국멀티미디어학회 춘계발표 논문지, 제5권, 제1호, pp.844-848, 2002.