

XML 기반 전자입찰시스템의 설계

박성은*, 이용규
동국대학교 컴퓨터공학과

Design of an Online Bidding System Based on XML

Sung Eun Park*, Yong Kyu Lee
Dept. of Computer Engineering, Dongguk University
E-mail : pse76@dgu.ac.kr, yklee@dgu.ac.kr

요 약

기존 전자상거래시스템들은 독자적인 기술로 개발되어 표준화와 확장성의 문제가 있다. 따라서 최근에는 XML을 전자상거래시스템에 도입하여 시스템간의 표준화 문제를 해결하려는 노력이 진행중이다. 이러한 노력의 일환으로 국제전자상거래 표준인 ebXML이 제정되었고, 관련 XML 기술로 SOAP과 XML Signature가 채택되었다. 본 논문에서는 이러한 최신기술을 실제 적용하기 위한 연구로 XML 기반 전자입찰시스템을 설계하고 프로토타입을 구현하였다. 먼저 분산객체시스템을 구축하기 위해 SOAP을 이용하였고, 기존 분산객체시스템과의 연동도 가능하도록 하였다. 또한 XML Signature를 이용하여 표준화된 인증 시스템을 구현할 수 있는 방안을 제시한다.

1. 서론

기존 전자상거래시스템들은 각각의 기술로 개발되어 표준화와 확장성의 문제가 있다. 이러한 문제는 기존 전자입찰시스템에서도 마찬가지이다. 전자입찰시스템은 입찰의 전 과정을 인터넷을 통해 시행함으로써, 입찰의 투명성과 공정성을 높이며 효율적인 시스템을 운용하려는데 그 목적이 있다. 그러나 전자입찰시스템은 이런 장점이 있음에도 불구하고 각 시스템이 독자적인 기술들로 개발되어 시스템간 호환성 문제가 있다. 따라서 최근에는 이러한 문제를 해결하기 위해 XML 기술을 전자상거래시스템에 도입하려는 움직임이 있다. 이러한 노력의 일환으로 XML 기반 국제전자상거래 표준인 ebXML(electronic business XML)[16]이 표준화되었다. 또한 관련 XML 최신 기술로 SOAP(Simple Object Access Protocol)[4][12][14]과 XML Signature[15]를 채택하였다. 본 논문에서는 이러한 최신기술을 적용하기 위한 연구로 전자입찰시스템을 설계하고 프로토타입을 구현한다. 전자입찰시스템은 대규모 분산객체시스템이면

서 데이터인증이 중요한 시스템이다. 따라서, SOAP과 XML Signature 같은 XML 최신 기술을 도입하여 시스템을 구축할 수 있다. 본 논문에서는 기존의 복잡한 분산객체시스템을 구축하기 위해 SOAP을 이용하고, 기존 분산객체시스템과의 연동도 가능하도록 고려한다. 또한 XML Signature를 이용해서는 표준화된 인증 시스템을 구축할 수 있는 방안을 제시한다. 위와 같은 XML 기술 이외에도 XML Schema, DOM, XSL 등의 여러 XML 관련 기술들을 적용한다. 본 논문에서 설계한 전자입찰시스템은 세가지 장점이 있다. 첫째, XML 기반이므로 표준화, 확장성 등의 이점이 있다. 둘째, SOAP을 이용해 분산객체시스템을 구축하고, 기존 분산객체시스템과의 연동도 가능하도록 고려한다. 셋째, XML Signature를 인증시스템 구축에 도입하여 XML 기반 시스템의 활용도를 높인다.

2. 관련 연구

본 절에서는 전자상거래시스템과 관련된 최근 표준인 ebXML, SOAP, XML Signature를 소개한다.

