論文
3-7-5

인터넷 기반 전자입찰시스템의 보안 설계 및 구현 (A Design and Implementation of Secure Electronic Bidding System)

윤 선 희*
(Sun-Hee Yoon)

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 소비자(Business to Customer)간 또는 기업과 기업간(Business to Business)의 전자 거래 관련 응용 프로그램의 개발이 다양해지고 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 웹 기술, 기업간의 문서 교환을 위한 XML/EDI기술 및, 입찰과 계약과정, 조달과정에서 안전성 및 신뢰성을 보장하기 위해 공개키 암호화 기술인 PKI기반 구조의 인증 및 전자서명을 활용한 보안 기능을 설계 및 구현한다.

ABSTRACT

The area of business applications in the internet are extended enormously in result of fast development of computing and communication technologies, increase of internet use, and use of intranet/extranet in enterprise information system. Widely spread the use of the internet, there are various applications for Business to Business (B to B) or Business to Customer(B to C) model that are based on the intranet or extranet. This paper designed and implemented the Web-based Electronic Bidding System for Business to Business (B to B) model. The technical issues of electronic bidding system in the internet are involved in the connection between web client and server, electronic data interchange for the contract document, and security solution during the bidding and contracting processes. The web-based electronic bidding system in this paper is implemented using Java applet and servlet as a connection interface for web client and server, XML/EDI-based documents for a bid and a contract, and bidding server and notary server for enhancing the security using PKI(Public Key Infrastructure)-based public key cryptography, digital signature and Certification Authority (CA).

* 정회원 : 숭의여자대학 인터넷정보과 교수

논문접수 : 2001. 6. 11.
심사완료 : 2002. 6. 28.

1. 서론

최근 인터넷 컴퓨팅의 확산으로 기업의 정보시스템에 인터넷을 활용한 응용시스템의 사용이 활성화되어지고 있다. 본 논문에서는 기업간의 전자상거래 분야에서 문서 교환의 표준으로 자리 잡아 가고 있는 XML/EDI를 기반으로 하며 기업간의 정보의 공유 또는 교환에 있어서 신뢰할 수 있는 보안 기능을 제공하는 전자 입찰 시스템을 제안한다. 본 논문에서 제안하는 전자 입찰 시스템의 특징은 구매 요구에서 입찰, 계약, 조달에 이르기까지 인터넷상에서 이루어지며 문서의 표준화를 통해 기업에서 필요로 하는 비즈니스의 글로벌화를 추구할 수 있으며 인증 절차와 전자 서명 및 공증 과정을 통한 보안 절차가 강화되어 입찰 과정에서의 신뢰성 및 투명성을 제공하는 전자 입찰을 구현한다.

2. 관련 연구

2.1 기존의 전자입찰 시스템 기술 동향 분석

국내에서 개발되었거나 개발 중인 전자입찰 시스템은 전자 입찰 시스템의 프로세스 중 일부가 수동으로 처리되거나 web-EDI를 통해 서식 또는 문서를 교환하는 형태로서 XML/EDI 등과 같은 표준화된 문서의 교환을 기반으로 하는 완전한 전자 입찰 시스템이 제공되고 있다고는 볼 수 없는 실정이다. 현재 일부 인터넷을 통해 제공되는 전자 입찰 시스템은 전자 입찰 신청이나 등록은 인터넷을 통해 가능하나 실제 입찰은 OMR카드를 통한 처리로 실행되고 있다. 또한 계약 과정에 있어서 신뢰할 수 있는 보안이 제공되어 인터넷상에서 전자 서명 또는 인증 및 공증 과정을 통한 계약서를 주고받는 형태의 전자 입찰 시스템이 일부 제공되고 있다.

국외의 전자 입찰 시스템의 경우, 국내에서 제공하는 웹 기반의 전자 입찰 시스템과 유사한 시스템으로 bidpay, Unicom systems 등이 있으며, 최근 타 시스템과의 문서의 공유를 목적으로 하여 표준화를 위해 XML을 기반으로 하는 전자 입찰 시스템에 개발되어 제공되고 있다[2]. 그러나 계약 과정을 포함하는 전자 입찰 시스템이 제공되어 있지 않은 실정이다.

