

XML/PKI기반의 전자세금계산서 시스템 구현

김진철* · 오영환**

The Implementation of A XML/PKI based Digital Tax Invoice System

Jin Cheol Kim* · Young Whan Oh**

■ Abstract ■

As the e-Commerce based on the XML technology is getting bigger, user authentication, integrity, non-repudiation and confidentiality has become important for security. Since the XML technology is widely used for exchanging information among the Internet e-business systems, the security of XML documents is essentially required and XML digital signature should be supported. To support the digital signature of XML documents, W3C proposed the XML-Signature specification as an international standard that describes five transform algorithms. In this paper, we design and implement a XML/PKI based digital tax invoice system. Our system supports the five transforming algorithms defined in the XML-Signature specification and exchanges digital tax invoices among enterprises securely. We design and implement the flexible and efficient system consists of reusable components using CBD(Component Based Development).

Keyword : XML Digital Signature, XML Transformer, Digital Tax Invoice

1. 서 론

최근 인터넷이 활성화되고 인터넷 사용자가 급속도로 증가하는 추세에 맞추어 기존의 기업들이 현재 갖고 있던 상거래 시장에서 인터넷을 통한 시

장 화장을 목표로 전자상거래에 관심이 모아지고, 각 기업들은 독자적인 전자 상거래 시스템 구축에 많은 투자를 하였다. 이에 차세대 웹 문서인 XML을 전자상거래 시장에서 수용하게 되었다. 전자상거래의 특성상 문서의 신뢰성과 투명성을

* 한전 KDN(주) 기술연구소

** 광운대학교 교수

요구하게 되었다. 이러한 요구사항을 해결하기 위하여 여러 업체들은 각각 자신들의 독자적인 디지털 서명을 사용하게 되었으나, 다른 시스템들과 상호운영에 있어서 많은 문제점이 발생하게 되었다[1].

W3C에서는 XML-Signature 표준 스펙을 제안하고 사용하도록 권고하고 있다. 이때에 서명할 문서를 표현하고, 기존에 존재하는 문서를 재사용하고, XML 문서에 다른 형식의 문서를 첨부하여 서명하기 위한 4가지 Transform 알고리즘과 송·수신되는 문서의 무결성을 보장하기 위하여 따로 Canonical XML 스펙을 제정하여 위의 네가지 Transform 알고리즘과 더불어 사용하도록 권고하고 있다[2].

본 논문은 다음과 같이 크게 세 가지 연구목적을 가지고 XML/PKI기반의 전자세금계산서 시스템을 구축하고자 한다. 첫째, 기업간 전자상거래 활성화에 따른 세무업무에 대한 전자적 문서 교류를 위하여 세금계산서를 XML 문서파일 형태의 전자세금계산서로 구현하고자 하였다. 둘째, 인터넷 상에서 안전하게 발급·전송·수신이 가능하도록 PKI기반의 XML 디지털 서명, XML Transform 알고리즘과 Canonical XML 스펙을 이용한 시스템을 구현하고자 하였다. 셋째, 세금계산서의 전자적 교류에 대한 컴포넌트 개발과 시스템 구축을 위하여 재사용성 높은 컴포넌트를 개발함으로써, 다른 전자상거래 페캐지와 유연하게 접목이 가능하고 관련 업무변경에 탄력적으로 대응할 수 있는 시스템이 되도록 구축하고자 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 XML디지털 서명, XML Transform 알고리즘과 Canonical XML Transform 알고리즘, 개발방법론 등 시스템 구현 관련 기본 이론들을 분석하고, 3장에서는 시스템 구성, 모듈 구성, 어플리케이션 아키텍쳐, 적용한 PKI 보안 기술, 데이터베이스 콜렉션 및 스키마, 클래스 다이어그램, 활용 예시 등 전자세금계산서 시스템 구현 결과에 대해서 기술하고, 마지막으로 4장에서는 결론을 맺는다.

2. 기본이론

2.1 XML 디지털 서명

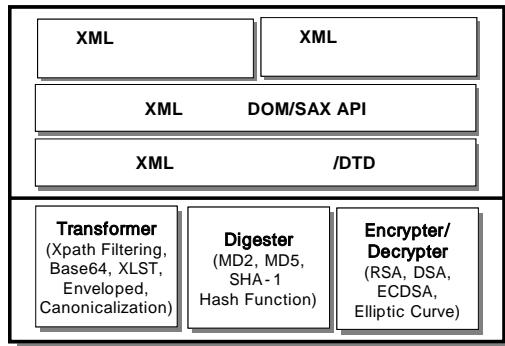
XML 디지털 서명은 크게 서명하고자 하는 XML 비즈니스 문서 부분과 서명부분의 두 부분으로 나누어 진다[3,4] 문서의 XML 비지니스 문서 부분은 서명을 적용해야 할 대상 문서 부분을 나타내고, 서명 부분은 XML 비즈니스 문서에 적용할 서명 부분을 나타낸다. XML 문서를 서명하고, 검증하기 위해서는 서명해야 할 문서를 Transformer를 통하여 문서를 표현하거나 변형하여 서명하고자 하는 문서를 얻어낸다.

Transform 과정을 마친 문서는 원본문서의 변형이 없음을 보장하기 위해서 Digester를 통하여 문서의 유일한 값인 Digest value를 얻는다. Digest value를 얻으면 DigestValue 엘리먼트의 내용으로 삽입하여 DigestValue 엘리먼트를 구성한다.

DigestValue 엘리먼트는 SignedInfo 엘리먼트의 하위 엘리먼트에 추가되어 Reference 부분(XML 비지니스 문서부분)을 생성한다. Reference 부분이 생성되면 SignedInfo 엘리먼트(child 엘리먼트를 포함한)를 물리적으로 보증하기 위해 다시 Transform 알고리즘의 하나인 Canonicalization Transform 알고리즘을 수행한다.

