제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

XSS 참조구현을 통한 XML 전자서명 관리 시스템에 관한연구

구자룡*, 송윤강**
* 동국대학교 컴퓨터공학과
**중부대학교 컴퓨터공학부
e-mail : jekal@dgu.ac.kr, reonar@joongbu.ac.kr

A Study on XML-DSignature Management System with the XSS reference implementation.

Ja-Ryong Koo*, Yun-Kang Song**
*Dept. of Computer Engineering, Dong-Guk University
**Dept. of Computer Science, Joong-Bu University

요 약

최근 차세대 인터넷 환경의 표준 데이터 포맷으로 각광받고 있는 XML(eXtensible Markup Language)을 사용한 전자상거래 규격에 대한 국 내외적 표준화 작업이 가속화 되고있으며, 아울러 기업간 전자문서 교환시의 인증및 보안문제 또한 필수적인 사항이 되어가고있다. 본 논문에서는 XML 표준화 기구에서 정의한 명세서 기반의 XSS(XML Security Suite) 라이브러리를 이용하여 기업간 전자문서 교환시 발생하는 보안문제를 해결하기 위한 전자서명 관리 시스템을 연구하였다.

1. 서론

정보 시스템의 발전과 증가는 비례적으로 보안의 필요성을 가져오게 되었다. 우리가 사는 정보사회는 하루가 다르게 변화하는 정보기술 분야의 발전과 함께 정보사회를 구성하는 개발요소들을 필요로한다. 정보의 무한한 보고로 일컫는 인터넷 시스템에 있어서 사용자의 요구가 다향해짐에 따라 이러한 요구를 충족시킬 수 있는 대안이 필요하게 되었으며, XML (eXtensible Markup Language) 이라는 새로운 문서표준이 나오게 되었다. 그러나 XML 을 이용한 각종 데이터 및 문서는 인터넷상에 존재하게 되므로 제 3 자에 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.

XML 의 초창기에는 보안관련 요소를 자체적으로 정의하지 않았다. 하지만 확장가능한 마크업 언어인 XML 의 이용범위가 확대됨에 따라 암호화(XML-Encryption)와 전자서명(XML-Signature), 키관리(XKMS-XML Key Management System)등을 위한 XML 표준이 제정되고 있으며, 현재 몇몇의 참조구현과 상용 라이브러리가 출시된 상태이다. 본 논문의 제 2 절에서는 XML 전자서명 명세와 그에 준하는 보안 라이브러리인 XSS(XML Security Suite)과 Java 언어 보안 라이브러리인 JCE(Java Cryptography Extension)에 대하여 알아보고, 제 3 절에서는 자바(JDK)와 XSS 그리고 XML 파서를 이용해 XML 전자서명 관리 시스템의 구성을 보도록 한다. 마지막으로 결론및 향후 연구 방향을 기술한다.

2. 관련연구

2.1 XML 전자서명(XML Digital Signature) 명세

XML 전자서명 명세는 W3C 와 IETF 가 공동으로 표준화를 추진한다. XML 전자서명은 W3C 에서

Recommendation 상태로 승격시킴으로써 표준화가 완료된 상태이다. [표 1]은 XML 전자서명을 통해 전자서명을 생성하고 표현하는데 대한 XML 구문과 문서구조를 나타낸다.

<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 기본구조

명세서에서 정의한 XML 전자서명 문서의 구조는 세가지 표준 출력 유형을 가지고 있는데, <Signature> 요소가 전송 문서의 최상위 요소로 되는 Enveloping 서명과 <Signature>요소가 문서내에 포함되어 하위 요소로 구성되는 Enveloped 서명 및 서명될 객체의 URI 만을 포함한 별도의 서명이 생성되는 Detached 서명으로 나뉜다.

