공인전자문서보관소 기반 IT 부가서비스모델 제안

서문석*

*대불대학교 컴퓨터응용기술학과

A Proposal of the Model for IT Value Added Services based on Certified e-Documents Authorities

Seo, Moon-Seog

Daebul University

E-mail : msseo@mail.dabul.ac.kr

요 약

비즈니스 환경에 전자문서를 활용함으로써 종이 없는 사회를 구현하기 위해 정부는 공인전자문서보관소 제도를 추진하고 있다. 이는 업무처리 과정에서 발생한 전자문서를 공인된 전자문서보관소에 보관하고 필요시에 해당 전자문서 혹은 증명서를 발급하여 활용하는 방식으로 업무처리의 간소화, 검색의 용이성 및 문서보관비용 절감 등의 효과를 기대할 수 있다. 그러나 공인전자문서보관소를 기반으로 하는 다양한 비즈니스 모델이 부족하여 기업이 업무환경에 공인전자문서보관소를 이용하는 사례가 부족한 실정이다. 본 논문에서는 전자문서 및 공인전자문서보관소 이용의 활성화를 위해 이를 기반으로 하는 IT 부가서비스 모델과 이의 적용 사례를 제시하고자 한다.

1. 서론

다양한 분야에서 많은 업무들이 IT를 활용하여 이루어지고 있지만 아직까지 종이문서가 병행 처리되고 있는 과도기적 상태이다. 이를 개선하기 위해서는 종이문서를 대신할 수 있는 전자문서 처리 기술의 발전이 이루어져야 하며, 법, 제도의 개선을 통해 다양한 종류의 전자문서들이 법적 효력을 인정받을 수 있어야 한다[1, 4]. 종이 없는 사회 구현의 촉진을 위해 정부는 공인전자문서보관소 제도를 정착시켜 전자문서의 이용 활성화를 이루고자 한다. 이는 생성된 전자문서를 공인된 전자문서보관소에 보관하고 필요시에 해당 전자문서 혹은 증명서를 발급하여 업무에 활용하는 방식으로 업무처리의 간소화, 검색의 용이성 및 문서보관비용 절감 등의 효과를 기대할 수 있다.

현재 공인전자문서보관소 시설기준 등을 충족하여 공인전자문서보관소로 지정된 기관들이 6개 기관에 이르고 있으나 이들을 기반으로 하는 실질적인 서비스들은 원활히 제공되고 있지 못한 실정이다. 이는 공인전자문서보관소를 활용한 다양한 비즈니스 모델이 부족하기 때문이며 IT기업들은 공인전자문서보관소를 기반으로 부가가치를 창출할 수 있는 다양한 서비스들을 제시하여야 한다[3]. 본 논문에서는 공인전자문서보관소 사업이 활성화될 수 있도록 공인전자문서보관소를 기반으로 하는 IT 부가서비스 모델과 신용카드 업무처리 분야에 이를 적용한 사례를 제안하고자한다.

2. 공인전자문서보관소 연계인터페이스

공인전자문서보관소를 이용하고자 하는 이용자

는 자체시스템을 통해 직접 전자문서를 보관하거나 조회하고자 할 때 이용자가 특정 보관소에 기술적으로 종속되지 않도록 하기 위해 공인전자문서보관소 연계인터페이스 기술규격을 준수하여 보관소에 접속하여야 한다.

이용자가 공인전자문서보관소의 서비스를 사용하기 위해 활용 가능한 방법으로는 웹에서 문서를 등록, 검색, 열람하거나 증명서를 발급 받을 수 있는 ASP(Application Service Provider) 기반의 포탈 어플리케이션 서비스와 이용자 내부의 시스템과 보관소가 네트워크를 통해 직접 연계하는 방법 그리고 CD나 FTP를 통해 전자문서를 교환하는 방법이 있다. 또한 이용자가 활용 가능한 장치로는 컴퓨터뿐만 아니라 핸드폰이나 PDA와 같은 모바일기기도 이용 가능하며, 이러한 장치를 통해서도 문서의 등록요청, 검색 및 열람 요청 등의 서비스를 제공받을 수 있다.

이용자가 자신의 시스템을 통하여 보관소와 통신하기 위해서는 연계인터페이스에서 정의한 표준 메시지 구조를 사용하여야 하며, 이러한 메시지 구조는 공인전자문서보관소가 외부 시스템과의 연계를 위한 통신시스템 구축 시 메시지에 반드시 포함하여야 하는 필수 인자들을 구조화한 것으로서, 연계인터페이스를 위한 표준 프로토콜에 해당된다. 공인전자문서보관소와 이용자시스템 연계 시 송수신 되는 문서는 반드시 보안처리가 되어야한다. 연계인터페이스에서 고려하고 있는 보안으로는 크게 네트워크 전송보안, 이용자 인증, 송수신 문서에 대한 보안을 들 수 있으며 네트워크 전송보안은 문서에 대한 기밀성을 보장하고 이용자 인증은 정당한 이용자임을 확인해주며, 송수신 문서에 대한 보안은 전송문서에 대한 송수신 부인방지 및 무결성을 보장한다[2].

