XML 전자서명 시스템의 설계 및 구현

김세영° , 원덕재, 송준홍, 김현희, 신동규, 신동일
세종대학교 컴퓨터공학과
e-mail : seykim@gce.sejong.ac.kr

Design and Implementation of XML Digital Signature System

Seyoung Kim, Duckjae Won, Junhong Song,
Hyunhee Kim, Dongkyoo Shin, Dongil Shin
Department of Computer Engineering, Sejong University

요 약

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. 그와 더불어 최근 차세대 웹 표준문서 포맷으로 부상되고 있는 XML(eXtensible Markup Language)을 사용한 B2B 전자상거래 규격에 대한 국내외적인 표준화 작업 또한 가속화되고 있다. 이에 본 논문에서는 기업 간 문서교환을 위한 B2B기반 XML 전자상거래 시스템을 구현하고, 시스템 내에서 보안상의 요구를 충족하기 위하여 XML 전자서명(Xml-Dsig : Disital Signature) 표준에 입각하여 기업 간 문서 교환시의 인증 및 보안문제를 해결하기 위한 XML 전자서명 기반 보안시스템을 설계하였다.

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 교환되어진다. EDI는 데이터의 오류를 최소화하고, 정보의 신속한 전송과 처리과정을 단순화하여 기업의 업무를 자동화시키고 있다. 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 실현할 수 있게 되었다 [2]. XML은 현재 웹에서 사용하고 있는 HTML (Hypertext Markup Language)의 한계를 극복하고, 시스템 및 소프트웨어 독립적인 문서와 메시지의 표현이 가능하도록 W3C에서 1998년 제정한 표준이며 [3], 특히 XML은 서로 상이한 시스템을 연동하는데 매우 유용하기 때문에 ebXML[1], Microsoft의 Biztalk Framework, CommerceNet의 eCo Framework, XML/EDI 등의 B2B 전자상거래 표준

으로 사용되고 있다. 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. 이에 본 논문에서는 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[5].

2. 관련 연구

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[6]. 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 XML 문서 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 XML 전자서명 문서에서 사용되는 알고리즘

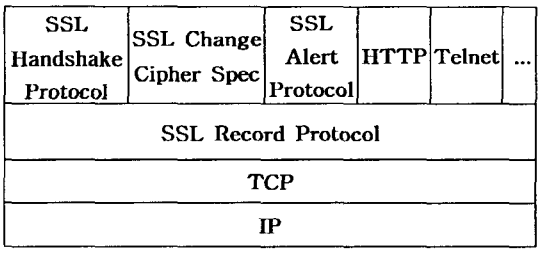
SignatureMethod는 서명 알고리즘을 선택할 수 있는 사항을 나타내고 있다. 현재, XML전자서명에서는 RSAwithSHA1과 DSAwithSHA1을 지원하고 있으며, 인코딩 방식은 인코딩 방식은 Base-64코드를 사용한다. 또한 메시지 다이제스트에 사용되는 알고리즘으로는 현재 SHA-1이 사용되고 있다. 메시지 인증을 위해서는 HMAC-SHA1 그밖에 CanonicalizationMethod 및 Transform을 위한 알고리즘들이 존재한다. 현재 사용되고 있는 알고리즘은 보다 효율적인 알고리즘으로 대체 가능하며, XML 전자서명에서 사용되는 알고리즘의 종류는 [그림 1]과 같다.

