전자거래 정보보호 기술의 적합성 및 상호운영성에 관한 연구

성백호°, 이형석, 차무홍, 신동일, 신동규

세종대학교 컴퓨터공학과

{guardia, bestehen, bidon, dshin, shindk}@gce.sejong.ac.kr

A Study on the Conformance and Interoperability of Information Security Technologies for Electronic Commerce

Baek-Ho Sung°, Hyoung-Seok Lee, Muhong Cha, Dong-il Shin, Dong-kyoo Shin

Dept. of Computer Engineering, Sejong University

요 약

확장성과 유연성, 그리고 변환 편이성 등 XML의 장점을 기반으로 한 ebXML의 기술이 점차 확대되어 가고 있다. 하지만 현재 대부분의 XML 기반 거래 프레임워크에 대한 연구 및 지원은 실제 비즈니스를 수행하기 위한 개별적인 구성 요소의 구현 방법 연구에만 집중되어 왔다. 이로 인해 현재 국내의 보안 요소 기술과 상호운영성에 대한 연구가 구성 요소의 구현에 비해 상대적으로 취약한 것이 현실이다. 이에 본 논문은 XML 기반 정보보호와 상호운영성의 관련기술과 동향을 연구하였다.

1. 서 론

웹 가능 브라우저와 HTML같은 정의된 데이터를 위한 언어가 세계의 디지털 문서를 이끌었고 HTML의 간단함을 이용한 새로운 개념이 도입된 XML이 급속하게 확산되어 가고 있다. 차세대 XML 기반 거래 프레임워크인 ebXML 또한 급성장을 하고 있는데 요인은 기존의 e-비즈니스 방식에 있어 커다란 걸림돌이 되었던 상호운용성의 문제를 XML이라는 확장성 있는 자료 형을 이용해 효과적으로 개선했기 때문일 것이다. 그러나 아직 표준이 정립되어 가는 시기로 충분히 완성되지 못하였기 때문에 타 프레임워크와의 관계 속에서 ebXML의 향방을 인식하기에 다소 혼란스러울 수도 있다. 물론 해외 주요 e-비즈니스 업체 및 국제 표준화 기구는 ebXML 프레임워크의 응용 및 표준화를 활발히 진행 중에 있기는 하지만 현재 XML을 전달하고 처리하여 저장 관리 및 활용까지의 전반적인 과정을 지원하기 위한 기반 기술과 정보보호기술의 완성도가 낮은 것이 현실이고 표준화의 주도권 역시 우리가 이끌어가고 있지 못하는 상황이다[1]. 바로 이러한 문제 인식에서 시작해서 전자상거래가 통합되어 운영되기 위해서는 현재 기술의 상호연동 관계의 확고한 정립과 새로운 기술 표준안에 대한 제시가 필요할 것이다. 그리고 통합된 전자 상거래 프레임워크가 안전하고 신뢰성 있게 운영되기 위해서 각 메시지의 전송과 등록과정에서 보안과 상호 신뢰를 위한 전자서명과 같은 정보보호기술의 적용이 불가피하다. 또한 이렇게 적용되는 정보보호 기술도 각 이기종간의 프레임 워크 간에 상호운영 방안을 모색하지 않으면 각 전자상거래 프레임워크는 스스로 고립될 수밖에 없다.

이에 본 연구에서는 ebXML로 대변될 수 있는 새로운 전자상거래 프레임 워크에 대한 정보보호기술의 적합성과 상호운영에 대한 연구를 위해 ebXML을 주도하는 W3C와 OASIS등에서 대안으로 제시하고 있는 XML기반 보안 기술 등 현재 표준화하거나 진행중인 XML 보안을 위한 명세와 상호운영성 테스트 기술을 분석 고찰하고 이러한 기술들을 기반으로 현재의 상황과 문제점을 제시하여 국내 전자거래 정보보호 기술의 적합성 및 상호운영성의 국내 적용방안을 연구했다.

2. 관련연구

전자상거래의 정보보호 적합성 및 상호운영성을 위해서는 W3C와 OASIS등에서 새로운 전자상거래 프레임 워크의 보안에 대한 대안으로 제시하고 있는 XML Signature[2], XML Encryption[3], XKMS [4], SAML[5]과 XACML[6]등 현재 표준화되었거나 진행중인 XML기반 보안기술을 적용해야한다. 따라서 본 관련연구에서는 XML 기반 보안 기술을 연구해봤다.

