웹기반 전자 입찰 시스템 보안 설계

윤선희° 주경준*
숭의여자대학 전자계산학과,° 한국전자통신연구원 컴소기술연구소*
{shyoon@sewc.ac.kr, kjju@etri.re.kr}

Design of Security for Web based Electronic Bidding System

Sunhee Yoon° Kyung-Joon –Ju*
Dept. of Computer Science, Soongeui Woman's College°, ETRI Computer Software Technology Lab*

요 약

최근 컴퓨팅 기술과 통신 기술의 급속한 발전으로 클라이언트/서버 컴퓨팅 환경에서 네트워크 컴퓨팅 시대를 지나 인터넷 컴퓨팅 시대가 도래하고 있다. 인터넷 사용이 보편화되어 감에 따라 기업의 정보 시스템이 인터넷 기반의 인트라넷/익스트라넷 시스템으로 구축되어 가고 있으며 인터넷 환경에서의 기업과 소비자간 또는 기업과 기업간의 전자 거래 관련 응용 프로그램의 개발이 다양해 지고 있다. 본 논문에서는 인터넷 환경에서 기업과 기업간 전자 거래에 있어서 기업의 글로벌화를 통해 조달 업무의 투명성과 신속성 및 질적 향상을 추구할 수 있도록 제공하기 위한 웹 기반 전자 입찰 시스템을 구현하는데 있어서 클라이언트와 서버 및 데이터베이스를 연동하기 위한 웹기술, 기업간의 문서 교환을 위한 XML/EDI 기술 및, 입찰과 계약과정, 조달과정에서 안전성 및 신뢰성을 보장하기 위해 공개키 암호화 기술인 PKI 기반 구조의 인증 및 전자서명을 활용한 보안 기능을 설계한다.

1. 서론

최근 인터넷 컴퓨팅의 확산으로 기업의 정보시스템에 인터넷을 활용한 응용시스템의 사용이 활성화되어지고있다. 본 논문에서는 기업과 기업간이 전자거래에 있어서 조달 업무의 투명성과 신속성 및 질적 향상을 추구할 수 있도록 제공되는 전자 입찰 시스맹의 구축을 위한 관련 연구를 분석하고 전자 입찰 시스템의 구조를 설계하며 전자 입찰 시스템의 핵심 기술인 보안에 대한 설계를 한다.

2. 관련연구

웹기반 전자입찰 시스템을 구현하기 위해서는 웹클라이언트/서버, 웹 DB 연동을 포함한 웹기술, 전자입찰에 필요한 문서 교환을 위한 XML/EDI 기술 및 입찰 및 계약 및 조달 과정에서 필요한 PKI 기반의 인증, 전자 서명을 포함한 보안기술로 분류될 수 있다.

(1) 웹 기술

본 논문에서 제안하는 전자 입찰 시스템은 인터넷 환경에서 클라이언트와 서버간의 통신은 자바 애플릿과 서블릿으로 구현되며 데이터베이스와의 연동은 JDBC 를 사용한다.

서블릿을 통한 데이터베이스 연결은 CGI 의 사용자 수가 증가함에 따라 프로세스의 증가로 발생하는 성능상의 문제를 해결하면서 2-tier 나 3-tier 등의 시스템 구조로 분산 환경 모델을 가능하게 해주는 방법이다. 서블릿은 웹 브라우저나 애플릿의 리턴값에 의해 전달 받으며 내부에서 JDBC 를 통해 데이터베이스에 연결한 후 질의를 보내고 해당 질의의 검색 결과를 HTML 형태나 여러 자료형으로 되돌려 준다. 이때 서블릿은 자바의 멀티 쓰레드를 이용해 질의를 처리하기 때문에 CGI 처럼 프로세스를 생성하는 과정에서의 오버헤드를 줄이고 있고, 한 번 로드된 서블릿은 메모리상에 계속 존재하기 때문에 여러 번의 데이터베이스 연결 요청에 대해 한번의 연결로 계속 처리할 수 있다. 또한 서블릿은 Java 의 플랫폼 독립적인 장점을 통해서 어느 웹서버에서도 실행될 수 있으며 보안 측면에서도 자바의 보안 구조에서 제공하는 기능을 모두 사용할 수 있다.

