XML Digital Signature에 기반한 XML/EDI System의 설계 및 구현

원덕재°, 이형석, 송준홍, 신동규, 신동일
세종대학교 컴퓨터공학과
e-mail : rkaxks@gce.sejong.ac.kr

Design and Implementation of XML/EDI System Based on XML Digital Signature

Duckjae Won, Hyungsuk Lee, Junhong Song,
Dongkyoo Shin, Dongil Shin
Department of Computer Engineering, Sejong University

요약

최근 차세대 웹 표준문서 포맷으로 부상되고 있는 XML(eXtensible Markup Language)을 사용한 B2B 전자상거래 규격에 대한 국내외적인 표준화 작업이 가속화되고 있다. 아울러 기업 간 문서 교환시의 인증 및 보안문제 또한 필수적인 사항이 되어가고 있다. 본 논문에서는 기업 간 문서교환 및 문서교환시의 보안문제 해결을 위한 XML 전자서명(XML-Dsig:Digital Signature)표준에 기반한 XML/EDI 시스템을 설계 및 구현하였다.

1. 서론

최근 개인 및 기업에서의 인터넷 활용이 급증함에 따라 인터넷 그 자체를 사업수단으로 이용하는 추세가 가속화되고 있다. 또한, 인터넷은 전자상거래를 활성화시킴으로써 새로운 시장의 창출과 효율성 극대화를 위한 활력소가 되고 있다. 특히, 기업 간 교역을 위한 B2B 문서의 교환은 EDI(Electronic Data Interchange) 메시지를 통해서 교환된다.

EDI는 데이터의 오류를 최소화하고, 정보의 신속한 전송과 처리과정을 단순화하여 기업의 업무를 자동화시키고 있다.[1] 그러나, 특정 분야에 한정된 기업 내에서의 성공적인 사례에 국한되어 있으며, EDI 소프트웨어의 구현과 통신비용으로 인해 중소규모의 기업에서는 광범위하게 채택되지 못하고 있는 실정이다. 이에 대한 대안으로, 최근 차세대 웹 표준문서 포맷으로 부상되고 있는 XML과 EDI의 접목으로 정보의 전달과 규격화를 위한 강력한 데이터 표현의 표준에 기반 한 EDI 메시지 교환을 실현하고 있다.[2] XML은 현재 웹에서 사용하고 있는 HTML (Hypertext Markup Language)의 한계를 극복하고, 시스템 및 소프트웨어 독립적인 문서와 메시지의 표현이 가능하도록 W3C에서 1998년 제정한 표준으로써[3], 서로 상이한 시스템을 연동하는데 매우 유용하기 때문에 다양한 전자상거래 응용업무 구현에 적합하다.

그러나, XML을 이용한 각종 데이터 및 문서는 웹상에 존재하게 되므로 제 3자에 의해 위조나 변경이 가능하기 때문에 현재 구축되고 있는 XML 기반 전자상거래 시스템 내에서 보안 요구사항들의 충족은 필수적인 사안이며, 전자상거래 상에서의 XML 문서 보안에 대한 연구 개발 또한 활발히 진행되고 있다. 따라서 XML기반 전자상거래 시스템의 무결성, 인증, 부인방지와 같은 보안 문제해결을 위해 XML 전자서명(XML-Digital Signature)표준이 발표되었다. 본 논문에서는 XML 전자서명과 웹기반 표준 보안 프로토콜인 HTTPS에 대하여 설명하고 XML 전자서명 표준에 기반한 XML/EDI시스템의 설계 및 구현에 대하여 논한다.