최종적으로 Canonicalization된 SignedInfo 엘리먼트는 암호와 알고리즘을 적용하여 서명하여 Signature Value를 얻어내고 Signature 엘리먼트를 생성하게 된다. 이렇게 완성된 XML 디지털 서명은 송신되고, 수신자는 문서를 수신한다.

수신자는 위의 과정을 통하여 동일한 방법으로 DigestValue를 생성하게 되며, 이렇게 생성된 DigestValue와 수신 받은 문서의 DigestValue 엘리먼트의 값을 비교함으로써 Reference가 유효한지 검사하고, 다시 위의 생성과정과 동일한 과정을 거치고 이번에는 생성자의 공개키를 이용하여 서명 부분이 유효한지 검증하게 된다. 이러한 처리를 수행하는 XML 디지털 서명의 구조는 [그림 1]과 같다.



[그림 1] XML 디지털 서명의 구조

2.2 XML Transform 알고리즘

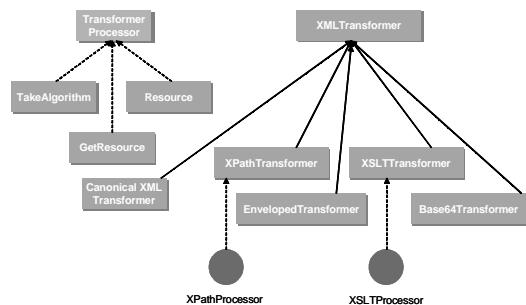
W3C에서는 서명할 XML 문서를 표현하고, 기존에 존재하는 문서를 재사용하고, XML 문서에 다른 형식의 문서를 첨부하여 서명하기 위하여 다음과 같이 네가지 Transform 알고리즘과 송·수신되는 문서의 무결성을 보장하기 위하여 따로 Canonical XML 스펙을 제정하여 사용하도록 권고하고 있다[4].

첫째, XPath Filtering Transformer는 원본 XML 문서 중 서명할 특정부분을 XPath로 표현한 것을 XPath Syntax와 Semantics를 이용하여 필터링 하므로 사용자가 서명하려는 문서의 특정 부분을 표현하기 위하여 사용된다. 둘째, XSLT Transformer는 사용자가 서명하려는 문서의 일부를 다른 Format으로 변환하여 서명하고자 하는 경우 사용된다. 셋째, Enveloped Transformer는 서명하려는 대상 문서 내에 또 다른 서명을 포함하고 있는 경우 서명부분을 제외한 XML 비지니스 문서만을 추출하여 서명하기 위해서 사용된다. 넷째, Base64 Transformer는 XML 비지니스 문서가 Base64로 Encoding되어 있는 문서일 경우 Base64로 Decoding하는 Transform 알고리즘을 수행하는 Transformer로 서명하려는 문서가 Raw Data일 경우 유용하게 사용된다.

마지막으로 Canonical XML Transformer는 논리적으로는 동일하나 물리적으로는 여러 가지 표현이 존재할 수 있는 XML 문서를 일관된 형태로 변형하는 Canonicalization을 수행한다. 즉, 문서의

처리 과정에서 파서 등에 의해서 나타나는 문서의 물리적인 변형을 처리하여 주므로 상호 교환되는 XML 문서의 무결성을 보장하여 준다. 따라서 XML 디지털 서명과 같이 Digest 값을 구해야 하는 시스템에서는 문서의 물리적 구조 또한 일관된 형태를 유지하여야 하므로 반드시 필요한 Transformer이다[5].

XML Transformer는 XML 디지털 서명 시 문서의 전체 혹은 원하는 부분만을 선택하여 서명함으로써 서명의 생성 및 검증의 처리 속도를 높일 수 있다. 따라서 송·수신 시 효율을 높이며, 기존의 문서의 재사용성을 높일 수 있게 한다.



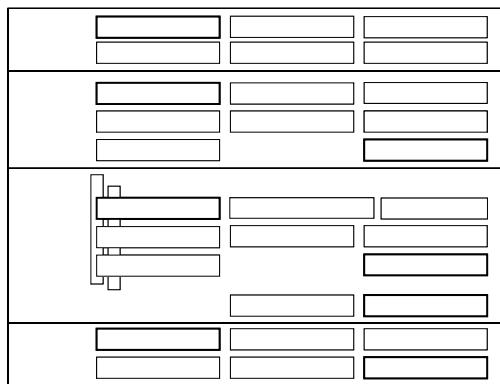
[그림 2] XML Transformer의 구조

2.3 개발방법론

세금계산서의 전자적 교부에 대한 재사용성이 높은 컴포넌트 및 시스템 구현을 위하여 한국전자통신연구원(ETRI)의 마르미III 방법론을 적용하였다[7]. 마르미III는 컴포넌트 자체를 개발하는 방법론(Component Development Methodology : CDM)과 컴포넌트를 기반으로 하는 시스템 구축 방법론(Component Based Development Methodology : CBD)으로 구성되어 있으나, 본 논문에서는 수행 목적에 따라 CBD에서 제시하는 Work Breakdown Structure와 산출물 중 핵심적인 작업과 산출물에 대해서만 수행하였다. 또한 본 논문에서는 제약상 EJB의 구현은 제외하기로 한다. 비록 마르미III가 EJB 명세기반일지라도, 보는 관점에 따라 CBD의

구현 범위가 달라질 수 있으므로, 방법론상의 산출물 및 Work Flow는 마르미III를 따르되 EJB의 적용은 제외하기로 한다.

