

ebXML에서의 XML 기반 보안 기술 적용 연구

송준홍^o, 차석일, 김현희, 성백호, 신동일, 신동규
세종대학교 컴퓨터공학과

{song0424^o, kiry, hyunhee, guardia, dshin, shindk}@gce.sejong.ac.kr

A Study on XML based Security Technologies for ebXML

Jun-hong Song^c, Suk-il Cha, Hyun-hee Kim, Baek-ho Sung, Dongil Shin, Dongkyoo Shin
Dept. of Computer Engineering, Sejong University

요 약

인터넷을 통한 e비즈니스는 기존의 상거래 방식의 획기적인 변화를 가져왔고 향후 그 발전 가능성 또한 무한하다. 시간이나 규모, 지리적 위치의 제약에서 벗어나 원하는 전 세계 누구와도 거래를 가능케 하는 것을 목표로 시작된 ebXML 프레임워크는 현재 폭넓은 지지를 받으며 글로벌한 환경에서의 전자 상거래 표준 프레임워크로 발전하고 있다. 본 논문에서는 신뢰성 있는 비즈니스를 위한 ebXML에서의 보안 요구 사항을 분석하고 XML 기반 보안 기술의 적용 방안에 대해 살펴본다.

1. 서 론

전자 상거래의 성장은 시장 규모나 거래의 양에 있어서 매년 폭발적으로 증가하고 있으며, 거래 대상에 있어서도 자국 내에만 국한되지 않고 글로벌한 환경으로 확대되어 가고 있다. 이러한 상황에서 반드시 선결되어야 할 사항은 기업 및 국가 간의 상이한 거래 방식에 따른 비효율성과 비용증대의 문제이며, 이를 해결하기 위해 UN/CEFACT와 OASIS의 국제 기구가 주도하여 XML을 기반으로 범 세계적인 전자 상거래 프레임워크 표준을 개발하여 ebXML (electronic business eXtensible Markup Language)[1] 1단계 프로젝트 결과로서 2001년 5월에 발표하였다.

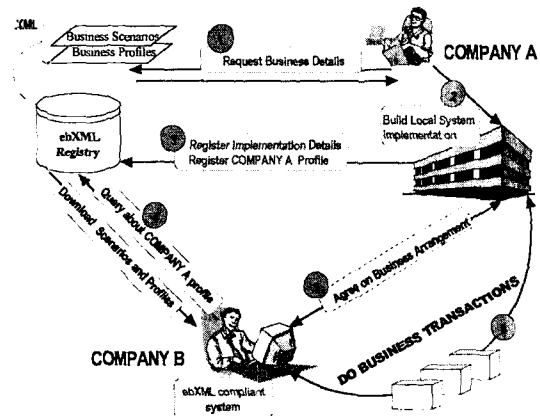
ebXML에서는 이미 승인된 기술명세 외에 향후 작업을 통해 기술명세로 발전시켜 나갈 기술보고서 중 보안 관련 보고서로 ebXML Security Team에서 제출한 "Technical Architecture Risk Assessment v1.0"과 Technical Architecture Security Team에서 제출한 "ebXML Registry Security Proposal"을 공개하였다. 이 보안 관련 보고서에서는 ebXML 메시지와 등록기/저장소(Registry/ Repository)의 상호 연동 시 보장되어야 할 각종 보안 요구사항을 어떻게 만족시킬 것인지에 대한 표준적 방법을 제시하고 있다.

본 논문에서는 ebXML의 개략적인 구조에 대해 살펴보고 메시징 서비스와 등록기/저장소를 중심으로 보안 위해 요소를 분석하고 ebXML에서 제안하고 있는 XML 기반 보안 기술들에 대해 살펴본 후 이 기술이 어떠한 측면에서 ebXML 보안 요구 사항을 만족 할 수 있는지에 대해 논한다.

2. 관련 연구

2.1 ebXML

ebXML은 기존의 전자 상거래 프레임워크 표준들과는 다르게 거래 당사자간의 송수신 메시지 형식뿐 아니라 각각의 비즈니스 프로세스와 분산된 등록기/저장소의 구축 모델까지 포함하는 포괄적인 시스템 구조를 제시하고 있다. 이러한 이유는 기존의 집중화된 시스템 적용 시 발생하는 각각의 거래 당사자별 비즈니스 프로세스 최적화 및 확장의 어려움 등의 문제를 극복하기 위한 것이며, 이를 위해 수평적(horizontal) 프레임워크를 정의하고 있는 것이다. ebXML에서의 거래 모델은 [그림 1]로 표현 할 수 있다.



[그림 1] ebXML 기반 거래의 개략적 수행 과정

2.2 XML 기반 보안 기술

ebXML에서는 송수신 메시지 및 등록기/저장소관련 보안 문제를 현재 표준화가 활발히 진행되고 있는 공개된 XML 기반 보안 기술을 적용해 해결할 것을 제안하고 있다. 아래에서는 현재 가장 중요한 XML 기반 보안 관련 기술들을 설명한다.

