전자상거래에서 안전한 정보 교환을 위한 웹 서비스 기반의 XML 보안 모델

조광문†

요 약

인터넷에 기반하고 있는 전자상거래에서 무엇보다도 중요한 기술 요소는 거래 정보를 교환하는데 있어서 안정성을 보장하는 것이다. 이러한 보안 문제를 위한 다양한 기술들이 표준으로 제시되고 있다. 그 중에서도 XML(eXtensible Markup Language)이 전자상거래 시스템의 문서 표준으로 다양한 분야에서 사용되면서 XML 보안이 새로운 분야로 등장하였다.

본 논문에서는 웹 서비스(Web Services) 기반의 전자상거래 시스템에서 거래 정보의 안전한 교환을 위한 XML 보안 모델을 제안한다. 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. 특히 전자상거래에 필요한 프로세스 관리 시스템과의 통합을 이룰 수 있는 방안을 제시한다.

키워드 : 전자상거래, XML, 웹 서비스, XML 보안 모델

Web Services based XML Security Model for Secure Information Exchange in Electronic Commerce

Kwang-Moon Cho†

ABSTRACT

The most important technology in the electronic commerce based on Internet is to guarantee the security of trading information exchange. Many technologies are proposed as a standard to support this security problem. One of them is an XML (eXtensible Markup Language). This is used in various applications as the document standard for electronic commerce system. The XML security has become very important topic.

In this paper an XML security model for web services based electronic commerce system to guarantee the secure exchange of trading information. To accomplish the security of XML, the differences of XML signature, XML encryption and XML key management scheme respect to the conventional system should be provided. The new architecture is proposed based on unique characteristics of XML. Especially the method to integrate the process management system need to the electronic commerce is proposed.

Keywords : Electronic Commerce, XML, Web Sevices, XML Security Model

1. 서 론

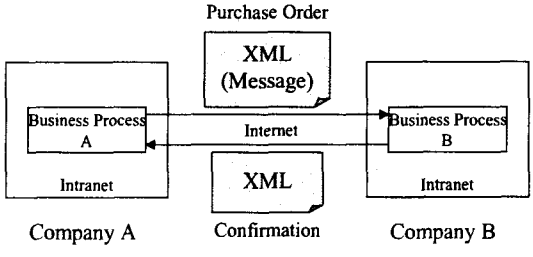
인터넷은 개방된 형태의 통신으로서 쉬운 프로토콜을 기반으로 한 브라우저와 다양한 정보 도구들이 제공되면서 인터넷을 통해 유통되는 정보가 많아지고 있다. 이에 따라 인터넷에서 사용되는 문서 처리

† 정 회 원: 천안대학교 정보통신학부 조교수(교신저자)
논문접수: 2004년 8월 24일, 심사완료: 2004년 9월 2일

표준들이 활발하게 개발되고 있으며 이에 기반한 전자상거래가 크게 확산되었다.

기업은 경쟁력 확보를 위하여 기업 내부의 조직 활동뿐만 아니라, 다른 기업과의 상호 협력적인 업무를 수행한다. 특히 기업간의 거래 업무는 계약된 문서 양식을 주고받으며 협의된 업무 프로세스에 따라서 정형적으로 실행되는 것이 일반적이다. 기존의 기업 내부 프로세스를 관리하는 비즈니스 프로세스 관리 시스템을 바탕으로, 기업간 전자상거래에서 요구되는 여러 가지 핵심 요소들을 분석하여 B2B 환경에 적합한 업무 모델을 제안하는 것이 본 논문의 목적이다. 특히, 기업간 정보 교환에 실질적인 표준 도구로 인정받고 있는 XML(eXtensible Markup Language) 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. 또한 전자상거래에서 필수적으로 요구되는 안전한 정보 교환을 보장한다.

인터넷 상에서 수행되는 전자상거래의 성공을 위협하는 가장 큰 부분은 보안 문제이다. <그림 1>과 같이 인터넷을 통한 교환 정보를 단순히 XML로 변경하는 경우는 두 거래 당사자의 사용자 인증이 보장되지 않으므로 메시지 교환이 안전하지 못하다[12]. 특히 비대면 거래를 수행하는 전자상거래에서 정당한 사용자임을 보장하기 위한 사용자 인증을 위해서는 공개키 암호 시스템에 바탕을 두고 실현되어야 한다. 따라서 사용자 공캐키의 신뢰성과 안전성을 보장 받을 수 있는 방안이 필요하다.