연계인터페이스 기술규격에서는 전자문서의 이용자가 공인전자문서보관소에 다양한 접근방법, 접근매체 등을 이용하여 연계하는 방법에 대해 정의하고 있다. 그러나 공인전자문서보관소가 신뢰기관으로서의 역할에 충실하고 이러한 신뢰기관을 활용하여 다양한 부가가치가 내재된 서비스를 개인 이용자들에게 제공하고자 하는 IT 부가서비스 사업자가 중재된 경우에는 전자문서의 이용자(생성자)가 아닌 중개자로서 공인전자문서보관소에 연계하기 위한 부분들이 연계인터페이스 기술규격에 반영되어져야 한다. IT 부가서비스 사업자가 다양한 형태의 시스템 및 네트워크를 구성하고 이를 기반으로 서비스를 제공하는 경우 자신의 사설 표준을 준용하여 업무를 처리하고 이를 공인 전자문서 표준으로 변환하여 공인전자문서보관소와 연계하는데 필요한 기술규격이 추가적으로 반영되어야 한다[6, 7, 8].

3. 공인전자문서보관소 연계 IT 부가서비스

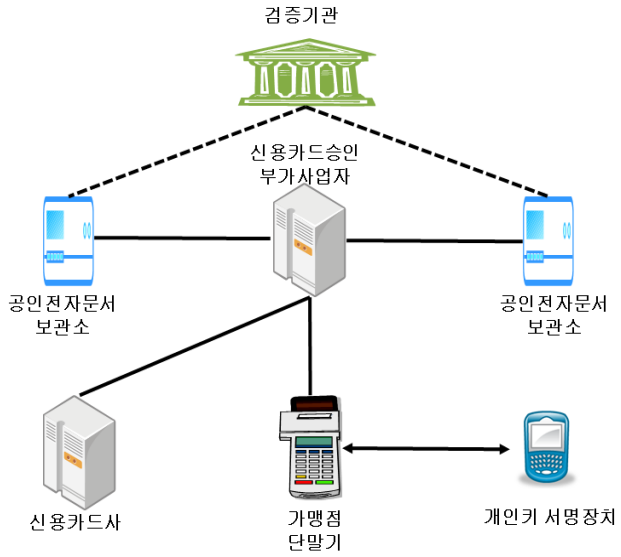
본 장에서는 공인전자문서보관소를 기반으로 부가가치를 창출할 수 있는 IT 부가서비스 예와 일반화된 모델을 제안하고자 한다.

3.1 IT 부가서비스의 예

기존의 신용카드 거래승인 서비스는 다수의 신용카드사와 가맹점을 신용카드 VAN(Value Added Network) 사업자가 네트워크를 구성하고 카드소지자가 가맹점에서 신용카드를 사용할 경우 가맹점 단말기를 통해 거래를 발생시키고 VAN 사업자가 해당 거래를 신용카드사로 중개하여 승인을 받는 구조로 이루어져 있다. 거래승인이 정상적으로 이루어진 경우 거래사실에 대한 증빙자료로서 신용카드사, 가맹점 및 고객용의 3매 1조로 된 신용카드 매출 종이전표가 생성되며 카드소지자가 이에 서명함으로써 거래가 완료된다. 2008년 1/4분기 카드 이용건수는 12,061천건으로 약36,183천장의 종이전표가 발생되었으며 이는 종이의 낭비 및 고객, 신용카드사 및 가맹점의 전표 관리 부담을 야기한다[5].

공인전자문서보관소를 기반으로 신용카드 거래승인 서비스가 이루어지는 경우 신용카드 종이전표의 발생을 방지할 수 있다. 공인전자문서보관소를 기반으로 하는 신용카드 거래승인 부가서비스는 [그림 1]과 같이 신용카드승인 부가서비스 사업자를 통한 거래승인이 정상적으로 이루어진 경우 카드사용자는 자신의 휴대용 개인키 서명장치를 이용하여 전자서명을 수행함으로써 신용카드 거래를 완료할 수 있다. 카드소지자의 전자서명이 추가된 신용카드 거래내역은 신용카드승인 부가서비스 사업자에 의해 공인 전자문서로 변환되어 보관소

에 저장 요청되어진다. 이 경우 신용카드승인 부가서비스 사업자는 카드사용자뿐만 아니라 신용카드사 및 가맹점을 대신하여 해당 전표의 전자문서를 저장 요청할 수 있다.