2.1 관련 XML기반 보안 기술

1) XML 전자서명(XML Digital Signature)

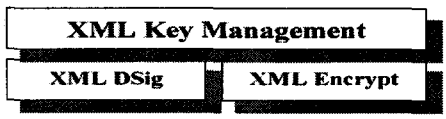
전자서명이란 전자화된 문서의 메시지 내용이 수정 및 변조되지 않았음을 보장하는 동시에 메시지의 주체인 사용자, 즉 송수신자가 올바른 사용자라는 것을 확인할 수 있게끔 하는 인증방식을 말한다. XML 컨텐츠 상에 존재하는 요소(element)에 포함된 서명은 XML 문서 내의 데이터 상에 존재한다. 또한, 분리된(Detached) 서명은 그 서명 요소의 외부데이터 상에 존재한다. 이 명세서는 자원, 알고리즘, 키 정보 및 관리의 조합에 대한 참조방법을 포함한 유용한 타입들을 정의한다. 현재 IETF와 W3C의 XML 전자서명 워킹 그룹에서 제정된 XML 전자서명 명세는 2002년 2월 12일 W3C의 Recommendation 상태로 승격됨에 따라 표준화가 완료된 상태이다[2].

2) XML 암호(XML Encryption)

현재 인터넷상으로 어떠한 데이터를 전송 할 때 IPSec나 SSL만으로도 충분한 데이터에 대한 기밀성을 보장 할 수 있으며 PGP(Pretty Good Privacy)나 S/MIME을 사용하면 송수신 및 저장 시 암호화를 수행할 수 있다. 하지만, 이러한 방법은 데이터 전체에 대한 암호화를 수행함으로써 데이터의 일부만 암호화가 필요한 경우에는 부적절할 방법이 된다. 이에 따라 데이터 중 일부분만을 암호화해 중간에 경유하게 되는 제 3자에게 특정 정보를 노출시키지 않으면서 최종 수신자에게 전달 할 수 있는 방법으로 현재 W3C에서 XML 기반의 표준화를 추진하고 있는 것이 XML Encryption이다. XML Encryption 명세는 현재 2002년 12월 10일 Recommendation 상태이다[3].

3) XKMS(XML Key Management Specification)

XKMS는 차세대 인터넷언어인 XML에 기반을 두고 있으며, 기업이나 개발자들이 XML 웹 서비스에 PKI (Public Key Infrastructure) 디지털 서명과 암호화의 사용을 도와준다. XML은 프로그래머들이 전자상거래 애플리케이션에 적용할 전자서명과 데이터 암호화를 보다 용이하게 할 목적으로 개발된 것으로, 디지털 서명 같은 보안 소프트웨어, 온라인 인증, 데이터 암호화 등은 전자상거래 사이트에서 이뤄지는 거래와 계약의 안전을 지원한다. 또한, XKMS 기술은 개발자들이 디지털 인증과 다른 온라인 보호 툴을 e-커머스 애플리케이션에 쉽게 접목할 수 있도록 해준다. XKMS는 애플리케이션을 공개 키 인프라에 결부시킴으로써 소프트웨어 개발자들이 PKI를 좀더 저렴하고 쉽게 사용할 수 있도록 하기 위한 새로운 방식이며, PKI를 보편화시키는 것이다. 전체적인 구조는 XML 전자서명과 XML Encryption 워킹 그룹 내에서의 W3C의 활동 결과를 보충하기 위해 설계되어졌다.



[그림 1] XKMS와 XML 전자서명, XML Encryption간의 관계

위에 [그림 1]은 XKMS의 전체 구조 내에서 XML 전자서명과 XML Encryption사이의 관계를 도식화한 것이다. XKMS는 현재 2002년 3월 18일 Working Draft 상태로 표준화 진행 중이다[4].