Algorithm Type	Algorithm	Requirements
Digest		
	SHA1	REQUIRED
Encoding		
	base64	REQUIRED
MAC		
	HMAC-SHA1	REQUIRED
Signature		
	DSAwithSHA1 (DSS)	REQUIRED
	RSAwithSHA1	RECOMMENDED
Canonicalization		
	Canonical XML with Comments	RECOMMENDED
	Canonical XML (omits comments)	REQUIRED
Transform		
	XSLT	OPTIONAL
	XPath	RECOMMENDED
	Enveloped Signature•	REQUIRED

[그림 1] XML 전자서명에서 사용되는 알고리즘

2.2 SSL(Secure Socket Layer)

SSL은 웹 브라우저 개발로 이미 잘 알려져 있는 넷스케이프사에 의해 제안되었고, 1995년 초에 SSL v2에 이어, SSL v3가 개발되었다. SSL 프로토콜은 TCP/IP와 같은 연결 지향적 네트워 계층 프로토콜과 HTTP와 같은 응용 계층 프로토콜 사이에 위치하는 프로토콜 계층상에서 상호 인증(Mutual Authentication), 무결성을 위한 메시지 인증 코드(MAC: Message Authentication Code), 기밀성을 위한 암호화 등을 제공함으로써 클라이언트와 서버 사이에 안전한 데이터 통신을 제공한다. 또한, 이 프로토콜은 암호화, 메시지 압축, 메시지 인증 코드(MAC)을 위해 사용되는 알고리즘을 선택하는 것이 가능하다. 이렇게 함으로써 암호 제품 사용에 대한 법적인 문제, 수출입 등에 따른 제반 문제에 맞춰 특정 서버에서 암호 알고리즘을 선택할 수 있으며, 새로운 알고리즘을 쉽게 이용하는 것이 가능하다. 다음의 [그림 2]는 SSL 프로토콜의 계층구조이다.

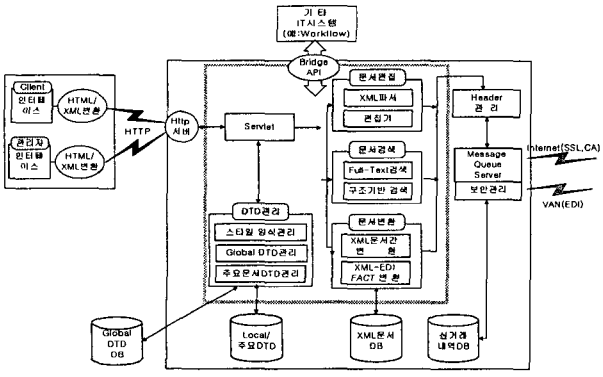


[그림 2] SSL 프로토콜의 구조

3. XML 전자서명 기반 보안시스템의 구현

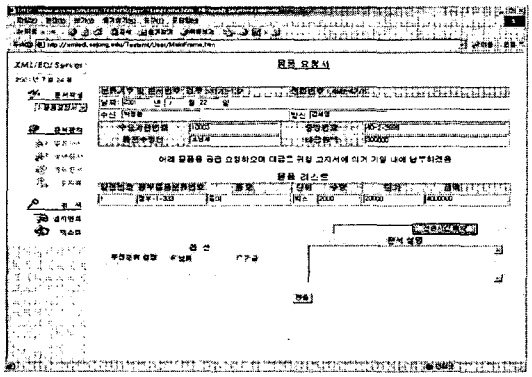
3.1 전체 시스템의 구조

현재 구현된 시스템의 내부 구조는 다음의 [그림 3]과 같다.

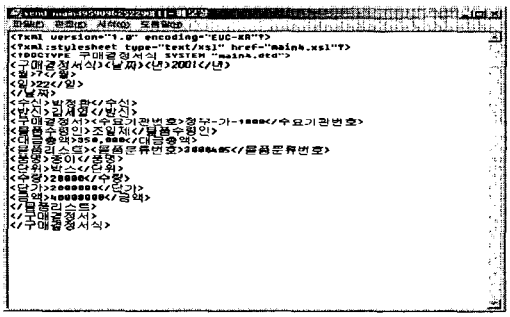


[그림 3] XML 기반 전자상거래 시스템의 내부 구조

구현된 XML기반 전자상거래 시스템에서 문서 작성 템플릿 인터페이스에 따라 B2B 교환을 위한 XML문서를 작성한다. [그림 4]는 문서작성을 위한 템플릿 인터페이스이며, 그 다음 나타낸 [그림 5]는 작성된 XML 문서를 보여주고 있다.



