「정보시스템연구」 제 10권 제 1호
한국정보시스템 학회
2001년 06월, pp. 127-146.

웹 기반의 XML을 활용한 전자 입찰 시스템의 설계 및 구현

윤 선 희 숭의여자대학 전자계산학과 shyoon@sewc.ac.kr

<목 차>

Ⅰ. 서 론

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 다양해지고 있다. 기업과 기업간의 전자 거래는 미래의 기업 형태가 특정 제품의 이익 실현을 여러 기업이 각 기업에서 제공 가능한 특성화 부분에 따라 공동으로 참여하였다가 해체되는 형태의 가상 기업의 토대가 될 수 있다. 이러한 기업간의 전자 거래에 있어서 정보의 공유 또는 교환의 필수 요소는 공유 또는 교환되어 지는 데이터의 형태가 표준화되어 추가적인 데이터의 가공 또는 변환 과정을 거치지 않고 사용할 수 있도록 제공되어져야 한다. 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 인터넷상에

서 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.

Ⅱ. 관련 연구

2.1 기존의 전자입찰 시스템 동향 분석

국내에서 개발되었거나 개발 중인 전자입찰 시스템은 전자 입찰 시스템의 프로세스 중 일부가 수동으로 처리되거나 e-mail을 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 주고 받는 형태의 전자 입찰 시스템은 제공되고 있지 않다.

국외의 전자 입찰 시스템의 경우, 국내에서 제공하는 전자 입찰 시스템과 유사하나 최근, 타 시스템과의 문서의 공유를 목적으로 하여 표준화를 위해 XML을 기반으로 하는 전자 입찰 시스템에 개발되어 제공되고 있다. 그러나 계약 과정을 포함하는 전자 입찰 시스템이 제공되어 있지 않은 실정이다.

2.2 XML/EDI (eXtensible Markup Language/ Electronic Data Interchange)

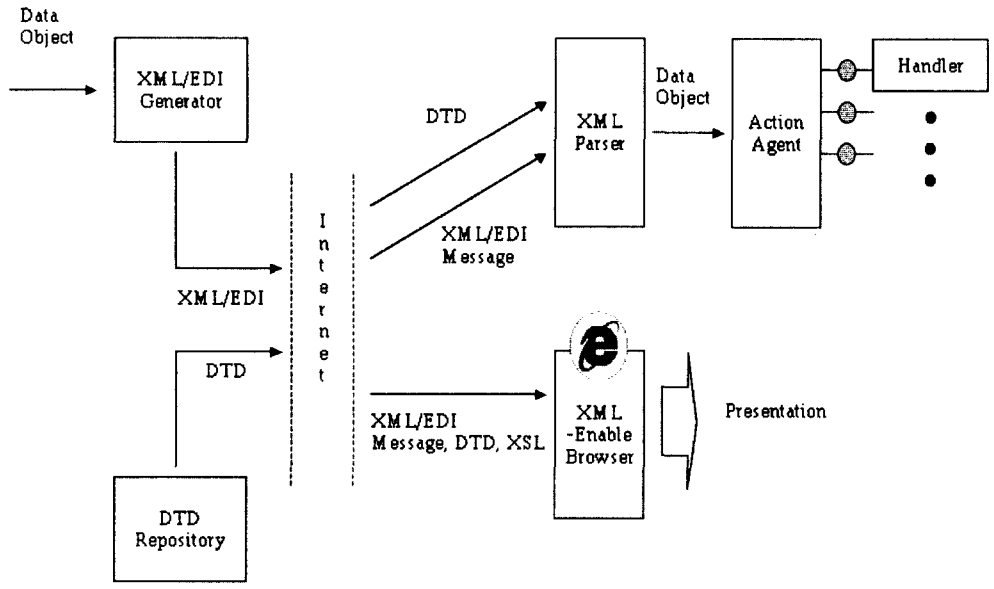
(1) XML/EDI

XML/EDI는 현재 무역, 금융, 유통, 조달 등의 분야에서 문서 교환에 이용하는 EDI를 XML로 정의하여 인터넷상에서 쉽게 표현하고 사용할 수 있도록 제안된 것이다. XML은 DTD(Document Type Definition)를 이용하여 다양한 문서를 쉽게 정의할 수 있고 Style Sheet 언어로 동일한 문서를 다양한 형태로 표현할 수 있으며, XML Viewer와 같은 하나의 소프트웨어만으로 다양한 분야에서 이용할 수 있고 VAN(Value Added Network)과 같은 별도의 네트워크를 구축하지 않고 인터넷을 이용함으로써 초기 구축비용이 절감된다는 장점 때문에 EDI에서도 XML을 이용하고자 XML/EDI가 탄생하게 되었다.

XML의 장점은 플랫폼이나 프로그램 및 언어에 상관없이 유니코드로 제공되어 독립적으로 실행 가능하다. 또한 HTML과 함께 웹프로그램에 있어서 응용 프로그램 자체 또는 객체로써 다른 응용 프로그램 개발에 있어서 유연하게 제공되며 추가

적인 가공 처리 없이 클라이언트를 위한 지역의 데이터 응용에 직접 사용 할 수 있으며 데이터베이스의 갱신 및 통합이 가능하다.

EDI는 현재 무역, 금융, 회계 유통, 조달 등의 분야에서 표준이 존재하며 이러한 분야에 이용되는 EDI 표준 전자 문서들은 모두 XML/EDI로 표현이 가능하다. 우선 EDI문서를 XML 문서로 재정의하기 위하여 문법을 나타내는 DTD를 작성해야 한다. DTD가 작성된 XML 문서는 실제 인터넷상에서 다양한 프로토콜을 이용하여 교환하게 되며, XML Viewer를 이용하여 XSL(eXtensible Stylesheet Language)에 정의된 형태로 사용자에게 보여지게 된다. XSL은 XML문서를 화면에 어떠한 형태로 출력할 것인가를 정의하는 것으로 같은 XML 문서가 다양한 형태로 표현될 수 있기 때문에 사용자들의 다양한 요구를 충족시킬 수 있게 된다. XML/EDI 시스템의 구성도는 [그림 1]과 같다.



