XML 전자서명에 기반한 EC서버 보안 설계 및 구현

성백호, 김현희, 신동규, 신동일
세종대학교 컴퓨터공학과
{guardia[0], hyunhee, shindk, dshin, }@gce.sejong.ac.kr

Design and Implementation of EC Server Security based on XML Digital Signature

Baek Ho Sung[0] Hyun Hee Kim Dongkyoo Shin Dongil Shin
Department of Computer Engineering, Sejong University

요 약

인터넷을 통한 전자상거래가 실제화 되고 확산되고 있는 가운데 개인과 기업에서 요구사항은 더욱 다양화되고 보안의 구축이 필수 조건으로 요구되고 있다. 이러한 다양한 요구사항에 대한 효율적인 조작과 처리를 XML(eXtensible Markup Language)을 통하여 해결하려는 시도가 이루어지고 있다. XML을 통한 전자상거래는 표준이 되어 가고 있으며 그 효율성은 전자상거래를 활성화시킴으로써 새로운 시장의 창출과 효율성 극대화하기 위한 활력소가 되고 있다. 본 논문에서는 B2B기반 XML전자상거래 시스템을 구현하고 문서교환에 SSL과 XML표준에 기초한 전자서명(XML Digital Signature)시스템을 구축하므로써 인증과 보안을 고려한 XML/EDI 전자서명 시스템을 설계, 구현하였다.

1. 서론

기업간에 인터넷을 통한 전자상거래가 실제화 되고 확산되는 가운데 개인과 기업에서의 요구사항은 더욱 다양화되고 보안의 구축이 필수조건으로 요구되고 있다. 특히 B2B에서의 문서교환은 일정한 규칙성을 가져야하고 데이터베이스에서의 활용성을 높이며 데이터 조작의 간결함을 요구하고 있으나 현재 대부분의 웹에서 사용하고 있는 HTML(Hypertext Markup Language)의 한계성은 이러한 문제를 해결하기 힘들었다. 이러한 다양한 요구사항에 대한 효율적인 데이터의 조작과 처리를 충족시키기 위하여 애플리케이션과 웹에서 XML(eXtensible Markup Language)[1]이라는 새로운 언어의 등장은 기존의 문제를 해결할 수 있는 차세대 언어로 주목받고 있으며 XML을 활용한 시스템이 꾸준히 등장하고 있어 XML에 기반한 시스템의 구축은 점차 확산되고 있는 추세이다.

XML 문서는 문서자체에 구조적인 정보를 담고 있고 소프트웨어와 시스템 환경에 독립적이며 간결성과 확장성으로 강력한 기능을 제공함으로써 현재 전자상거래에 사용되고 있는 EDI(Electronic Data Interchange)[2]문서의 적용에 가장 적합한 표준으로 자리 잡아 나가고 있다.

인터넷의 확산과 XML의 장점으로 데이터의 교환이 어느 곳에서나 가능하게 된 반면 보안상의 취약점이 드러나고 있는데 특히 금전적인 정보를 교환하는 전자상거래 상의 메시지 전달에 있어 보안은 가장 중요하게 요구되고 있는 부분이 되었으며 시스템의 필수 조건이 되었다. 본 논문에서는 보안에 취약한 웹 환경에서 SSL과 XML전자서명(XML Digital Signature)을 이용하여 XML EDI 문서를 생성, 검증하고 보안을 강화한 전자상거래 서버 시스템을 설계하고 구현하였다.

2. 관련 연구

2.1 XML 전자서명(XML Digital Signa

ture)

전자서명이란 전자화 된 문서의 메시지 내용이 수정 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 XML전자서명 표준에 대해 기술하고 있으며 2001년 8월 20일 "Proposed Recommendation" [3]인 상태로 계속적인 표준화 작업이 진행되고 있다. XML 전자서명(XML Digital Signature) 문서는 서명을 새롭게 생성하고 표현하는데 대한 XML 구문과 처리규칙을 명시하고, 어떤 디지털 컨텐츠에도 적용이 가능하며, XML 문서를 포함한 다양한 자원에 적용되어질 수 있다.

전체적인 문서의 내용은 전자서명을 생성할 문서에 대한 해시 값(<DigestValue>)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. XML전자서명 문서의 포맷은 Enveloping signature, Enveloped signature, Detached signature로 나뉘며, 이 포맷들은 XML로 작성된 문서와 전자서명의 부분이 전체 문서에서 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[그림 1 참조].

