2001 년 한국정보처리학회 춘계 학술발표논문집 제 8 권 제 1 호

XML/EDI 와 XML 전자서명 통합 시스템의 설계

장우영*, 유승범, 장인걸, 차석일, 신동일**, 신동규*
*세종대학교 컴퓨터공학과
e-mail : ouyoung@gce.sejong.ac.kr

Design of an Integrated System of XML Digital Signature to XML/EDI

Wooyoung Jang*, Seungbum Yoo , Ingual Jang, Sukil Cha,
Dongil Shin **, Dongkyoo Shin *
** Dept. of Computer Engineering, Sejong University

요 약

EDI 시스템은 많은 기업들에게 정보통신기술을 활용하여 업무처리시간 및 비용을 절감하고, 품질을 향상시키기 위한 대안으로 사용 되어졌다. 그리고, 인터넷으로 인해 세계 어느 곳에서나 필요한 정보를 볼 수 있게 되었으며, 그 와중에 차세대 EDI 시스템들이 출현 하였다. 그 중 다양한 문서구조 표현이 가능한 XML 을 활용한 XML/EDI 가 급속하게 확산되었다. 이러한 시스템들은 네트워크를 통해 정보가 전달 되므로 보안에 아주 예민하다. 보안 서비스에도 여러 가지가 있지만 전자서명은 큰 비중을 차지한다. 현재 공개키 암호 알고리즘을 이용한 일반적인 전자 서명을 사용하고 있으나 웹에서 표준화가 되어 가고있는 XML 을 이용한 전자서명 기법이 W3C 에서 제안되어 표준화가 진행되고 있으며 이는 EDI 시스템에서 아주 유용하게 이용 가능한 기술이다. 본 논문에서는 전자 문서 교환에 있어서 중요하다고 할 수 있는 XML 전자서명을 XML/EDI 에 적용하여 시스템을 설계하였다.

1. 서론

EDI 는 오늘날과 같은 세계화 된 시장에서 경쟁력을 강화하기 위한 필수적인 요소로써 세계 각국은 EDI 를 빠른 시간 안에 확산하는 것을 강조하여 왔으며, 시스템의 안정화 및 확산에 많은 노력을 기울이고 있다. 현재 인터넷의 이용이 확산되면서 Open-EDI, 인터넷 EDI, Interactive-EDI, 객체지향 EDI, XML/EDI 등이 출현하였다. 이러한 EDI 시스템의 적용 시에는 필연적으로 수반되는 위험성이 충분히 고려되어야 한다. 적절한 수준의 보안 및 통제 체제가 없으면 EDI 를 통한 업무처리가 신뢰성을 얻을 수 없고, 법적으로 심각한 문제가 발생할 수 있으며, 특정 분야에서는 EDI 의 적용 자체가 불가능하게 됨으로써 EDI 의 효과가 축소되는 경우가 발생할 것이다. 따라서 EDI 에는 다음과 같은 보안 서비스를 제공하여야 한다.

- 메시지 무결성 : 전송도중 불법적인 사용자에 의한 메시지의 변경을 방지하기 위한 방법
- 전자문서 순서의 무결성 : 전자문서의 불법적인 중복, 첨가, 삭제, 유실, 재전송 등을 방지하는 보안 서비스이다. 효과가 제한적이다.
- 전자문서 발신처 인증 : 수신자가 전자문서를 송신한 사람의 실체를 확인할 수 있도록 하는 서비스
- 발신부인방지 : 송신자가 전자문서의 송신사실을 부인하는 경우 수신자가 이를 제 3 자에게 증명하는 것
- 수신부인방지 : 수신자가 전자문서의 수신사실을 부인하지 못하도록 하는 보안 서비스
- 메시지 기밀성 : 불법적인 사용자에 의하여 네트워크상에서 전자문서가 도청 되어 전자문서 내용의 열람, 복사, 유출을 방지함으로써 불법적인 사용을 막는 보안 서비스

보안 서비스 중 부인방지는 중요한 보안 서비스라

할 수 있는데 현재의 EDI 시스템에서의 보안에서는 이러한 무결성과 부인방지를 막기 위해 일반적인 전자 서명 방식을 채택하고 있다. 즉, 공개키 기반 구조 알고리즘을 이용하여 구현한 문서 전체에 대한 전자서명만을 제공한다. 다양한 문서구조 표현이 가능한 XML 을 활용한 EDI 서비스 환경에서도 역시 기존의 EDI 시스템이 제공하는 보안 서비스를 제공한다. 본 논문에서는 XML/EDI 시스템 기반에 기존의 전자서명이 아닌 XML 전자 서명을 이용한 시스템을 설계한다. 이 시스템은 문서 전체가 아닌 문서의 특정 부분을 추출해서 메시지 다이제스트를 생성하기 때문에 기존의 전자서명보다 효율적이다.[1][2]