2.1 ebXML(electronic business XML)

ebXML은 UN/CEFACT와 OASIS에 의해 제안되었고, 그 목표는 XML 기반의 일괄적인 환경에서 전자상거래를 위한 프레임워크를 제공함으로써 전 세계 단일 시장을 형성하려는 데 있다. 즉, ebXML을 기반으로 시스템을 구축하면 XML을 사용하기 때문에 전자상거래가 단순하고, 언제 어디서든지 가능해 진다는 장점이 생긴다. 또한 데이터 표준화 문제를 쉽게 해결할 수 있다. ebXML은 국제적인 표준일 뿐 아니라, 국내에서도 이를 채택하여 많은 관련 업체들이 XML 기반의 시스템을 구축하려고 한다. 한편, 최근에 ebXML은 데이터 전송표준으로 SOAP을 채택하였고, 보안을 위해 XML Signature를 도입하였다.

2.2 SOAP(Simple Object Access Protocol)

기존 전자입찰시스템에서 분산객체시스템을 구축하기 위해서 CORBA, COM/DCOM(Distributed Component Object Model), EJB(Enterprise JavalBeans)와 같은 표준을 사용한다. 이것은 네트워크 상에서 분산프로그램 객체를 생성, 참조, 관리하는 역할을 할 수 있게 한다. 그러나 이들은 독자적인 기술을 기반으로 개발되었기 때문에, 서로 객체를 공유하여 사용하기가 어렵다. 그러나 이러한 문제는 SOAP의 등장으로 쉽게 해결하였다. SOAP은 XML과 HTTP(Hypertext Transfer Protocol)를 기반으로 네트워크 상에 존재하는 각종 컴포넌트간의 호출을 효율적으로 할 수 있게 하는 통신 프로토콜이다. SOAP 크게 두가지 특징이 있다. 첫째, XML 기반이므로 서로 다른 컴포넌트 기술로 구현한 시스템간에 객체를 공유하여 사용할 수 있다. 둘째, 인터넷 표준인 HTTP를 사용함으로써 널리 사용되고, 기존 분산객체 시스템에서의 방화벽 문제를 해결할 수 있다.

2.3 XML Signature

W3C에서는 XML로 표현된 문서들이 인터넷을 통한 B2B거래에서 안전하게 서로 교환될 수 있도록 XML Signature라는 표준을 정하였다. XML Signature는 보안의 개념과 함께 서명의 의미를 가짐으로써 데이터에 대한 부인방지와 무결성을 보장하는데 사용한다. XML Signature는 전자서명에 활용한 알고리즘, 키 정보와 전자서명을 적용한 결과 값 등에 관련된 정보들을 XML 형식으로 표현한 것이다. XML Signature는 다음의 세 가지 특징이 있다. 첫째, 태그형식이므로 문서 전체에 서명을 할 수 있을 뿐

아니라 문서의 일부분에도 서명을 할 수 있다. 둘째, XML의 기반이므로 플랫폼에 독립적인 인증시스템을 구축할 수 있다. 셋째, 쉬운 XML 문법을 사용함으로써 용이성으로 갖고 태그를 활용하여 전자서명에 대한 정보를 추가하는 확장성도 가진다.

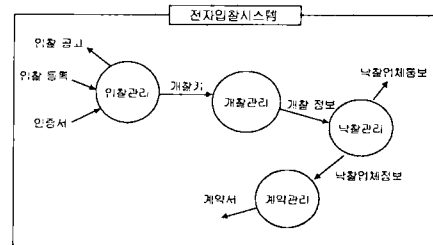
3. 전자입찰시스템 설계

기존 전자입찰시스템은 단일 플랫폼의 시스템에서는 큰 문제가 없으나 다양한 시스템간에 연동이나 통합이 필요할 때는 호환성에 문제가 생긴다. 또한 분산객체시스템을 구축하는 과정이 복잡하며, 분산시스템 구현에 대한 표준이 다양해 다른 표준기술을 사용한 시스템간 객체를 공유하여 사용할 수 없다. 본 논문에서는 이러한 단점을 개선하기 위해 XML 기반의 전자입찰시스템을 설계하고 프로토타입을 구현한다.

3.1 프로세스 설계

전자입찰은 입찰 참여업체가 인터넷 기반의 전자입찰시스템을 통해 물품구매, 시설공사, 용역 등의 입찰 업무를 수행하는 전 과정을 의미한다.