<그림 1> 안전하지 않은 메시지 교환

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

이와 더불어 XML 기술이 인터넷 e-비즈니스 시스템 등에서 메시지 교환 형식으로 이용되면서 XML 문서의 보안 역시 필수적 요구 조건이 되고 있고, 안전한 전자상거래를 수행하기 위해서 XML 디지털 서명(Digital Signature)이 반드시 지원되어야 한다[2-6].

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 위한 웹 서비스를 설계하고, 또 B2B간의 메시지 교환 정보의 보안과 부인방지 문제를 해결하기 위해 PKI와 XML 기반의 디지털 서명 프로토콜을 설계한다.

2. 기반 기술 연구

2.1. 공개키 기반 구조

공개키 암호 시스템은 비대칭 키 암호 시스템으로서, 수학적 함수를 기반으로 하며 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 인증 기관(CA: certification authority)이 거래 주체(subject)를 인증하는 전자 증명서 역할을 수행하며, 주체 사용자가

합법적인 사용자임을 입증하기 위해 인증 기관은 자신의 개인키로 디지털 서명을 생성하여 인증서에 첨부한다. 인증서는 인증서 사용자에 대한 공개키와 주체 사용자의 신분에 대한 정보를 포함한다.

2.2. 웹 서비스

웹 서비스란 위치나 플랫폼에 관계없이 웹 상에서 다른 프로그램에 의해 발견될 수 있고, 호출될 수 있는 소프트웨어 인터페이스이다. 웹 서비스는 플랫폼이나 디바이스 및 위치에 독립적이고, 동적인 기능을 제공하며 효율적인 비용으로 기존 시스템에도 적용할 수 있다는 특징을 갖는다.

전자상거래에 있어서 웹 서비스란 인터넷 상에서 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 웹 서비스는 거래업체간의 이질적인 운영 시스템, 이질적인 프로그램 언어간의 커뮤니케이션 차이를 극복해주는 연결고리 역할을 해준다. 즉, 웹 서비스는 e-Business 표준을 따르며 인터넷을 통해 제공되는 비즈니스 로직을 갖는 소프트웨어 컴포넌트이다. 웹 서비스는 단순히 웹을 통해 제공되는 서비스만을 의미하지 않는다. 웹 서비스라는 용어에서 연상되는 서비스는 ASP나 웹 호스팅 등이지만 최근 Microsoft, IBM, HP 등의 대형 IT 업체들이 차세대 제품 전략의 핵심이 되고 있는 웹 서비스는 순수 서비스라기보다는 애플리케이션에 가깝다. 웹 서비스는 벤더나 SI 업체에게는 애플리케이션이나 소프트웨어 컴포넌트로 인식되지만, 사용자에게는 관련 정보가 모두 캡슐화(encapsulation)되어 있어서 기술이나 컴퓨팅이 아닌 서비스로 인식되기 때문에 서비스라는 용어를 강조하고 있다.

2.3. XML

XML 표준은 XML 문서(XML document)라는 데이터 객체들의 클래스를 기술하고, 이 XML 문서들을 처리하는 컴퓨터 프로그램의 연산 내용을 기술한다. XML은 일종의 SGML(Standard Generalized Markup Language) 응용이다.

XML 문서들은 엔티티(entity)라는 저장 단위들로 구성된다. 엔티티는 파싱되는 데이터 또는 파싱되지 않는 데이터 중의 하나를 포함한다. 파싱되는 데이터는 문자(character)들로 구성된다. 이 문자들의 일부는 문자 데이터(character data)가 되고, 또 일부는 마크업(markup)이 된다. 마크업은 XML 문서의 물리적 저장소 배치도 및 논리적 구조에 대한 설명을 부호화한다. XML은 저장소의 배치도 및 논리적 구조를 강제하는 매커니즘을 제공한다.

XML 프로세서(XML processor)라는 소프트웨어 모듈은 XML 문서를 읽어 들여 그 콘텐츠와 구조에 접근할 수 있도록 한다.

XML은 자료를 구분하는 방법에 대한 표준이고, XSL(XML Stylesheet Language)은 구분된 자료를 출력하는 방법에 대한 표준이다. XSL은 일종의 변환 기술로서 XML의 각 필드를 HTML의 어떤 태그로 변환하여 웹 브라우저에 출력할 것인가에 대한 규칙을 정하는 언어이다.

