한국경영과학회/대한산업공학회 2003 춘계공동학술대회
2003 년 5 월 16 일-17 일 한동대학교(포항)

전자상거래 정보교환을 위한 XML 보안

XML Security for E-Business Information Exchange

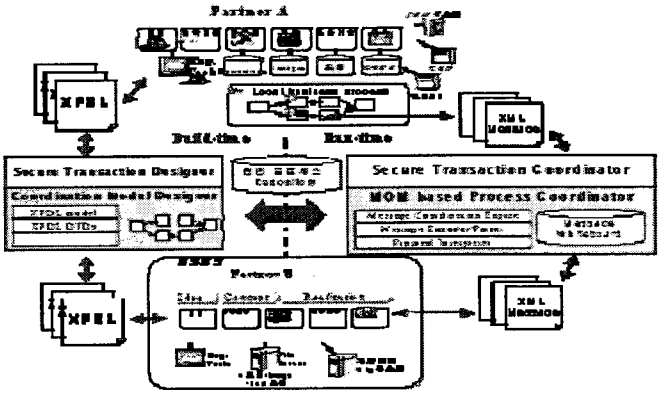
배준수*
*성결대학교 전자상거래학부
(우) 430-742 경기도 안양시 만안구 안양8동 산 147-2
Tel: 031-467-8102 E-Mail: jsbae@sungkyul.edu

초 록

본 논문은 웹서비스 기반의 전자상거래 시스템의 안전한 정보 교환을 위해 XML 보안 구조를 제안하고 구현한다. 전자상거래에서 무엇보다도 중요한 기술 요소가 안전성을 보장하는 보안이므로 다양한 기술들이 표준으로 제시되고 있다. 그 중에서 XML이 전자상거래 시스템의 문서 표준으로 다양한 분야에서 사용되면서 XML 보안이 새로운 분야로 등장하기 시작했다. XML 문서에 대한 보안을 이루기 위해서 XML 서명, XML 암호화와 XML 키 관리 체계가 기존의 보안과 다른 차이점을 제시하고 고유 특성에 바탕을 둔 새로운 구조를 제시한다. 이것을 XML 기반 프로그램의 보안을 지킬 수 있는 RSA의 BSAFE Cert-J SDK를 이용하여 프로토타입을 개발한다. 특히 전자상거래에 필요한 프로세스 관리 시스템과의 통합을 이룰 수 있는 방안을 제시한다.

1. 서론

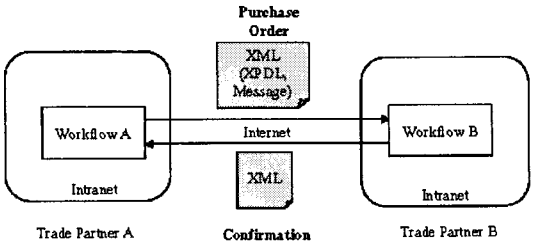
기업은 경쟁력 확보를 위하여 기업 내부의 조직 활동들뿐만 아니라, 다른 기업과의 상호 협력적인 업무를 수행하고 있다. 특히 기업간 업무 거래는 계약된 문서 양식을 주고받으며 협의된 업무 프로세스에 따라서 정형적으로 실행되는 것이 일반적이다. 기존의 기업 내부의 프로세스를 관리하는 워크플로우 관리 시스템(WFMS)을 바탕으로, 기업간 전자상거래에서 요구되는 여러 가지 핵심 요소들을 분석하여 B2B 환경에 적합한 협업 프로세스 관리 시스템인 x-ebFMS(XML-based eBusiness Flow Management Systems)를 구현하는 것이 본 연구의 목적이다. 특히, 기업간 정보 교환에 실질적인 표준 도구로 인정받고 있는 XML 메시지를 사용하여 기업들이 교환하는 문서나 데이터들을 정형화하고, 이들을 처리하는 비즈니스 프로세스들을 XML 메시지 교환을 통하여 진행함으로써 모든 과정에서 메시지를 통한 효율적인 업무 통합을 지원하게 된다. 아래의 [그림 1]은 두 기업이 x-ebFMS를 통하여 협업 프로세스를 설계하고 진행하는 과정을 나타내고 있다.