[그림 1]에서 보면 전자입찰시스템은 내부적으로 입찰, 개찰, 낙찰, 계약과 관련 있는 프로세스를 가진다.

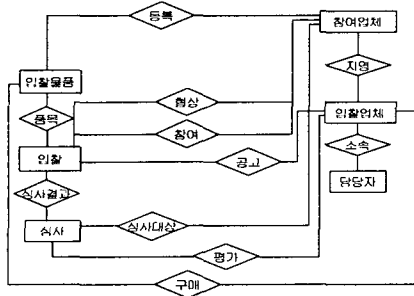


[그림 1] 전자입찰시스템의 프로세스

입찰참여업체는 인터넷상의 입찰공고를 보고, 입찰서를 제출함으로써 입찰에 참가하게 된다. 이 때, 업체의 인증정보를 확인하기 위하여 외부 인증기관과 연동하기도 한다. 입찰 마감날짜가 되면 개찰을 통해 참여업체들의 입찰제출사항을 파악하고, 몇몇 낙찰업체와 협상을 하게 된다. 협상결과를 바탕으로 최종 심사를 거쳐 가장 우수한 참여업체를 낙찰업체로 선정한다. 낙찰업체가 정해지면 결과를 낙찰업체에게 통보하고 계약관계를 성립한다. 계약과정은 공증기관과 연동해서 이루어지거나 전자입찰시스템의 내부적인 모듈을 통해 이루어진다. 계약 관계가 성립되면 입찰 업무는 마무리된다.

3.2 데이터베이스 설계

데이터베이스 구축을 위해 전자입찰업무에 필요한 개체들간의 관계를 [그림 2]에서 보는 바와 같이 E-R 다이어그램으로 나타낼 수 있다.

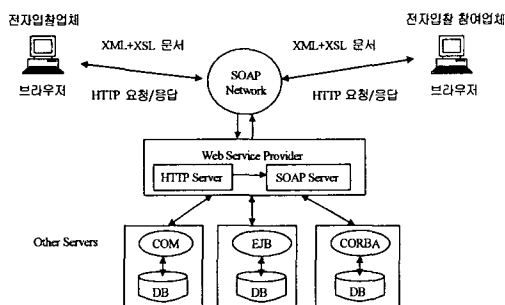


[그림 2] 전자입찰시스템의 E-R 다이어그램

[그림 2]에서 보면, 입찰업체와 입찰 사이에는 공급이라는 관계가 있어, 입찰업체가 입찰을 공급한다는 것을 나타낸다. 반면에 참여업체는 입찰에 참여하기 위해 참여라는 관계와 심사를 위해 협상하는 협상의 관계를 가진다. 본 논문에서 구현한 시스템은 물품입찰 업무에 관한 사항이므로 입찰과 물품사이에도 품목이라는 관계가 성립한다. 참여업체를 심사하기 위해 심사라는 개체와 관계를 가지며, 입찰 업체와는 평가라는 관계를 가진다. 최종적으로 낙찰업체가 정해지면 물품에 대한 구매가 이루어진다.

3.3 데이터 전송구조 설계

XML 기반의 시스템에서는 데이터를 전송하기 위해 XML 기반의 프로토콜인 SOAP을 이용한다. [그림 3]은 본 논문에서 데이터 전송을 위한 구조를 설계한 그림이다.



[그림 3] 전자입찰시스템의 데이터 전송 구조

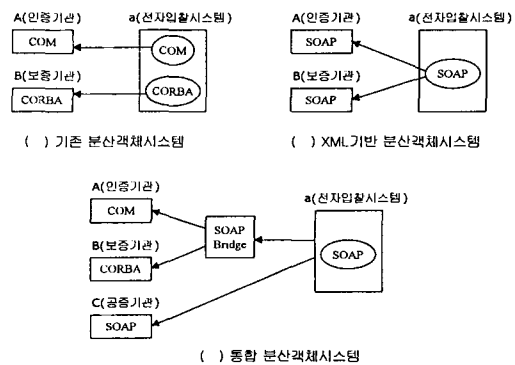
본 논문에서는 [그림 3]과 같이 SOAP을 데이터 전송 뿐만 아니라 외부 협력사들과의 연동을 위해서도