SignatureMethod는 서명 알고리즘을 선택할 수 있는 사항을 나타내고 있다. 현재, XML전자서명에서는 RSAwithSHA1과 DSAwithSHA1을 지원하고 있으며, 인코딩 방식은 Base-64 코드를 사용한다. 또한 메시지 다이제스트에 사용되는 알고리즘으로는 현재 SHA-1이 사용되고 있다. 메시지 인증을 위해서는 HMAC-SHA1을 사용한다. CanonicalizationMethod는 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. 현재 사용되고 있는 알고리즘은 환경에 따라 보다 효율적인 알고리즘으로 대체할 수 있다.

```
<?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

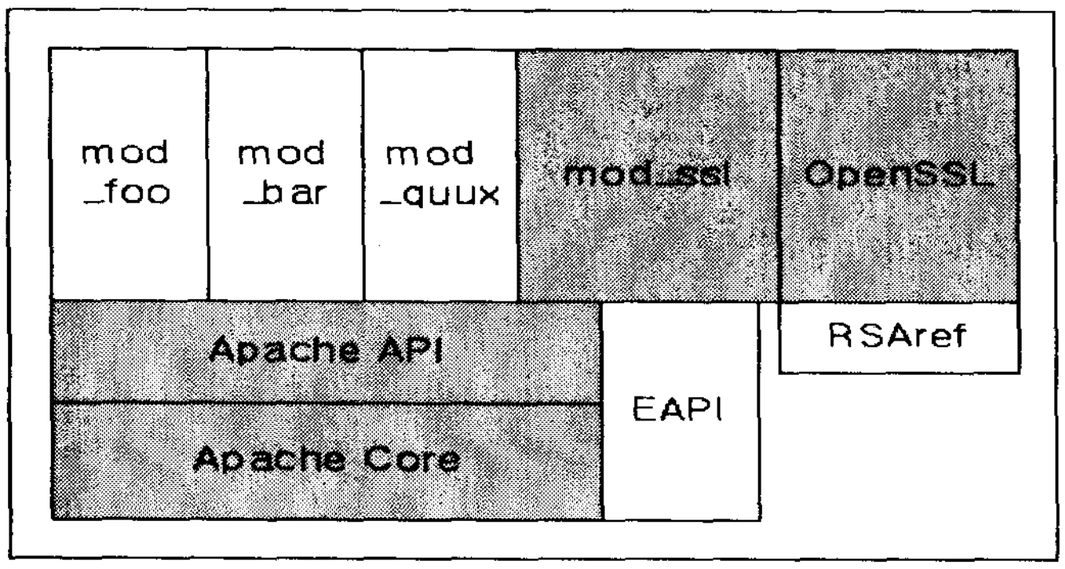
2.2 웹에서의 SSL구현

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. HTTPS는 실제로 넷스케이프의 SSL을 정규 HTTP 응용계층 하에서 서브 계층으로서 사용한다. 클라이언트의 사용자가 페이지를 서버에 전송하면, 브라우저의 HTTPS 계층이 그 페이지를 암호화한다. 서버가 받았음을 알리는 회신내용 역시 암호화된 형식으로 도착되지만, 그 내용은 브라우저의 HTTPS 서브 계층에 의해 해석된다.

본 연구에서는 OpenSSL과 mod_ssl을 사용하여 HTTPS를 구현하였다. [그림 2]는 Apache WebServer상에서의 OpenSSL과 mod_ssl의 관계도이다. mod_ssl은 HTTPS를 Apache WebServer에서 수행할 수 있도록 지원하는 모듈이며 HTTPS를 수행하면서 필요한 암복호화에 관련된 모듈은 OpenSSL에서 제공받는다[4].



[그림 2] Apache WebServer에서
OpenSSL과 mod_ssl 관계도.

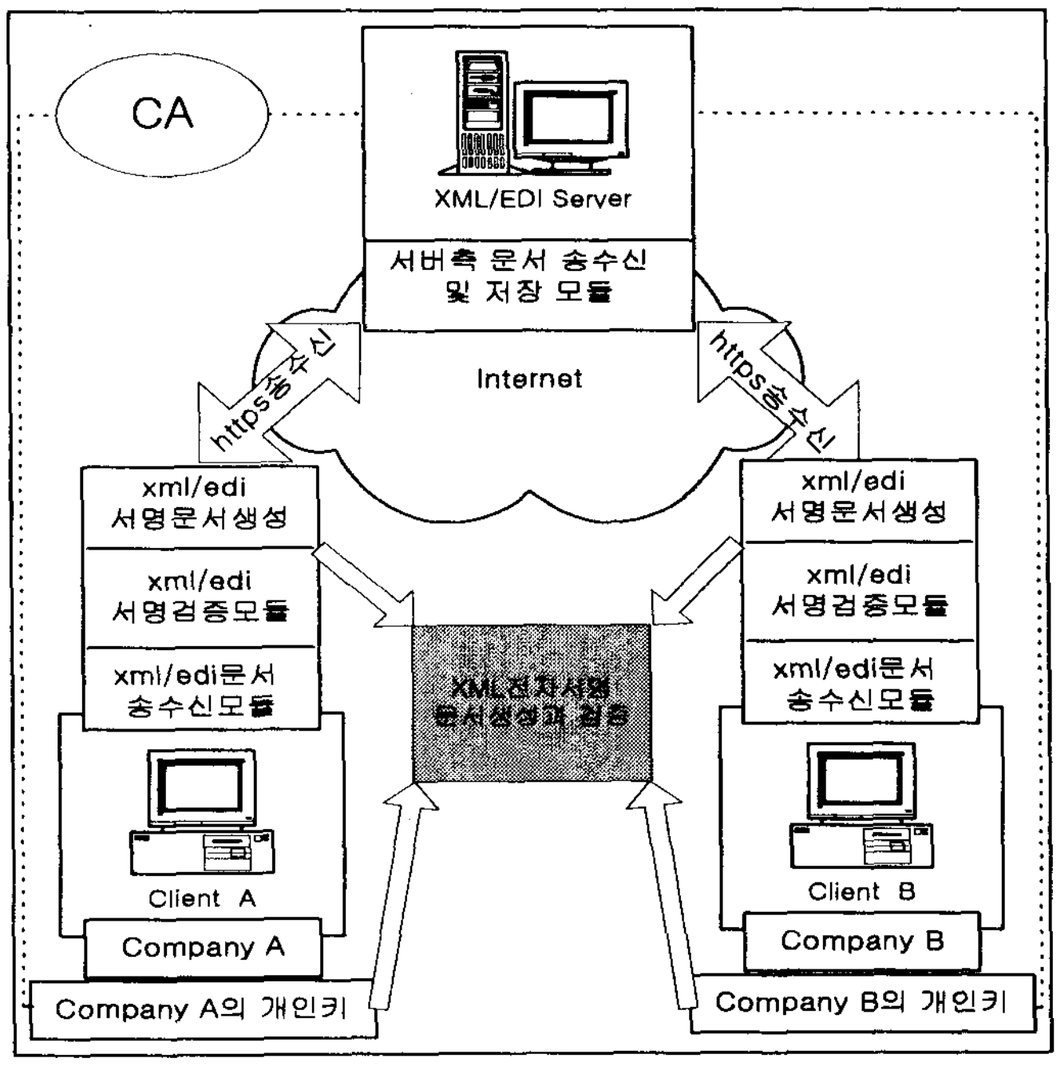
3. XML전자서명 기반 EC서버 보안 시스템의 구현

3.1 XML/EDI 시스템의 구성 모듈

XML 전자서명 기반 전자상거래 보안 시스템의 전체구조는 다음의 [그림 3]과 같다.

XML/EDI시스템 구성 모듈의 전체구조는 크게 문서 생성 모듈, 문서 저장 모듈, 문서 검색 모듈, 문서 관리 모듈, E-mail 전송 모듈, XML전자서명 생성, 검증 모듈로 구성되어 있다.

• 문서 생성 모듈 : 클라이언트로부터 전송된 Data와 Template문서내의 엘리먼트 정보를 통해 XML 인스턴스 문서를 생성한다. 생성된 문서는 클라이언트 측의 XML 전자서명 생성 모듈을 통해 서명된다.



[그림 3] XML전자서명 EC서버 시스템 전체구조도

• 문서 저장 모듈 : 생성된 XML 인트턴스 문서와 서명문서를 문서정보와 함께 DB에 저장한다.

• 문서 검색 모듈 : 각 사용자들이 가지고 있는 문서 Instance Table의 문서 정보를 통해 검색을 수행한다.

• 문서 관리 모듈 : 사용자의 보낸 문서, 받은 문서, 서명문서확인, 휴지통보기 등의 기능을 처리한다.

• E-mail 전송 모듈 : 서명문서의 도착 및 재전송 요구 등과 같은 메세지를 사용자에게 E-mail로 전송한다.

• XML 전자서명 생성 모듈 : 송신자의 개인키를 얻기 위한 정보 입력 부분과 서명할 문서 미리 보기, 최종 생성된 XML 전자서명 문서 확인 등의 기능을 포함한다. 서명 문서는 Enveloping 형식으로 생성된다.

• XML 전자서명 검증 모듈 : 검증모듈은 수신된 문서에 포함되어있는 송신자의 인증서를 통해 전자서명의 유효성을 검증한다.

3.2 XML문서의 전자서명 생성, 검증 과정

XML/EDI 문서의 송신자는 서블릿으로 작성된 문서작성 인터페이스를 통해 XML문서를 작성하게 되며 작성된 문서는 수신자에게 XML/EDI문서전송 마법사를 통해 XML Digital Signature로 서명되어 전달된다[그림 4 참조]. 또한 서버 측과 송, 수신자간에 주고 받는 메시지는 HTTPS를 이용하여 주고받기 때문에 서버 측과의 교환 메시지는 안전하다.

XML/EDI 문서 전송 마법사(5/5 단계)

서명된 문서를 성공적으로 전송했습니다.