또한 국내외에서 진행 중이거나 사용 중인 전자 입찰 시스템의 대부분이 정부를 상대로 하여 국방, 건설, 토목, 조달 등 특정 분야를 대상으로 실행되는 전자 입찰 시스템으로 구성되어 있어 범용성이 떨어지는 단점을 가지고 있다.

<표 1> 기존 시스템과 제안된 전자입찰시스템의 비교

<Table 1> Analysis Between Electronic Bidding System and Proposed Electronic Bidding System

기존 전자입찰 시스템	제안된 전자입찰 시스템
· Client/Server 환경으로 특정한 프로그램이 있어야만 동작함.	· Internet 환경에서 XML기반의 JAVA Applet의 사용으로 프로그램의 제약이 없어짐
· 보안문제의 취약성으로 신용 및 프로세스에 많은 제약이 있었음.	· 완벽한 128bit보안으로 인하여 사용자의 신용 및 안정성 확보
· 다양한 입찰 프로세스를 지원하지 못하므로 인해 특정 분야에만 적용 가능	· 다양한 입찰 프로세스를 지원하여 특정 분야만의 편중 해소
· 다양한 낙찰 프로세스를 지원하지 못하므로 인하여 특정 분야의 낙찰만 가능함	· 다양한 낙찰 프로세스를 지원하여 범용적인 낙찰이 가능함
· 각 필요에 맞는 서류들의 저장이 매우 불편함	· EDI표준문서의 저장으로 인하여 통일된 서류의 저장이 가능
· 종류에 맞는 서류들의 생성 및 적용이 어려움	· XML/EDI문서를 바탕으로 동적으로 서류들의 생성 및 적용이 가능함
· 복잡한 인터페이스로 처음사용자의 사용이 어려움	· 단순한 Web기반의 인터페이스 제공으로 처음사용자의 사용이 용이함.
· 프로그램에 종속적인 Tag 사용으로 인하여 다른 프로그램에서의 호환이 불가능함	· XML의 특징인 동적 TAG 사용으로 인하여 서버에서 생성된 TAG들이 바로 적용됨

본문에서 제안하여 구현한 전자 입찰 시스템과 기존의 전자 입찰 시스템을 비교 분석하면 다음과 같다.<표 1>.

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

2.2 웹 기술

본 논문에서 제안하는 전자 입찰 시스템은 인터넷 환경에서 클라이언트와 서버간의 통신은 자바 애플릿과 서블릿으로 구현되며 데이터베이스와의 연동은 JDBC를 사용한다. 서블릿을 통한 데이터베이스 연결은 CGI의 사용자 수가 증가함에 따라 프로세스의 증가로 발생하는 성능상의 문제를 해결하면서 2-tier나 3-tier등의 시스템 구조로 분산 환경 모델을 가능하게 해주는 방법이다. 서블릿은 웹 브라우저나 애플릿의 리턴값에 의해 전달 받으며 내부에서 JDBC를 통해 데이터베이스에 연결한 후 질의를 보내고 해당 질의의 검색 결과를 HTML형태나 여러 자료형으로 되돌려 준다. 이때 서블릿은 자바의 멀티 쓰레드를 이용해 질의를 처리하기 때문에 CGI처럼 프로세스를 생성하는 과정에서의 오버헤드를 줄일 수 있으며, 한 번 로드된 서블릿은 메모리상에 계속 존재하기 때문에 여러 번의 데이터베이스 연결 요청에 대해 한번의 연결로 계속 처리할 수 성능향상을 가져올 수 있다. 또한 서블릿은 Java의 플랫폼 독립적인 장점을 통해서 어느 웹서버에서도 실행 될 수 있는 장점을 가지며 보안 측면에서도 자바의 보안 구조에서 제공하는 기능을 모두 사용할 수 있다.