4) SAML(Security Assertion Markup Language)

SAML은 인터넷상에서의 자원 요청자에 대한 인증, 승인, 속성 확인 등을 수행하는 역할을 하며 이는 XML 기반의 다른 보안 기술들(XML 전자서명, XML Encryption, XKMS, XACML 등)과 통합되어 전체 보안 시스템을 구성하는 일부 요소로서 기능을 가진다. SAML 명세는 Assertion, 프로토콜, 바인딩으로 구성되어 있다. Assertion은 인증 및 승인 정보를 포함하는 XML 기반 구조를 가진다. 또한 Assertion의 인증을 위해 XML 전자서명을 적용한다. SAML 프로토콜은 XML 기반의 메시지 형태로서 요청 및 응답의 쌍으로 구성되어 각 Assertion에 대한 전송을 담당한다. 일반적으로 Assertion은 SAML 프로토콜의 응답을 통해 얻어진다. SAML 바인딩은 SAML Assertion 요청 및 응답 프로토콜을 표준 메시지 전송 프로토콜과 연동함에 있어 처리되어야할 방식을 정의하고 있다. 현재 SOAP-over-HTTP[7] 바인딩이 기본적으로 사용된다. 현재 oasis committee specification으로 표준화가 진행 중이다 [5].

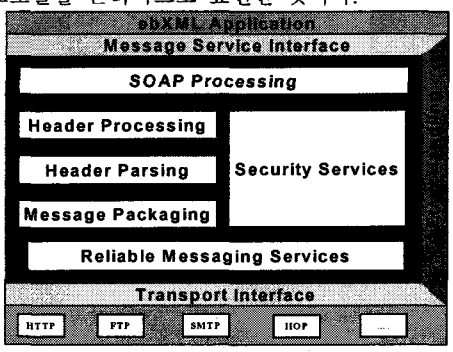
5) XACML(eXtensible Access Control Markup Language)

XACML은 XML문서에 대한 접근을 정책리스트를 이용하여 제어할 수 있는 XML기반의 언어이다. XACML TC(Technical Committee)에서는 XACML로 정의된 기술로 정책과 인증을 표현하기 위한 XML 스키마를 제공하고 있다. 이 정책에서의 리소스는 XML을 사용하여 표현되는 어떠한 객체도 될 수 있으며 XACML은 XPath [8]나 LDAP 등 다양한 프로토콜과 함께 바인딩 하여 사용될 수 있으며 새로운 프로토콜과도 함께 사용될 수 있다. XACML은 인증시스템의 접근과 접근자 요청의 특징적인 역할에 대한 제어를 할 것으로 기대된다. XACML은 공통의 산업 명세를 만드는 국제적인 컴소시엄인 OASIS(the Organization for the Advancement of Structured Information Standards)에 의해 표준화되고 있으며 가장 최근의 기술문서는 2003년 2월 18일 문서로 현재 표준 완료 상태이다 [6].

6) 메세징 보안

메시징 서비스는 거래 당사자간의 표준화된 방식으로 비즈니스 메시지를 교환 할 수 있는 기능을 제공한다. 또한 SOAP 프로토콜을 이용한 메시지 서비스는 특정 기술과 솔루션에 종속되지 않고 비즈니스 메시지를 안전하게 교환할 수 있는 수단을 제공한다.

다음 [그림 2]는 메시징 서비스 구조 내에서 기능적인 요소들을 논리적으로 표현한 것이다.



[그림 2] 메시징 서비스 구조

송·수신 메시지는 라우팅 정보와 전달 정보를 포함하고 있는 메시지 헤더와 페이로드(Payload) 부분으로 구성되어 있으며 개념적으로 세 부분으로 나누

어진다.

① 추상적인 서비스 인터페이스
② 메시징 서비스 계층에서 제공되는 기능들
③ 하부 전송 서비스와의 연계

메시징 서비스에서는 메시지 보안 요구를 MSH(Message Service Handler)에게 전달하고 중복 전송을 막기 위한 정보 및 메시지 전송 순서 등을 명시 할 수 있는 속성을 가지고 있다. 그리고 메시지가 전자서명 된 경우에는 XML 전자서명 명세에 따라 생성된다. 이 기능은 비즈니스 트렌젝션 모두에 사용될 수 있다. 이러한 부인 방지에 대한 처리는 MSH내에서 이뤄질 수도 있으며, 별도의 어플리케이션에서 처리할 수도 있다.