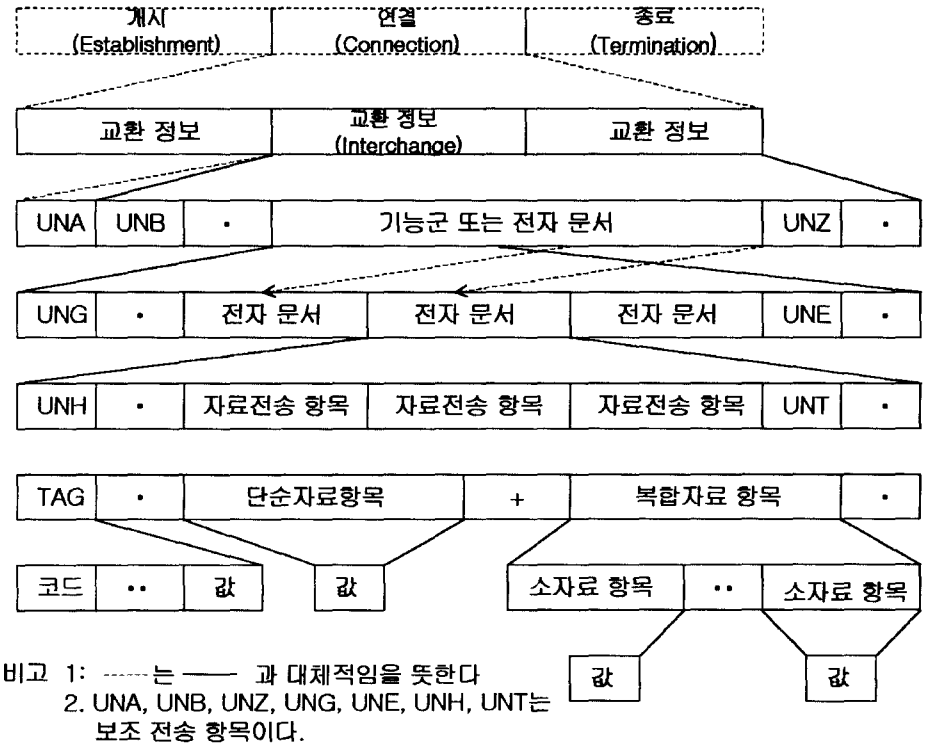
[그림 1] XML/EDI 시스템 구성도

(2) EDI(Electronic Data Interchange)

EDI는 기업간 정보 시스템의 문서 교환의 대표적인 형태로 주문서, 계산서와 같이 기계가 직접 읽고 처리할 수 있는 정형화된 문서에 대하여 자료의 내용을 표현하는 기호(data code 또는 semantic) 및 자료의 항목별 표준 배열 순서 (data format 또는 syntax)에 의해 표준화된 형태로 전자 문서 통신 매체를 통하여 교환하는 방식

을 말한다. 간단하게 '기업간의 전자적 문서 교환'으로 정의할 수 있다. 우리 나라에서는 국가 효율성 증대와 경쟁력 강화 차원에서 1980년대 후반부터 EDI가 도입되어 초기에는 무역 자동화 업무를 중심으로 실행되었으며 최근에는 물류, 의료, 제조업, 금융기관, 정부 조달 등에까지 확산되고 있는 추세이다. 그러나 아직까지 법, 제도, 시장 구조, 상호 접속과 요금, 이용자 환경 등 EDI 발전을 위한 환경적인 제반 요소들이 정착되지 못하고 있고, 중소 기업의 경우, 막대한 초기 EDI 시스템 도입 비용 때문에 어려움을 겪고 있어 EDI 사업의 확산과 보급에 장애요인으로 작용하고 있다. 이에 전통적 EDI의 문제점들을 보완하려는 차세대 EDI 기술에 대한 연구가 급속히 진행되고 있으며 최근 가장 현실적인 대안으로 떠오르고 있는 것이 XML/EDI이다. EDI의 구조도는 [그림 2]와 같다.

[그림2]의 EDI 구조도에 따라 조달 요청서를 EDI메시지로 변환하면 다음과 같이 표현할 수 있다 [그림 3].



[그림2] EDI 구조도

```
JNH+1+SUPREQ:S:93A:KE'
BGM+SUPREQ001'
DTM+2:19990728:203'
ALI+++1' (1:내자, 2:외자, 3:시설공사)
FTX++++일반회계'
NAD++J123456+(주)장미디자인 인터랙티브 홍길동+강남구 청담동 59-8 은성빌딩 15
층+서울++135-763+KR'
CTA++1:임호희연구소'
COM+512-7241(39)'
UNS+D'
UNH+1'
RFA+COM123456'
MOD+++:::컴퓨터, 주변기기'
QTY+1:5:SET'
ALI+++1:2' (1:선정수, 2:후정수) (1:선고지, 2:후고지)
DTM+2:19990828:203'
MOA+9:5000000:WON'
FTX++++인터넷PC'
PRI+CAL:1000000'
LOC++KR:82-5+:::청담동 은성빌딩 15층
TOD+++:::직접전달'
UNH+2'
RFA+MON123456'
MOD+++:::모니터'
QTY+5'
ALI+++1:2' (1:선정수, 2:후정수) (1:선고지, 2:후고지)
DTM+2:19990828:203'
MOA+9:2000000:WON'
FTX++++SAMSUNG SyncMaster17CLS'
PRI+CAL:400000'
LOC++KR:82-5+:::청담동 은성빌딩 15층
TOD+++:::직접전달'
UNS+S'
```