2.3 XML/EDI 기술

2.3.1 XML/EDI

XML/EDI는 현재 무역, 금융, 유통, 조달 등의 분야에서 기업간의 문서 교환에 이용하는 EDI를 XML로 정의하여 인터넷상에서 쉽게 표현하고 사용할 수 있도록 하기 위해 제안된 것으로 XML에 적용되는 모든 기술들을 그대로 이용할 수 있기 때문에 확장성, 유연성, 연동성 등이 뛰어나다[4,5].

2.3.2 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 XML문서가 파싱될 때 사용되며, DTD를 따르고 있는 XML문서를 유효한(valid) 문서라 하고, DTD는 정의되어 있지 않지만 XML 기본 구문규칙에 충실한 XML 문서를 적격(Well-formed) 문서라 한다.

2.3.3 XSLT(extensible Stylesheet Language Transformation)

XSLT는 XML문서를 HTML문서로 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..

2.4 보안 기술

2.4.1 PKI(Public Key Infrastructure)

전자상거래의 안전성, 신뢰성을 만족하기 위해서는 암호기술이 필요하며 암호기술은 크게 비밀키 암호기술과 공개키 암호기술로 나뉜다. 비밀키 암호기술은 속도는 빠른 반면 비밀키의 분배가 복잡하므로 기밀성을 보장하기 위한 많은 양의 암호화에 주로 이용되며 공개키 암호기술은 비밀키 암호화나 키 분배에 주로 이용된다. 공개키 암호기술은 PKI(Public Key Infrastructure)를 기반으로 해서 이루어지며 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 말하며 프

라이버시, 접근 제어, 무결성, 인증, 부인 봉쇄 기능을 제공해야 한다. PKI동작 방식은 최상위 인증기관을 두게 되는데 이를 CA(Certificate Authority 혹은, root CA)라고 하며 CA는 인증서와 공개키를 관리하는 역할을 하게 된다. 인증기관이 구축되고 나면 사용자의 인증서를 발급할 수 있게 되며 사용자가 자신의 공개키를 가지고 인증서를 신청하게 되면 인증서 등록 기관인 RA(Registration Authority)에서 인증서 신청인의 신원을 확인해서 CA에게 인증서 발급을 요청하게 된다. CA는 사용자의 인증서를 발급해서 RA에게 전송하고 RA는 사용자에게 인증서를 송신한다. 발급된 인증서로 사용자는 신분확인을 할 수가 있고 이를 이용하여 안전한 거래가 가능하다[6].

2.4.2 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. 인증서의 형식은 1988년에 ITU-T가 X.509 초기 버전을 공표하고 1993년에 버전 2를 공표했으며 1995년 이후로는 ISO/IEC 9594-8의 문서와 동일시되어 공동 개발되어 왔다. 현재에는 X.509 버전 3까지 공표되었고 인증서의 extensions영역에 대한 개정이 진행되고 있다.

인증서는 인증된 공개키에 해당하는 비밀키가 노출된다든지, 공개키의 소유자가 다른 도메인으로 옮기는 경우 등 여러 가지 이유로 유효기간이 만기 되기 전에 그 효력이 상실될 수 있다. 인증기관은 이렇게 효력이 상실된 인증서들에 대한 목록을 생성해 PKI내에서 관리한다. 인증서 취소 목록(CRL : Certificate Revocation List)은 X.509 버전2 형식을 따르며 인증 정책에 따라 주기적으로 생성된다.

2.4.3 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.

2.4.4 XMLDSIG(XML Digital SIGnature)

EDI문서를 XML로 표현하는데 있어서 전자서명이 적용된 XML 전자서명 문서의 표준 형식으로 IETF(Internet Engineering Task Force)에서 XMLDSIG Working Group이 결성되어 활발한 연구가 진행되고 있다[7].

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

사용자에 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.