자체적으로 전자서명 기법을 제공할 수 있지만, 송·수신 메시지가 SOAP(Simple Object Access Protocol) 컨테이너 내에 포함되는 것을 고려 할 때 SOAP 자체에서 지원하는 전자서명 방식을 사용 할 수도 있다.

MSH의 주요 기능 중 하나는 전자서명 된 메시지를 검증하기 위해 적합한 키를 획득하고 각 메시지에 대한 서명 검증 과정을 수행하는 것이다. 이때 요구되는 키 관리에 따른 제반 사항을 XKMS를 통해 수행할 수 있다[7].

3. 정보보호 기술의 적합성 및 상호운영성 적용방안

상호운영성을 확보하기 위해서는 표준을 준수하면서 안정성과 상호운영성을 유지하는 프레임워크를 구현을 했는지에 대한 평가와 제도적인 협력을 들 수 있다. 기술적인 측면에서 명세에 따라서 각 요소들이 구현되어야지만 그 상호운영성이 증명될 수 있고 기관을 통한 제도적인 협력과 추진에 의해서만 표준화된 프레임워크는 성공적으로 그 기능을 다할 것이다. 현재 미국 및 몇몇 유럽 국가에서는 민간 기관을 중심으로 일부에 대한 테스트를 진행하고 있으며, 일본의 경우 정부주도 하에 정보보호 기술 테스트가 추진되고 있는 상황이다. 국내에서는 정보보호기술 분야에 대한 관심이 높아지고 있으나, 아직까지 체계적이고 표준화된 연구는 미진한 상황이다. 현재 ebXML 표준 적합성 및 상호운영성 테스트와 관련된 활동을 진행중인 국제기관 또는 단체로는 OASIS ebXML IIC TC, NIST, Drummond Group등이 있다. 따라서 본 장에서는 적합성 평가와 정보보호 적합성 및 상호운영성 Test Suit를 소개하고, 추후 나아갈 방향을 모색해 보겠다.

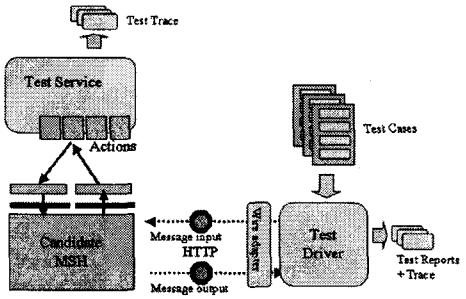
3.1적합성 평가

범세계적으로 동일한 명세를 구현하고 각 구현물 간의 상호연동성을 보장하기 위해 적합성 평가는 반드시 필요하다. 적합성은 각 구현물이 명세를 얼마나 정확하게 준수하고 있는 가에 대한 척도가 된다. 이 준수사항의 척도를 위해 적합성평가를 실시하고 평가도구에 의해 수행된다. 평가 결과에 따른 인증부여의 근거자료를 제시한다. 이러한 적합성 평가의 대상은 전자상거래 시스템 전체가 될 수도 있으며 혹은 일부분만이 평가의 대상이 될 수 있다. 적합성 평가 후 받게 되는 인증에 의해 상호연동 가능성을 예측할 수 있다.

적합성 인증이란 전자거래 표준에 따라 솔루션들이 개발되었는지를 심의하고 적정한 경우 인증을 부여하는 것을 말한다. 적합성 인증의 궁극적 목적은 공개적인 인증을 통해 기업들이 개발하여 제공하는 솔루션들이 서로 호환이 되어 전자거래가 원활하게 이루어질 수 있도록 하는 것이다. 현재 산업 분야에 대한 인증으로는 ISO 9002 등의 여러 인증 체계가 존재하나 전자거래 분야에 있어서는 국제적으로나 국내적으로 그 체계가 마련되어 있지 않은 것이 현실이다. 특히 국제적으로는 미국의 OASIS 및 NIST 등이 적합성 인증에 대한 표준화 작업을 진행 중에 있다.