마르미III 방법론의 특징은 다음과 같다. 첫째, 마르미III는 어플리케이션 패밀리 개념으로써 공통성, 가변성 분석을 통한 컴포넌트의 재사용성 증대시킬 수 있다. 둘째, OMG의 UML을 객체 지향 모형화 언어 표준안으로 채택함으로써 Process와 Tool에 Independent하다. 셋째, Use case 기반의 개발 방법론이기 때문에 사용자 요구사항 분석 중심의 기법이고, 반복적, 점진적 개발이 가능하고 개발자의 Motivation 유지나, 리스크 관리가 수월하다. 또한, 아키텍처 중심의 기법이기 때문에 시스템 품질을 고려한 재사용성이 증대될 뿐 아니라 개발 초기에 견고한 아키텍처를 정의할 수 있다. 마르미III 프로세스는 [그림 3]과 같다.



[그림 3] 마르미III 프로세스

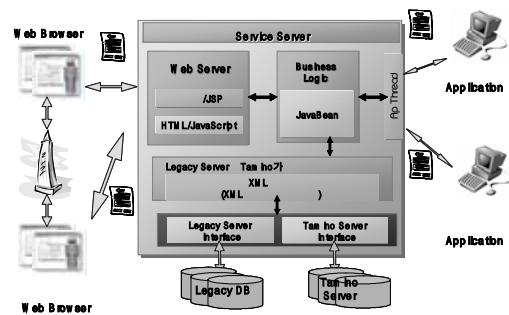
3. 시스템 구현

3.1 시스템 구성

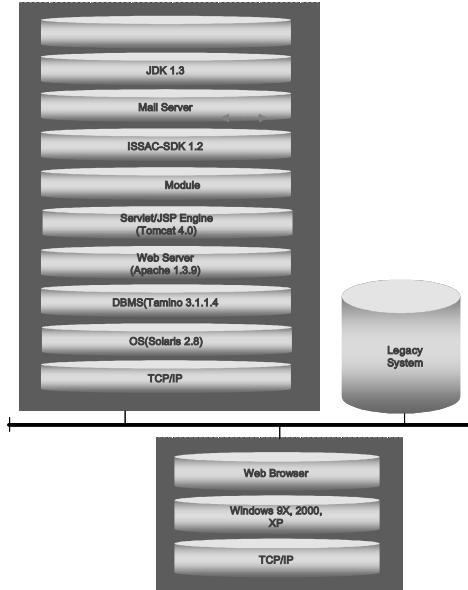
XML/PKI기반의 전자세금계산서 시스템의 구성은 [그림 4]와 같다. 공급자와 공급받는자는 인증기 관으로부터 발급받은 인증서를 통하여 시스템에 접근할 수 있다. 전자세금계산서 시스템은 서비스 서버, 웹서버, 비즈니스 로직, XML DB

인터페이스, Legacy DB 인터페이스 등으로 구성된다.

XML Transform 알고리즘은 XML 로직에 구현하였으며, 공급자와 공급받는자의 XML 디지털 서명이 이루어진 전자세금계산서는 XML DB인 Tamino에 저장하고, 전자서명을 제외한 일반적인 세금계산서 관리 정보들은 RDB에 저장하도록 하였으며, Legacy 시스템과 연동할 수 있도록 구현하였다. XML/PKI기반의 전자세금계산서 시스템의 소프트웨어 구성은 [그림 5]와 같다. 본 시스템에서는 암호화 모듈로는 ISSACK-SDK 1.2, Servlet/



[그림 4] 시스템 구성도



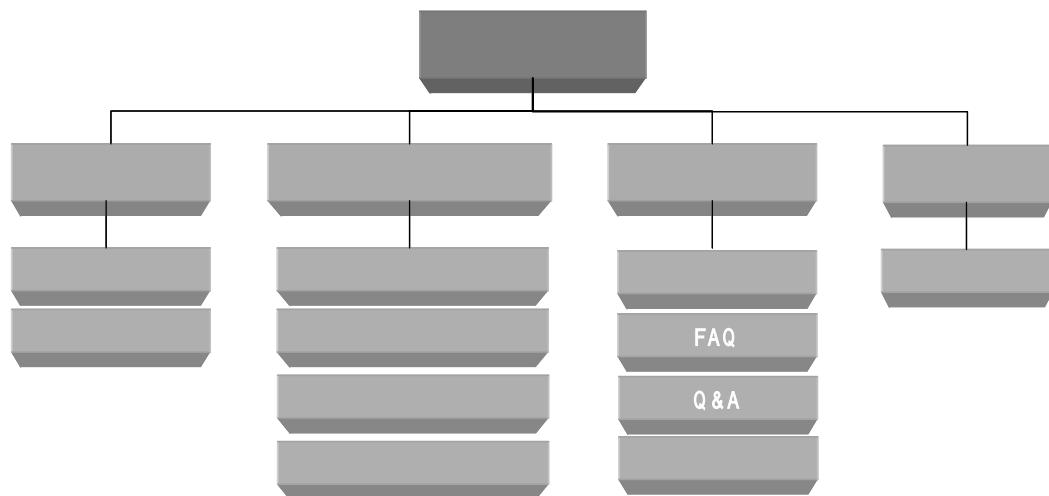
[그림 5] 시스템 소프트웨어 구성도

JSP엔진으로는 Tomcat 3.0, 웹서버로는 Apache 1.3.9, DBMS는 Tamino 3.1.1.4, OS는 Solaris 2.8을 사용하였다.