사용하였다. 이는 일종의 미들웨어를 두어 기존 시스템이 SOAP을 도입하지 않고도 XML 기반의 새로운 시스템과 연동 할 수 있도록 한 설계이다. 이 미들웨어는 SOAP 형태로 전송된 문서를 해석하여 각각의 분산객체시스템이 인식할 수 있는 데이터 형태로 전송하는 역할을 한다. 미들웨어를 이용하면 이기종간의 분산객체시스템에 SOAP 형태의 데이터를 전송할 수도 있지만, 분산객체시스템 내에 존재하는 객체도 쉽게 사용할 수 있다. 본 논문에서는 이 미들웨어 역할을 하는 부분을 SOAP 브리지(Bridge)라 명명하였고, 구체적인 구조 설계는 다음 장에서 좀 더 자세히 살펴보기로 한다.

4. SOAP을 이용한 분산객체시스템

현재 많이 사용되는 분산객체시스템 표준으로는 CORBA, COM, EJB 등이 있다. 그리고, 이러한 표준의 핵심인 컴포넌트의 주요 목적은 프로그래밍 언어, 프로그래밍 모델에 관계없이 상호 운용될 수 있는 소프트웨어 모듈의 개발이라고 볼 수 있다. 하지만 이와 같은 장점에도 불구하고 서로 다른 컴포넌트 기술에 기반한 컴포넌트를 호출한다는 것은 어렵고 복잡한 작업을 수반한다. 그러나 XML과 HTTP 기반의 SOAP은 이러한 문제점을 해결한다.

4.1 SOAP과 기존 분산객체시스템의 연동



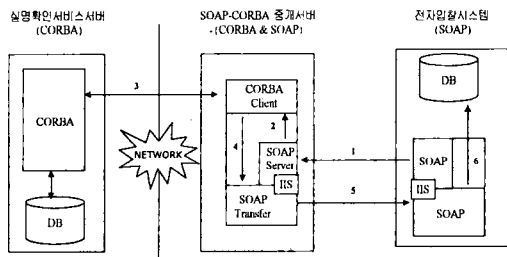
[그림 4] SOAP과 분산객체시스템의 연동

[그림 4]의 (가)은 기존 분산객체시스템을 의미하는데, 그림에서 보는 바와 같이 분산환경에 있는 객체에 접근하려면 동일한 기술에 기반한 분산객체시스템 표준, 즉 CORBA는 CORBA, COM은 COM 방식을 따라야 한다. 현재 CORBA와 COM의 객체를 서로 공유하기 위해서 브리지라는 것을 사용하지만, 구현 방법

이 매우 복잡하여 잘 쓰이지 않는다. 이러한 문제점을 해결하기 위해 SOAP을 이용한 분산객체시스템은 [그림 4]의 (ㄴ)이다. XML 기반 시스템에서는 SOAP을 통해 데이터 전송 뿐만 아니라 분산객체의 접근도 쉽게 가능하다. 그러나, 현재 CORBA나 COM 기반의 분산객체시스템을 SOAP 기반으로 모두 바꾼다는 것은 무리가 있다. 따라서, 본 논문에서는 (ㄷ)에서 보는 바와 같이 미들웨어 역할을 하는 SOAP 브리지를 두어 기존의 분산객체시스템이 SOAP을 지원하지 않아도 SOAP 기반의 새로운 시스템과 연동 가능하도록 설계한다.

4.2 SOAP 브리지 설계

본 절에서는 분산객체시스템의 표준으로 널리 쓰이는 CORBA와 SOAP의 연동을 설명한다.