XML 스키마(XML Schema)는 XML 문서의 구조와 콘텐츠를 정의하는 파일을 일컫는 용어이다. DTD(Document Type Definition)도 이러한 스키마의 일종이지만 많은 문제점을 가지고 있었다. DTD와의 가장 큰 차이점은 DTD는 EBNF라는 복잡하고 약간은 어려운 언어로 기술해야 하지만 XML 스키마는 그냥 XML을 사용하여 기술한다는 것이다. 또한 XML 스키마에서는 DTD에서 표현할 수 없었던 각종 데이터 타입과 엘리먼트 재사용 등이 가능하다. 즉 XML 스키마는 DTD를 대폭 확장한 모델로서 XML 문서가 가질 수 있는 엘리먼트 타입, 엘리먼트 간의 관계, 각 엘리먼트가 가질 수 있는 타입에 대해 상세히 정의할 수 있다.

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

2.4. XML 디지털 서명

최근 XML은 B2B와 B2C 등과 같은 기본적인 응용과 더불어 여러 분야에 적용할 수 있는 기술로서 각광을 받고 있다[2]. 특히 전자상거래 상에서의 대부분의 서비스가 전자적으로 처리됨에 따라 그에 따른 보안의 중요성이 대두되고 있다. 특히, XML을 활용한 전자상거래 상의 문서 교환 과정에서 필요한 보안에 대한 표준화 작업이 활발히 진행되고 있는데, IETF와 W3C의 XML-Signature Working Group에서 제정된 "XML-Signature Syntax and Processing" 명세서에서 XML 디지털 서명의 구문과 처리 과정을 기술하고 있다[4].

XML 디지털 서명을 사용하기 위한 보안 관련 고려 사항은 다음과 같다.

- 비밀성(Confidentiality): 전송되는 자료의 일부 또는 전부를 제 3자가 볼 수 없도록 하는 기능.
- 무결성(Integrity): 원격에서 전송된 문서가 위조 또는 변조되지 않았음을 증명하는 기능.
- 인증(Authentication): 사용자가 정당한 사용자임을 인증하는 기능.
- 승인(Authorization): 거래 요청에 대하여 상대방의 거래를 승인하고 이에 대한 처리 결과를 거래 요청자에게 통보하는 기능.
- 부인 방지(Non-Repudiation): 문서를 송수신하는 경우 해당자가 송수신에 대한 행위를 부인할 수 없도록 하는 기능.

3. XML 보안 모델

3.1. XML 서명

XML 서명(XML Signature) 문법은 매우 다양한 기능을 제공하는 복잡한 표준으로서 고수준의 확장성과 유연성을 갖도록 설계되어 있으므로 어느 서명에나 적용할 수 있다. W3C 권고안은 XML 서명 문법과 그에 관련된 처리 규칙을 정의하고 있다[4].

<그림 2>는 디지털 서명의 XML 문법을 보여준다.

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

<그림 2> 디지털 서명의 XML 문법

XML 서명은 <Signature> 엘리먼트로부터 시작된다. <Signature> 엘리먼트는 서명을 구성하고 식별하게 해 주는 중요한 엘리먼트이다. <SignedInfo> 엘리먼트는 우리가 서명할 대상 즉 "서명된 정보"를 나열하고 있다. 다이제스트(digest)를 위한 특정한 데이터 스트림은 <References> 엘리먼트로 표현되며, URI(Uniform Resource Identifier) 문법이 이 스트림을 규정하는데 사용된다. <KeyInfo> 엘리먼트가 검증 키에 대한 식별 매커니즘을 제공함으로써 XML 서명의 처리 자동화에 유용하게 사용된다. <Object> 엘리먼트는 어떤 타입의 데이터 객체도 담을 수 있는 컨테이너이다. <Object> 엘리먼트 내부에 포함되는 <SignatureProperties>와 <Manifest>라는 두 가지의 특별한 엘리먼트가 XML 서명 권고안에 의해서 정의된다. <SignatureProperties> 엘리먼트는 편리함을 제공해 주는 서명 확인을 위해 미리 정의된 컨테이너이다. <SignatureProperties> 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 문서에 서명하는 다중 서명자를 위한 편리한 방법을 제공한다. <Manifest> 엘리먼트를 사용하지 않는다면, 서명 결과물은 중복되는 데이터의 존재로 부피가 상당히 커질 것이며 생성과 검증 시에 성능이 저하된다.

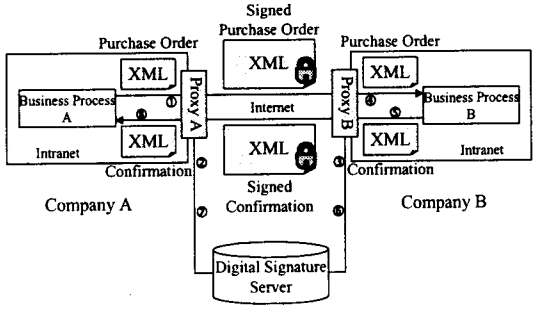
인증서 생성 정보와 발급된 인증서는 XML 문서로 교환되며, 중요 정보는 XML 엘리먼트 단위로 암호화를 한다. 인증서 생성 정보에 대한 DTD는 <그림 3>과 같다.