2.4.6 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 구현한 전자 입찰 시스템은 인터넷 환경을 기반으로 하여 웹 브라우저를 통한 클라이언트와 서버간의 인터페이스는 자바의 애플릿과 서블릿으로 구현되었으며 서버와 데이터베이스 시스템과의 연동은 JDBC 드라이버를 사용하였다. 전자 입찰 시스템의 클라이언트는 수요 기관과 공급 업체로 분류되며 서버측은 입찰 서버로써 구매, 입찰 및 조달

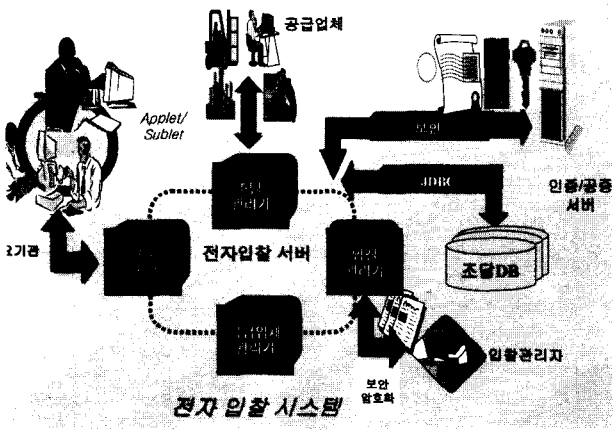
관리를 포함하는 입찰 관리기가 담당하며, 입찰가 등록 및 계약 과정에서 전자 서명키를 사용하기 위한 인증 서버와 공증 서버가 사용된다. 전자 입찰 시스템의 구성도는 다음과 같다[그림1][3].

본 논문에서 구현한 전자 입찰 시스템의 구조는 각종 문서의 생성은 서버가 담당하며 클라이언트 측에서는 문서의 자료만 입력하는 형식으로 Thin Client 모델로 구성되어 진다.

[그림 2]는 전자 입찰 시스템 프로세스의 흐름도를 분석한 것이다.

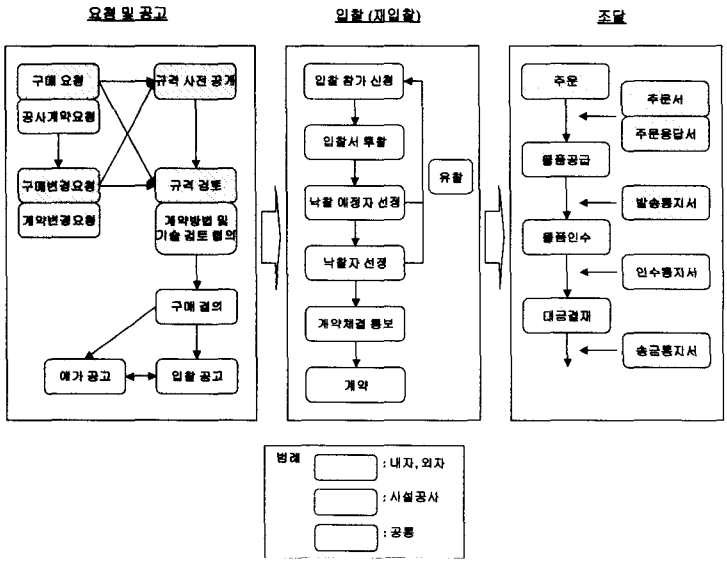
위의 전자 입찰 시스템의 흐름도를 분석하면 다음과 같다.

1) 해당 수요가 필요한 기관은 전자입찰 서버에 접속 수요요청서를 작성하여 전송한다.