[그림 5] SOAP-CORBA 브리지

[그림 5]는 SOAP 기반 전자입찰시스템이 입찰참여자의 정보를 입력받으면, CORBA 기반 분산객체시스템에서 정보를 확인해 주는 프로세스 과정을 나타낸 그림이다. 먼저, 전자입찰시스템에서 사용자로부터 입력받은 내용을 SOAP 형태로 SOAP-CORBA 브리지로 전송한다. 그러면 브리지 안의 SOAP Server가 이 메시지를 해석하여 CORBA Client를 호출한다. CORBA Client는 매개변수를 CORBA 서버에게 넘겨주게 되고, CORBA 서버는 결과값을 데이터베이스 검색을 통해 얻어낸다. 이 결과값은 CORBA Client를 통해 SOAP Transfer에게 전달이 되는데, SOAP Transfer는 얻은 결과값을 적정한 SOAP 메시지 형태로 변경한 후에 요청했던 전자입찰시스템에게 전송한다.

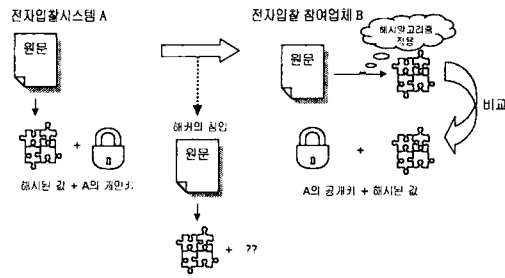
5. XML Signature를 이용한 인증구조

본 논문에서는 전자입찰시스템과 입찰참여업체간 전자서명이 이루어진다. 또한 XML 기반의 시스템이므로 전자서명도 XML Signature를 이용한다. XML

Signature는 표준화되고 확장 가능한 전자서명 형식을 제공함으로써, 전자서명시스템간의 상호작용성을 높인다.

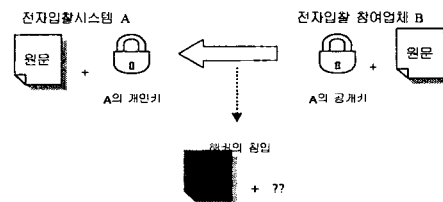
5.1 XML Signature를 이용한 인증구조 설계

본 논문에서는 XML Signature를 이용한 인증구조로 두 가지를 설계한다. 첫째는 원문 내용의 부인방지와 변조방지를 위해 XML Signature를 써서 원문에 추가 정보를 덧붙이는 것이다. 둘째는 외부에 노출되어서는 안되는 중요 데이터를 숨기기 위해 공개키 구조를 도입해 XML Signature를 구성하는 것이다.



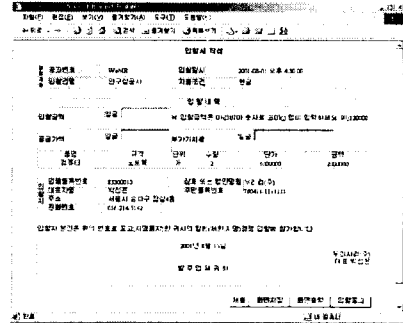
[그림 6] 사용자 인증을 위한 시나리오

[그림 6]은 A(전자입찰시스템)에서 B(입찰참여업체)로 문서가 전송될 때, B가 전송 받은 문서가 해커가 아닌 A의 문서임을 확인하는 시나리오이다. 예를 들어 A가 <입찰공지>에 관련된 정보를 B에게 전송한다고 가정하자. A는 원문에 해시알고리즘을 적용한 해시값을 자신의 개인키로 암호화한 후에 원문과 함께 B에게 전송한다. B는 전송 받은 원문을 A가 명시한 해시알고리즘을 적용하여 해시값을 얻는다. 그리고 전송 받은 암호화된 해시값을 A의 공개키로 해독한 값을 앞의 해시값과 비교해 A임을 확인한다. 만일 해커가 침입한다고 해도 A의 개인키를 알 수 없으므로 원문을 변조할 수 없다. 따라서 B는 변조되지 않은 <입찰공지> 정보를 얻을 수 있고, 그 정보가 A의 것임을 확인할 수 있다.