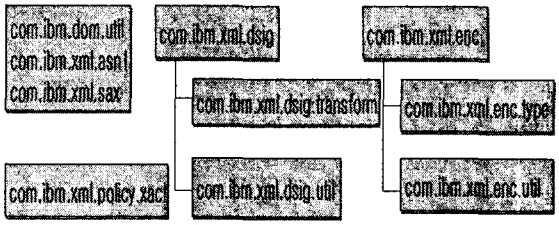
[표 1]의 주요 요소의 역할을 설명하면 다음과 같다. <SignatureValue>은 실제 전자서명 값을 포함하는 요소이다. <SignedInfo>은 실제 서명할 자료에 대한 정보를 포함 하는 요소이며, <KeyInfo> 요소는 서명을 검증할 키에 대한 정보를 포함하는 요소로 인증서 정보를 포함할 수 있다. 또한, <Object>요소는 어플리케이션에 종속적인 정보를 포함하고있는 선택적 요소이다.

기존의 전자서명의 경우, 수신자 측에서는 송신자가 보낸 데이터를 메시지와 서명으로 분리한 후 각각의 다이제스트 값을 생성하여 비교하였다. 따라서 수신자 측에서 다이제스트를 계산해야 하는 단점이 있지만, XML 의 경우 문서에 수신자가 생성한 다이제스트와 서명 값이 포함되어 있기 때문에, 수신자 측에서 송신자가 보낸 데이터를 메시지와 서명으로 분리하여 다이제스트 값을 계산할 필요가 없다는 장점을 가지고 있다.

2.2 XSS(XML Security Suite)

XSS(XML Security Suite)는 W3C 의 표준화 그룹에서 제공한 XML 보안 표준을 IBM 에서 참조구현 하여 배포중이다.

XSS 라이브러리는 [그림 1]과 같이 여러 패키지로 구성되는데 XML 문서의 전자서명을 위한 패키지와 암호화에 사용되어지는 패키지, 접근 권한 관리를 위한 패키지를 포함하고있다, 해당 패키지 경로를 살펴보면 다음과 같이 com.ibm.xml.dsig, com.ibm.xml.enc, com.ibm.xml.policy.xacl 등의 위치에 참조구현된 패키지들을 확인할 수 있다. 또한 XML 문서의 파싱과 처리를 위한 DOM, SAX, XPATH 등의 클래스와 ASN.1 구문을 처리하기위한 클래스를 포함하는 몇 개의 유틸리티 패키지로 구성되어있다.



[그림 1]XSS 패키지의 구성

실제로 XSS 는 DOM 이나 SAX 등의 파싱에는 Xerces 라이브러리를, 암호화 관련은 JCE 라이브러리를 이용하고 있으며, 자체적으로는 W3C 의 XML 암호화/서명 표준과 관계된 엘리먼트를 구성하는데 기능을 구현하고 있다.

XML 전자서명을 위한 dsig 패키지는 [표 2]와 같이 전자서명의 형식(Signature 엘리먼트)을 구성하거나, 전자서명 연산을 수행하는 것외에 다수의 클래스를 포함한다. transform 패키지와 util 패키지는 주로 dsig 패키지 내부에서 사용되는 클래스를 구현하고 있는데, 정규화(Canonicalization)나 Transform 과 관련된 처리를 담당하고 있다.

종 류	설 명
KeyResolver	KeyInfo 엘리먼트에서 java.security.Key 타입의 키를 얻어서 리턴해주는 클래스
TemplateGenerator	실제 서명을 위한 엘리먼트 (signature 엘리먼트) 의 템플릿을 생성하기 위한 유틸리티 클래스
SignatureContext	서명 연산을 실제 진행하는 클래스
KeyInfo	XML 서명 표준안의 KeyInfo 엘리먼트를 구현한 클래스
CertUtil	인증서 체인을 처리하기 위한 클래스
KeyInfo.X509Data	인증서 정보와 인증기관 인증서를 포함하는 X509Data 엘리먼트를 구현한 클래스
Reference	템플릿을 만드는데 사용되는 Reference 엘리먼트를 구현한 클래스
Transform	Transform 을 진행하기 위한 클래스