2. 관련 연구

2.1 XML 전자서명(XML Digital Signature)

전자서명이란 전자화 된 문서의 메시지 내용이 수

정 및 변조되지 않았음을 보장하는 동시에 메시지의 주체인 사용자, 즉 송수신자가 올바른 사용자라는 것을 확인할 수 있게끔 하는 인증방식을 말한다. W3C에서 제정된 "XML-Signature Syntax and Processing"명세서는 2001년 8월 20일 "Proposed Recommendation"인 상태이며 계속적인 표준화 작업이 진행되고 있다.[4,5]

XML 전자서명(XML Digital Signature) 문서는 XML문법을 사용하여 디지털 컨텐츠에 대한 서명을 생성 및 검증하는데 필요한 문서 구조를 정의한다. 즉 전자서명을 생성할 문서에 대한 해시 값(<Digest Value>)을 생성 후 서명 생성자의 개인 키 정보를 통해 최종적인 전자 서명 값(<SignatureValue>)을 생성함으로써 송신 문서에 대한 메시지 무결성 및 인증을 처리하며, 공개 키 정보와 X.509형식의 인증서 정보를 포함해 서명 검증 시 서명자 인증 정보를 제공 할 수 있다. [그림1]에 XML 전자서명의 예를 나타내었다.

```
<?xml version="1.0" encoding="EUC-KR"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://..."/>
    <SignatureMethod Algorithm="http://..."/>
    <Reference URI="#Res0">
      <Transforms>
        <Transform Algorithm="http://..."/>
      </Transforms>
      <DigestMethod Algorithm="http://..."/>
      <DigestValue>DAYOBxZA...=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>
    Nq/6l0FS.....HJsBpMfK51THS/81w7SjWjQy1Y=
  </SignatureValue>
  <KeyInfo>
    사용된 키 정보와 인증서(X.509)정보
  </KeyInfo>
  <dsig:Object Id="Res0"...." xmlns:dsig="http://...">
  <물품구입요청서 xmlns:xsi="http://...">
    XML문서 내용 ...
  </물품구입요청서>
</dsig:Object>
</Signature>
```

[그림 1] XML 전자서명 Enveloping Signature의 예

XML전자서명 문서의 전체적인 포맷은 Enveloping signature, Enveloped signature, Detached signature로 나뉘어지며, 이 포맷들은 작성된 문서와 전자서명의 부분이 전체 문서 구조상 어느 부분에 위치되고, 구성되어 있는지에 따라 결정된다. Enveloping signature방식은 전자서명된 문서의 루트 엘리먼트로 전체 문서가 <signature>로 시작해서 </signature>로 끝나며 실제적인 문서의 내용과 전자서명에 사용된 알고리즘과 서명 값, 공개 키 정보, 인증서 정보가 <signature>태그 안에 포함된다.

2.2 XML 전자서명 문서에서 사용되는 알고리즘

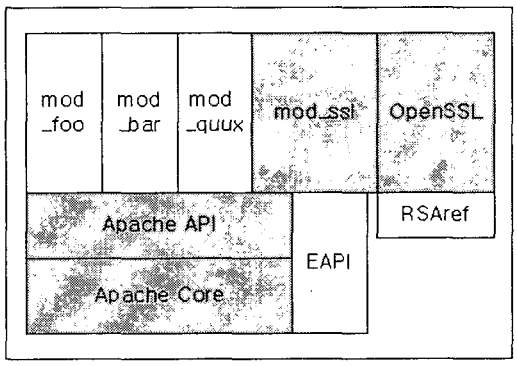
XML전자서명에서는 RSAwithSHA1과 DSAwithSHA1을 지원하고 있으며, 인코딩 방식은 Base-64코드를 사용한다. 또한 메시지 다이제스트에는 현재 SHA-1 알고리즘이 사용되고 있다. 메시지 인증을 위해서는 HMAC-SHA1을 사용한다. Canonicalization Method는 XML문서의 서명을 수행하기 전 문서를 정규화하기 위해 필요한 알고리즘이다. Transforms는 문서 검증 시 필요한 정보, 즉 검증 전에 수행하여야 할 알고리즘이나 메소드를 명시하고 있으며 생성할 때 사용했던 정보나 처리결과를 밝힘으로써 검증에 필요한 정보를 나타낸다.

2.3 웹에서의 SSL구현

SSL은 Netscape사에서 처음으로 제안되었으며, 자사의 웹 어플리케이션에 처음으로 구현함으로써 현재 웹 보안의 대명사로 알려져 있는 보안 프로토콜이다. 그러나 SSL은 웹과 같은 특정 응용을 위한 보안 프로토콜이 아닌 일반적인 인터넷 보안 프로토콜로 사용되며 웹 보안은 HTTP프로토콜을 SSL로 암호화시킨 HTTPS가 사용된다.