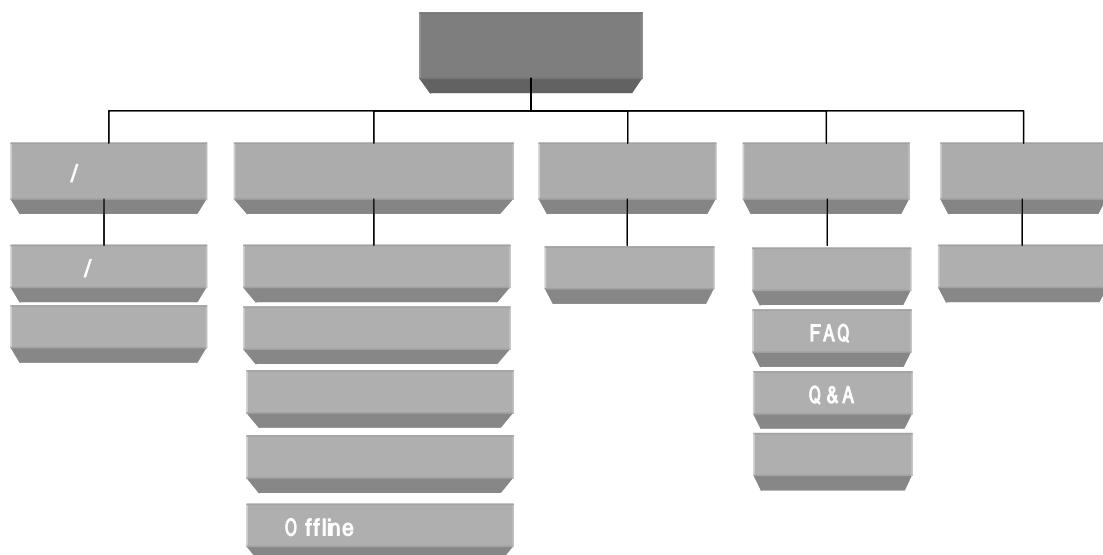
3.2 모듈 구성

XML/PKI 전자세금계산서 시스템의 모듈은 [그림

6a], [그림 6b]와 같이 공급자 모듈과 공급받는자 모듈로 구성된다. 공급자 모듈에는 공급자 정보 관리, 전자세금계산서 발행, 조회, 반송처리 등의 기능들을 구현하였으며, 공급받는자 모듈에는 공급자 및 공급받는자 정보관리, 전자세금계산서 조회, 승인, 반송 등의 기능들을 구현하였다.



[그림 6a] 공급자 모듈



[그림 6b] 공급받는자 모듈

3.3 어플리케이션 아키텍처

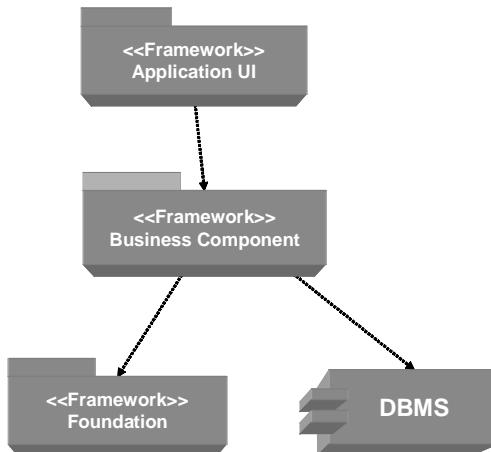
어플리케이션 아키텍처는 어플리케이션 UI(User Interface), 비즈니스 컴포넌트, 파운데이션 등으로 구성되고 [그림 7]과 같다. 첫째, 어플리케이션 UI는 전자세금계산서 시스템의 사용자 인터페이스를 담당하는 패키지로써, JSP를 기반으로 작성하며, Custom Tag 및 Bean Tag 등을 이용하였다.

둘째, 비즈니스 컴포넌트는 데이터 중심의 컴포넌트로 구성된 계층으로써, Java Bean으로 구성되어 있고, Facade Pattern을 적용하였다. 또한 DBMS와 접속을 위한 별도의 Persistence 컴포넌트를 사용하였다.

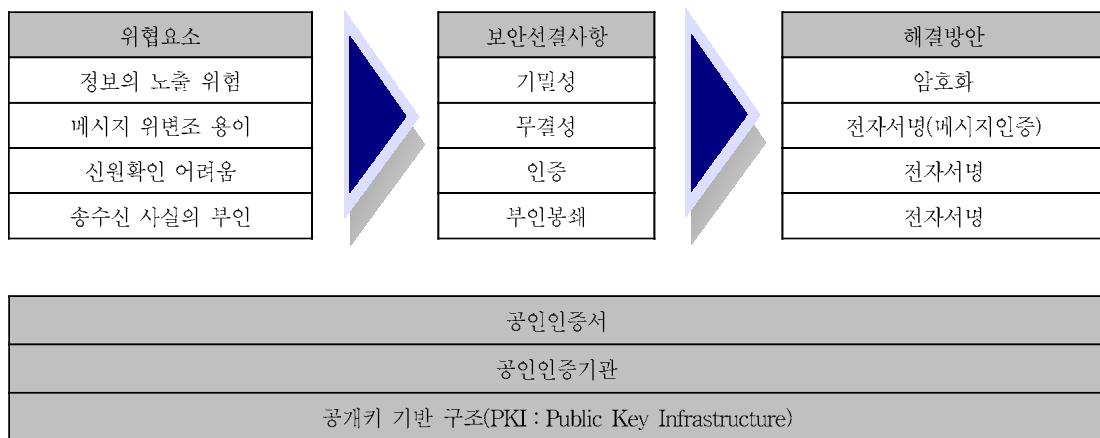
셋째, 파운데이션 컴포넌트는 인증기관의 인증서 검증 및 XML 디지털 전자서명, 보안 컴포넌트, XML문서 생성, 변환 등을 위한 파서, 프로세스, 에러처리 등의 기능적 재사용 컴포넌트이다.