2. 관련연구

2.1 전자서명

전자서명이란 인감도장 혹은 사인과 같이 개개인의 고유성을 인정 받기 위해 전자 문서에 서명하는 방법이라 할 수 있다. 전자서명은 그 문서를 작성한 사람만이 생성할 수 있어야 하기 때문에 그 사람만이 알고 있는 비밀 정보가 적용되어야 하지만 인증 작업은 공개된 방식에 의해서 누구든지 수행할 수 있어야 한다. 그림 1 은 전자서명 시스템을 나타낸다.

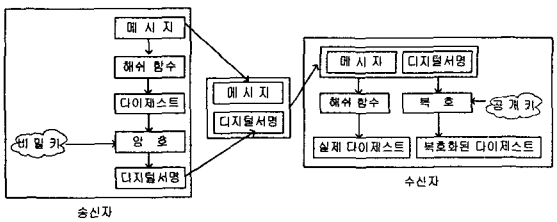

그림 1 전자 서명 수행 과정

전자 서명 과정은 메시지를 해쉬함수에 의해 다이제스트를 하고 수신자의 공개키로 암호화를 한다. 암호화된 메시지를 송신자의 개인키를 이용하여 전자서명하게 되고 원래 메시지와 함께 수신자에게 보내면, 수신자는 이를 받아 해쉬하여 실제 다이제스트한 값을 얻어낸다. 전자서명은 CA 에 인증확인요청을 하여 공개키를 이용하여 복호화한다.

2.2 XML Digital Signature Spec.

XML 을 이용한 전자서명은 기존에 존재하는 전자서명 알고리즘에 XML 을 적용한 전자서명 기법이며 W3C 에서 표준화가 진행 중 이다.

XML Digital Signature Spec.에 정의된 XML 전자서명 문서의 전체적인 구조는 그림 2 와 같다.

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

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

그림 2 XML 전자서명 문서 구조

1) Signature : XML 전자 서명 문서의 Root 엘리먼트
2) Signaturevalue : 디지털 서명의 실제적인 값을 포함하며, SignatureMethod 에 정의된 알고리즘을 선택하여 생성된 값이다.
3) SignedInfo : Canonicalization 알고리즘, Signature 알고리즘, 하나 혹은 그 이상의 References 를 포함
4) CanonicalizationMethod : XML 문서를 정규화 하기 위해 필요로 하는 알고리즘 제공
5) SignatureMethod : 실제적인 서명 값을 발생하기 위한 알고리즘 제공
6) Reference : 선택적이며 ID 를 통해서 다른 곳에서 참조할 수 있다.
7) Transforms : 서명자가 메시지 다이제스트 객체를 어떻게 얻는지를 묘사
8) DigestMethod : 다이제스트 값을 생성하기 위한 다이제스트 알고리즘 제공
9) DigestValue : DigestMethod 를 통해 생성된 다이제스트 값을 포함
10) KeyInfo : 키 발생기를 통해 생성되는 키에 대한 정보를 입력

이외에도 다량의 문서를 포함하여 문서의 서명값을 생성하기 위한 엘리먼트인 Maifest 가 있으며, 서명의 발생과 관련한 추가적인 정보를 포함하는 SignatureProperties 엘리먼트가 있다.

기존의 전자서명과 마찬가지로 XML 전자서명 역시, 수신자 측에서는 송신자가 보낸 데이터를 메시지와 서명으로 분리한 후 각각의 다이제스트 값을 생성하여 비교한다. 하지만 XML 은 그 특성상 문서의 논리적인 구조를 이용한다. 즉, Manifest 라는 것이 있어서 XML 문서의 특정한 부위를 추출해서 다이제스트 값을 생성할 수 있게 하는 기능이 있다. 이 기능을 이용하면 기존에 전자서명 시스템이 다이제스트를 생성할 때 보다 훨씬 효율적인 측면을 가지게 된다.

XML 전자서명에 사용되는 알고리즘은 RSAwithSHA1 과 DSAwithSHA1 을 지원하고 있으며, 인코딩 방식은 Base-64 코드를 사용한다. 또한 메시지 다이제스트에 사용되는 알고리즘으로는 현재 SHA-1 이 사용되고 있다. 메시지 인증을 위해서는 HMAC-SHA1 그밖에 CanonicalizationMethod 및 Transform 을 위한 알고리즘들이 존재한다. 그림 3 은 XML 전자서명에서 사용되는 알고리즘의 종류들이다.