HTTPS는 사용자의 페이지 요청들과 웹서버에 의해 반환되는 페이지들을 암호화하고 해석한다. 서버에서 생성되어 서명된 EDI문서는 그 내용에 대한 정보를 암호화하지 않기 때문에 인터넷상에서 노출된다. SSL은 프로토콜 계층상에서 상호인증, 무결성을 위한 메시지 인증 코드, 기밀성을 위한 암호화등을 제공함으로써 클라이언트와 서버 사이에 안전한 데이터 통신을 제공한다.

Https의 구현은 OpenSSL[6]과 mod_ssl[7]을 사용하는 방법과 Apache SSL[8]을 사용하는 두가지 방법이 있다. 본연구에서는 OpenSSL과 mod_ssl을 사용하여 Https를 구현하였다. [그림2]는 Apache WebServer상에서의 OpenSSL과 mod_ssl의 관계도이다. mod_ssl은 Https를 Apache WebServer에서 수행할수 있도록 지원하는 모듈이며 Https를 수행하면서 필요한 암복호화에 관련된 모듈은 OpenSSL에서 제공받는다.

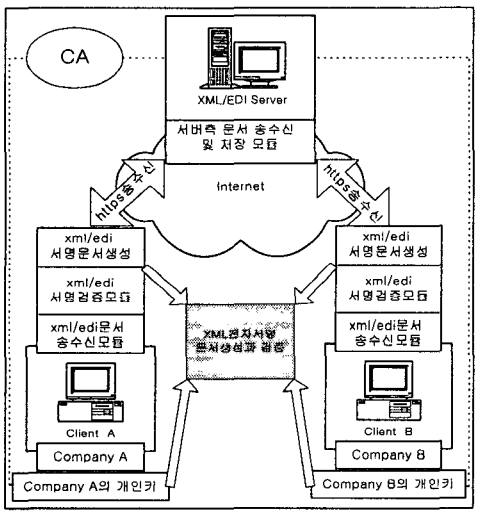


[그림2] Apache WebServer상에서 OpenSSL과 mod_ssl의 관계도

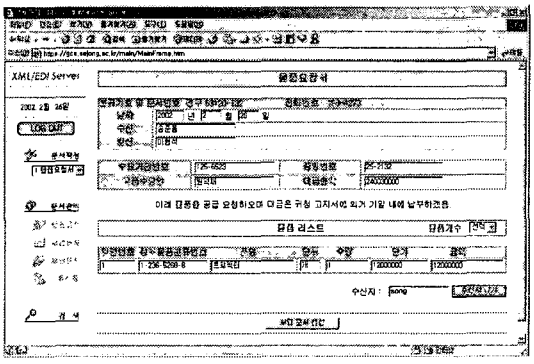
3. XML 전자서명 기반 보안시스템의 구현

3.1 시스템의 구조 및 인터페이스

구현된 XML/EDI 시스템의 전체구조는 다음의 [그림3]과 같다. Company A를 송신자라 하고 Company B를 수신자라 하였을때 송신자는 XML/EDI 서버에 접속하여 [그림 4] 화면의 서블릿으로 작성된 사용자 인터페이스를 통해 XML/EDI문서를 작성하게 된다. 서버와 클라이언트간에 주고 받는 메세지는 HTTPS를 통해 암호화 되어 전달되며 이로서 주고 받는 모든 메세지는 안전하다. 또한 XML전자서명 수행을 위한 모듈은 Applet의 형태로 존재하여 사용자는 사전에 추가로 특정 프로그램을 설치할 필요없이 전체 작업을 수행할 수 있게 구성하였다.