3.4 시스템 보안

기존 오프라인상 종이문서 형태의 세금계산서를 인터넷 기반의 전자문서로 대체함에 따라 발생할 수 있는 보안적인 문제를 해결하고 안전하게 전자세금계산서의 발행, 승인, 반송 등이 이루어질 수 있도록 XML 디지털 서명, PKCS#7, SSL 등과 같



은 PKI기반의 보안 기술을 활용하였다. 본 논문에서 시스템 보안을 위하여 고려한 사항은 [그림 8]과 같다. 인터넷은 개방형 정보통신망으로써 이용자의 익명성으로 인해 정보의 노출위험, 메시지 위변조 용이, 신원확인의 어려움, 송수신 사실의 부인 등의 정보화의 역기능이라 할 수 있는 위협요소가 존재한다. 이를 방지하기 위해서는 기밀성, 무결성, 인증, 부인봉쇄와 같은 각각에 대한 보안 선결 사항의 충족과 더불어 이를 뒷받침할 수 있는 공인인증기관이 발행한 전자서명 인증서, 전자서명법, 전자거래기본법과 같은 법/제도적 보호장치를 고려해야 한다.



[그림 8] 시스템 보안을 고려사항

이러한 위협요소, 보안선결사항, 해결방안을 고려하여 XML/PKI기반의 전자세금계산서 시스템에 적용한 업무별 적용 PKI 보안 기술은 <표 1>과 같다.

전자세금계산서 시스템에 적용된 XML 디지털 서명의 구조 및 구성요소는 [그림 9]와 같다. 첫째 XPath Filtering Transformer 알고리즘을 사용하여 원문(Plain text)인 전자세금계산서 XML 문서중 XML 디지털 전자서명의 대상이 되는 특정 부분을 표기하였다.

둘째, Base64 Transformer를 활용하여 송신자는 전송해야 할 원문(Plain text)인 전자세금계산서에 RSA-SHA1 알고리즘을 이용하여 PKCS#7의 signedData 태입을 추출하고, 이를 ASN 인코딩하여 바이너리로 바꾼 후 다시 base64 인코딩한

<표 1> 업무별 적용 보안기술

적용기술	행 위 주체	
	공급자	공급받는자
XML 디지털 서명	세금계산서 발행 세금계산서 재발행	세금계산서 승인
PKCS#7	세금계산서 폐기요청	세금계산서 폐기승인
SSL	로그인 회원가입 관리자 정보수정 암호변경 사용자 등록 관리자 교체 사용자 변경 자기정보 변경 자기암호 변경	로그인 회원가입 관리자정보 수정 자기정보 수정 사용자 정보수정 암호변경 자기암호변경 사용자 등록 관리자 정보수정 관리자 등록

```

- <ti:Signatures ino:id="3" xmlns:ti="http://www.kiec.or.kr/schemas/DTIFormat">
  - <ds:Signature Id="berria" xmlns:ds="http://www.w3.org/2000/09/xmldsig#
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#ebxml_signature.xsd">
    - <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      - <ds:Reference URI="">
        - <ds:Transforms>
          - <Transform Algorithm = "http://www.w3.org/TR/2000/CR-xml-c14n-20001026"/>
            <Transform Algorithm = "http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            - <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
              <ds:XPath xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" not(ancestor-or-self::Signature)</ds:XPath>
            </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>Q4QEOniAjGO17kNtL0iXw4s4qys=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      Z5jM/7ZBxjKUusbgsjVmWJtab/C0kvqK1Q27K/sstdaZ7K+5roXAdPqpwhJw785lP2UJgWDr0vLpVzUU93SiU/zHZt
      vZshfthi8qwjGtTaEQGrxup2PDaAOOGGx/oSGt39NzS62eUnWfdQDbNNTx7qeZteG6yDlh3d3crpZOysIo=</ds:SignatureValue>
    - <ds:KeyInfo>
      - <ds:X509Data>
        <ds:X509Certificate xmlns="http://www.w3.org/2000/09/xmldsig#">
          MIIIDIDCCAomgAwIBAgICM/4wdDQYJKoZIhvcNAQEFBQAwTTELMAkGA1UEBhVDQxMjAxMzM1
          OVowbDELMAkGA.....</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
  </ti:Signatures>

```

[그림 9] XML 디지털 서명 생성

결과를 전송한다. 또한 수신자는 위 내용을 base64 디코딩하여 ASN 디코딩을 하면 PKCS#7의 signed Data 탑입의 C-structure를 얻을 수 있음. 여기서 원문을 추출하면 서명 원문을 얻을 수 있다.

셋째, Enveloped Transformer를 활용하여 공급자와 공급받는자가 서명 대상인 전자세금계산서 문서에만 서명하도록 하였다. 즉, 공급자의 서명 후 공급받는자가 서명하려는 대상 문서 내에 공급자의 서명을 제외한 XML 비지니스 문서인 전자세금계산서 XML 문서만을 추출하여 서명하도록 하였다.

넷째, XML 디지털 서명시 사용한 공개키 기반 알고리즘은 RSA 알고리즘을 사용하였고, 메시지 다이제스트를 위한 해쉬 알고리즘은 SHA-1을 사용하였다.

다섯째, Canonical XML Transformer를 활용하여 문서의 처리 과정에서 파서 등에 의해서 나타나는 문서의 물리적인 변형을 일관된 형태로 변형 처리하여 줄 수 있도록 하였다[6].