[그림 1] x-ebFMS 의 구조

하지만 인터넷상에서 실행되는 전자상거래의 성공을 위협하는 가장 큰 걸림돌은 보안에

관한 것일 것이다. [그림 2]와 같이 인터넷을 통한 교환 정보를 단순히 XML로 변경하는 경우는 두 거래 당사자의 사용자 인증이 보장되지 않으므로 안전하지 않은 메시지 교환이라고 할 수 있다. 특히 비대면 거래를 수행하는 전자상거래에서 정당한 사용자 임을 보장하기 위한 사용자 인증을 위해서는 공개키 암호 시스템에 바탕을 두고 실현되어야 한다. 따라서 사용자 공캐키의 신뢰성과 안전성을 보장 받을 수 있는 방안이 강구되어야 한다.



[그림 2] 안전하지 않은 메시지 교환

공개키 기반 구조(PKI: Public Key Infrastructure)[1]는 공개키 암호 방식을 사용하는 암호 시스템에서 사용자의 공개키를 안전하고 신뢰성 있게 공표하는 수단을 제공한다. 따라서 안전하고 신뢰성 있게 사용자의 공개키를 공표하기 위한 공개키 기반 구조는 인터넷 전자상거래 시스템에서 매우 중요한 역할을 수행할 것이다.

이와 더불어 XML 기술이 인터넷 e-비즈니스 시스템 등에서 메시지 교환 형식으로 이용되면서 이들 XML 문서의 보안 역시 필수적 요구 조건이 되고 있고, 안전한 전자상거래를 수행하기 위해서 XML 전자서명(Digital Signature)은 반드시 지원 되어야 한다 [2][3][4][5][6].

따라서 본 논문에서는 전자상거래에서 표준으로 자리 잡고 있는 PKI 기반의 X.509 인증서를 이용한 안전하고 신뢰할 수 있는 전자상거래 보안 애플리케이션을 설계하는데, 상호 인증을 위해 PKI 기반 보안 애플리케이션을 구현하기 위해 웹서비스를 설계하고, 또 B2B간의 메시지 교환 정보의 보안과 부인 방지 문제를 해결하기 위해 PKI와 XML기반 전자서명 프로토콜을 설계한다.

본 논문에서 설계한 전자상거래 애플리케이션은 Java와 XML기반으로 설계되고 인증서의 검증 및 기밀 정보의 암,복호화가 클라이언트 측 보안 모듈에서 처리되므로 현재 웹 보안의 문제점을 플랫폼 독립적으로 해결할 수 있다.

논문의 구성은 1절 서론에 이어서 2절 관련 연구, 3절 XML Security, 4절 결론과 향후 연구에 대해서 논한다.

2. 관련 연구

2.1 공개키 기반 구조(PKI: Public Key Infrastructure)

공개키 암호 시스템은 비대칭 키 암호 시스템이라고도 불리며, 수학적 함수를 기반으로 하여 비밀키 암호 시스템과 달리 키 쌍이 존재하여 하나의 키는 누구든지 사용할 수 있도록 공개하며 다른 하나는 자신만이 비밀스럽게 보관하는 방식을 말한다. 이때 공개하는 키를 공개키(public key)라고 하며 비밀스럽게 보관하는 키를 개인키(private key)라고 한다. 키 관리와 분배에 어려움이 많고, 익명성과 사용자 인증을 이루기 위해서 전자상거래를 위한 대부분의 보안 응용은 공개키 알고리즘에 바탕을 두고 있다.

공개키 기반 구조는 공개키 인증서에 바탕을 두고 구축되어야 한다. 인증서는 인증기관(CA: certification authority)이 최종객체(EE: end entity)를 인증하는 전자 증명서 역할을 수행하며, 주체(subject) 사용자가 합법적인 사용자임을 입증하기 위해 CA는 자신의 개인키로 디지

털 서명문을 생성하여 인증서에 첨부한다. 인증서에는 인증서 사용자에 대한 공개키와 주체 사용자의 신분에 대한 정보들을 포함하고 있다.