```
<?xml version="1.0" encoding="EUC-KR"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/20
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmld
    <Reference URI="#Res0">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2000/WD-xml
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsi
      <DigestValue>WzXYXg4FyIzZkNKyeFR55hv2SDA=</DigestValu
    </Reference>
  </SignedInfo>
```

마침

[그림 4] 서명 생성된 XML/EDI문서

XML Digital Signature 적용 시에 필요한 암복호화 모듈은 최초 접속 시 서버 측으로부터 애플릿의 형태로 수신하게 된다. 송신자가 작성한 XML/EDI문서는 서명되어 수신자에게 전송된 후 수신자는 문서의 수신여부를 E-mail을 통하여 통보 받게 된다. 이후 수신자는 서버에 접속하여 수신한 서명된 문서를 전자서명 검증 마법사를 통해 서명문서의 유효성 확인 및 송신자의 인증서를 검증한 후 XML/EDI문서의 내용을 확인해 볼 수 있다[그림 5 참조]. 수신자가 문서의 검증을 실패하였을 경우 송신자에게 재 송신여부를 E-mail로 통보하게 된다.

3.3 구현환경

- 운영체제 : Redhat Linux 6.2, Windows 2000 pro
- 웹 서버 : Apache Web server 1.3.20
- 데이터베이스 : Oracle 8.1.6
- 사용언어(API) : Java 1.3.1, JSDK 2.0, Xerces 2.1, Xalan 2.0, XSS4J[5]
- HTTPS : openssl-0.9.6, mod_ssl-2.8.4-1.3.20

XML 전자서명 검증 마법사(3/4 단계)

서명 검증 결과