2.2.1 XML 전자 서명(XML Digital Signature)

XML 전자서명[1] 명세는 W3C와 IETF가 공동으로 표준화를 추진한 XML 기반의 전자서명 기술이다. 현재 XML 전자서명은 2월 14일부로 W3C에서 Recommendation 상태로 승격 시킴으로써 표준화가 완료된 상태이다[2].

XML 전자 서명 요소 중 주요 요소의 역할을 개략적으로 설명하면 아래와 같다.

- <SignatureValue> : 실제 전자 서명 값을 포함하는 요소이다.
- <SignedInfo> : 실제 서명할 자료에 대한 정보를 포함하는 요소이다.
- <KeyInfo> : 서명을 검증할 키에 대한 정보를 포함하는 요소로 인증서 정보를 포함 할 수 있다.
- <Object> : 어플리케이션에 종속적인 정보 포함하고 있는 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 전자서명의 경우 문서에 송신자가 생성한 다이제스트와 서명 값이 포함되어 있기 때문에, 수신자 측에서 송신자가 보낸 데이터를 메시지와 서명으로 분리하여 다이제스트 값을 계산할 필요가 없다는 장점을 갖고 있다.

2.2.2 XML Encryption

현재 인터넷 상으로 어떠한 데이터를 전송 할 때 IPsec나 SSL만으로도 충분한 데이터에 대한 기밀성을 보장 할 수 있으며 PGP나 S/MIME를 사용하면 송수신 및 저장 시 암호화를 수행 할 수 있다. 하지만, 이러한 방법은 데이터 전체에 대한 암호화를 수행함으로써 데이터의 일부만 암호화가 필요한 경우에는 부적절할 방법이다. 이에 따라 데이터 중 일부만을 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 Encryption[3]이다.

XML Encryption 처리 규칙 중 암호화 방식을 살펴보면 아래와 같다.

- ① 데이터를 암호화 하고자하는 알고리즘을 선택한다.
- ② 키를 얻는다.
 - 만일 키가 적당한 인증경로에 의해 확인 된 것이라면 ds:KeyInfo를 생성하여 적당한 경로를 생성한다.
 - 만일 키 자체가 암호화되어 있는 것이라면 암호화 과정에 적용 시켜 EncryptedKey 엘리먼트를 생성한다. 그리고 그 결과 값을 ds:KeyInfo에 적용시킬 수 있다.
- ③ 데이터를 암호화한다.
- ④ EncryptedType구조를 생성한다. 전체적인 암호화인자 특정 요소에 관한 암호화인자를 정하는 것이다.
- ⑤ 암호화된 데이터를 처리한다.
 - 복호화 하는 과정은 아래와 같다.
 - ① 알고리즘을 결정하는 요소를 처리한다. 여기서 ds:KeyInfo요소의 사용 여부를 확인한다.
 - ② ds:KeyInfo 요소에 따른 데이터 암호화키를 찾는다. 만일 키가 암호화되어 있다면 그것을 복구하여 찾아 복호화 준비를 한다.
 - ③ CipherData 요소에 포함되어 있는 데이터를 복호화 한다.
 - ④ Element 타입, Element Content타입인지를 알아내어 복호화 과정을 처리한다.

2.2.3 XKMS(XML Key Management Specification)

XKMS[4]는 마이크로소프트와 베리사인, 웹엑스드 사가 2001년 4월 W3C에 제안한 XML 기반의 공개 키 관리 명세이다. XKMS명세는 현재 Draft상태이며 최초 설계 목적은 XML 전자서명과의 연동 시 기존 PKI(Public Key Infrastructure) 시스템에 대한 복잡성을 클라이언트에게 숨겨 키 관리 부담을 트러스트 서비스(trust service)에 위임해 그 구현을 용이하게 하기 위함이었다. XKMS는 X-KISS(XML Key Information Service Specification)과 X-KRSS(XML Key Registration Service Specification) 2부분으로 구성된다.

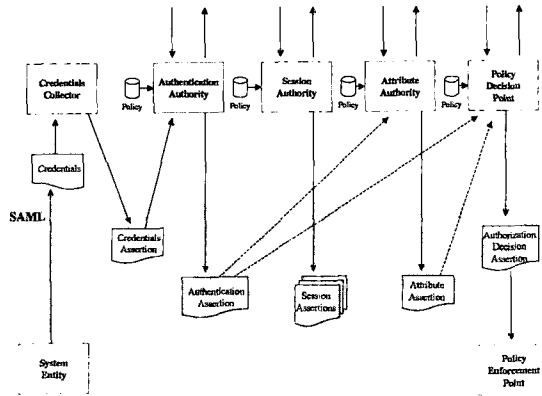
X-KISS는 티어 서비스 모델(tiered service model)로 구성되어 각각의 필요에 맞는 서비스를 구분해 요청 할 수 있다. 공개 키 쌍에 대한 관리리는 X-KRSS가 담당하면 주요 기능은

키 등록(key registration), 키 폐지(key revocation), 키 복구(key recovery) 등이다.