[그림3] 조달 요청서의 EDI 문서 예제

(3) XML/EDI 문서 변환

XML/EDI는 최근 기업 내부의 통합 정보 시스템의 전자 문서 표준으로 많이 사용되고 있는 XML 기술을 메시지에 적용함으로써 여러 가지 전통적인 EDI 시스템의 문제점을 해결하고자 하는 것이다. XML/EDI는 EDI를 통하며 교환된 데이터를 XML을 적용한 다른 업무 프로세스에 바로 적용될 수 있는 개방적 구조를 가지기 때문에 업무 효율성의 제고 등 실질적인 EDI 도입의 효과를 얻을 수 있게 된다. 또한 인터넷을 기반으로 하기 때문에 수많은 중소 기업들이 저렴한 구축/운영 비용으로 EDI에 참여할 수 있기 때문에 향후 EDI를 활성화 할 수 있는 대안으로 받아들여지고 있다. 그림[2-3]의 EDI 문서를 XML/EDI문서로 변환한 결과는 다음과 같다[그림4].

```
<DTM>19990728</DTM>
<AU1 C="1"/>
<ACCNAME>일반회계</ACCNAME>
<REQUESTER>
<NAD Code="J123456" Company="(주)정보디자인인터넷트레이드" PName="홍
길동" City="서울"
PostCode="135-763" Country="KR">강남구 청담동 53-8 은성빌딩 15층
</NAD>
 <CTA Id="DEPT">암호화연구소</CTA> <CTA Id="PER">이인영</CTA>

 <COM Qualifier="TEL">518-7241(39)</COM> <COM
Qualifier="FAX">516-6395</COM>
</REQUESTER>
<ITEMS> <ITEM><LIN>1</LIN>
  <PIA>COM123456</PIA>
  <IMD>컴퓨터, 주변기기</IMD>
  <QTY Unit="SET">5</QTY>
  <AU2 C1="1" C2="2"/>
  <DTM>19990828</DTM>
  <MOA>5000000</MOA>
  <NORM>인터넷PC</NORM>
<PRI>1000000</PRI>
  <LOC Country="KR" City="서울">청담동 은성빌딩 15층</LOC>

  <TOD>직접전달</TOD> </ITEM>
 <ITEM><LIN>2</LIN>
  <PIA>MON123456</PIA>
  <IMD>모니터</IMD>
  <QTY>5</QTY>
  <AU2 C1="1" C2="2"/>  <DTM>19990828</DTM>
  <MOA>2000000</MOA>
  <NORM>SAMSUNG SyncMaster 17GLSI</NORM>
```

[그림 4] 조달 요청서의 XML/EDI 변환 문서 예제

(4) DTD(Document Type Definition)

DTD 마크업 언어(Markup Language)의 구문 규칙을 정의하기 위한 표준으로 요소(Element)에 포함될 수 있는 항목(Attribute)의 자료형 등을 정의한다. DTD는 XML파서에 의해 XML문서가 파싱될 때 사용되며, DTD를 따르고 있는 XML문서

를 유효한(valid) 문서라 하고, DTD는 정의되고 있지 않지만 XML 기본 규칙에 충실한 문서를 XML문서를 적격(well-formed) 문서라 한다. 문서의 적격성이라고 하는 것은 어떤 문서가 하나의 XML문서로 간주되는 데 필요한 최소한의 필수 조건들의 집합을 의미하며 그러한 필수 조건들은 문서에 쓰인 용어들이 정확하고 적절한가, XML 사양에 정의된 방식대로 짜여져 있는가에 관련된 것을 말하며 필수 조건들 중 하나라도 만족하지 못할 경우에는 심각한 오류로 간주되어 문서 처리를 중단해야 하는 발생한다. 유효한 문서가 되기 위해서는 DTD에 정의된 문서의 전반적 구조와 요소나 특성에 사용할 수 있는 데이터형들을 정확히 지켜야만 한다. XML/EDI문서는 모두 유효한 문서이어야 한다. [그림 5]는 조달 요청서 예제의 DTD를 나타낸 것이다.

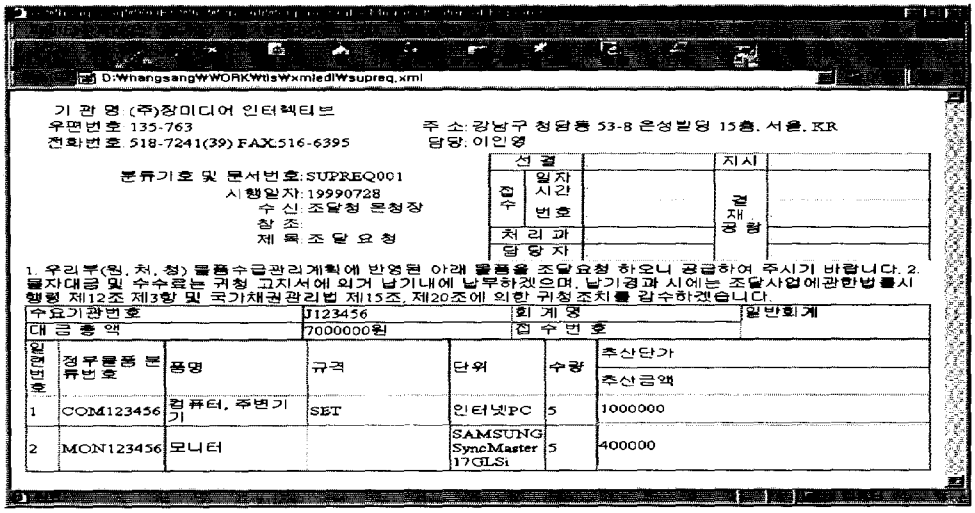
```
<!-- SUPREQ 조달요청서, 구매요청서 -- >
<!ELEMENT SUPREQ        (BGM, DTM, ALI1, ACCNAME, REQUESTER, ITEMS, TotalMOA) >
<!ATTLIST SUPREQ
          KEDIFACT-Prefix       CDATA   #FIXED                 "UNH"
          RefNo                 CDATA   #IMPLIED
          MessageTypeID         CDATA   #FIXED          "SUPREQ"
          Version               CDATA   #FIXED                  "D"
          ReleaseNumber         CDATA   #FIXED          "96A"
          Agency                CDATA   #FIXED          "UN"
          AssociationCode       CDATA   #FIXED                  ""      >

<!ELEMENT REQUESTER     (NAD, CTA*, COM*)+ >
<!ELEMENT ITEMS         (ITEM+) >
<!ELEMENT ITEM          (LIN, PIA, IMD, QTY, ALI2, MOA, NORM, PRI, LOC*, TOD*) >

<!-- BGM 전자문서시작(Beginning of message)-- >
<!ELEMENT BGM           (#PCDATA) >
<!ATTLIST BGM
          KEDIFACT-Prefix       CDATA   #FIXED                  "BGM"
          Type                  CDATA   #FIXED          ""
          Agency                CDATA   #FIXED          ""      >
```