```
**********************************************************
Core Validity : 유효함
Signature Validity : 유효함
**********************************************************

송신자 인증서 정보 :
        Version: 1
        Validity: OK
        SubjectDN: CN=Duk Jae Won, OU=DMLAB, O=SJU, L=Kai
        IssuerDN: CN=Duk Jae Won, OU=DMLAB, O=SJU, L=Kan
        Serial#: 1006334183
```

확인

[그림 5] 서명 검증된 XML/EDI문서

4. 결론 및 향후 연구방향

본 논문에서는 XML로 작성된 EDI문서교환을 위한 EC서버 보안 시스템으로서 SSL과 XML 전자 서명 생성 및 검증 클라이언트 S/W를 설계, 구현하였다. 현재 XML 전자서명과

더불어 XML Encryption[6], ebXML등 보안과 전자상거래의 많은 표준안들이 지속적으로 연구되고 있다. 새로운 보안과 전자상거래상의 XML 표준안들과 더불어 더욱 향상된 시스템을 구축할 예정이다.

5. 참고 문헌

[1] W3C, Extensible Markup Language (XML), http://www.w3c.org/XML

[2] Miyazawa, T., Kushida, T. , "An advanced Internet XML/EDI model based on secure XML documents" Parallel and Distributed Syems: Workshops, Seventh International Conference on, 2000,2000,Page(s): 295 -300

[3] XML-Signature Syntax and Processing, http://www.w3.org/TR/2001/PR-xmldsig-core-20010820

[4] http://www.apache.org/,http://www.openssl.org/ ,http://www.modssl.org/

[5] http://www.alphaworks.ibm.com/tech/xmlsecuritysuite

[6] http://www.w3.org/Encryption/2001/