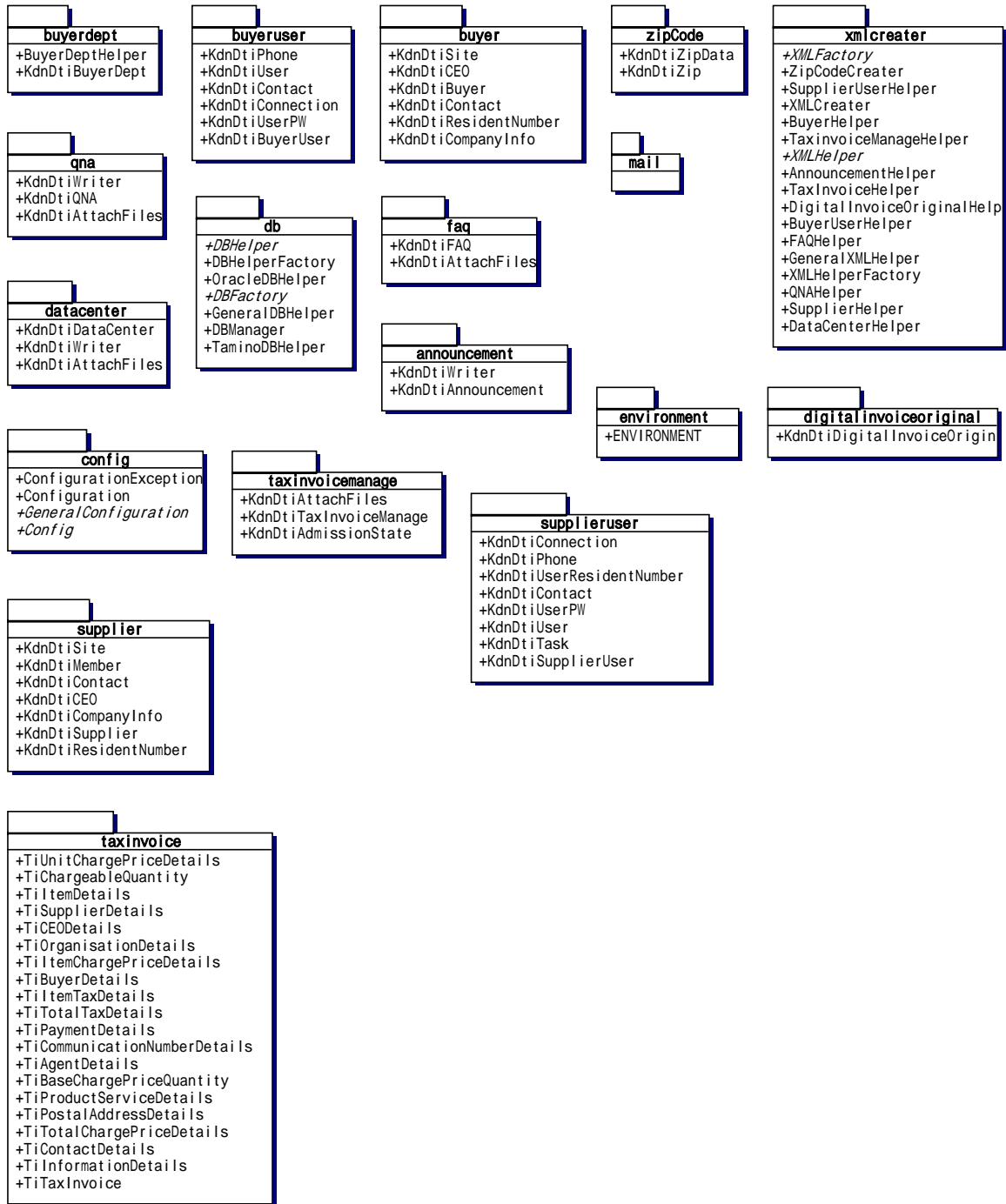
XML 디지털 서명을 이용한 전자세금계산서 발행/승인 정보의 XML 디지털 전자 서명 구조는 [그림 10]과 같고 <TaxInvoice>~<TaxInvoice>는 전자세금계산서 원본 정보와 전자서명 정보가 같이 들어가는 루트 엘리먼트이고, <ti:Information.Details.....>~<ti:TotalTax.Details.....>는 세금계산서 원본에 포함되는 정보가 들어가는 엘리먼트들이며, <ti:Signatures.....>~</ti:Signatures.....>는 공급자와 공급받는자의 전자서명이 들어가는 엘리먼트로써, [그림 9]와 같은 추가되어

```
<TaxInvoice>
+ <ti:Information.Details .....>
+ <ti:Supplier.Details .....>
+ <ti:Buyer.Details .....>
+ <ti:Item.Details .....>
+ <ti:TotalChargePrice.Details .....>
+ <ti:TotalTax.Details .....>
- <ti:Signatures ino:id="1" xmlns:ti="http://www.kiec.or.kr/schemas/DTIFormat">
    + <ds:Signature Id="berra" .....> .....> 공급자 서명
    + <ds:Signature Id="heera" .....> .....> 공급받는자 서명
</ti:Signatures>
</TaxInvoice>
```