[그림 5] 조달 요청서의 DTD 예제

(5) XSLT(eXtensible Stylesheet Language Translation)

XSLT는 XML문서를 HTML문서로 변환해 줄 수 있기 때문에 HTML 브라우저를 통해서 볼 수 있다. XSLT를 사용할 경우, 하나의 XML/EDI문서를 HTML브

라우저를 통해서 다양한 형태로 출력할 수 있다는 장점이 있으므로 사용자가 원하는 형태로 서비스를 제공해 줄 수 있으며 동일한 문서를 프레젠테이션 레벨에서 다양하게 처리를 해줄 수 있기 때문에 소프트웨어 개발 비용이 절감될 수 있다 다음은 조달 요청서 예제를 XSLT로 변환한 문서를 웹 브라우저를 통해서 확인한 것이다[그림 6].


D:₩hangsang₩WORK₩tis₩xmledi₩supreq.xml

기 관 명 (주)장미디어 인터렉티브
우편번호 135-763 주 소: 강남구 청담동 53-8 은성빌딩 15층, 서울, KR
전화번호 518-7241(39) FAX:516-6395 담당: 이인영

분류기호 및 문서번호: SUPREQ001
시행일자: 19990728
수 신: 조달청 본청장
참 조:
제 목: 조 달 요 청

선결		지시	
접수	일자 시간	결재 공람	
	번호		
처리과			
담당자			

1. 우리부(원, 처, 청) 물품수급관리계획에 반영된 아래 물품을 조달요청 하오니 공급하여 주시기 바랍니다. 2. 물자대금 및 수수료는 귀청 고지서에 의거 납기내에 납부하겠으며, 납기경과 시에는 조달사업에관한법률시행령 제12조 제3항 및 국가채권관리법 제15조, 제20조에 의한 귀청조치를 감수하겠습니다.

수요기관번호	J123456	회 계 명	일반회계
대 금 총 액	7000000원	접 수 번 호	

일련번호	정부물품 분류번호	품명	규격	단위	수량	추산단가 / 추산금액
1	COM123456	컴퓨터, 주변기기	SET	인터넷PC	5	1000000
2	MON123456	모니터		SAMSUNG SyncMaster 17GLSi	5	400000

[그림 6] 조달 요청서의 XSLT변환 결과 예제

2.3 보안 적용 기술

전자 입찰 과정에서 발생하는 문서교환과 일련의 작업들이 인터넷상에서 이루어지기 때문에 서로 안전하고 신뢰할 수 있도록 암호 기술들을 적용해야 하며 특히, 공개키 암호 기술로써 안전한 통신을 하기 위해서는 다음과 같은 보안 기술과 알고리즘이 적용 된다.

(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 제공하

는 객체들의 네트워크를 말하며 프라이버시, 접근 제어, 무결성, 인증, 부인 봉쇄 기능을 제공해야 한다. PKI동작 방식은 최상위 인증기관을 두게 되는데 이를 CA(Certificate Authority 혹은, rootCA)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.

(2) X.509 Certificate, CRL(Certificate Revocation List)

인증서는 사용자의 신분과 공개키를 연결해 주는 문서로 인증기관의 비밀키로 전자 서명하여 생성된다. 이는 사용자의 공개키가 실제로 사용자의 것임을 증명해 주며 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 만기되기 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.

(3) XMLDSIG, S/MIME(Secure Multi-purpose Internet Mail Extension), PKCS#7(Public-Key Cryptography Standards#7)

XMLDSIG는 XML에 전자서명이 적용된 XML 전자서명 문서의 표준 형식으로 IETF(Internet Engineering Task Force)에서 XMLDSIG Working Group이 결성되어 활발한 연구가 진행되고 있다.

S/MIME(Secure Multi-purpose Internet Mail Extension)는 개인의 프라이버시 보호 즉, 거래 당사자와 거래 내역의 보호를 위해서는 전자서명 기술과 암호화 기술이 사용된다. 또한, 전자화폐의 이중 사용 방지를 위해서는 암호 프로토콜 기술이 사용되는데 전자상거래 행위의 부인 방지는 암호 프로토콜의 인증 기술로 구현이 된다. 사용자에 대한 인증과 거래 내용 인증을 동시에 제공하는 전자서명 기술은 전자상거래에 있어서 중요한 보안 기술로서 그 중에서 다양한 플랫폼에 걸친 안전한 전자우편 서비스를 하는 것이 S/MIME이며 공개키 암호화와 전자서명을 활용하는 전자우

편 패키지에 응용될 수 있다.

(4) 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. 이 표준은 서명된 데이터에 대해서 Privacy-Enhanced Mail(PEM)과 상호호환이 되며 PEM에서 제안한 것과 같이 인증서 기반의 키 관리에 있어서 다양한 구조를 제공해 준다.