2.2 XML(Extensible Markup Language)

XML 표준은 XML 도큐먼트라고 불리는 데이터 객체들의 클래스를 기술하고, 일부 이 XML 도큐먼트들을 처리하는 컴퓨터 프로그램들의 행동을 기술한다. XML은 일종의 SGML 애플리케이션 또는 SGML(Standard Generalized Markup Language [ISO 8879])의 축약된 형태이다. 그 구성을 보면 XML 도큐먼트는 SGML 도큐먼트와 동일하게 하고 있다.

XML 도큐먼트들은 엔터티(entity)라고 불리는 저장 단위들로 구성된다. 엔터티는 파싱되는 데이터 또는 파싱되지 않는 데이터 중의 하나를 포함한다. 파싱되는 데이터는 문자들(character)로 구성된다. 이 문자들의 일부는 문자 데이터(character data)가 되고, 또 일부는 마크업(markup)이 된다. 마크업은 XML 도큐먼트의 물리적 저장소의 배치도 및 논리적 구조에 대한 설명을 부호화하게 된다. XML은 저장소의 배치도 및 논리적 구조를 강제하는 매커니즘을 제공한다.

XML 프로세서(XML processor)라고 불리는 소프트웨어 모듈은 XML 도큐먼트를 읽어 들여서 그 컨텐츠와 구조에 접근할 수 있도록 하는데 사용된다. XML 프로세서는 응용프로그램(application)이라고 불리는 또 다른 소프트웨어 모듈의 일부로서 작동하는 것으로 가정된다. 이 스펙은 XML 프로세서가 "XML 데이터와 응용프로그램에 제공되어야 하는 정보를 어떻게 읽어야만 하는지"와 관련되어 XML 프로세서에 필수적으로 요구되는 행동에 대해서 기술한다.

XML은 어떻게 자료를 구분할 수 있는가에 대한 표준이라면, XSL(XML Stylesheet Language)은 구분된 자료를 어떻게 출력할 것인가에 대한 표준이라고 할 수 있다. XSL은 일종의 변환 기술로 XML의 각 필드를 HTML의 어떤 태그로 변환하여 웹 브라우저에 출력할 것인가에 대한 규칙을 정할 수 있는 언어이다.

XML Schema는 XML 문서의 구조와 컨텐츠를 정의하는 파일을 일컫는 일반적인 용어이다. DTD(Document Type Definition)도 이러한 스키마의 일종이지만 많은 문제점을 가지고 있었다. DTD와의 가장 큰 차이점은 DTD는 EBNF라는 복잡하고 낯설은 언어로 기술해야 하지만 XML Schema는 XML을 사용하여 기술한다는 것이다. 또한, DTD에서 표현할 수 없었던 각종 데이터 타입과 엘리먼트 재사용 등을 XML Schema에서는 기본적으로 가능하게 할 수 있다. 즉 XML Schema는 DTD를 대폭 확장한 모델로 XML 문서가 가질 수 있는 엘리먼트 타입, 엘리먼트간의 관계, 각 엘리먼트가 가질 수 있는 타입에 대해 상세히 정의할 수 있다. Working Draft로 표준화가 진행 중이다.

- 한번 정의한 엘리먼트의 계승을 통한 재활용
- XML로 정의하여 하나의 파서로 엘리먼트/XML 문서를 모두 분석
- 데이터 타입을 사용
- 컨텐츠 자체는 스트링 데이터를 사용하므로 플랫폼간의 통신 가능

XML 문서는 일반적으로 각 엘리먼트를 트리 구조로 분리하는 파싱과정을 거쳐야 한다. 파싱한 자료를 트리구조로 분석, 저장하여 특정 엘리먼트에 대한 접근을 허용하는 모델을 DOM(Document Object Model)이라 한다. DOM에 따르면 XML문서는 최상위 엘리먼트가 루트 노드가 되어 계층적인 트리 구조로 문서를 분석하게 된다. 트리 구조로 표현되기 때문에 특

정 노드에 대한 접근이 자유로워 Random Access Protocol이라고도 불린다. DOM은 W3C의 Recommendation으로 표준으로 확정되어 있다.