(2) XML/EDI 기술

1) XML/EDI

XML/EDI 는 현재 무역, 금융, 유통, 조달 등의 분야에서 기업간의 문서 교환에 이용하는 EDI 를 XML 로 정의하여 인터넷상에서 쉽게 표현하고 사용할 수 있도록 하기 위해 제안된 것으로 XML 에 적용되는 모든 기술들을 그대로 이용할 수 있기 때문에 확장성, 유연성, 연동성 등이 뛰어나다.

2) DTD(Document Type Definition)

DTD(Document Type Definition)는 마크업 언어(Markup Language)의 구문 규칙을 정의하기 위한 표준으로 요소

(Element)에 포함될 수 있는 항목(Attribute)의 자료형 등을 정의한다. DTD는 XML 파서에 의해 XML 문서가 파싱될 때 사용되며, DTD를 따르고 있는 XML 문서를 유효한(valid) 문서라 하고, DTD는 정의되어 있지 않지만 XML 기본 구문규칙에 충실한 XML 문서를 적격(Well-formed) 문서라 한다.

3) XSLT(extensible Stylesheet Language Transformation)

XSLT는 XML 문서를 HTML 문서로 변환해 줄 수 있다. 이렇게 변환된 HTML 문서는 HTML 브라우저를 통해서 볼 수 있게 된다. XSML를 사용할 경우 하나의 XML/EDI 문서를 HTML 브라우저를 통해서 다양한 형태로 출력할 수 있다는 장점을 가지고 있다. 따라서, 고객이 원하는 형태로 서비스를 제공해 주고 동일한 문서를 프리젠테이션 레벨에서 다양한 처리를 해줄 수 있다..

(3) 보안 기술

1) PKI(Public Key Infrastructure)

전자상거래의 안전성, 신뢰성을 만족하기 위해서는 암호기술이 필요하며 암호기술은 크게 비밀키 암호기술과 공개키 암호기술로 나뉘며, 공개키 암호기술은 PKI(Public Key Infrastructure)를 근간으로 해서 이루어진다. PKI에 대한 정의는 정보시스템 보안, 전자상거래, 안전한 통신 등의 여러 응용 분야에서 인증서(certificate)의 사용을 용이하도록 하는 정책, 수단, 도구 등을 수립하고 제공하는 객체들의 네트워크를 말한다.

2) X.509 기반 인증서

인증서는 사용자의 신분과 공개키를 연결해 주는 문서로 인증기관의 비밀키로 전자 서명하여 생성된다. 이는 사용자의 공개키가 실제로 사용자의 것임을 증명해주며, PKI에서 인증서의 발행대상은 인증기관과 사용자, 서버 등으로, 인증기관에게는 상위 인증기관이 인증기관의 적법성을 증명하기 위해 인증서를 발행하고, 사용자와 서버에게는 사용자의 신원, 서버 등의 적법성을 증명하기 위해 인증기관에서 발행한다.

3) RSA(Rivest Shamir Adleman)

인수분해 문제 해결의 높은 난이도를 이용한 가장 대표적인 공개키 암호 시스템으로 1978년 미국의 MIT에서 최초로 개발되었다. RSA 암호 시스템은 암호화 뿐만 아니라 전자서명의 용도로도 사용될 수 있다. 이 때에는 비밀키로 전자서명을 하고 공개키로 복호화하는 것만 다르고 암호화와 동일하다.

4) XMLDSIG(XML Digital SIGnature)

EDI 문서를 XML로 표현하는데 있어서 전자서명이 적용된 XML 전자서명 문서의 표준 형식으로 IETF(Internet Engineering Task Force)에서 XMLDSIG Working Group이 결성되어 활발한 연구가 진행되고 있다.