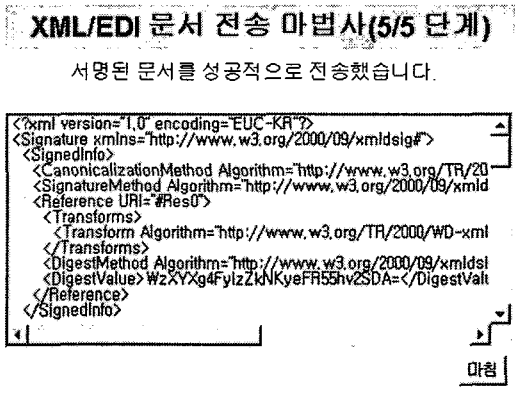
[그림3] XML/EDI 시스템의 전체구조



[그림4] XML/EDI사용자 인터페이스

작성된 문서는 수신자에게 전송시 [그림5]화면의 XML/EDI문서전송 마법사를 통해 XML Digital Signature로 서명되어 수신측에 전달된다.

송신자가 작성한 문서는 서명되어 수신자에게 전송된 후 수신자는 문서의 수신여부를 E-mail을 통하여 통보받게 된다.

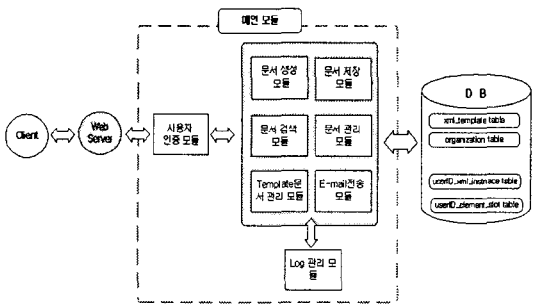


[그림5] XML전자서명된 XML/EDI 문서

이후 수신자는 문서의 확인을 위해 서버에 접속하여 수신한 서명된 문서를 전자서명 검증 마법사를 통해 서명문서의 유효성 확인 및 송신자의 인증서를 검증한 후 XML/EDI문서의 내용을 확인하게 된다.

3.2 XML/EDI 시스템의 구성 모듈

XML/EDI시스템 구성 모듈은 서버측 모듈과 클라이언트 측의 모듈로 나누어진다. 서버측 모듈의 전체구조는 [그림6]과 같이 크게 문서 생성 모듈, 문서 저장모듈, 문서 검색 모듈, 문서 관리 모듈, Template 문서 관리 모듈, E-mail 전송 모듈로 구성되어 있으며 클라이언트 측의 모듈은 XML 전자서명 생성모듈, XML 전자서명 검증모듈로 나눌수 있다.



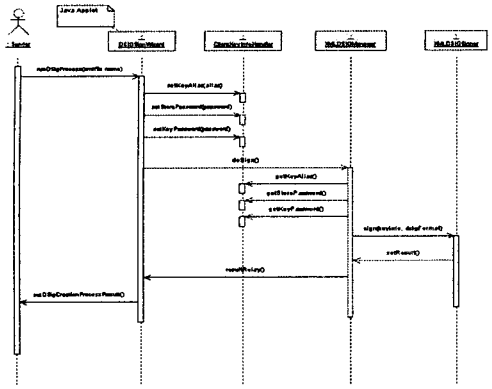
[그림6] XML/EDI시스템의 서버측 모듈도

서버에서 작성된 XML 문서는 전송에 앞서 인증을 위한 XML 전자서명 생성 과정을 거쳐야 하며, 마찬가지로 서명된 문서를 검증하고자 XML문서 검증 과정을 거쳐야 한다. 구현된 XML 전자 서명 수행 클라이언트는 크게 XML 전자 서명 생성 모듈, XML 전자 서명 검증 모듈로 구성된다.

-XML 전자 서명 생성 모듈

송신자의 개인 키를 얻기 위한 정보 입력 부분과 서명할 문서 미리 보기, 최종 생성된 XML 전자서명 문서 확인 등의 기능을 포함한다. 서명 문서는

Enveloping 형식으로 생성된다. [그림7]에 XML전자서명 생성과정을 Sequence Diagram으로 나타내었다.