(5) SEED(128-bit Symmetric Block Cipher), RSA(Rivest Shamir Adleman), KCDSA(Korean Certificate-based Digital Signature Algorithm), HAS-160(Hash Algorithm Standard-160)

암호 알고리즘은 암·복호화에 사용되는 키의 특성에 따라 암·복호화 키가 같은 대칭키 암호알고리즘과 암·복호화 키가 서로 다른 공개키 암호 알고리즘으로 크게 구분할 수 있으며, 대칭키 암호 알고리즘은 데이터 처리 형식에 따라 스트림 암호 알고리즘과 블록 암호 알고리즘으로 나눌 수 있다. SEED는 국내 표준으로 개발, 규정되어 전자상거래, 전자 금융 거래, 무역 업무 자동화 등에 활용되고 있는 대칭키 암호 알고리즘으로, 블록 단위로 메시지를 처리하는 블록 암호 알고리즘이다. 대칭키 블록 암호 알고리즘은 비밀성을 제공하는 암호시스템의 중요 요소이다. n비트(블록 크기) 블록 암호 알고리즘이란 고정된 n비트 평문을 같은 길이의 n비트 암호문으로 바꾸는 함수를 말하며 이러한 변형 과정에 암·복호화 키가 작용하여 암호화와 복호화를 수행한다.

RSA(Rivest Shamir Adleman)는 인수분해 문제 해결의 높은 난이도를 이용한 가장 대표적인 공개키 암호 시스템으로 1978년 미국의 MIT에서 최초로 개발되었다. 암호학에서 관심을 갖는 인수분해 문제는 두 소수의 곱으로 이루어진 큰 정수 n을 다시 소수 분해하는 것으로 RSA 암호 시스템의 키 값은 이러한 정수 n과 e(1과 n-1사이의 적당한 수)의 쌍으로 이루어져 있으며 일반적으로 이러한 큰 정수 n에 대한 인수분해는 매우 어렵다고 알려져 있다. 따라서 인수분해를 위한 효과적인 알고리즘이 없으므로 정수 n을 매우 큰 수로 정하면 시스템의 보안성을 크게 향상시킬 수 있다. RSA 암호 시스템은 암호화뿐만 아니라 전자서명의 용도로도 사용될 수 있다. 이 때에는 비밀키로 전자서명을 하고 공개키로 복호화하는 것만 다르고 암호화와 동일하다.

1993년 말 전자서명의 국내 표준의 필요성으로 인해 개발된 KCDSA(Korean Certificate-based Digital Signature Algorithm)는 1998년 말 정보통신단체표준으로 제정이 되었으며 인증서를 기반으로 하는 전자서명 알고리즘이다. 전자서명은 인감도장이나 사인처럼 개인의 고유성을 주장하고 인정받기 위해 전자적 문서에 서명하는 방법으로 위조 불가(unforgeable), 서명자 인증(authentic), 부인 방지(non-repudiation), 변경 불가(unalterable), 재사용 불가(non reusable)의 5가지 특성들

을 만족해야 한다.

1998년에 제정된 국내 표준 해쉬 알고리즘으로 해쉬 알고리즘은 임의의 유한 길이의 입력 값을 고정된 크기의 출력 값(160비트)으로 바꾸는 함수로 이때 출력 값을 해쉬 값(hash value), 혹은 메시지 다이제스트(message digest)라 부른다. 암호학적으로 이용되는 해쉬함수는 일방향 해쉬 함수로 변수를 통해 함수 값을 구하는 연산 즉, 주어진 x에 대해 f(x)를 구하는 것은 쉽지만, f(x)=0에서 x를 구하는 것은 매우 어려운 함수를 말하며 공개키 암호화에 있어서 핵심적인 개념이다. 일방향 해쉬 함수는 다음의 3가지 조건을 만족해야 한다.

- 해쉬 값을 이용해 원래의 입력 값을 추정하는 것은 계산상으로 불가능해야 한다.

- 입력 값과 해당하는 해쉬 값이 있을 때, 이 해쉬 값에 해당하는 또 다른 입력 값을 구하는 것은 계산상으로 불가능하여야 한다.

- 같은 해쉬 값을 갖는 두 개의 다른 입력 값을 발견하는 것은 계산상으로 불가능하여야 한다.

해쉬 함수의 이러한 성질은 전자서명에서 송신자 이외의 제3자에 의한 문서 위조를 방지하는 부인 방지 서비스를 제공하기 위한 필수 조건이다.

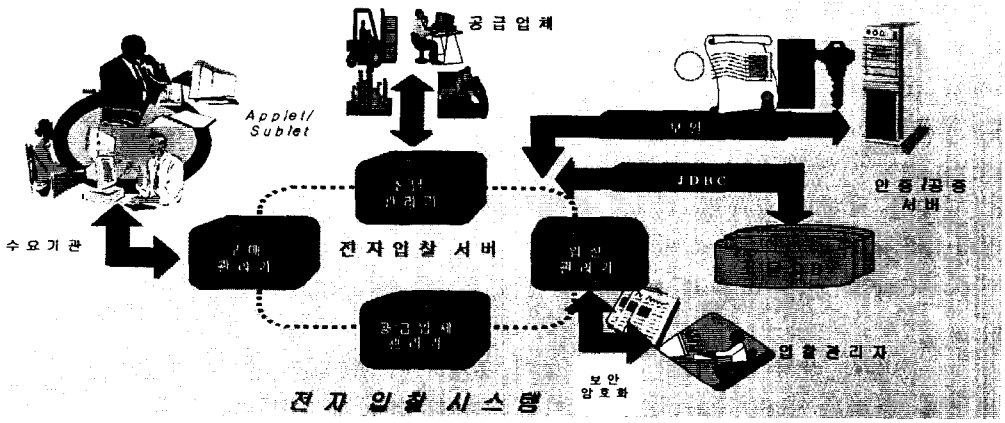
본 논문에서 구현한 전자 입찰 시스템은 이러한 기술들을 적용함으로써 안전한 문서교환이 가능하게 되며 입찰 과정 및 계약 과정에서 발생할 수 있는 보안을 보장하여 안전한 전자상거래가 이루어질 수 있도록 설계 및 구현되었다.