- 객체 지향 프로그램(OOP)에서 HTML과 XML문서를 다루기 위한 API
- 플랫폼, 프로그래밍 언어에 독립적인 인터페이스
- 문서의 논리적 구조, 동적 접근, 동적 제어 방법을 정의
- 엘리먼트, 컨텐츠의 조회, 추가, 수정, 삭제

2.3 XML 전자서명(XML Digital Signature)

최근 XML[2]은 B2B와 B2C 등과 같은 기본적인 응용과 더불어 여러 분야에 적용할 수 있는 기술로 각광 받고 있다. 한편 전자상거래상에서의 대부분의 서비스가 전자적으로 처리됨에 따라 그에 따른 보안의 중요성이 대두되고 있다. 특히, XML을 활용한 전자상거래상의 문서 교환 과정의 보안에 대한 표준화 작업이 활발히 진행되고 있는데, XML 전자서명은 IETF와 W3C의 XML-Signature Working Group에서 제정된 "XML-Signature Syntax and Processing" 명세서[4]에서 XML 디지털 서명의 구문과 처리 과정을 기술하고 있다.

XML 전자서명을 사용하기 위한 보안 관련 고려 사항은 다음과 같다.

- 기밀성(Confidentiality): 전송되는 자료의 일부 또는 전부를 제 3자가 볼 수 없도록 하는 기능.
- 인증(Authentication): 사용자 인증은 사용자가 정당한 사용자임을 증명하는 기능.
- 무결성(Integrity): 원격지에서 전송된 문서가 위, 변조되지 않았음을 증명하는 기능.
- 승인(Authorization): 거래 요청에 대하여 상대방의 거래를 인증하고 이에 대한 처리 결과를 거래 요청자에게 통보하는 기능.
- 부인방지(Non-Repudiation): 문서를 송, 수신하는 경우 해당자가 송, 수신에 대한 행위를 부인할 수 없도록 하는 기능

2.4 웹 서비스(WS: Web Service)

웹서비스란 인터넷상에서 단일한 비즈니스 또는 다수의 비즈니스 업체간의 기존 컴퓨터 시스템 프로그램을 결합시키는 표준화된 소프트웨어 기술로서 이러한 표준 기술을 이용해 모든 비즈니스 기능 또는 서비스를 가능케 하는 활동을 일컫는다. 인터넷을 통한 웹서비스는 거래업체간의 이질적인 운영시스템, 이질적인 프로그램언어간의 커뮤니케이션 차이를 극복해주는 연결고리 역할을 해준다. 다시 말하면 웹서비스는 e-Business 표준을 따르며 인터넷을 통해 제공되는 비즈니스 로직을 갖는 소프트웨어 컴포넌트이다. 웹서비스는 단순히 웹을 통해 제공되는 서비스만을 의미하지 않는다. 웹서비스라는 용어에서 연상되는 서비스는 ASP 나 웹호스팅 등이나 최근 Microsoft, IBM, HP 등의 대형 IT 벤더사 들이 차세대 제품 전략의 핵심이 되고 있는 웹서비스는 순수 서비스라기보다는 어플리케이션에 가깝다. 웹서비스는 벤더나 SI 업체에게는 애플리케이션이나 소프트웨어 컴포넌트로 인식되지만, 사용자에게는 관련 정보가 모두 캡슐화(encapsulation)되어 있어서 기술이나 컴퓨팅이 아닌 서비스로 인식되기 때문에 서비스라는 용어를 강조한 것으로 생각된다.

3. XML Security

3.1 XML Signature

XML 서명 문법은 매우 다양한 기능을 제공하는 복잡한 표준으로서 고수준의 확장성과

유연성을 갖도록 설계되어 있으므로 어느 서명에나 적용할 수 있다. "XML-서명 문법과 처리에 대한 W3C 권고안(XML-Signature Syntax and Processing W3C Recommendation)"은 XML 서명 문법과 그에 관련된 처리 규칙을 정의하고 있다. 이 권고안은 Joint Working Group of the Internet Engineering Task Force(IETF) and World Wide Web Consortium(W3C)에 의해서 수립되고 있다.