3.2 표준적합성 및 상호운영성 Test Suit

e비즈니스의 특성상 솔루션들 간의 상호운용성은 반드시 필요한 요소이며, 이러한 상호운용성의 기반이 되는 것이 바로 표준적합성이다. 이에 사용자뿐만 아니라 개발자의 입장에서도 표준적합성 테스트의 필요성을 제시하고 있는 실정이다. 현재 OASIS에는 NIST(National Institute of Standards and Technology), OAG(Open Applications Group) 및 Drummond Group 등을 중심으로 한 ebXML IIC (ebXML Implementation, Interoperability and Conformance) 기술위원회가 구성되어 ebXML 테스트 슈트 스펙들을 만드는 작업을 진행 중에 있다. 작업 중인 스펙으로는 ebXML 테스트 요구사항, 메시징 적합성 테스트 슈트 스펙 및 메시징 상호운영성 테스트 슈트 스펙, 그리고 ebXML 테스트 프레임워크 스펙 등이 있다. 이러한 스펙 제정 작업을 통하여 표준에 적합한 e-비즈니스 솔루션 개발을 장려한다는 것을 주요 활동 목표로 하고 있다.



[그림 3] MS 적합성 테스트 구조도[8]

[그림 3]은 ebXML IIC 기술위원회에서 표준화 연구 중인 메세징 서비스 적합성 Testing Suit에서 제안한 구조를 보여준다. 이 적합성 테스트 구조에는 모든 테스트 case를 처리하고 운용하는 Test Driver 컴포넌트는 메시지를 전송하는데 사용하는 전송 Adapter와 연결되어 있다. Test Service 컴포넌트는 시작하는 Action에 반응한다. 메시지를 전송하는데 사용되는 transport Driver Adapter는 MSH를 사용하지 않는 생성되고 전송된 메시지를 처리한다. 이 Test Suit는 Transport 층에서 작동한다.

3.3 국내 상호상호운영성 적용방안

현재 ebXML을 중심으로 상호운영성을 위한 기술요소간의 표준을 확립하려는 노력이 되고 있지만 그 완성도가 아직 낮은 상태이다. 현재 국내에서는 국내 산재된 전자상거래 표준 기술을 통합하기 위한 전자상거래 통합포럼을 출범하였지만 표준전문인력, 법적 및 제도적 장치 미비, 기관 독립성 미비, 표준개발 예산의 미비 등으로 본래 의도한 표준 활동을 수행하고 있지 못하고 있다. 현재 우리나라 전자상거래 표준화 활동에 대해 언급해 보겠다.

먼저 외국과의 연계를 생각해야하는데 이를 위해서는 국제적인 표준을 수용하여 우리나라 상황에 맞게 개발하는 것이 현재 상호운영성에 대한 문제를 해결하는 근본적인 방법이다. 그러나 국제 전자상거래 표준을 위한 국내 전문가의 참여는 매우 저조한 상태이고 이에 따라 국제 표준 개발에 기득권을 얻기가 어렵게 된다. 국가 및 기관은 ebXML을 중심으로 한 전자상거래 표준 활동에 적극적인 참여를 통하여 표준 동향을 빠르게 인식하여야 하며 국내에서의 실천이 올바른 방향으로 나아갈 수 있도록 지원해야 할 것이다. 이러한 참여 없이는 확정되지 않은 표준안의 실천으로 더욱 혼란을 야기할 것이다.

또한 현재 실질적인 산업 부문간의 상호운영성의 표준화 완성도도 상당히 낮다. 상호운영성 대한 개념과 의도는 이미 알려져 있지만 그 실현을 위한 구체적인 방법에 대한 뚜렷한 성과가 없고 현재 각국에서 기존에 쓰여 오는 방식에 급급해 하고 있다. 상호운영성 표준화 작업은 이제 시작단계로 추진하고 있다. 이제 이런 표준화 작업을 실행하는 데는 국내기업에서의 표준화제정에 대한 여건이 충분치 안으며 기업간 정보공유를 회피하려는 기업적 속성도 문제가 되고 있다. 따라서 업종간의 공유체계를 확립하여 중복성 있는 요소에 대한 통합 적용 방안을 도출하여 업종간 DB통합 운영 시스템 등을 구축하도록 하여 업종간 문서 교환 시스템과 연동시키도록 해야 한다. 하지만 이런 통합 운영은 국가의 관리 기관을 통해서 표준화를 이루어 상호운영성의 문제를 해결해야 한다. 따라서 산업발주기관, 사업주관기관 및 표준 관련 기관들 간의 상호협력 체제가 구축되어야 한다.