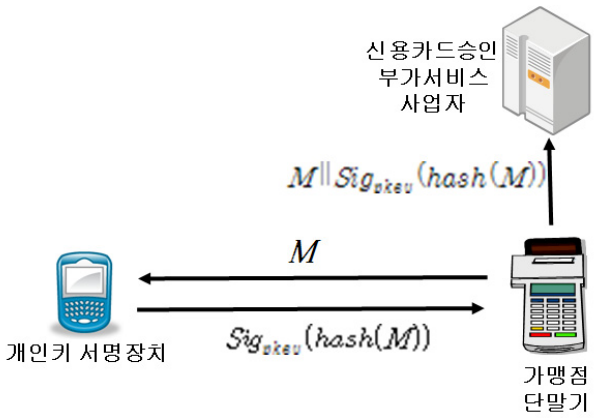


[그림 1] 신용카드승인 부가서비스

신용카드 사용자가 거래내역을 확인한 후 전자서명을 생성하고 가맹점 단말기를 통해 전자서명을 수신하는 방법은 [그림 2]과 같다. 가맹점 단말기에서 전표 데이터(M)를 카드사용자의 개인키 서명장치로 전송하고 사용자가 데이터의 주요내용을 확인한 후 서명장치는 저장된 개인키($pkey$)를 이용하여 해당 데이터에 대한 전자서명($Sig_{pkey}(hash(M))$)을 생성하고 이를 가맹점 단말기로 전송한다[9, 10]. 가맹점 단말기는 수신된 전자서명값과 메시지를 신용카드승인 부가서비스 사업자로 전달한다.

가맹점단말기와 개인키 서명장치 간에 짧은 처리시간을 요구하는 서비스 환경과 무선네트워크 환경 하에서는 무결성을 보장하는 단말기로 부터의 해쉬값 만을 전달하는 방법이 효율적이다. 이 경우 단말기는 전표 데이터의 무결성을 보장하여 위조된 해쉬값이 생성될 수 없음을 보장하여야 한다. 이를 위해서는 부가서비스 사업자로부터 인증받은 단말기의 사용이 전제되어져야 한다.

추후 신용카드사, 가맹점 또는 신용카드 사용자 간의 거래사실에 대한 부인이 발생하는 경우 당사자의 요청에 의해 신용카드승인 부가서비스 사업자는 공인전자문서보관소에 요청하여 관련 전자문서를 검증기관에 제출하고 거래내역에 대한 전자서명의 확인 등을 통해 거래사실에 대한 분쟁이 해결될 수 있다.



[그림 2] 신용카드—거래 전자서명

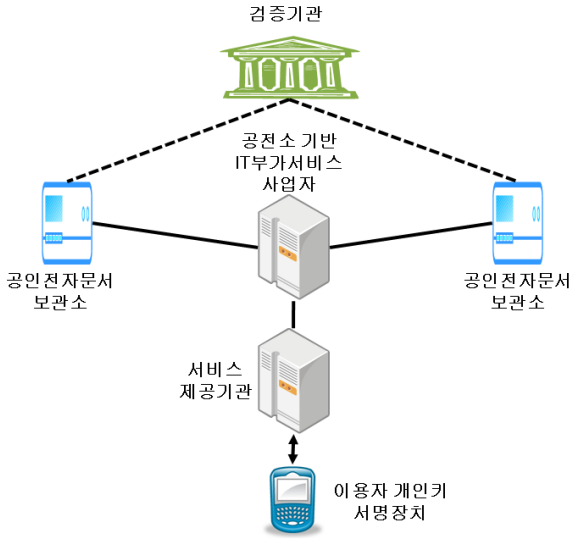
3.2. IT 부가서비스 모델

공인전자문서보관소 기반의 IT 부가서비스 사업 모델은 부가서비스 사업자, 서비스 제공기관 및 이용자로 구성되며, 구성요소들의 기능이 정의된 IT 부가서비스 모델을 기반으로 다양한 IT 부가서비스들이 제시되어질 수 있다. 부가서비스를 제공하고자 하는 서비스사업자는 공인전자문서보관소와의 연계 인터페이스뿐만 아니라 제공하고자 하는 부가서비스에 따라 필요한 업무처리 방법을 개발하여야 하고 요구되는 소프트웨어 및 시스템 환경을 제공하여야 한다.