[그림 1] 전자 입찰 시스템 구성도

[Fig. 1] Electronic Bidding System Architecture



[그림2] 전자 입찰 시스템 흐름도

[Fig. 2] The Processes of Electronic Bidding System

2) 전자입찰 서버는 수요요청서를 접수 받아 해당 수요요청서를 검색 및 조회할수 있도록 LIST를 작성한다.
3) 수요요청의 변경이 생겼을 때에는 수요요청 변경서를 작성하여 전송한다.
4) 전자입찰 서버는 수요요청변경서를 접수 받아 해당 수요요청 LIST에서 해당 정보를 변경할 수 있다.
5) 규격검토를 위해서 전자입찰 서버는 규격검토서를 작성하여 수요기관에 전송하며 그밖에 규격협의 요청서를 작성하여 수요기관에 규격검토를 의뢰한다.
6) 최종 규격협의를 위하여 전자입찰 서버는 최종규격 협의서의견서를 작성하여 수요기관에 전송하며 수요기관은 해당정보를 다시 전자입찰 서버에 전송한다.
7) 전자입찰 서버에서 계약조건의 협의를 위하여 계약조건 협의서를 작성하여 해당 기관에 전송한다.
8) 해당 기관에서는 계약조건 협의서를 수신한 후 정보를 입력 전송한다.
9) 계약조건 협의서가 완료된 후 전자입찰 서버는 구매결의서를 작성하여 전송한다.
10) 해당기관에서 구매결의서를 수신하여 정보를 전송하면 구매결의가 이루어진다.
11) 전자입찰 서버에서 구매결의 LIST를 출력하여 해당기관에서 신청한 수요요청의 진행 여부를 쉽게 조회할 수 있다.
12) 구매결의 단계 후 전자입찰 서버에서는 입찰공고 의뢰서를 작성하여 수요기관에 전송한다.
13) 수요기관에서 입찰공고 의뢰서를 수신하여 검토한 후 재전송하면 입찰공고가 완료된 것으로 전자입찰 서버가 등록한다.
14) 입찰공고 완료 후, 전자입찰 서버는 입찰공고를 게시한다.
15) 입찰 당일 담당자는 이미 결재를 받아둔 예정가격을 입찰 시스템에 입력한다.
16) 입찰 종결 후, 낙찰기준에 의하여 낙찰예정자에게 낙찰예정 통보를 하는 동시에 전자입찰 서버에서는 낙찰가격이 자동으로 등록되어 입찰의 공정성을 알린다.
17) 개찰 조서, 낙찰통보서등 입찰에 관련된 분석자료 및 보고자료들이 출력되고 입찰업체들의 입찰금액은 예정가격과 낙찰가격비율로 입찰적중률을 계산하고 이것을 업체 등록 자료에 등록시킨다.
18) 낙찰 받은 업체는 주문응답서, 발송통지서, 인수통지서, 송금통지서. 대금결제서등 필요한 서류들을 전자입찰서버와 교환하여 조달을 완료한다.

전자 입찰 시스템의 흐름도에 따라 각 세부 프로세스에서 서비스되는 주요 기능들은 다음과 같다<표2>.

<표 2> 전자 입찰 시스템 주요 기능

<Table 2> The functions of an Electronic Bidding System

구분	관련 기능
요청 및 공고	구매요청 기능, 구매변경요청 기능, 입출품목접수/변경/분류 기능, 제약조건협의 기능, 구매결의 기능, 구매결의 변경 기능, 입출공고 기능, 예가책정 기능, 예가공고 기능, 규격 검토 관리 기능, 규격 사전 공개 기능, 검색기능, 관리자 및 담당자지정 기능
입찰	입찰 참고 신청서 작성 기능, 입찰서 투찰 기능, 낙찰 예정자 선정 기능, 낙찰자 선정 기능, 계약 체결 통보 기능, 계약 기능, 재입찰 기능, 입찰 방법 지정 기능, 낙찰 방법 지정 기능
조달	주문서 작성, 주문 응답서 작성 기능, 발송 통지서 작성 기능, 인수 통지 작성 기능, 송금 통지서 작성 기능, 무너 수신 및 통보 기능

전자입찰시스템의 기능들은 클라이언트와 서버의 기능으로 세부적으로 분류되며 서버의 기능 중 회원의 ACL(Access Control List) 등급에 따른 회원관리 및 인증서 등록, 변경, 폐지 등을 관리하는 인증 관리, 보안키의 생성 및 저장 등에 관련된 기능 등이 지원된다.