Ⅲ. 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[그림7].

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

전자 입찰 시스템의 구조도에 따라 각 구조에서 서비스되는 주요 기능들은 다음과 같다<표1>.



[그림7] 전자 입찰 시스템 구성도

기능	설명
구매 요청관리	수요기관에서 어떤 종류의 물자가 필요할 경우 해당 물자의 종류를 구분하여 전자입찰 서버에 구매요청 관리
입찰품목 변경 관리	입찰프로세스 수행 중 입찰 품목 변경이 필요할 경우에 해당 변경 작업 관리
입찰품목 접수 관리	해당 입찰 요청 및 입찰 공고 등을 취합하여 입찰 품목접수를 관리
구매결의 관리	각종 계약 조건 및 변동 사항 등을 적용하여 구매 결의를 관리
규격 검토 관리	가장 경제성이 있는 구매가 가능하고 경쟁이 가능하도록 규격을 검토 및 관리
입찰 계약 관리	낙찰 프로세스와 입찰 프로세스 관리 및 입찰정보 분석 및 낙찰 정보 분석
조달관리	계약 후 조달에 필요한 문서 및 프로세스 관리
관리자 모드	전자입찰 서버의 회원 및 수요 업체 , 공급업체 관리 등을 수행
보안 모듈	각 프로세스마다의 공정성과 신뢰성, 기밀성을 위해 적절한 인증과 암호화, 전자서명 등을 수행

<표1> 전자 입찰 시스템 주요 기능

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

전자 입찰 시스템의 기능들을 수행하기 위해 사용되는 문서의 교환은 XML/EDI의 형식으로 프로세스에 따른 문서 목록은 다음과 같다<표2>.

	요청/ 입찰	조달
XML/EDI 문서 목록	- 조달 요청서 - 조달 변경 요청서 - 조달 변경 응답서 - 입찰서 - 입찰 응답서 - 낙찰 통보서 - 계약서	- 주문서 - 주문 응답서 - 발송 통지서 - 인수 통지서 - 송금 통지서

<표 2> 전자 입찰 시스템 XML/EDI 문서 목록

[그림8]은 전자 입찰 시스템 프로세스의 일반적인 흐름도를 분석한 것이다.

흐름도상에 나타나지 않은 프로세스 중, 규격 검토가 이루어지는 입찰일 경우, 클라이언트의 규격 검토관리에서 규격 협의 요청서를 수신하여 규격 협의 의견서를 작성 및 발송하여 서버로부터 최종 규격 협의서를 수신하며, 예가 산정일의 결정 통보를 수신한다. 또한 서버의 규격 관리 기능에서는 규격 검토서를 작성하여 클라이언트에 발송하며, 최종 규격 협의 의견서의 작성 및 발송 기능 등을 담당한다.

전자 입찰 시스템의 계약 프로세스 과정에서 비밀성, 인증, 무결성 및 부인 봉쇄를 보장하기 위한 보안 및 인증 처리는 다음과 같다.

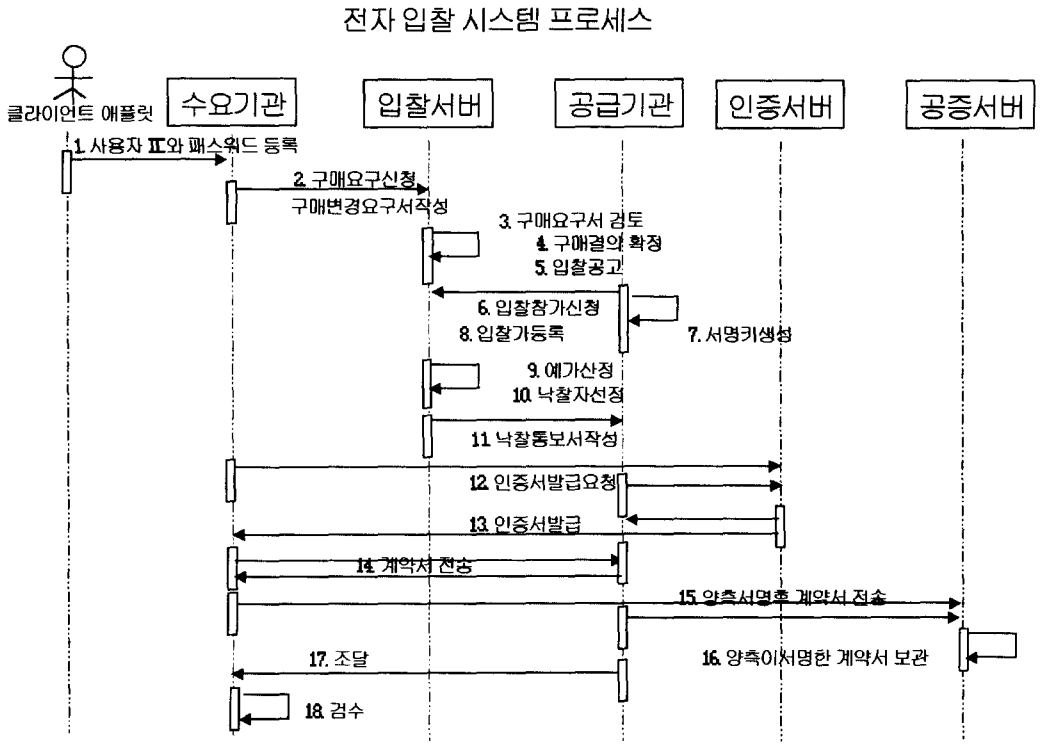
단계 1. 수요 기관과 공급 기관은 인증 서버에 인증서 발급을 신청한다.

단계 2. 인증 서버는 각 기관에 인증서를 발급한다.

