XML 전자서명을 지원하는

XML 기반 전자상거래 시스템의 설계 및 구현

김세영[0] , 이재일, 박정환, 신동규
세종대학교 컴퓨터공학과, 한국정보보호진흥원
{seykim, shindk}@gce.sejong.ac.kr {jilee, pjh}@kisa.or.kr

Design and Implementation of e-commerce system Suppoting XML Digital Signature

Seyoung Kim[0] , Jaeil Lee, Junghwan Park, Dongkyoo Shin
Department of Computer Engineering, Sejong University & Korea Information Security Agency

요 약

정보통신 기술의 비약적인 발전으로 인해 인터넷은 현재 필수 불가결한 생활의 도구가 되고 있으며, 개인 및 기업에서의 인터넷 활용이 급증함에 따라 인터넷 그 자체를 사업수단으로 이용하는 추세가 가속화되고 있다. 또한, 최근 차세대 웹 표준문서 포맷으로 부상되고 있는 XML(eXtensible Markup Language)을 사용한 B2B 전자상거래 표준인 ebXML(e-business eXtensible Markup Language), Microsoft의 Biztalk Framework, CommerceNet의 eCo Framework, XML/EDI 등의 개발이 활발히 진행되고 있다. 이에 본 논문에서는 기업 간 문서교환을 위한 XML 전자상거래 시스템을 구현하고, 전체 시스템 내에서 보안상의 요구를 충족하기 위하여 W3C(World Wide Web Consortium)의 XML 전자서명(Xml-Dsig : Disital Signature) 표준에 입각한 기업 간 문서 교환시의 인증 및 보안을 위한 시스템을 설계하였다.

1. 서 론

정보통신 기술의 비약적인 발전으로 인해 인터넷은 현재 필수 불가결한 생활의 도구가 되고 있으며, 개인 및 기업에서의 인터넷 활용이 급증함에 따라 인터넷 그 자체를 사업수단으로 이용하는 추세가 가속화되고 있다. 또한, 인터넷은 기업과 개인, 기업과 기업, 개인과 개인 간의 거래를 활성화함으로써 새로운 시장의 창출과 효율성 극대화를 위한 활력소가 되고 있다. 특히, 기업 간 교역을 위한 구매 주문서, 상업 송장, 선적 통보와 같은 B2B 문서의 교환은 EDI(Electronic Data Interchange) 메시지를 통해서 교환되어진다. EDI는 데이터의 오류를 최소화하고, 정보의 신속한 전송과 처리과정을 단순화하여 기업의 업무를 자동화시키고 있다. 그러나, 특정 분야를 취급하는 대규모 기업에서의 한정된 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 실현할 수 있게 되었다[3]. XML은 현재 웹에서 사용하고 있는 HTML (Hypertext Markup Language)의 한계를 극복하고, 시스템 및 소프트웨어 독립적인 문서와 메시지의 표현이 가능하도록 W3C에서 1998년 2월에 제정한 표준이며[4], 특히 XML은 서로 상이한 시스템을 연동하는데 매우 유용하기 때문에 ebXML, Microsoft의 Biztalk Framework, CommerceNet의 eCo Framework, XML/EDI 등의 B2B 전자상거래 표준으로 사용되고 있다. 그 중 ebXML은 단일한 글로벌 전자시장을 창조한다는 목표아래 그 동안 국제 EDI 표준을 추진해 왔던 UN/CEFACT(United Nations Center for the Facilitation of Procedures and Practices for Administration, Commerce and Transport)와 OASIS등 국제적 기구가 주도가 되어, XML을 이용하여 인터넷 기반의 전자상거래를 실현하도록 제정하고 있는 표준이다[2]. ebXML은 UN이 주도로하고 있어 국가 내 거래 뿐 아니라 국가 간 거래에도 적용될 수 있는 표준으로 주목받고 있다. 현재 ebXML의 표준 명세서 및 기술보고서에 따라 구축되고 있는 시스템 내에서 보안 요구사항들의 충족은 필수적인 사안이며, 전자상거래 상에서의 XML 문서 보안에 대한 연구 개발 또한 활발히 진행되고 있다. 이에 본 논문에서는 전자상거래시스템 상에서의 기업 간 문서교환을 위한 XML기반 EDI시스템을 구축하고, 보안상의 요구를 충족하기 위하여 W3C의 XML 전자서명 표준에 입각한 기업 간 문서 교환시의 인증 및 보안을 위한 시스템을 설계하였다[6].

2. 관련 연구

전자상거래 상에서의 대부분의 서비스가 전자적으로 처리됨에 따라 그에 따른 보안의 중요성이 대두되고 있다. 특히, XML을 활용한 전자상거래 문서 교환시의 보안에 대한 표준화 작업 또한 활발히 진행되고 있다. 기존의 보안과 비교하여 XML 보안이 가지는 장점은 다음과 같다.

① 기존의 XML의 장점인 문서 자체 내에서의 구조적인 정보를 활용하여 전자 서명을 일부 혹은 문서전체에 적용시킬 수 있다.

② Namespace를 사용할 수 있다.
③ XML 보안을 활용하여 전자상거래(BtoB, BtoC)를 한 층 더 촉진시킬 수 있다.