4. 전자 입찰 시스템의 보안 설계 및 구현

전자 입찰 시스템을 위한 보안 설계를 위해서는 크게 인증, 접근제어 및 암호화.전자 서명 기술이 요구된다.

4.1 인증 (Authentication)

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

4.2 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.

4.3 암호화, 전자서명(Cryptography, Digital Signature)

XML/EDI 메시지는 S/MIME을 이용하여 암호화 또는 전자서명을 한다. 전자서명된 XML/EDI 메시지는 새로 제안된 기술인 XMLDSIG를 이용하며 암호화나 전자서명이 필요한 문서만을 선택적으로 수행한다.

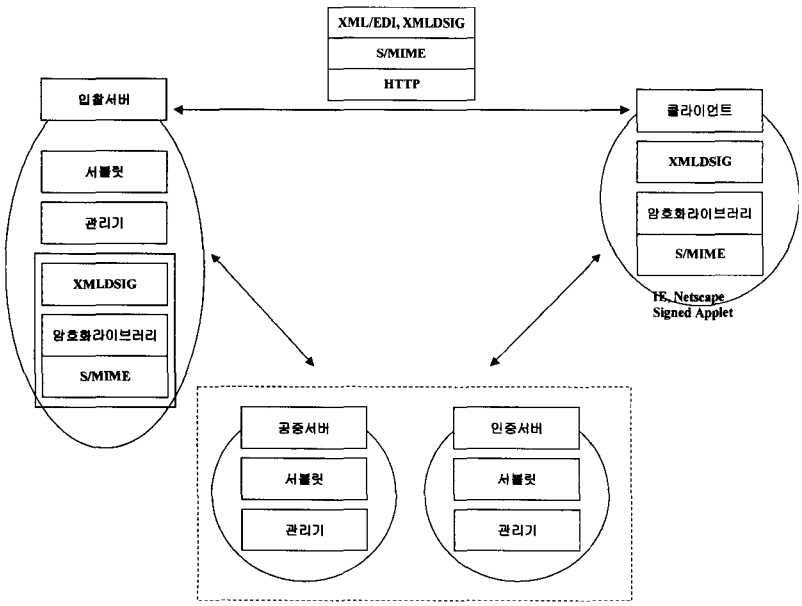
전자 입찰시스템의 보안 모듈에 관한 설계는 다음과 같다[그림 3].

각 모듈에서 사용되는 전자 입찰 시스템에 필요한 보안 문서들은 다음과 같다 <표 3>.

<표 3> 전자 입찰 시스템에 필요한 보안 문서

<Table 3> Security Document List for Electronic Bidding System

종류	적용문서
전자 서명 문서	· 구매 요청서, 구매 변경 요청서, 계약 조건 협의서 · 구매결의서, 입출 공고 의뢰서 · 납품 변경 요구서, 규격 협의 요청서, 규격 협의 의견서, 예가 산정 관련 문서 · 입찰 보증금 정보 문서, 입찰 참가 신청서, 입찰서 (입찰가격) 낙찰 통보서 · 구매 계약 수락 통지서, 구매 계약서 · 주문서, 주문 응답서, 주문 변경요청서 · 발송 통지서, 인수 통지서, 송금 통지서
전자 서명 암호화 문서	· 계약 조건 협의서 · 규격 협의 요청서, 규격 협의 의견서, 산정 관련 문서 · 입찰서 · 구매계약서