[그림 3]과 같은 서비스 모델에서 IT 부가서비스 사업자의 주요 기능은 다수의 서비스 제공기관을 유무선 등 다양한 형태의 네트워크로 연결하는 통신망을 구성하고 서비스처리를 위해 필요한 전문을 사설 전문 표준으로 제정하여 관련 기관들이 이를 처리할 수 있게 하여야 한다. 서비스 제공기관으로부터 수신한 사설 표준 전문을 공인전자문서보관소 기술규격에서 정의한 공인전자문서로 변환하여 보관소에 저장 요청하는 기능이 필요하며, 서비스 제공기관 및 이용자의 전자문서관련 처리요구에 대해 이들을 대신하여 공인전자문서보관소에 요청하여 처리하는 서비스들을 제공할 수 있다.

서비스 제공기관은 부가서비스사업자로부터 인증 받은 시스템을 활용하여 사설 표준 전문의 처리가 가능한 소프트웨어를 구현하여야 하며 이용

자로부터 메시지에 대한 서명값을 수신하여 전문을 구성하고 이를 부가서비스 사업자로 안전하게 전송하는 업무를 처리하여야 한다. 이용자의 개인키 서명장치가 무선 환경에서 운영되는 경우 서명값의 적절한 수신을 위해 서비스 제공기관의 시스템도 무선 환경의 수용이 가능하여야 한다.



[그림 3] 부가서비스 시스템구성 모델

이용자의 개인키 서명장치에는 전자서명의 생성이 가능하도록 전자서명 알고리즘 및 공인인증서 처리모듈이 사전에 설치되어 있어야 하며, 서비스 제공기관으로부터 수신한 데이터에 대해 이용자가 이를 확인하고 이용자의 개인키를 이용하여 전자서명을 생성하고 이를 서비스 제공기관으로 송신하여야 한다. 이러한 전자서명장치로는 휴대폰, 스마트폰, 휴대용 컴퓨터 및 전자서명생성 전용장치가 이용될 수 있다.

4. 결론

본 논문에서는 공인전자문서보관소를 기반으로 하는 IT 부가서비스의 예로 신용카드승인 부가서비스를 제시하였고, 다양한 비즈니스 환경에 적용 가능할 것으로 판단되는 IT 부가서비스 모델을 제안하였다. 이러한 서비스들의 활성화는 종이서류의 이용 및 관리 부담을 줄여 종이 없는 사회의 구현을 앞당기고 친환경 IT산업의 육성을 도모하고자 하는 정부 및 관련 당국의 공인전자문서보관소 설치 기본 취지에도 부합한다고 할 수 있다.

공인전자문서보관소가 신뢰기관으로서의 역할을 충실히 수행하고 이를 활용하는 IT 부가서비스사업자들이 많이 생겨날수록 종이 없는 사회의 구현이 앞당겨질 수 있을 것이다. 부가서비스를 제공하고자 하는 사업자는 자신의 사업모델을 정의하여 시스템을 구현하고 필요한 부분을 공인전자문서보관소 관련 기술규격에 부가하는 작업이 필요할 것으로 예상된다.

[참고문헌]

[1] 한국전자거래진흥원, 「전자문서 정보패키지 기술규격」, v1.00, 2006. 11.

[2] 한국전자거래진흥원, 「이용자시스템과 공인전자문서보관소 간 연계인터페이스 기술규격」, v1.00, 2006. 11.

[3] 한국전자거래진흥원, 「공인전자문서보관소 시설 및 장비 등에 관한 평가지침」, v1.00, 2006. 11.

[4] 한국전자거래진흥원, 「전자화문서의 생성 절차와 방법에 관한 지침」, v1.00, 2006. 9.

[5] 한국은행 금융결제국, 「2008년 1/4분기중 지급결제 동향」, KDI 경제정보센터, 2008. 5.

[6] Ronald Jantz and Michael J. Giarlo, "Digital Preservation - Architecture and Technology for Trusted Digital Repositories", D-Lib Magazine, Vol.11, No.6, June 2005.

[7] Cornell University Library, "Digital Preservation Management Tutorial: Implementing Short-term Strategies and Long-term Problems", ICPSR, http://www.icpsr.umich.edu/dpm/dpm-eng/eng_index.html.

[8] Consultative Committee Space Data System, "Reference Model for An Open Archival Information System", CCSDS 650.0-B-1 Blue-Book, Jan 2002.

[9] Robshaw, M. MD2, MD4, MD5, SHA and Other Hash Functions. RSA Laboratories Technical Report TR-101, July 1995. http://www.rsasecurity.com/rsalabs/index.html.

[10] Akl, S. "Digital Signatures: A Tutorial Surveys.", Computer, Feb 1983.