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

<그림 3> XML 인증서의 DTD

3.2. XML 보안 구조

본 논문에서는 기존 애플리케이션과 독립적으로 XML 서명을 수행하고 검증하는 보안 시스템을 웹 서비스 플랫폼 기반으로 설계하였다. <그림 1>에서와 같이 주문서(Purchase Order)를 제출하고, 이에 대해 확인(Confirmation)을 해 주는 경우에 인터넷을 통해 송수신될 때 회사 A에서 발송 전에 디지털 서명을 수행하고, 상대편 회사 B에서 수신 후에 검증함으로써 안전한 SOAP 메시지 교환이 가능하도록 한다. 이 때 전달되는 메시지를 감시하여 디지털 서명 여부를 체크하는 역할을 수행하는 것을 프록시(Proxy)라고 하며, 실제로 디지털 서명을 수행하고 검증하는 역할을 수행하는 것은 웹 서비스로 구현한다. 이 구조는 <그림 4>와 같다.



<그림 4> XML 메시지의 안전한 교환 구조

<그림 4>의 실행 과정은 다음과 같다.

① 회사 A의 비즈니스 프로세스 A는 주문서 메시지를 회사 B의 비즈니스 프로세스로 전송한다.
② 주문이 프록시 A를 통과할 때 메시지를 디지털 서명 서버로 보내어 디지털 서명을 수행한다.
③ 회사 B의 프록시 B는 서명된 메시지를 받고 그것을 검증 서버로 보낸다. 검증 서버는 서명된 메시지를 검증한다.
④ 검증 결과를 프록시 B에게 보내고, 만약 서명이 유효하면 프록시 B는 서명 부분을 제거한 다음 메시지를 비즈니스 프로세스 B에게 보낸다. 이 때 서명자에 대한 정보를 보관할 수도 있다.
⑤ 비즈니스 프로세스 B는 메시지를 받아서 주문서를 처리한 다음 답장 메시지를 생성하고 회사 A로 전송한다.
⑥ 답장 메시지가 프록시 B를 통과할 때에 그 메시지는 디지털 서명 서버로 보내져 회사 B의 개인키로 서명한 다음 회사 A로 전송된다
⑦ 회사 A에서는 프록시 A가 메시지를 검증 서버로 보낸다.
⑧ 디지털 서명이 유효하면 서명 부분을 제거한 후 비즈니스 프로세스 A로 메시지를 보낸다.

프록시는 네트워크 상의 XML 메시지를 검사하여 디지털 서명을 수행할 것인지 검증할 것인지를 결정하기 때문에 워크플로우 A와 B는 서명 수행과 검증에 대해서 신경 쓸 필요가 전혀 없다. 따라서 기존에 존재하는 응용이 변경될 필요가 없는 장점이 있다.

프록시 서버의 내용 검증기는 DTD에 존재하는 <Signature> 엘리먼트가 존재하는지 여부를 검사하여 디지털 서명이 필요한지 결정한다. 만약 필요하면 일반 XML 메시지를 SOAP 메시지 형태로 웹 서비스 형태의 디지털 서명 서버에게 전달하기 위해서 SOAP 메시지로 변경하고 다시 해제하는 모듈이 필요하다.

3.3. 디지털 서명의 처리

<그림 5>는 디지털 서명된 주문서 메시지의 예를 보여준다.

```
<?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.acompany.com/news/2000/03_27_00.htm">
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>j6lwx3rvEP00vKtMup4NbeVu8nk=</DigestValue>
</Reference>
<Reference
URI="http://www.w3.org/TR/2000/WD-xmldsig-core-20000228/signature-sample.xml">
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>UrXLDLBIta6skoV5/A8Q38GEw44=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MCOE~LE=</SignatureValue>
<KeyInfo>
<X509Data>
<X509SubjectName>CN=Ed Simon, O=XMLSecurity Inc.,
ST=OTTAWA, C=CA</X509SubjectName>
<X509Certificate> MIID5jCCAO+gA...IVN </X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
```

<그림 5> XML 디지털 서명

이 메시지가 디지털 서명 웹 서비스에서 처리되는 절차는 다음과 같다.