2.1 XML 전자서명(XML Digital Signature)

IETF와 W3C의 XML-Signature WG(Working Group)에서 제정된 "XML-Signature Syntax and Processing" 명세서는 2001년 8월 20일 W3C의 "Proposed Recommendation" 상태로 승격되어 지속적인 표준화 작업이 진행되고 있다[7]. 이 문서는 XML 전자서명에 대한 규칙과 구문처리를 명시한다. XML 전자서명은 무결성, 메시지 인증(message authentication) 및 어떤 데이터의 유형에 대해서도 서명자 인증 서비스를 제공하기 위한 목적으로 개발되었다. 즉, 전자서명을 새롭게 생성하고 표현하는데 대한 XML 구문과 처리규칙을 명시하고, 어떤 디지털 컨텐츠에도 XML전자서명을 적용 가능하도록 하며, XML문서의 포함과 동시에 다양한 데이터에 적용되어질 수 있다.

XML 전자 서명 문법에 따른 종류 및 기본적인 문법구조는 다음과 같다.

① Enveloping signature

서명이 전송 문서의 부모 엘리먼트로 전체 문서가 <signature>로 시작해서 </signature>로 끝난다.

② Enveloped signature

서명이 전송 문서의 자식 엘리먼트로 전체 XML문서 내부에 <signature>로 시작해서 </signature>로 끝나는 XML 전자서명 엘리먼트들이 포함되어 있다.

③ Detached signature

전자서명 문서와 전송하고자하는 XML 문서 혹은 다른 문서들이 분리되어 표현 및 전달되는 것을 말한다.

```
<Signature>
  <SignedInfo>
    (CanonicalizationMethod)
    (SignatureMethod)
    (<Reference (URI=)? >
      (Transforms)?
      (DigestMethod)
      (DigestValue)
    </Reference>)+
  </SignedInfo>
  (SignatureValue)
  (KeyInfo)?
  (Object)*
</Signature>

1. "?" = zero or one occurrence
2. "+" = one or more occurrences
3. "*" = zero or more occurrences
```

[표 1] XML 전자서명 문서의 기본 구조

2.2 ebXML의 개요

2001년 5월 11일 개최된 ebXML 비엔나 총회에서 주요 7개의 ebXML 명세서가 만장일치로 승인됨에 따라 단일 국제 전자상거래 표준이 확립됨으로써 전자상거래 활성화에 크게 기여할 것으로 보인다.

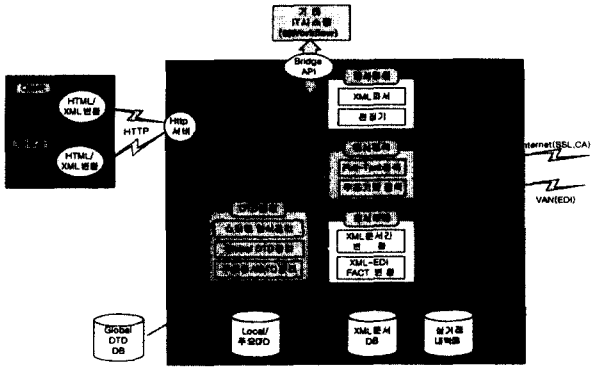
ebXML이 EDI등 기존의 B2B 전자상거래 표준과 다른 특징은 다음과 같다.

- 기존 EDI의 VAN(Value Added networks)경유 방식과는 달리 거래 당사자간의 개방된 표준거래 방식의 채택으로 유연한 거래 형태를 가지는 인터넷 기반 B2B 전자상거래 표준을 제공한다.
- 기업 내부의 문서교환을 위한 표준 방법론을 제공하며, 공통 비즈니스 프로세스(Common Business Process)와 컴포넌트(Core Component)를 제공한다.
- 분산된 Repository의 구축을 지원한다.

3. XML 전자서명 적용 전자상거래 시스템의 구현

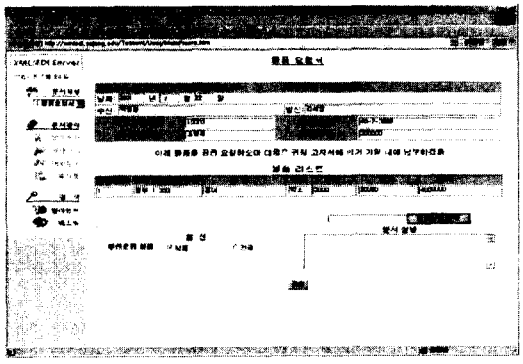
3.1 전체 시스템의 구조

현재 구현된 시스템의 내부 구조는 다음의 [그림 1]과 같다.



[그림 1] XML 기반 전자상거래 시스템의 내부 구조

구현된 XML기반 전자상거래 시스템에서 문서 작성 템플릿 인터페이스에 따라 B2B 교환을 위한 XML문서를 작성한다. [그림 2]는 문서작성을 위한 템플릿 인터페이스이다.