XML 서명은 <Signature> 엘리먼트로부터 시작되며, 이 엘리먼트는 서명을 구성하고 식별하게 해 주는 중요한 엘리먼트가 된다. 다음으로 <SignedInfo> 엘리먼트에 대해서 알아봤는데, 이것은 우리가 서명할 대상 즉 "서명된 정보"를 나열하고 있다. 다이제스트를 위한 특정한 데이터 스트림은 <References> 엘리먼트로 표현되며, URI 문법이 이 스트림을 규정하는데 사용된다. 더욱이 <KeyInfo> 엘리먼트가 검증키에 대한 식별 매커니즘을 제공함으로써 XML 서명의 처리 자동화에 유용하게 쓰인다. 마지막으로 <Object> 엘리먼트가 있는데, 이것은 어떤 타입의 데이터 객체도 담을 수 있는 컨테이너이다. <Object> 엘리먼트 내부에 포함되는 두 가지 특별한 종류의 엘리먼트가 XML 서명 권고안에 의해서 정의되는데, <SignatureProperties>와 <Manifest> 이다. <SignatureProperties> 엘리먼트는 편리함을 제공해 주는 서명 확인을 위해 미리 정의된 컨테이너이다. 이 엘리먼트는 서명에 관한 확인(assertion)들을 담고 있다. 이러한 확인들은 단순히 서명 유효성과 데이터 무결성 검증에 의해 제공되는 것 이상의 추가적인 신뢰성을 판단하는데 유용하게 쓰인다. <Manifest> 엘리먼트는 애플리케이션 도메인을 위한 참조 검증에 사용되며, 다중 도큐먼트에 서명하는 다중 서명자를 위한 편리한 방법을 제공한다. <Manifest> 엘리먼트를 사용하지 않는다면, 서명 결과물은 중복되는 데이터의 존재로 부피가 상당히 커질 것이며 생성과 검증시에 성능이 저하된다.