[그림 7] 원문보안에 대한 시나리오

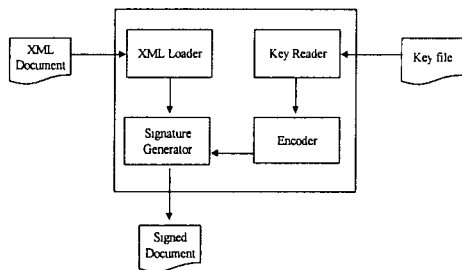
[그림 7]은 [그림 6]과 반대로 B가 A로 문서를 전송할 때, 해커가 B의 원문의 중요내용을 알 수 없게 하는 시나리오이다. 예를 들어 유출되면 안되는 <입찰가격>과 같은 중요한 정보를 B가 A에게 전송해야 한다고 가정하자. [그림 7]에서 보는 시나리오와 같이 B는 A의 공개키로 문서를 암호화한다. 그런 후 A에게 전송하면, A는 자신의 개인키로 문서를 복호화해서 내용을 확인한다. 만일 해커가 중간에서 문서를 가로챌다고 해도 A의 개인키를 알 수 없으므로 복호화를 할 수 없다.



[그림 9] 입찰서 작성화면

5.2 XML Signature 생성기 설계

XML Signature 생성기(Generator)는 크게 네 가지 모듈로 나뉜다. 인증이 필요한 XML 문서를 읽어 메모리에 적재하는 XML Loader, 사용자의 키 값을 입력으로 받아들여 이를 Encoder에 전달하는 Key Reader, Key Reader로부터 전달받은 키 값을 이용해 지정된 알고리즘을 적용해 암호화된 값을 만드는 Encoder, XML Loader의 데이터와 Encoder의 암호화된 값을 받아 XML Signature 태그를 생성하는 Signature Generator로 이루어진다. [그림 8]은 이 4가지 모듈간의 관계를 표현한 그림이다.



[그림 8] XML Signature 생성기 구조

[그림 9]는 공고된 입찰 건에 대해 입찰참여업체가 입찰서를 제출할 수 있게 하는 화면이다. 입찰서 제출은 온라인 상에서 할 수 있고, 입찰참가에 필요한 사항들을 기재할 수 있는 화면이다.

6.2 SOAP-CORBA 브리지를 이용한 연동화면

전자입찰시스템에서 SOAP 브리지를 이용하여 기존의 분산객체시스템과의 연동을 위한 예로 실명확인 애플리케이션을 구현하였다. 먼저, 실명확인을 위해 데이터를 검색하고 실명확인을 하는 CORBA 서버는 접속대기 상태가 되면서 Agent(ORB)에 자신을 등록한다. Agent는 CORBA Client의 요청이 올 때까지 CORBA 서버의 위치와 정보를 등록하고 대기한다.



[그림 10] ORB와 CORBA 서버 실행화면과 SOAP 클라이언트화면

6. 전자입찰시스템의 구현

본 장에서는 앞에서 살펴본 설계를 기반으로 프로토타입을 구현한 화면들을 설명한다.

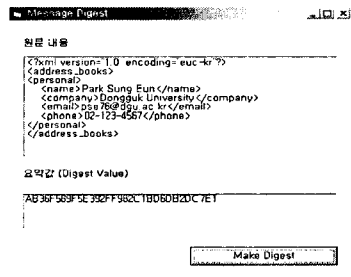
6.1 사용자 인터페이스 화면

전자입찰을 수행하기 위한 기본적인 인터페이스 화면은 XML과 XSL을 이용하여 구현하였다. 사용자 인터페이스 주요 화면은 입찰, 개찰, 낙찰, 계약에 관련된 화면이다.

[그림 10]의 왼쪽화면이 CORBA Client와 비저브로커의 Smart Agent가 요청 대기 상태로 실행되고 있음을 나타낸 화면이다. [그림 10]의 오른쪽 화면은 SOAP 클라이언트를 나타낸 화면이다. 즉, 사용자가 입력한 파라미터값을 SOAP 메시지로 변환하고, 이를 HTTP 프로토콜을 통해 등록된 웹서버의 SOAP 브리지로 전달한다. 브리지로 전달했던 메시지에 대한 응답으로 서비스의 결과값이 리턴되고, 해당 필드에 결과값을 출력하게 한다.