[그림 10] XML 디지털 서명을 이용한 전자세금계산서 발행/승인정보의 전자서명 구조

```
<kdn_dti:TaxInvoiceINOID ino:id="1".....>1</kdn_dti:TaxInvoiceINOID>
<kdn_dti:Reason ino:id="1" ...>폐기사유
</kdn_dti:Reason>
<kdn_dti:RequesterIdentifier ino:id="1" xmlns:kdn_dti="http://www.kdn-dti.com/" RequesterID="berra">
    0123457890
</kdn_dti:RequesterIdentifier>
<kdn_dti:RequestDate ino:id="1".....>2002-11-11T10:20:45
</kdn_dti:RequestDate>
<kdn_dti:Signature ino:id="1" xmlns:kdn_dti="http://www.kdn-dti.com/">
    MIIGUwIBATEJMAcGBSsOAwIaMIIIBvwYJKoZIhvcNAQcBoIIBsASCAaw8P3htbCB2ZXJ6VGF4SW52b2ljZ
    .....>PKCS#7 형태의 서명정보(공급자)
</kdn_dti:Signature>
<kdn_dti:Signature ino:id="1" xmlns:kdn_dti="http://www.kdn-dti.com/">
    MIIGYgIBATEJMAcGBSsOAwIaMIIIBzgYJKoZIhvcNAQcBoIIBvwSCAbs8P3htbCB2ZXJz6VGF4SW52b2ljZUI
    OT0lEPjE8L.....>PKCS#7 형태의 서명정보(공급받는자)
</kdn_dti:Signature>
```

[그림 11] XML 디지털 서명을 이용한 전자세금계산서 발행/승인정보의 전자서명 구조



[그림 12] 클래스 다이어그램

지고, 다음으로 공급받는자의 전자서명이 들어간다.

또한 본 시스템에서는 전자세금계산서 폐기 시에는 PKCS#7 형식을 적용한다. 전자세금계산서의 폐기는 세금계산서의 원본이 아닌 폐기할 세금계산서의 위치, 사유, 날짜 등의 정보에 서명한다. 이 서명정보가 PKCS#7의 형식을 취하며, 이 스트링열을 [그림 11]과 같이 XML 형태의 전자세금계산서 폐기문서 내의 한 엘리먼트로 포함시킨다.

3.5 클래스 다이어그램

본 시스템의 클래스 다이어그램은 [그림 12]와 같다.

3.6 데이터베이스 콜렉션 및 스키마

전자세금계산서 시스템의 데이터베이스 콜렉션과 스키마는 <표 2>와 같이 구현하였다.

3.7 활용사례

본 장에서는 구현한 XML/PKI기반 전자세금계

산서 시스템의 주요 화면을 통하여 활용 사례를 보고자 한다. 먼저 구현한 시스템의 메인화면은 [그림 13]과 같고, 사용자별(공급자, 공급받는자, 관리자) 사용권한을 분리하였다.

공급자가 발행한 전체 전자세금계산서를 [그림 14]와 같이 확인할 수 있으며, 공급자가 금일 발행한 세금계산서, 금일 반송된 세금계산서, 전체 발행세금계산서, 공급받는자의 최종 승인된 세금계산서 등을 세부 목록으로 확인 가능하다.



[그림 13] 시스템 메인화면

<표 2> 데이터베이스 콜렉션과 스키마

콜렉션명	스키마	내용
AdditionInfo	Announcement	공지사항 스키마
	DataCenter	자료실 스키마
	FAQ	FAQ관련 스키마
	QNA	Q&A관련 스키마
Buyer	Buyer	공급받는자 정보
	BuyerDept	공급받는자의 부서코드 및 해당 부서명
	BuyerUser	공급받는자의 사용자 정보
Etc	ErrorMsg	에러코드와 메시지를 저장
	Zip	우편번호 데이터 저장
Supplier	Supplier	공급자 정보
	SupplierUser	공급자의 사용자 정보
TaxInvoice	TaxInvoice	세금계산서원본(signature포함)
	TaxInvoiceDisuse	세금계산서폐기정보(폐기된 세금계산서에 한해 생성됨)
	TaxInvoiceManage	세금계산서관리정보
	TaxInvoiceSum	합계표 제작시 사용되는 스키마
	TaxInvoiceView	세금계산서view만을 위해 만들어진 스키마. 세금계산서원본과 동일한 정보를 가지며, TaxInvoiceID항목이 추가되어진다.



[그림 14] 공급자 세금계산서 발행 현황

공급자측 담당자는 [그림 15]와 같이 XML 전자세금계산서를 인터넷상에서 발행할 수 있으며, 필요시 증빙 서류들을 첨부할 수 있다. 공급자가 발행버튼을 누르면 공급자의 XML 디지털 전자서명이 생성된다. 공급자자 서명한 전자세금계산서는 공급받는자측의 담당자에게 전송된다.



[그림 15] 공급자의 세금계산서 발행

공급받는자측의 담당자는 전자세금계산서를 확인하고 필요시 [그림 16]과 같이 반송할 수 있으며 반송사유를 기입할 수 있다. 이때는 XML 디지털 서명이 생성되지 않으며, 전자세금계산서는 공급자와 공급받는자의 디지털 서명이 모두 있을 때 법적

으로 유효함을 원칙으로 한다.



[그림 16] 공급받는자의 세금계산서 반송

공급받는자측의 담당자는 전자세금계산서를 확인하고 [그림 17]과 같이 전자세금계산서를 승인할 수 있으며 XML 전자세금계산서 문서에 공급받는자의 XML 디지털 서명이 생성된다.



[그림 17] 공급받는자의 세금계산서 승인

본 논문에서 구현한 XML/PKI 전자세금계산서 시스템은 대기업과 협력업체간 거래, 전자쇼핑몰에서 쇼핑몰 운영업체와 쇼핑몰 이용자 또는 쇼핑몰 납품업체간 거래, 전자세금계산서 ASP(Application

Service Provider) 사업자의 전자세금계산서 서비스 사업 등에 활용가능하다.