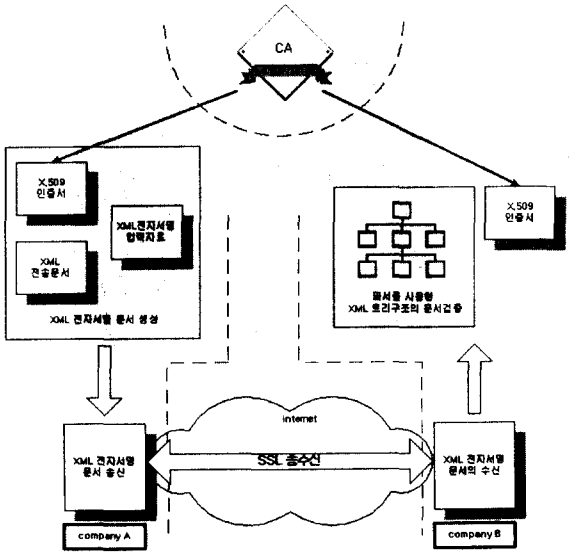


[그림 2] XML 문서작성을 위한 템플릿 인터페이스

3.2 XML 전자서명 적용 설계

구현된 시스템에서 작성된 XML 문서는 전송에 앞서 인증을 위한 XML 전자서명 생성 과정을 거쳐야 하며, 전송하고자하는 XML문서, XML전자서명 문서 생성을 위한 데이터, 인증서 등을 입력 값으로 하여 Enveloping signature, Enveloped signature 및 Detached signature 형식의 XML 전자서명 문서를 생성하게 된다.

또한, 생성된 전자서명문서는 데이터 전송 프로토콜인 SSL(Secure Socket Layer)을 사용하여 송수신하게 된다. SSL은 인증, 기밀성, 메시지 무결성과 같은 세 개의 암호화 확인 방법을 제공하며, 인터넷 브라우저와 인터넷 서버 사이의 비밀키 교환을 하는 역할을 수행한다. 그러나, SSL은 보안에서 제공되어야 할 기능중 부인 방지에 관한 역할은 수행하지 않는다. 시스템 상에서 XML 전자서명 문서에 포함된 송수신 자료들에 의해 이를 해결할 수 있으므로, XML을 사용하는 B2B 문서교환에 있어서 보안이 강화된 완벽한 시스템을 실현할 수 있다. [그림 4]는 현재 시스템 내에서 XML 전자서명 문서의 생성과 송수신 및 검증에 대한 구조도이다.



[그림 3] XML 전자서명문서의 생성, 검증 및 송수신

XML 전자서명 문서의 생성을 위한 처리 과정은 다음과 같다.

- 참조 생성 (Reference Generation)
  - 데이터 객체에 Transforms를 적용한다.
  - Transforms 처리 이후 결과 값에 대한 digest값을 구한다.
  - reference 구성요소를 생성한다.
- 서명 생성 (Signature Generation)
  - SignatureMethod, CanonicalizationMethod, Reference를 가지는 SignedInfo를 생성한다 [1].
  - SignedInfo에 지정된 알고리즘에 따라 SignatureValue를 Canonicalize의 수행 이후 계산한다.
  - SignedInfo, Object, KeyInfo, SignatureValue를 포함하는 Signature를 생성한다.

XML 전자서명 문서의 검증은 다음과 같은 단계로 진행된다.

- 참조 검증 (reference Validation)
  - SignedInfo내의 CanonicalizationMethod에 따라 *canonicalize*한다.
  - digest될 데이터 객체를 얻는다.
  - Reference에 지정된 DigestMethod를 이용하여 데이터 객체를 digest한다.
  - SignedInfo Reference에 있는 DigestValue와 생성한 digest결과 값을 비교하여 일치하면 검증 성공한 것이고, 그렇지 않으면 검증실패가 된다.
- 서명 검증 (Signature Validation)
  - CanonicalizationMethod를 기반으로 하여 SignedInfo 요소를 canonicalize 한다.
  - KeyInfo 혹은 외부에서 검증 키(validation key)를 획득한다.
  - SignedInfo내의 SignatureMethod에로 SignatureValue를 검증한다.

4. 결론 및 향후 연구방향

본 논문에서는 기업 간 문서교환을 위한 XML 전자상거래 시스템을 구현하고, 시스템 내에서 보안상의 요구를 충족하기 위하여 XML 전자서명 표준을 지원하는 보안 시스템을 설계하였다. 향후 본 시스템과 연동하여 차세대 PKI 기술인 XKMS(Xml Key Management Specification)[5]의 도입으로 응용 프로그램에서 요구하는 보안 요구사항을 분석하고, 사용자의 편의성과 보안성을 동시에 만족시키는 응용 시스템을 개발할 예정이다.

5. 참고 문헌

[1] Canonical XML Version 1.0, http://www.w3.org/TR/2001/REC-xml-c14n-20010315

[2] e-business eXtensible Markup Language(ebXML), http://www.ebxml.org/

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

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

[5] XML Key Management Specification (XKMS), http://www.w3.org/TR/2001/NOTE-xkms-20010330/

[6] XML-Signature Requirements, http://www.w3.org/TR/1999/WD-xmldsig-requirements -19991014.html

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