[표 2] XSS 의 전자서명관련 주요클래스

2.3 JCE(Java Cryptography Extension)

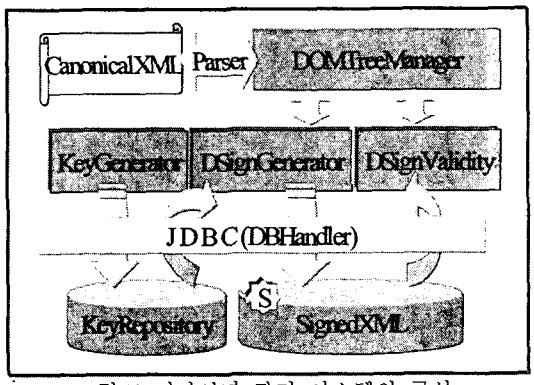
JDK 는 기본적으로 전자서명과 메시지 다이제스트를 위한 라이브러리만 포함하고 있으며, 다양한 암호 알고리즘과 관련된 기능을 포함하는 JCE 는 JDK1.2 버전부터 지원되기 시작했다.

또한 JCE 1.2 버전은 강한비도(Security Strength)를 가진 암호를 일종의 무기로 취급하는 미국의 수출제한법 때문에 미국과 캐나다를 제외한 다른나라에서는 사용할 수 없도록 되어 있다.

그러나 JCE1.21 버전이 발표되면서 JCE 프로바이더에 전자서명을 적용함으로써 지역에 따라 암호의 강도를 제한할 수 있도록 하는 제한 정책이 포함되었고, 이로인해 미국 이외의 나라에서도 JCE 를 사용할 수 있게 되었으며, J2SE 1.4 버전에서는 JCE 가 기본 JDK 와 통합되어 배포된다.

3. 시스템 구성

시스템은 크게 키생성기(Key Generator), 서명생성기(DSignGenerator), 서명검증기(DSignValidity)와 같은 세 개의 모듈로 구성된다. 그 외에도 JCE 프로바이더를 설정할 수 있는 기능이나 서명에 사용될 암호 알고리즘등을 선택할 수 있는 기능등을 담당하는 클래스들과 전자서명 표준 명세에 대한 처리규정에 준하는 인증, 무결성, 승인, 부인방지 서비스를 위한 서브 클래스 들이 존재한다. [그림 2]는 설계된 전자서명 관리 시스템의 구성을 나타내며 각각의 특징은 다음과 같다.



[그림 2] 전자서명 관리 시스템의 구성

3.1 키생성기(KeyGenerator)

일반적인 전자서명이 그러하듯이 XML 데이터의 전자서명을 위해서는 자신의 개인키와 공개키 쌍이 필요하다. 또한 서명시에 서명자의 신원보증을 위한 인증서 형태의 공개키를 사용한다. 키생성기는 전자서명에 사용될 키를 생성한후에 키저장소에 저장하는 기능을 담당하며, 키는 여러가지 형태로 저장될 수 있지만 본 논문에서는 JCE 에서 지원하는 jceks 키저장소 형식을 사용한다.

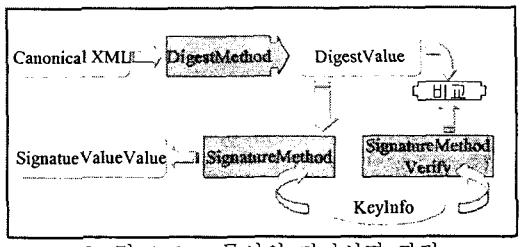
종 류	설 명
alias	키 저장소의 다른이름
keyalg	키생성 알고리즘
keypass	키자체보호를 위한 키암호화 패스워드
keystore	키저장소의 이름
storetype	저장소 형태
storepass	저장소 보호를 위한 패스워드

[표 3] 키생성을 위한 입력 데이터

키생성시 입력되어지는 정보리스트는 [표 3]과 같으며, 키생성 알고리즘은 기본적으로 전자서명을 위한 공개키 알고리즘을 이용한다.