[그림 4] XML 문서작성을 위한 템플릿 인터페이스



[그림 5] 전송을 위한 XML문서

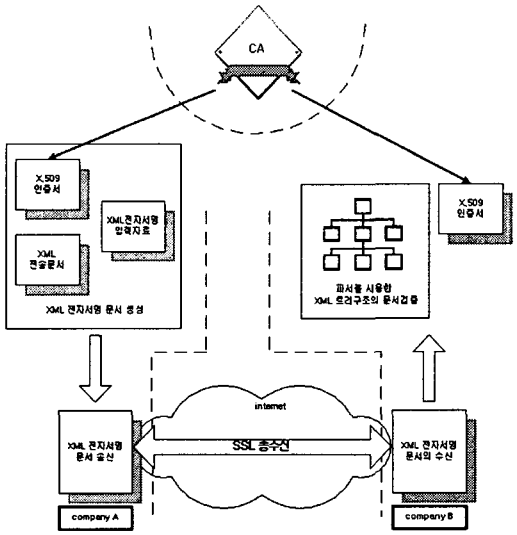
3.2 XML 전자서명 적용을 위한 시스템 설계

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 6]은 현재 시스템 내에서 XML 전자서명 문서의 생성과 송수신 및 검증에 대한 구조도이다.



[그림 6] XML 전자서명문서의 생성, 검증 및 송수신

XML 전자서명 문서의 생성을 위한 처리 과정은 다음과 같다.

① 참조 생성 (Reference Generation)

XML 전자서명 문서의 참조 부분의 값에 대한 생성을 위하여 먼저 데이터 객체에 Transforms를 적용한다. Transforms의 처리이후 결과 값에 대한 digest값을 구한다. 마지막으로 reference의 구성요소를 생성한다.

② 서명 생성 (Signature Generation)

XML 전자서명 내에서의 핵심부분인 서명의 생성을 위하여 우선 SignedInfo에서 SignatureMethod, CanonicalizationMethod, Reference를 포함하는 요소들을 생성한다. SignedInfo에 지정된 알고리즘에 따라 SignatureValue를 Canonicalize의 수행 이후 계산한다. 계산된 값에 따라, SignedInfo, Object, KeyInfo, SignatureValue를 포함하는 Signature를 생성한다.

생성된 전자서명 문서에 근거하여 수신된 XML 전자서명 문서의 검증은 다음과 같은 단계로 진행된다.

① 참조 검증 (reference Validation)

참조의 검증 절차는 우선 SignedInfo내에 포함된 CanonicalizationMethod에 따라 canonicalize한다. 다음 digest될 데이터의 객체를 얻은 이후, Reference에 지정된 DigestMethod를 이용하여 데이터 객체를 digest한다. 마지막으로 참조의 검증은 SignedInfo Reference에 있는 DigestValue와 생성한 digest결과 값을 비교하여 일치하면 검증 성공한 것이고, 그렇지 않으면 검증실패가 된다.

② 서명 검증 (Signature Validation)

서명의 검증은 CanonicalizationMethod를 기반으로 하여 SignedInfo 요소를 canonicalize 하는 절차를 먼저 수행한 후, KeyInfo 혹은 외부에서 검증 키(validation key)를 획득한다. SignedInfo내의 SignatureMethod에로 SignatureValue를 검증한다.

4. 결론 및 향후 연구방향

본 논문에서는 B2B 문서교환을 위한 XML기반 시스템을 구현하고, XML문서 교환시의 보안상의 요구를 충족하기 위하여 XML 전자서명 표준을 지원하는 보안 시스템을 설계하였다. 향후 본 시스템과 연동하여 차세대 PKI 기술인 XKMS(Xml Key Management Specification)[4]를 도입하여 전자상거래 상에서 요구되는 보안사항을 충족하기 위한 응용 시스템에 대한 연구 및 개발을 해 나갈 예정이다.

5. 참고 문헌

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

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

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

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