Algorithm Type	Algorithm	Requirements	Algorithm URI
Digest			
	SHA1	REQUIRED	http://www.w3.org/2000/09/xmldsig#sha1
Encoding			
	Base64	REQUIRED	http://www.w3.org/2000/09/xmldsig#base64
MAC			
	HMAC-SHA1	REQUIRED	http://www.w3.org/2000/09/xmldsig#hmac-sha1
Signature			
	DSAwithSHA1 (DSS)	REQUIRED	http://www.w3.org/2000/09/xmldsig#dsa-sha1
	RSAwithSHA1	RECOMMENDED	http://www.w3.org/2000/09/xmldsig#rsa-sha1
Canonicalization			
	minimal	RECOMMENDED	http://www.w3.org/2000/09/xmldsig#minimal
	Canonical XML with Comments	RECOMMENDED	http://www.w3.org/TR/2000/WD-xml-c14n-20000119.html#WithComments
	Canonical XML (omits comments)	REQUIRED	http://www.w3.org/TR/2000/WD-xml-c14n-20000907
Transform			
	XSLT	OPTIONAL	http://www.w3.org/TR/1999/REC-xslt-19991116
	XPath	RECOMMENDED	http://www.w3.org/TR/1999/REC-xpath-19991116
	Enveloped Signature	REQUIRED	http://www.w3.org/2000/09/xmldsig#enveloped-signature

그림 3 XML 전자서명에서 사용되는 알고리즘

3. XML 전자서명을 적용한 XML/EDI 시스템의 설계

3.1 XML/EDI 시스템의 전체 구조

본 논문에서는 XML 전자서명을 적용하여 XML/EDI 시스템을 설계 하였다.

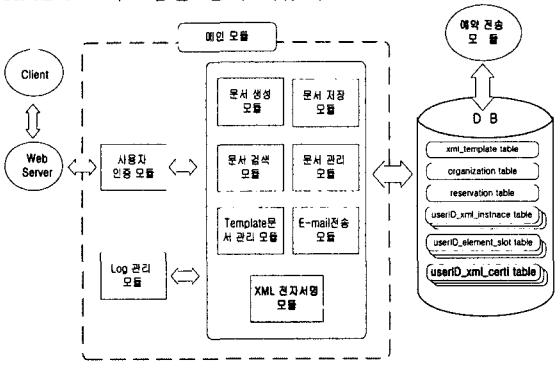

그림 4. XML/EDI 구조도

- 사용자 인증 모듈
  cookie 를 이용하여 웹 애플리케이션 개발 시 필수적인 사용자 추적을 가능하게 한다.
- 문서 생성 모듈
  클라이언트로부터 전송된 multipart form data 형식의 문자 스트림을 전송 받아 엘리먼트 컨텐트에 해당하는 값을 추출하고, 동시에 템플릿 문서를 파싱하여 같은 이름의 엘리먼트 컨텐트를 치환함으로써 XML 인스턴스 문서를 생성한다.
- 문서 저장 모듈
  생성된 XML 인스턴스 문서를 파싱하여 DOM tree 를 구성하고 엘리먼트와 그 경로에 대한 정보를 DB 에 저장한다.
- 문서 검색 모듈
  각 사용자들이 가지고 있는 문서 인스턴스 테이블, 엘리먼트 슬롯 테이블 그리고 템플릿 문서 테이블로부터 SQL 의 JOIN 연산으로서 검색을 수행한다.
- 문서 관리 모듈
  문서 관리 모듈은 보낸 문서, 받은 문서, 전송예약 문서, 휴지통의 보기 기능을 이용하여 문서 송수신에 대한 확인과 문서의 일시삭제, 완전삭제의 기능을 웹에서 수행하게 한다.
- Template 문서 관리 모듈
  관리자가 XML, DTD, XSL 템플릿을 추가, 수정, 삭제 할 수 있다.
- E-mail 전송 모듈
  문서 생성시 사용자가 E-mail 전송 기능을 선택할 경우 문서 전송에 대한 간단한 정보를 포함한 E-mail 을 전송한다.
- Log 관리 모듈
  사용자의 시스템 접근에 대한 User log, 사용자의 문서 접근에 대한 Access log, 시스템에서 발생하는 예외상황에 Error log 파일에 대한 기록,유지,삭제를 관리.
- 예약 전송 모듈
  메인 모듈 서블릿이 초기화될 때 예약전송 모듈이 데몬으로 수행된다. 예약 전송 모듈은 DB 의 reservation 테이블을 참조하여 주기적으로 체크하여 전송이 해당되는 레코드들에 대한 스케쥴링을 통해 전송을 수행한다.
- XML 전자서명 모듈
  생성된 XML 문서를 다이제스트하고 암호화하여 서명을 수행한다. 키 쌍과 인증서를 생성하여 서명과 검증을 수행한다.