3.2 서명생성기(DSignGenerator)

서명생성기는 키저장소에 저장된 인증서 형식의 전자서명키를 읽어들여 정규화된(Canonical) XML 문서를 전자서명 결과가 적용된 새로운 XML 문서로 만들어내는 기능을 담당한다. 정규화된 XML 문서는 정규표현은 형식상 다르지만 의미상 같은 문서를 동일하게 취급할 수 있도록 같은 형식으로 만들어주는 방법이다.



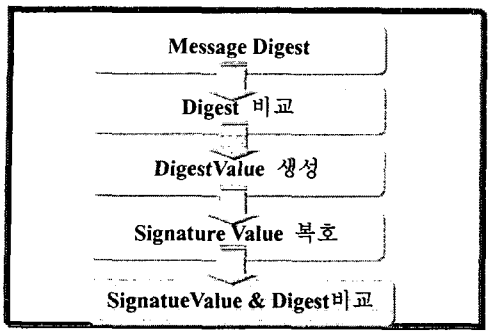
[그림 3] XML 문서의 전자서명 과정

그림[3]은 XML 문서의 전자서명 과정을 나타내고 있다. 정규화된 XML 문서를 축약메소드를 이용하여 축약한후 그결과 값에 서명 메소드를 이용하여 서명된 XML 문서를 생성하며, 키정보와 축약값을 이용하여 서명에 대한 검증을한다.

3.3 서명검증기(DSignValidity)

서명검증기는 두가지 검증유형으로 나뉘는데 한가지는 전자 서명된 XML 문서를 읽어들여 서명의 유효성이나 타당성을 검증하고, 다른 한가지는 서명에 사용된 인증서의 검증을 수행한다.

XML 의 전자서명의 검증은 [그림 4] 와 같은 순서로 진행된다.



[그림 4] 전자서명 XML 문서 검증순서

4. 결론 및 향후연구

기업간 문서 혹은 데이터 교환에 있어 XML/EDI 시스템은 이미 대세로 자리잡아 가고 있으며 그에 따른 보안문제는 반드시 해결해야 할 문제가 되고 있다. 따라서 본 논문에서는 XML 에서의 XML-DSig 표준을 따르는 XML 전자서명 생성 및 검증에 대한 전자서명 관리 시스템에 대해 고찰해보았다. 향후에는 XSS 뿐만 아니라 기타 벤더에서 제공하는 툴킷이나 라이브러리를 선택적으로 활용하여 전자서명뿐만 아니라 XML 암호화(XML-Encryption)와 키관리(XKMS) 기법에 대한 연구가 요구된다.

참고문헌

[1] " XML-Signature Syntax and Processing", W3C Candidate Recommendation, April 2001
[2] " XML-Encryption Syntax and Processing", W3C Working Draft, October 2001
[3] " Java Security" : 스콧오스크, O'Reilly.
[4] " 자바보안과 암호화" : Jonathan Knudsen(이재광 외 2 인 역),O'Reilly.
[5] " XML 보안을 위한 암호 API 설계" : 반용호외 2, 2002 년 정보과학회 춘계발표논문집.
[6] " ebXML 보안 요구사항 분석 및 XML 기반 보안 기술 적용 연구" : 송준홍 외 4, 2002 년 한국정보처리학회 춘계발표논문집 제 9 권 1 호.
[7] " XML Digital Signature 에 기반한 XML/EDI 시스템의 설계 및 구현" : 원덕재 외 3, 2002 년 한국정보처리학회 춘계발표논문집 제 9 권 1 호.
[8] " XML 보안참조구현을 통한 XML 보안" : 마이크로 소프트웨어, 소프트뱅크미디어.
[9] XML Security Page : http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/xml_security.html
[10] W3C Website : http://www.w3.org
[11] XML Security Suite Discussion Forum : http://alphaworks.ibm.com/tech/xmlsecuritysuite