단계 3. 수요 기관은 원본 계약서에 서명을 한 후 공급 기관에 전송하며 공급 기관도 마찬가지로 원본 계약서에 서명을 한 후 수요 기관에 전송한다.

단계 4. 수요 기관은 공급 기관에서 전송한 계약서에 서명을 한후 공증서버에 전송하며 공급 기관도 수요 기관에서 전송한 계약서에 서명을 한 후 공증 서버에 전송한다.

단계 5. 공증 서버는 각 기관에서 전송한 계약서에 서명을 하여 최종 계약서 쌍을 보관한다.



[그림8] 전자 입찰 시스템 흐름도

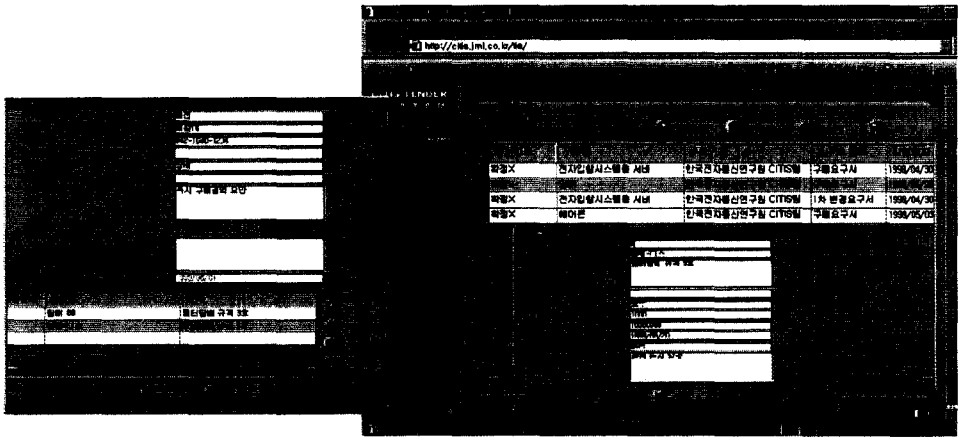
Ⅳ. 전자 입찰 시스템의 구현

구현된 전자 입찰 시스템 프로토타입의 개발 환경은 다음과 같다.

- 플랫폼 - 펜티엄 PC, Windows NT 서버, SUN 워크스테이션
- 운영체제 - Windows95, NT, Solaris
- 데이터베이스 시스템 - 오라클
- 웹 브라우저 -MS Explore, Netscape
- 웹 서버 - NT IIS 5.0
- JDBC 드라이버 - 오라클 JDBC Thin Driver
- 개발언어/도구 - Java JDK, Java JFC Swing, Jbuilder, Plug & Play1.1

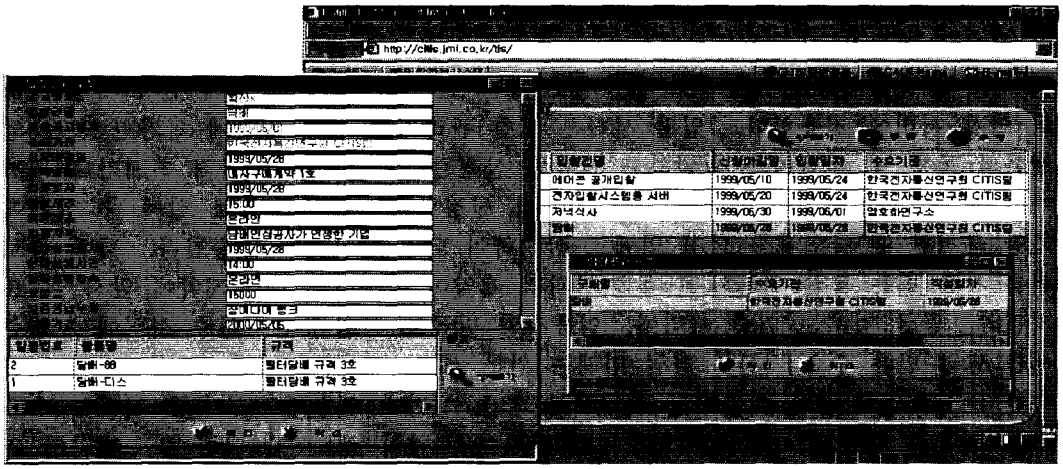
[그림9]는 클라이언트 측의 수요 기관에서 입력하는 구매 요구 신청 및 구매 변

경 신청 화면으로써 구매 요구서를 작성할 때 물품 내역이나 규격에 대한 내역도 함께 등록한다. 입찰 서버는 수요 기관에서 등록한 구매 요구를 검토하여 구매 결의가 확정되면 구매 결의서 관리기에 등록한다. 또한 결의된 구매 요구서는 입찰 공고 관리기를 통해 입찰 공고에 등록된다[그림10]. 공급 업체에서는 웹 브라우저를 통해 입찰 공고를 확인한 뒤, 입찰 참가서를 신청하고 입찰가를 등록한다 [그림11]. 이때 입찰 참가 공급업체임을 보증하고 입찰가에 대한 보안을 유지하기 위해 전자 서명을 하여 입찰 서버에 전송한다. 입찰 서버는 입찰 관리기를 통해 입찰에 참가한 공급 업체들의 목록 및 입찰가를 확인하고 예가를 산정한다. 예가는 제한적 최저가나 최저가 등에 의해 산정된다. 낙찰 후보 업체를 선정한 뒤 선정된 후보 업체 중 예가에 가장 근접한 후보 업체를 낙찰 업체로 선정하여 낙찰 통보서를 전송한다. 낙찰 통보서를 전송 받은 공급 업체와 수여 기관과의 계약이 이루어 진다. 계약에 앞서 수요 기관과 공급 업체는 인증 서버에 인증서의 발급을 신청한다. 인증 서버에서 인증서를 발급 받은 수요 기관과 공급 업체는 원본 계약서에 서명을 한 후 상대방에게 전송한다. 각각 서명이 이루어진 계약서를 공증 서버에 전송한다. 공증 서버는 수요 기관과 공급 업체가 서명한 계약서를 보관하여 계약이 완료된다[그림12]. 계약이 완료되면 물품 납부와 대금 청부 검수 등으로 조달 프로세스 과정이 이루어진다.