그리고 위의 사항과 더불어 염두에 두어야 할 것은 표준화 기술 개발의 중복 문제이다. 현재 기술이 웹과 인터넷환경으로 변화되고 많은 전문영역과 학문이 세분화되면서 어느 한 집단이 표준을 제정하거나 수행하는 일은 사실상 불가능하게 되었다. 따라서 여러 단체들이 협력을 통해 일을 처리하면서 불가피하게 나오는 문제는 하나의 표준개발 업무가 중복된다는 것이다. 이런 중복의 문제는 물적, 질적 낭비를 초래할 뿐만 아니라, 개발 단체들 간에도 혼란을 일으킬 수도 있다. 그러나 상호 유기적으로 연동되는 요소 기술들을 완전히 분리하여 개발을 시행하는 것 또한 불가능하다. 그러므로 이런 중복의 문제를 완전히 제거가 아니라 최소화하는 방법에 중점을 두어야 한다. 법적 제도적인 관리가 가능한 기관들 간의 상호 협력과 개발자들을 위한 시스템이 체계적으로 이루어져야만 이 표준 개발의 중복을 피할 수 있고 이를 사용하는 기업들도 일관된 개발에 착수할 수 있다. 이는 시간과 업무효율을 증대시키는 요소와 직결된다. 또한 이를 위해 충분한 예산과 지원이 절대적으로 필요하다. 결론적으로 국내의 전자상거래 표준 관련기관들의 활동을 지원하기 위한 체제의 정비는 불가피하다. 법적, 제도적인 근거를 갖고 있는 기관이 표준화 관련 업무를 협력, 총괄하고 충분한 지원체제를 구축해야 중복성을 최소화한 일관성 있고 신속한 개발을 이룰 수 있을 것이다 [9].

4. 결론

국외 주요 국가들은 정보보호 기술에 대해 다양한 정보보호의 표준적합성 및 상호운영성 및 시험평가 기술을 개발하여 정부기관 및 민간 분야에서 테스트를 수행하고 있다. 국내의 경우 정보통신 관련 일부 제품에 대해서 시험평가를 진행하고 있으나, 정보보호 기술의 경우, 보안성 평가 분야를 제외한 표준 적합성 및 상호운영성 등은 체계적이고 일관된 기준 및 평가 체계의 부재로 좀 더 연구가 진행되어야 할 과제로 남아있다. 더욱이 정보보호제품에 대한 국외 선진국들은 표준 적합성 및 상호 운영성기술에 대한 공개가 미비하기 때문에 독자적인 기술 개발하는 것이 현실이다. 하지만 통합된 전자상거래 프레임워크를 위해서는 다른 국가와 더불어 표준안들의 제정과 개발이 다른 국가들에게도 확산되어 진정한 상호연동성을 보장하는 수평적인 개발이 이루어져야 한다.

따라서, 국내 정보보호기술에 대한 적절한 시험평가와 이에 기반을 둔 사용자들의 안정적인 제품 선택 및 사용, 나아가 세계 시장에서의 제품경쟁력 확보를 위해 국내외 정보보호기술에 충분히 적용될 수 있는 표준 적합성 및 상호운영성 기술의 개발 및 보급이 조속히 요구된다.

5. 참고문헌

[1] 차세대 전자상거래 표준화 웹사이트, http://www.ebxml.or.kr.

[2] XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/

[3] XML Encryption WG, http://www.w3.org/Encryption/2001/

[4] XML Key Management Specification (XKMS), http://www.w3.org/TR/xkms/

[5] Security Assertion Markup Language, http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf

[6] OASIS eXtensible Access Control Markup Language (XACML), http://www.oasis-open.org/committees/xacml/

[7] Simple Object Access Protocol (SOAP), http://www.w3.org/2000/xp/Group/

[8]http://www.oasis-open.org/committees/ebxml-iic/

[9] 김성혁, 한국전자거래 진흥원, 표준화 워킹그룹 보고서-전자상거래 통합 상호협력방안