① 디지털 서명을 할 대상을 결정한다. 이것은 일반적으로 URI 형태로 주어진다.

② 각 서명 대상별로 다이제스트 값을 계산한다. XML 디지털 서명에서 서명 대상은 <Reference> 엘리먼트에 정의되고, 각각의 다이제스트는 <DigestValue> 엘리먼트에 저장된다. <DigestMethod> 엘리먼트는 사용될 알고리즘을 정의한다.

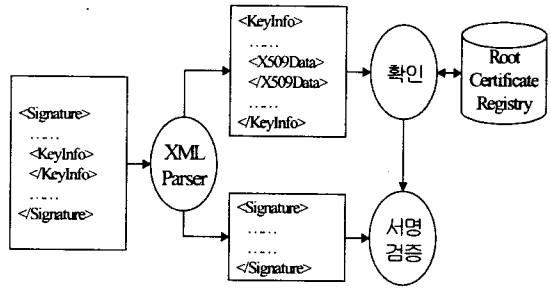
③ 서명 대상별로 <Reference> 엘리먼트를 구성하는데 이것은 <SignedInfo> 엘리먼트에 속한다. <CanonicalizationMethod>는 <SignedInfo> 엘리먼트를 정형화하는 알고리즘을 지정한다. <SignatureMethod>는 디지털 서명 알고리즘을 지정한다.

④ <SignedInfo> 엘리먼트의 다이제스트를 계산하고 서명한 다음 <SignatureValue> 엘리먼트에 저장한다.

⑤ 공개키 정보가 필요한 경우는 <KeyInfo> 엘리먼트에 저장한다. 이것은 송신자의 X.509 인증서로서 디지털 서명의 검증에 필요하다. 이를 검증하는 절차는 <그림 6>과 같다.

⑥ 지금까지 생성한 모든 엘리먼트를 <Signature> 엘리먼트에 포함시킴으로써 XML 디지털 서명을 생성한다.

디지털 서명의 신뢰성을 검증하는 절차는 <그림 6>과 같다.



<그림 6> XML 디지털 서명의 신뢰성 검증

생성한 디지털 서명을 검증하는 과정으로서 먼저 <KeyInfo>에 있는 인증서 정보를 추출하여 인증서 저장소(Root Certificate Registry)에 있는 인증서와 비교함으로써 신뢰성을 검증할 수 있음을 보여준다.

4. 결 론

본 논문에서는 전자상거래 상에서 안전한 거래를 보장하고 부인 방지를 위해 PKI 기반의 디지털 서명을 XML 기반의 웹 서비스로 설계하였다. 전자상거래를 수행하는 두 회사 간에 거래 정보를 XML 메시지로 주고받을 경우에 필요한 XML 디지털 서명을 설계하였고, 그 운영 구조도 제시하였다. 프록시와 웹 서비스 개념을 도입하여 기존에 존재하는 응용 프로그램은 전혀 변경없이 운영될 수 있는 구조를

제시하였다. 모든 문서 교환 정보는 XML로 표현하였고, XML 문서 내 기밀 정보가 담긴 엘리먼트들만 암호화하고, 문서 전체에 디지털 서명함으로써 거래의 안정성 및 부인 방지를 보장하였다.

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.

참 고 문 헌

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

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

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

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

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

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

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

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

[9] KwangMoon Cho, "Framework of Content Distribution in Mobile Network Environment," Proceedings of the 2003 International Conference on Internet Computing (IC '03), pp.429-434, Jun. 2003.

[10] KwangMoon Cho, "Packaging Strategies of Multimedia Content in DRM," Proceedings of the 2003 International Conference on Internet Computing (IC '03), pp.243-248, Jun. 2003.

[11] 김만수 외 2 인, "PKI 기반 e-Commerce ,보안 애플리케이션 설계," 정보처리학회 추계 학술발표대회 논문집, 제9권, 제2호, 2002. 11.

[12] 배준수, "전자상거래 정보교환을 위한 XML 보안," 경영과학회/산업공학회 춘계공동학술대회논문집, pp.889-896, 2003.

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

조 광 문

1988.2 고려대학교 컴퓨터학과 (이학사)

1991.8 고려대학교 컴퓨터학과 (이학석사)

1995.8 고려대학교 컴퓨터학과(이학박사)

1995.9~2000.2 삼성전자 통신연구소 선임연구원

2000.3~현재 천안대학교 정보통신학부 조교수

관심분야: 콘텐츠 유통, 모바일 콘텐츠, 전자상거래, 데이터베이스

E-Mail: ckmoon@cheonan.ac.kr