5) S/MIME(Secure Multi-purpose Internet Mail Extension)

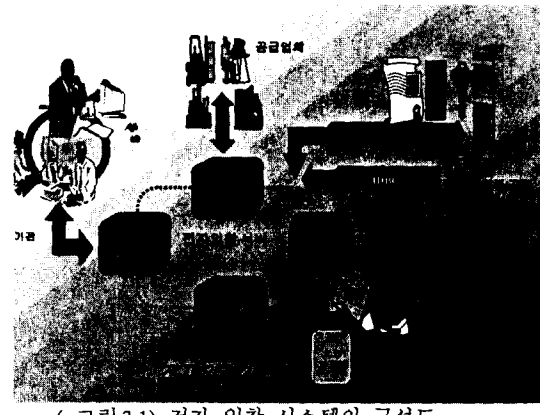
사사용자에 대한 인증과 거래 내용 인증을 동시에 제공하는 전자서명 기술은 전자상거래에 있어서 중요한 보안 기술로서, 그 중에서 다양한 플랫폼에 걸친 안전한 전자 우편 서비스를 제공하는 것이 S/MIME이며 공개키 암호화와 전자서명을 활용하는 전자우편 패키지에 응용될 수 있다.

6) PKCS#7(Public-Key Cryptography Standards#7)

전자서명에 적용되는 문서의 일반적인 구문을 정의하는 표준으로서 서명 시간, 메시지의 내용에 따라 달라지는 인증, 서명한 순서와 같은 항목들을 제공한다.

3. 전자 입찰 시스템

본 논문에서 구현된 전자 입찰 시스템의 주요 기능은 구매 관리기, 입찰/계약 관리기 조달 관리기로 구성된다 (그림 3.1).



(그림 3.1) 전자 입찰 시스템의 구성도

전자 입찰 시스템의 구성도에 나타난 각 관리기의 주요 기능은 다음과 같다(표 3.1).

기능	설명
구매요청관리	수요기관에서 어떤 품목의 물자가 필요할 경우 해당 물자의 종류를 구분하여 전자입찰 서버에 구매요청 관리
입찰품목변경 관리	입찰프로세스 수행 중 입찰 품목 변경이 필요할 경우에 해당 변경 작업 관리
입찰품목접수 관리	해당 입찰 요청 및 입찰 공고 등을 취합하여 입찰 품목접수를 관리
구매결의관리	각종 계약 조건 및 변동 사항 등을 적용하여 구매 결의를 관리
규격검토관리	가장 경제성이 있는 구매가 가능하고 경쟁이 가능하도록 규격을 검토 및 관리
입찰계약관리	낙찰 프로세스와 입찰 프로세스 관리 및 입찰정보 분석 및 낙찰 정보 분석
조달관리	계약 후 조달에 필요한 문서 및 프로세스 관리
관리자모드	전자입찰 서버의 회원 및 수요 업체 , 공급업체 관리 등을 수행
보안모듈	각 프로세스마다의 공정성과 신뢰성, 기밀성을 위해 적절한 인증과 암호화, 전자서명 등을 수행

(표 3.1) 전자 입찰 시스템의 주요 기능

위의 기능들을 수행하기 위해 사용되는 문서의 교환은 XML/EDI의 형식으로 프로세스에 따른 문서 목록은 다음과 같다(표 3.2).

XML/EDI 문서 목록	요청, 입찰	조달
	-조달요청서	-주문서
	-조달변경요청서	-주문응답서
	-조달변경응답서	-발송통지서
	-입찰서	-인수통지서
	-입찰응답서	-송금통지서
	-낙찰통보서	
	-계약서	

(표 3.2) XML/EDI 문서 목록

4. 전자 입찰 시스템의 보안 설계

전자 입찰 시스템위한 보안 설계를 위해서는 크게 인증, 접근제어 및 암호화/전자서명 기술이 요구된다.

(1) 인증 (Authentication)

클라이언트와 서버간의 인증은 PKI(Public Key Infrastructure)를 기반으로 이루어 지며 X.509 Strong Authentication 표준을 기반으로 인증서를 구성해서 인증 절차를 수행한다.