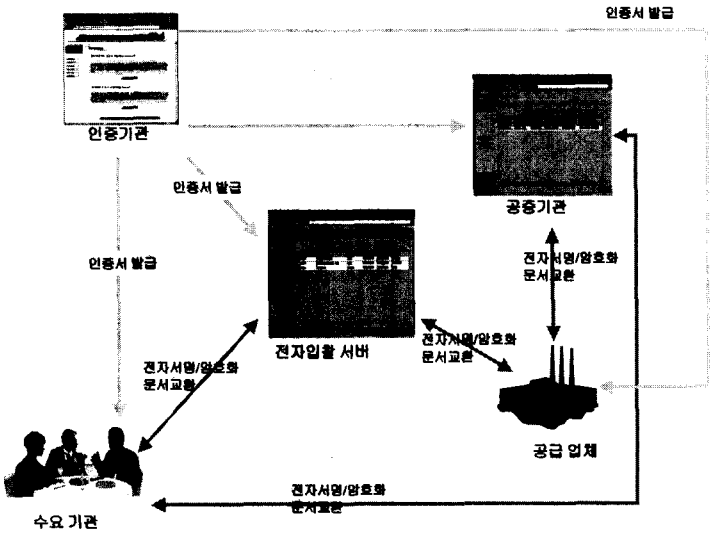
[그림 3] 전자 입찰 시스템의 보안 모듈 설계

[Fig. 3] Security Module Design of Electronic Bidding System

각 모듈을 사용한 전자 입찰시스템의 보안 절차는 다음과 같다[그림 4].

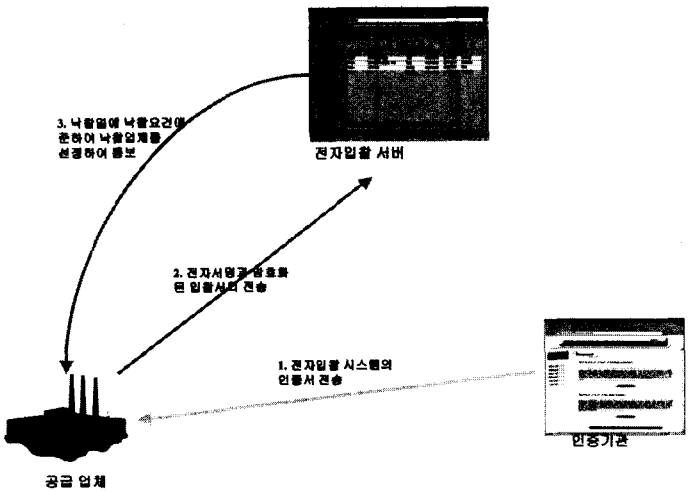
전자 입찰에서의 보안 설계 및 구현은 입찰 과정에서 입찰 가격을 제출하는 과정에서의 보안과 낙찰이 되어 계약서를 주고받는 과정에서의 보안 설계 및 구현으로 구분할 수 있다.