3.2 XML 전자서명 모듈의 상세 구조

XML 전자서명 모듈의 구조는 그림 5 와 같다. 문서 생성모듈에 의해 생성된 XML 문서를 XML 전자 서명 명세에 정의되어진 SHA-1 알고리즘을 사용하여 다이제스트를 생성한다. 이 다이제스트한 문서를 수신자의 공개키를 이용하여 암호화를 한다. 그리고, CA 에 의해 XML 전자서명 명세에 맞도록 RSA, DSA 알고리즘에 맞는 키 쌍을 생성하고, 생성된 자신의 개인키와 다이제스트한 값에 의해 서명 값이 생성되고, 이 서명 값을 바탕으로 유효한 XML 문서를 생성한다. 사용자 정보와 키에 대한 정보를 담고 있는 인증서를 생성하고 인증서 확인 요청시 이용하기 위해 데이터베이스에 저장한다. 이렇게 생성된 문서와 인증서를 함께 예약 전송 모듈에 의해 수신자에게 전송한다.

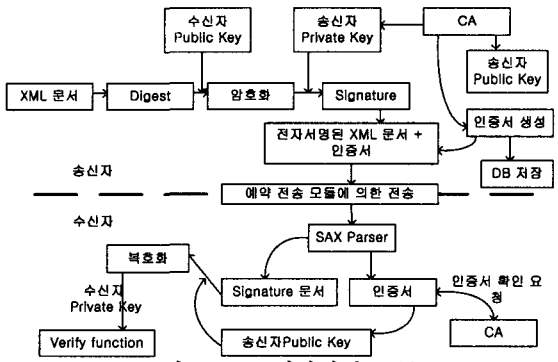

그림 5 XML 전자서명 모듈

여기까지가 송신측에서 XML 전자서명을 하는 설계부분이며, 예약 전송에 의해 보내어진 문서는 수신자측

에서 SAX 파서로 파싱하고 인증서에 따라 CA 에 인증 확인 요청을 하여 얻어낸 공개키로 전자서명된 XML 문서를 검증하는 단계를 갖는다.[3][4]

여기서 인증서는 CA(공인인증기관)에서 생성, 관리, 확인하게 된다. 이 인증서는 X.509 v3 인증서를 따르고 있으며, 이 구조에는 인증서의 데이터 형식들과 인증기관에 의해 발행된 인증서를 이용한 공개키의 효율적인 분배 방법을 정의하고 있다. 초기 버전은 X.509 v1 이었으며 현재는 X.509 v3 에서 서명 알고리즘을 선택 가능하도록 확장 영역을 추가 하였다. 그림 6 은 인증서의 일반적인 구조이다.

version
serial number
CA signature algorithm
issuer name
validity period
subject name
subject public key information
issuer unique identifier
subject unique identifier
extension field
issuer's signature

그림 6 X.509 v3 인증서 형식

4. 결론

본 논문에서는 XML 이 가지고 있는 특징을 이용하여 전자서명을 적용한 XML/EDI 시스템을 설계하였다. 기존의 전자서명은 문서의 논리적인 구조를 이용할 수가 없었다. 따라서 메시지 다이제스트는 문서 전체에 대해서 수행되었다. 하지만 XML 전자서명은 XML 문서 자체에 대한 Manifest 기능을 통해서, 문서의 특정 부위를 추출할 수 있다. 그러므로, 전자보다 훨씬 효율적이다.

본 논문에서 설계된 XML/EDI 시스템은 일부기능을 제외하고 구현된 상태이다. XML 전자서명 명세가 아직까지 표준안이 나오지 않았으며, 명세에서 사용되는 알고리즘이 한정되어 있다. XML 전자서명 모듈의 구조에서 CA(인증기관)의 관계부분이 앞으로의 과제로 남아있으며 생성한 키 쌍에 대한 정보를 데이터베이스에 입력해야 할 것이다. 그리고, 수신자측에서 문서를 받아 파싱하는 부분과 인증서 확인 요청하는 부분 또한 구현되어야 할 부분이며, 공개키를 사용하여 검증하는 단계가 구현되어야 한다.

참고문헌

[1] W3C, "Extensible Markup Language", http://www.w3.org/XML/
[2] XML/EDIGroup, "XML/EDI Transaction Models", http://www.geocities.com/WallStreet/Floor/5815/
[3] W3C, "W3C-Signature Core Syntax and Procession", http://www.w3.org/TR/2000/CR-xmldsig-core-20001031/
[4] W3C, "W3C-Signature Requirements", http://www.w3.org/TR/xmldsig-requirements/
[5] *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,