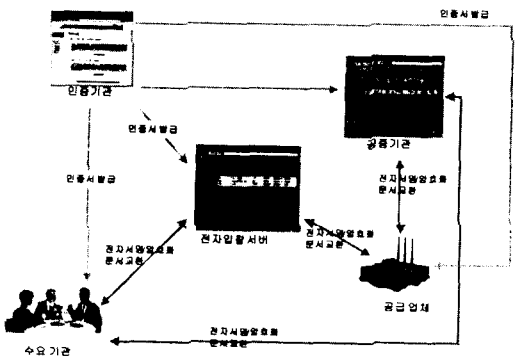
(2) 접근 제어 (Access Control)

접근 제어는 인증된 사용자나 인증되지 않은 사용자에게 권한을 부여해서 특정한 자원에 접근을 허가할 지를 결정하는 것으로써 관리자를 두어서 권한을 설정할 수 있도록 하고, 권한에 따라서 Access Control List(ACL)를 작성하여 자원에 접근할 수 있도록 한다.

(3) 암호화, 전자서명(Cryptography, Digital Signature)

XML/EDI 메시지는 S/MIME 을 이용하여 암호화 또는 전자서명을 한다. 전자서명된 XML/EDI 메시지는 새로 제안된 기술인 XMLDSIG 를 이용하며 암호화나 전자서명이 필요한 문서만을 선택적으로 수행한다.

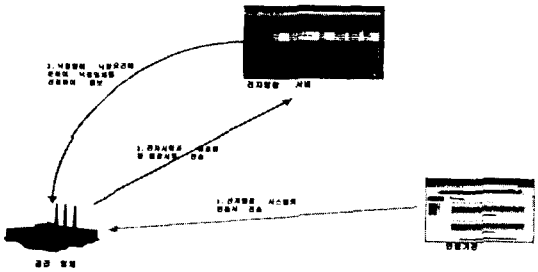
위의 기술들을 기반으로 하는 전자 입찰의 보안 절차는 다음과 같다(그림 4.1).



(그림 4.1) 전자 입찰 시스템의 보안 절차

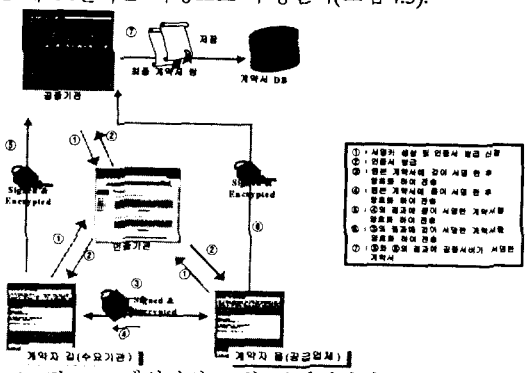
전자 입찰에서의 보안 설계는 입찰 과정에서 입찰 가격을 제출하는 과정에서의 보안과 낙찰이 되어 계약서를 주고 받는 과정에서의 보안 설계으로 구분할 수 있다.

입찰 과정에서 입찰 가격을 제출하는 과정에서의 보안은 입찰에 참가하는 공급업체가 입찰가가 적힌 입찰서를 작성하여 전자 서명과 암호화를 한뒤 전자 입찰 시스템으로 전송하는 과정과 전자 입찰 시스템의 관리자가 낙찰일에 입찰서를 복호화하여 낙찰업체를 선정하는 과정이다(그림 4.3).



(그림 4,2) 입찰 가격 제출과정에서의 보안

계약서의 교환 과정에서의 보안은 공증 기관이 계약자들간의 교환하는 계약서의 유효성을 공증하는 과정과 최종 계약서 쌍은 전자서명/암호화하여 XML/EDI 문서로 DB 에 보관하는 과정으로 구성된다(그림 4.3).



(그림 4.3) 계약서의 교환 과정에서의 보안

5. 참고 문헌

[1]. Sunhee Yoon, Kyun Joon-Ju, In Young Lee, "Desingn and Implementation of Web based Electronic Bidding System", CALS/EC Korea'99, July, Korea

[2] Kate Maddox, Dana Nlankenhorn, Web Commerce, John Wile & Sons, Inc. 1998

[3] Karl Moss, Java Servelets, McGraw-Hill, 1998

[4] XML/EDI, http://www.geocities.com

[5] F.Boumphrey, O. Direnzo et al, "Professional XML Applications", WROX, 1999

[6] S.Berkovits, S.Chokhani, A. Furlong, A.geiter, C.Guild, "public Key Infrastructure Study Final Report", 1997

[7] RFC2026, "Digital Signature for XML", SMLDSIG Working Group, 1999