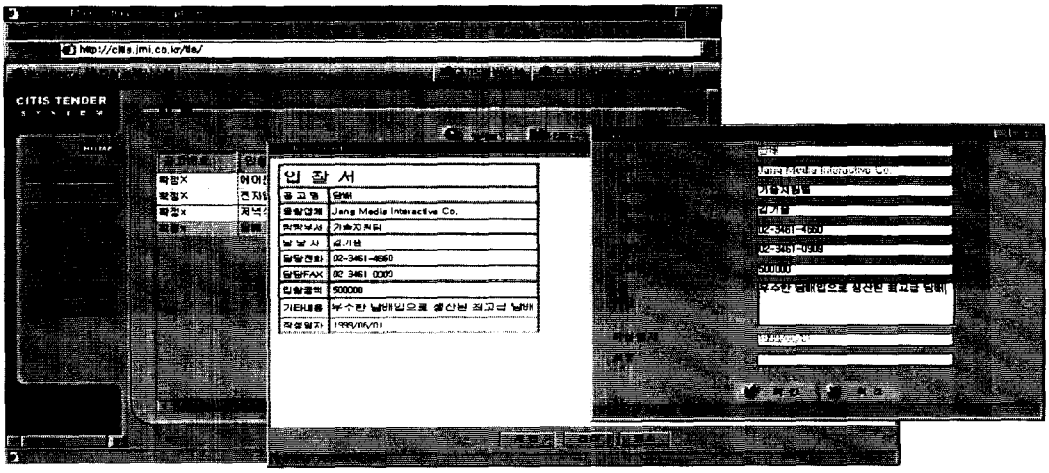
[그림 9] 구매요구등록 및 구매 변경 신청서등록 화면

입찰 공고

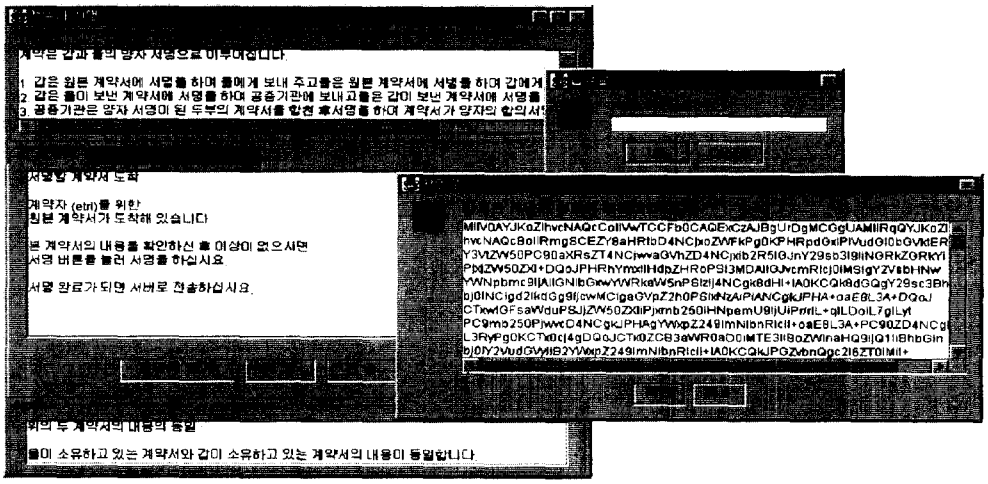


[그림 10] 입찰 공고 화면

입찰서



[그림 11] 입찰서 및 전송 화면



[그림 12] 계약 서명 하기

V. 결론

컴퓨팅 기술과 통신 기술의 급속한 발전으로 인터넷 환경에서의 기업과 소비자간의 전자 거래 및 기업과 기업간 전자 거래가 활성화되고 있다. 특히 인터넷 사용의 폭발적인 증가로 기업과 소비자간 전자 거래 형태는 일반화되었으며 기업과 기업간 전자 거래는 매년 그 증가 속도가 기업과 소비자간의 전자거래의 10배에 달한다. 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 프로세스 중 입찰 가격이나 계약의 보안 및 인증을 위해 PKI 기반의 전자 서명 방식을 사용하는 보안 기술을 적용하였으며 인터넷 상에서 입찰 과정의 전체 프로세스가 실행될 수 있도록 구현하였다.

추후 과제로는 본 논문에서 포함하지 않은 확장형 데이터 타입을 정의 할 수 있으며 DTD의 문제점을 보완한 스키마 기반의 XML문서에 관한 연구 및 전자 입찰 프

로세스뿐만 아니라 타 업무 시스템으로도의 전환이 용이할 수 있도록 비즈니스 흐름 관리를 위한 연구가 이루어 져야 한다.

참고문헌

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

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

XML/EDI, http://www.geocities.com

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

ISO 9735, UN/EDIFACT, EDI Standard

X.Berkovits, S.Chokhani, A. Furlong, A, Geiter, C. Guild, Public Key Infrastructure Study Final Report, 1997

RFC2026, Digital Signature for XML, SMLDSIG Working group, 1999

윤선희, 주경준, 전자입찰시스템 보안설계, 한국정보과학회 춘계학술대회 논문집, 2000,4

윤선희, 인터넷 기반 XML/EDI 활용 전자 입찰 시스템, 한국컴퓨터산업교육학회 논문지, 2000,12

<Abstract>

Design and Implementation of Web-based Electronic Bidding System using XML

Sunhee Yoon SoongEui Women's College shyoon@sewc.ac.kr

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).