입찰 과정에서 입찰 가격을 제출하는 과정에서의 보안은 입찰에 참가하는 공급업체가 입찰가가 적힌



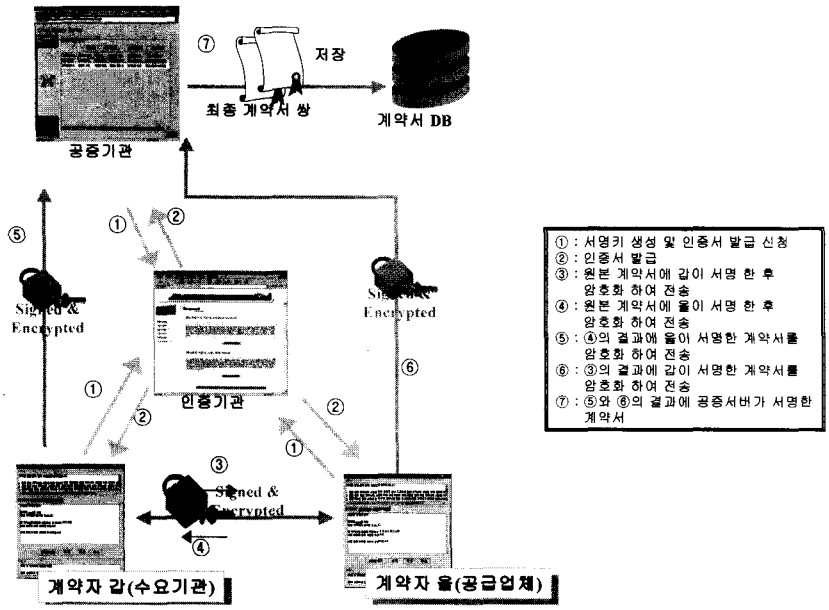
[그림 4] 전자 입찰 시스템의 보안 절차

[Fig. 4] Security procedure of Electronic Bidding System



[그림 5] 입찰 가격 제출과정에서의 보안

[Fig. 5] Security procedure for Submission of Bidding Price



[그림 6] 계약서의 교환 과정에서의 보안

[Fig. 6] Security Procedure of Contract Exchange

입찰서를 작성하여 전자 서명과 암호화를 한 뒤 전자 입찰 시스템으로 전송하는 과정과 전자 입찰 시스템의 관리자가 낙찰일에 입찰서를 복호화하여 낙찰업체를 선정하는 과정이다 [그림 4].

계약서의 교환 과정에서의 보안은 공증 기관이 계약자들 간의 교환하는 계약서의 유효성을 공증하는 과정과 최종 계약서 쌍은 전자서명/암호화하여 XML/EDI문서로 DB에 보관하는 과정으로 구성된다 [그림6].

5. 결론

본 논문에서는 인터넷 환경에서 기업과 기업간 전자 거래 형태인 응용 프로그램의 하나로 전자 입찰 시스템을 설계 및 구현하였다. 구현된 전자 입찰 시스템은 클라이언트와 서버간의 인터페이스를 애플릿과 서블릿으로 구현하여 Java의 플랫폼 독립적인 장점을 통해서 어느 웹 서버에서도 실행 될 수 있는 장점을 가지며 서블릿을 통한 데이터베이스 연결로 CGI의 사용자 수가 증가함에 따라 프로세스의 증가로 발생하는 성능상의 문제를 해결하였다. 또한 각 기업간에 교환되는 문서의 형식을 XML/EDI로 기업간의 문서 공유 및 교환의 호환성이 이루어지게 한다. 또한 입찰 과정에서 필요한 보안 문서들을 생성하며 입찰 프로세스 중 입찰 가격이나 계약의 보안 및 인증을 위해 PKI 기반의 전자 서명 방식을 사용하는 보안 기술을 적용하였으며 인증 서버와 공증서버를 사용하여 기업간의 교환되는 문서의 안정성 및 신뢰성을 보장하도록 보안 설계를 강화하였다.

추후 과제로는 본 논문에서 포함하지 않은 확장형 데이터 타입을 정의 할 수 있으며 DTD의 문제점을 보완한 스키마 기반의 XML문서에 관한 연구 및 전자 입찰 프로세스뿐만 아니라 타 업무 시스템으로도의 전환이 용이할 수 있도록 비즈니스 흐름 관리를 위한 연구가 이루어 져야 한다.

※ 참고문헌

[1] 윤선희, 웹기반의 XML을 활용한 전자 입찰 시스템의 설계 및 구현 , 정보시스템연구 논문지, 제10권 제1호, 한국정보시스템학회, 2001

[2] XML implementation white paper Version 1.2, Bid.com International Inc, May, 2000

[3] Sunhee Yoon, Kyung Joon Ju, In Young Lee, Design and Implementation of Web based Electronic Bidding System, CALS/EC Korea'99, July, Korea

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

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

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

[6] X.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

윤 선 희

1983.2 숭실대학교 전자계산학과 졸업(학사)
1986.12 웨인주립대학교 전자계산학과 졸업(석사)
2000.2 성균관대학교 정보공학과 졸업 (박사)
1986년 ~ 1990년 CSDC, DUCOM, 시스템 분석가
1991. 2 ~ 1998. 7 KIST시스템공학연구소 선임연구원
1998.7 ~2000.2 한국전자통신연구원 선임연구원
2000. 3 ~ 현재 숭의여자대학 인터넷정보과 교수