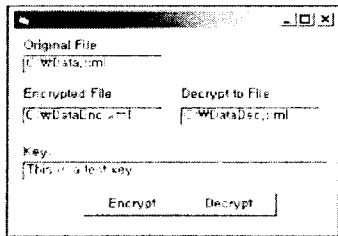
6.3 XML Signature 생성기를 이용한 인증생성화면

XML Signature를 생성하는 애플리케이션은 앞에서 설계한 두 가지 시나리오를 가능하게 하는 기능을 갖는다. 첫째, 메시지 다이제스트(Message Digest)를 통해 Signature 코드를 생성하여 사용자 인증과 부인방지를 한다. 둘째, 암호화 알고리즘으로 중요한 데이터를 암호화해서 타인에게 데이터가 노출되지 않게 한다.



[그림 11] 메시지 다이제스트 애플리케이션 화면

[그림 11]은 XML 원문을 다이제스트하는 애플리케이션을 나타내는 화면이다. 요약 알고리즘을 써서 XML 원문을 요약하면 다이제스트 값을 얻을 수 있다. 이 애플리케이션에서는 요약 알고리즘으로 MD5를 사용했다.



[그림 12] 암호화 애플리케이션 화면

[그림 12]는 원본 XML 파일에 암호화 알고리즘을 적용하여 암호화(Encryption)한 파일을 생성하고, 다시 이를 복호화(Decryption)할 수 있는 애플리케이션을 나타낸 그림이다.

7. 결론 및 향후 연구

본 논문에서 설계한 XML 기반의 전자인찰시스템은 크게 세 가지 장점이 있다. 첫째, XML을 기반으로 하기 때문에 구축의 용이성, 플랫폼의 독립성, 확장성 등의 장점을 가진다. 둘째, XML 기반의 프로토

콜인 SOAP을 이용해 분산객체시스템을 구현했을 뿐 아니라 SOAP 브리지를 두어 기존의 분산객체시스템과의 연동도 가능하도록 고려하였다. 셋째, XML 최신 표준인 XML Signature를 이용한 인증시스템을 설계하였다. XML Signature가 현재는 많이 활용되고 있지 않지만, XML 기반의 시스템에서는 인증시스템 또한 XML 기반의 XML Signature를 도입해야 활용도를 높일 수 있을 것이다. 본 논문에서는 핵심적인 부분의 프로토타입을 구현하였으며, 향후에는 완전한 시스템의 구현이 필요하다. 또한 CORBA뿐만 아니라 DCOM과의 연동을 고려할 것이며, 보안측면을 더 강화시킬 수 있도록 연구하겠다.

[참고문헌]

- [1] Andrew Watt, Jon Duckett and Nikola Ozu, "Professional XML 2E," WROX Press, 2001
- [2] Benoit Marchal, "XML by Example," Que, 1999
- [3] Bill Kropog, Mark Baartse and Steven Hahn, "Professional ASP XML," WROX Press, 2000
- [4] Brain E, Travis, "Microsoft XML and SOAP Programming for BizTalk Servers," Microsoft Press, 2000
- [5] Dan Harkey, Jeri Edwards and Rober Orfali, "Instant CORBA," WILEY, 1999
- [6] David Hunter, "Beginning XML," WROX Press, 2000
- [7] Douglas R. Stinson, "Cryptography : Theory and Practice," CRC, 1995
- [8] Elliotte Rusty Harold, "XML Bible," IDG Books, 1999
- [9] Erik T. Ray, "Learning XML," O'Reilly, 2001
- [10] George M. Doss, "CORBA Developer's Guide with XML," WORDWARE, 1999
- [11] Jon C. Graff, "Cryptography and E-Commerce," John Wiley & Sons, 2000
- [12] Kent Sharkey and Scott Seely, "SOAP Cross Platform Web Service Development Using XML," Prentice Hall, 2001
- [13] Steven Holzner, "Inside XML," New Riders Publishing(NRP), 2000
- [14] SOAP 1.1 spec. www.w3.org/TR/SOAP
- [15] XML Signature spec. www.w3.org/Signature/
- [16] 표준화 동향 www.ebxml.or.kr