국세청에서 2001년 1월, “전자적으로 세금계산서를 교부하는 제도에 관한 고시”를 제정, 고시하였다. 국세청 고시에 의거하여 많은 SI업체에서 전자세금계산서 시스템을 개발하였고 사용 중에 있다. 하지만, 국세청 고시가 최소한의 내용만으로 구성되어 있어 이를 구현하는 단계에서 다양한 파일 형식이 개발되어 호환성이 결여에 의한 솔루션별로 다른 뷰어(Viewer)를 필요로 하는 등 사용자 불편이 야기되었다. 대기업을 중심으로 대기업별 독자적인 규격의 전자세금계산서 시스템을 운영함으로써, 중소기업은 거래하는 대기업별 다른 형식의 전자세금계산서를 사용해야 하고, 금융기관 제출 또는 국세청 세무감사시 전자세금계산서와 솔루션별 뷰어를 제출해야 한다.

본 시스템은 W3C에서 제정한 XML 디지털 서명을 위한 XML Transformer를 구현하고, 전자상거래 표준화 통합포럼에서 제정한 ebXML 전자문서인 전자세금계산서 표준 규격에 따라 시스템을 구현함으로써 솔루션별로 다른 뷰어(Viewer)를 필요로 하는 호환성이 결여된 기존 전자세금계산서 시스템의 단점을 보완하였다[8].

본 시스템에서 적용한 ebXML은 인터넷 환경에서 입종의 제약을 배제하고, 세계적으로 거래 당사자간에 문서를 전자적으로 주고받기 위한 목적에서 개발된 프레임워크이지만, 자료의 크기가 커지고 전송이 지연되는 단점이 있다. 세금계산서는 우리나라 전 사업자가 공통적으로 사용해야 하는 문서이므로 전자세금계산서 활성화 뿐 아니라 e-business 활성화를 위해서는 표준 규격으로 구현하는 것이 타당하다고 사료된다.

전자상거래 표준화 통합포럼에서 제정한 전자세금계산서 표준 규격은 현실적으로 즉시 적용하기 위해서 표준 전송규약으로는 적용하지 못하였다. 향후 발행된 전자세금계산서를 표준화된 포맷으로 관세청, 금융기관 등 기타 기관에 제출하기 위해서는 표준 전송규약에 대한 연구가 필요하다.

3. 결 론

최근 인터넷이 활성화되고 인터넷 사용자가 급속도로 증가하는 추세에 맞추어 기존의 기업들이 현재 갖고 있던 상거래 시장에서 인터넷을 통한 시장 확장을 목표로 전자상거래에 관심이 모아지고, 각 기업들은 독자적인 전자 상거래 시스템 구축에 많은 투자를 하였다. 이에 차세대 웹 문서인 XML을 전자상거래 시장에서 수용하게 되었다.

본 논문은 기업간 전자상거래 활성화에 따른 세무업무에 대한 전자적 문서 교부를 위하여 세금계산서를 XML 문서파일 형태의 전자세금계산서로 구현하고자 하였다.

인터넷 상에서 전자세금계산서가 안전하게 발급·전송·수신이 가능하도록 XML 디지털 서명, XML Transform 알고리즘과 Canonical XML 스펙을 이용한 시스템을 구현하였다. 또한 전자상거래 표준화 통합포럼에서 제정한 ebXML 전자문서인 전자세금계산서 표준 규격에 따라 시스템을 구현함으로써 호환성이 결여된 기존 전자세금계산서 시스템의 단점을 보완하였다.

또한, 세금계산서의 전자적 교부에 대한 컴포넌트 개발과 시스템 구축을 위하여 재사용성 높은 컴포넌트를 개발함으로써, 다른 전자상거래 폐기지와 유연하게 접목이 가능하고 관련 업무변경에 탄력적으로 대응할 수 있는 시스템이 되도록 구축하였다.

참 고 문 헌

- [1] T. Miyazawa & T. Kushida, “An Advanced Internet XML/EDI Model Based on Secure XML Documents,” *ICPADS’00 Workshops*, 2000.
- [2] W3C, XML-Signature Syntax and Processing, Candidate Recommendation, 19, April, 2001, (<http://www.w3.org/TR/xmldsig-core/>).
- [3] W3C, “Extensible Markup Language (XML) Version 1. 0,” Recommendation, 10, February.

- 1998.
- [4] 박종현, 김병규, 강지훈, 한우용 “XML Transform 알고리즘의 구현”, 「한국정보과학회 추계 학술 발표논문집」, 제28권, 제2호(2001), pp.694-696.
- [5] 박종현, 김병규, 강지훈, 한우용 “Canonical XML 알고리즘의 구현”, 「한국정보과학회 춘계 학술발표논문집」, 제29권, 제1호(2002), pp.787-789.
- [6] W3C, Canonical XML Version 1.0, Recommendation, (<http://www.w3.org/TR/xml-c14n>, 15, March, 2001.
- [7] 한국전자통신연구원, 「컴포넌트기반 S/W 개발방법론 (마르미-III)」, 2005.
- [8] 전자상거래 표준화 포럼, 「전자세금계산서 (ECIF 75-2003)」, <http://www.ecif.or.kr/>, 2003.



김 진 철 (kjc@kdn.com)

광운대학교 전자통신공학과 학사, 동대학원 석사, 동대학원 박사과정을 수료하였고 현재 한전KDN(주) 기술연구소에 재직하고 있다. 한국전자공학회, 한국통신학회 등에 논문과 프로젝트 실적이 있다. 주요 연구분야는 e-Commerce, Network Security, Ad-hoc Network 등이다.



오 영 환 (yhoh@daisy.gwu.ac.kr)

광운대학교 산업대학원장 등을 역임하고, 현재 광운대학교 교수로 재직하고 있다. 한국전자공학회, 한국통신학회 등에 다수의 논문, 저서, 특허 및 프로젝트 실적이 있다. 주요 연구분야는 전자공학, 통신공학, 신뢰성공학 등이다.