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

[그림 3] 전자서명의 XML 문법

인증서 생성 정보와 발급된 인증서는 XML 문서로 교환되며, 중요 정보는 XML 엘리먼트(Element) 단위로 암호화를 한다. 인증서 생성 정보에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT validity_period (notbefore, notafter)>
<!ELEMENT DAICertificateCreateInfo (X500Name, validity)>
<!ELEMENT X500Name (c_name, o_unit, organization, local, county)>
<!ELEMENT validity (validity_period)>
<!ELEMENT DAICertificate (version?, issuer, subject, delegation?, tag,
    validity, comment?), cert>
<!ELEMENT issuer (X500Name)>
<!ELEMENT subject (X500Name)>
<!ELEMENT cert (#PCDATA)>
```

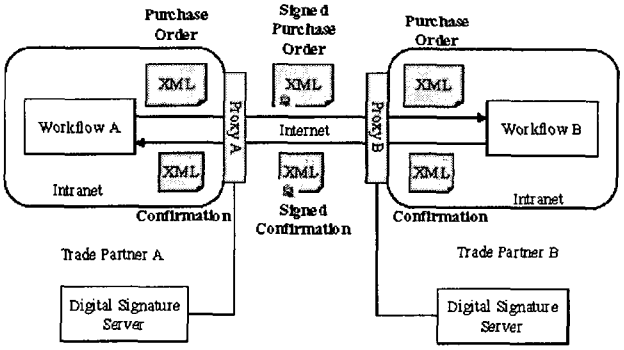
[그림 4] XML 인증서의 DTD

3.2 Security Architecture

본 논문에서는 기존 애플리케이션과 독립적으로 XML 서명을 수행하고 검증하는 보안 시스템을 웹서비스 플랫폼기반으로 개발하였다. 앞에서 언급한 구매주문(PO)을 내리고 그에 대해 확정을 해 주는 경우에 개방적인 인터넷을 통과할 때에는 A회사에서 발송 전에 전자서명을 수행하고, 상대편 B회사에서 수신 후에 검

증함으로써 안전한 SOAP 메시지 교환이 가능하도록 한다. 여기서 전달되는 메시지를 감시하여 전자서명 여부를 체크하는 역할을 수행하는 것을 프록시(Proxy)라고 하며, 실제로 전자서명을 수행하고, 검증하는 역할을 수행하는 것을 웹서비스로 구현한다. 이 구조의 작동 과정은 다음과 같다([그림 5] 참조).

- 회사 A의 워크플로우 A는 구매주문 메시지를 B회사의 워크플로우로 보낸다.
- 주문이 프록시 A를 통과하면 그 메시지를 전자서명 서버로 보내어 전자서명을 수행한다.
- 회사 B의 프록시 B는 서명된 메시지를 받고 그것을 검증 서버로 보낸다. 검증 서버는 서명된 메시지를 검증한다.
- 검증 결과를 프록시 B에게 보내어 지고, 만약 서명이 유효하면 프록시 B는 서명부분을 제거한 다음 메시지를 워크플로우 B에게 보낸다. 이 때에 서명자에 대한 정보를 보관할 수도 있다.
- 워크플로우 B는 메시지를 받아서 구매주문을 처리한 다음 답장 메시지를 생성하고 A 회사로 전송한다.
- 답장 메시지가 프록시 B를 통과할 때에 그 메시지는 전자서명 서버로 보내어져 B 회사의 개인키로 서명한 다음 A 회사로 보내어 진다.
- A 회사에서는 프록시 A가 메시지를 검증 서버로 보내어 전자서명이 유효하면 서명부분을 제거한 다음 워크플로우 A로 메시지를 보낸다.



[그림 5] 안전한 XML 메시지 교환 구조

여기서 프록시는 네트워크 상의 XML 메시지를 검사하여 전자서명을 수행할지 검증할지를 결정하기 때문에 워크플로우 A와 B는 서명 수행과 검증에 대해서 신경쓸 필요가 전혀 없다. 따라서 기존에 존재하는 응용이 변경될 필요가 없는 장점이 있다.

프로시 서버의 동작 원리는 다음과 같다. 먼저 내용 검증기는 DTD에 존재하는 <Signature> 엘리먼트가 존재하는지 여부를 검사하여 전자서명이 필요한지 결정한다. 만약 필요하면 일반 XML 메시지를 SOAP 메시지 형태로 웹서비스 형태의 전자서명 서버에게 전달하기 위해서 SOAP 메시지로 변경하고 다시 해제하는 모듈이 필요하다.

4. Prototyping

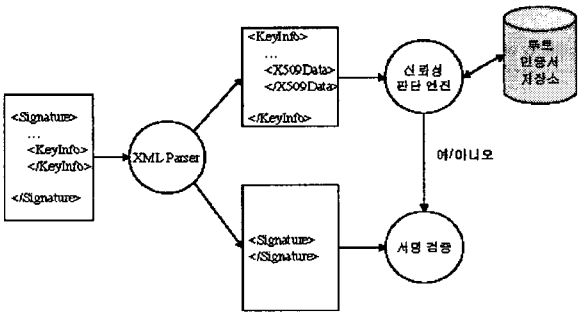
다음 [그림 6]은 전자서명된 구매지시 메시지를 나타낸다. 이 메시지가 전자서명 웹서비스에서 처리되는 절차는 다음과 같다.