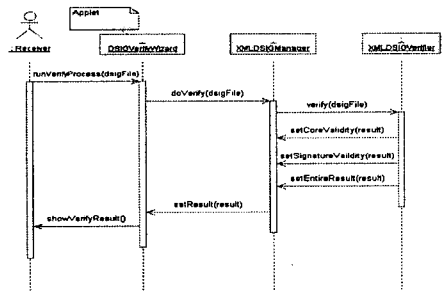


[그림7] XML 전자 서명 생성 Sequence Diagram

전자서명 생성과정의 상세 처리내역은 다음과 같다.
①runDSigProcess: 서버로 부터 수신한 서명할 XML/EDI문서를 DSIGSignWizard에 전달한다.
②setKeyAlias, setStorepassword, setKeypassword: ClientKeyInfoHandler에 사용자의 keystore로부터 개인키를 인출하기 위한 인출정보를 전달한다.
③doSign: XMLDSIGManager는 서명 생성에 필요한 서명 생성 방식 설정 플래그 및 서명 문서 파일 이름을 생성한다.
④getKeyAlias,getStorePassword,getKeyPassword: XMLDSIGManager는 ClientxKeyInfoHandler로부터 서명자의 개인 키 정보를 얻어 서명 생성 시 XMLDSigSigner에게 전달한다.
⑤sign: 전달 받은 개인 키 정보 및 XML 전자서명 생성 형식, 서명 파일 이름을 전달받아 XML 전자서명 문서를 생성한다.
⑥setResult, resultDisplay, setDSigCreationProcess Result: XML 전자 서명 생성 결과를 서버에게 되돌린다.

-XML 전자 서명 검증 모듈

검증모듈은 수신된 문서에 포함되어있는 송신자의 인증서를 통해 전자서명의 유효성을 검증한다. [그림8]에 XML전자서명 검증과정을 Sequence Diagram으로 나타내었다.



[그림8] XML 전자 서명 검증 Sequence Diagram

전자서명 검증과정의 상세 처리내역은 다음과 같다.
①runVerifyProcess: 서명 검증할 XML 전자서명 문서를 DSIGVerifyWizard에 전달한다.
②doVerify: XMLDSIGManager는 전달 받은 서명 파일을 실제 서명 검증 작업을 수행 할 XMLDSIGVerifier에 전달한다.
③verify: 전달받은 XML 전자 서명을 전자서명내에 포함되어 있는 공개 키 정보를 사용하여 검증한다.
④setCoreValidity, setSignatureValidity, setEntire Result:XMLDSIGVerifier는 서명 검증 결과를 XMLDSIGManager에 전달한다.
- Core Validity는 서명 생성 시 참조 문서에 대한 검증 및 수신 XML 전자 서명 문서에 대한 검증을 모두 만족하는 값이다. 둘 중 하나만 만족 할 때는 서명 검증에 실패하게된다.
⑤setResult, showVerifyResult: Core Validity를 통해 최종 검증결과를 서버에게 되돌린다.
- 서명 실패시 문서 재전송 요청을 서명 문서 송신자에게 전달한다.

4. 결론 및 향후 연구방향

기업간 문서교환에 있어 XML/EDI시스템은 이미 대세로 자리잡아 가고 있으며 그에 따른 보안문제는 반드시 해결해야 할 문제가 되고 있다.

따라서 본 논문에서는 XML/EDI 서버 시스템과 XML DSig표준을 따른 XML 전자서명생성 및 검증 클라이언트 S/W를 설계 및 구현하였다. 향후 CA와의 연동을 통해 통합적인 보안 XML/EDI 시스템을 연구 개발할 예정이며 XML/EDI문서의 효율적인 저장 방법을 통한 문서 검색, 관리 방법을 연구할 예정이다.

5. 참고 문헌

[1] 한국전자상거래 진흥원, EDI표준, http://www.kiec.or.kr/
[2] Miyazawa, T., Kushida, T. , "An advanced Internet XML/EDI model based on secure XML documents" Parallel and Distributed Sysems: Workshops, Seventh International Conference on, 2000 , 2000 , Page(s): 295 -300
[3] W3C, Extensible Markup Language (XML), http://www.w3c.org/XML
[4] W3C, XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/
[5] W3C, XML-Signature Requirements, http://www.w3.org/TR/xmldsig-requirements
[6] OpenSSL, http://www.openssl.org
[7] ModSSL, http://www.modssl.org
[8] Apache SSL, http://www.apache-ssl.org/