```
<?xml version="1.0" encoding="UTF-8"?>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo Id="foobar">
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
        <Reference URI="http://www.abccompany.com/news/2000/03_27_00.htm">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>j61wx3rvEPO0vKtMup4NbeVu8nk=</DigestValue> </Reference>
        <Reference URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-example.xml">
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue> </Reference>
    </SignedInfo>
    <SignatureValue>MC0E~LE=</SignatureValue>
    <KeyInfo>
        <X509Data>
            <X509SubjectName>CN=Ed Simon,O=XMLSec Inc.,ST=OTTAWA,C=CA</X509SubjectName>
            <X509Certificate> MIID5jCCA0+gA...lVN </X509Certificate>
        </X509Data>
    </KeyInfo>
</Signature>
```

[그림 6] XML 전자서명

- 전자서명될 대상을 결정한다. 이것은 주로 URI(Uniform Resource Indentifier) 형태로 주어진다.
- 각 서명 대상별로 다이제스트(digest)값을 계산한다. XML 전자서명에서는 서명 대상은 <Reference> 엘리먼트에 정의되고, 각각의 다이제스트는 <DigestValue> 엘리먼트에 저장된다. <DigestMethod> 엘리먼트는 사용될 알고리즘을 정의한다.
- 서명 대상별로 <Reference> 엘리먼트를 구성하는데 이것은 <SigedInfo> 엘리먼트에 속한다. 여기서 <CanonicalizationMethod>는 <SignedInfo> 엘리먼트를 정형화하는 알고리즘을 지정한다. <SignatureMethod>는 전자서명 알고리즘을 지정한다.
- <SignedInfo> 엘리먼트의 다이제스트를 계산하고 그것을 서명한 다음 <SignatureValue>엘리먼트에 저장한다.
- 공개키 정보가 필요한 경우는 <KeyInfo> 엘리먼트에 저장한다. 이것은 송신자의 X.509 인증서로서 전자서명의 검증에 필요하다. 이것을 검증하는 절차는 그림과 같다.
- 마지막으로 위에서 생성한 모든 엘리먼트를 <Signature> 엘리먼트에 포함시킴으로써 XML 전자서명을 생성한다.

여기서 전자서명의 신뢰성을 검증하는 절차는 다음 [그림 7]과 같다. 즉 위에서 생성한 전자서명을 검증하는 과정으로서 먼저 <KeyInfo>에 있는 인증서 정보를 추출하여 인증서 저장소에 있는 인증서와 비교함으로써 신뢰성을 검증할 수 있음을 보여준다.



[그림 7] XML 전자서명의 신뢰성 검증 절차

5. 결론

본 논문에서는 전자상거래상에서 안전한 거래를 보장하고 부인 방지를 위해 PKI 기반의 전자서명 을 XML 기반의 웹서비스 기반으로 설계하였다. 전자상거래를 수행하는 두 회사간에 거래 정보를 XML 메시지로 주고 받을 경우에 필요한 XML 전자서명을 설계하였고, 그 운영 구조도 제시하였다. 프록시와 웹서비스 개념을 도입하여 기존에 존재하는 응용프로그램은 전혀 변경없이 운영될 수 있는 구조를 제시하였다. 모든 문서 교환 정보는 XML로 표현하였고, XML 문서 내 기밀 정보가 담긴 엘리먼트들만 암호화하고, 문서 전체에 디지털 서명 함으로써 거래의 안정성 및 부인 방지를 보장하였다.

또한 본 논문에서는 기업간 전자상거래 지원을 위한 프로세스 관리 도구인 x-ebFMS에 적용가능성을 제시함으로써 전자상거래보안에 관련된 여러 문제들을 플랫폼 독립적으로 해결할 수 있는 하나의 방법을 제시하였다.

향후 공인인증기관과의 연동에 관한 연구와 인증서의 폐기에 따른 CRL(Certificate Revocation List)의 배포, CA의 키 갱신에 따른 기존 인증서의 인증 방법에 대한 연구가 필요하다.

Acknowledgement

본 연구는 한국과학재단의 특정기초연구과제 (과제번호 R01-2002-000-00155-0)의 지원을 받았음.

참고 문헌

[1] RFC: 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 1996.

[2] W3C, Extensible Markup Language (XML), http://www.w3c.org/XML, February 1998.

[3] www.w3.org "XML Signature Requirements WD," W3C Working Draft, October 14, 1999.

[4] www.w3c.org "XML-Signature Syntax and Processing" W3C Recommendation, February 12, 2002.

[5] www.w3c.org "XML Encryption Syntax and Processing," W3C Working Draft, October 18, 2001.

[6] www.w3c.org "Decryption Transform for XML Signature," W3C Working Draft, October 18, 2001.

[7] Y. Nakamur et al, "Towards the Integration of Web Services Security on Enterprise Environments," Proceedings of the 2002 Symposium on Application and the Internet, 2002, pp. 166-175

[8] T. Takase et al, "XML Digital Signature System Independent Existing Applications," Proceedings of the 2002 Symposium on Application and the Internet, 2002, pp.150-157

[9] E. Xavier, "XML based Security for E-Commerce Applications," Eighth Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2001, pp. 10-17

[10] E. Damiani et al., "Controlling Access to XML Documents," IEEE Internet Computing, Nov.~Dec. 2001, pp. 18-28

[11] 김만수 외 2 인, "PKI 기반 e-Commerce ,보안 애플리케이션 설계," 제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호, 2002. 11

[12] 문기영 외 1 인, "XML 기반 전자상거래 정보보호 기술 개발," ETRI 연구개발보도자료, 2001, 11.29