2.2.4 SAML(Security Assertion Markup Language)

SAML[5]은 OASIS의 STTC(Security Services Technical Committee)가 제안한 XML 기반의 인증(authentication) 및 승인(authorization) 정보를 안전하게 교환하기 위한 프레임워크이다.

[그림 2]는 SAML을 이용하여 시스템 엔티티가 접근 제한된 자원에 접근하는 유스케이스(use-case)의 흐름을 나타낸 것이다. 우선, 보증 정보(credential information)를 모아 credential assertion을 구성한다. 다음으로는 수집된 보증 정보를 이용해 사용자를 인증하게된다. 인증 시 authentication assertion을 전달하기 위해 외부 PKI 서비스를 이용할 수도 있다. 추가적인 요구에 따라 session assertion또는 authorization decision assertion 단계로 진행된다.



[그림 2] SAML 처리과정

2.2.5 XACML(XML Access Control Markup Language)

XACML[6]은 접근제어 리스트(access control list)를 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공할 수 있는 XML 기반의 언어이다. XACML은 SAML PDP(Policy Decision Point)의 일부로서 역할을 수행 할 수 있다. XACML의 정의에 따라 각각의 사용자 별 XML 문서 접근 정책을 수립하고 적용 할 수 있다.

XACML은 크게 <object>, <subject>, <action>의 3가지 요소로 구성되는데 subject는 사용자의 ID 나 그룹, 또는 역할 등을 나타낼 수 있으며, object 요소는 subject가 접근할 데이터를 의미하며 그 데이터 참조로서 단일 XML 문서에서 개별 요소 수준까지 지정 할 수 있다. action은 4가지 수행 가능 동작으로 구성되며 각각은 읽기, 쓰기, 생성, 삭제 작업이다.

XACML 명세는 현재 개발 중에 있으며 2002년 5월에 일반에 공개 할 예정이다.

2.3 ebXML 보안 요소 분석 및 XML 보안 기술 적용

이미 언급한 것과 같이 현재 ebXML 명세에서는 전체 시스템을 위한 완전한 보안 모델이 제시되지 않고 있으나, 위에서 살펴본 XML 기반의 보안 기술을 적용해 보안 요소를 해결하기 위한 노력이 진행되고 있는 상황이다.

아래에서는 "Technical Architecture Risk Assessment v1.0"에서 언급한 5가지 보안 문제를 살펴보고 ebXML 메시징 서비스 및 등록기/저장소 보안을 중심으로 XML 기반 보안 기

술의 적용 기법을 살펴본다.

2.3.1 ebXML 보안 요소 분석

ebXML에서의 보안은 모든 구성 요소를 포함하는 방법이 아니라 각각의 구성요소에 맞는 보안 위협 요소의 파악과 대응 기법을 중심으로 연구되고 있다. 현재 ebXML Security 팀에서는 ebXML Technical Architecture Risk Assessment v1.0 기술 보고서에서 ebXML의 보안 위해 요소(Risk)를 크게 5가지 범주로 나누어 기술하고 있다. 아래는 5가지 보안 위해 요소를 간략히 설명한 것이다.

① 비인가된 거래 및 사기 - ebXML은 개방된 네트워크인 인터넷을 이용하기 때문에 거래 메시지에 있어 무결성 검증과 거래 당사자의 인증 없이는 신뢰 할 수 있는 거래를 수행 할 수 없다.

② 기밀성 - 인터넷 상에서는 기밀성이 요구되는 메시지에 대해 각별한 주의를 필요로 한다.

③ 여러 감지 - 거래 메시지 처리 시 오류가 발생한다면 잘못된 메시지를 전송할 수 있기 때문에 거래 활동에 있어 지속성을 해칠 수 있다.

④ 관리 및 회계에 있어서의 잠재적 손실

거래 시 발생하는 각종 데이터에 대한 부주의한 처리는 추후 중요한 법적인 증거물로서의 역할을 수행 할 수 있다는 점에서 그 관리의 중요성을 인식해야한다.

⑤ 잠재적인 법적 책임

ebXML에서의 기본적인 보안 위해 요소라고 할 수는 없지만, 전자적 거래에 있어서 법적인 제도가 뒷받침이 되지 않는다면, 거래에 대한 근본적인 신뢰성에 문제가 될 수 있다.

2.3.2 ebXML 메시징 서비스 보안

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

메시징 서비스에서는 거래당사자들의 정보를 표현하는 CPP(Collaboration Protocol Profile)에 포함되어 있는 <ReliableMessaging> 요소와 <NonRepudiation> 요소를 통해 메시지 보안 요구를 MSH(Message Service Handler)에게 전달한다. <ReliableMessaging> 요소는 중복 전송을 막기 위한 정보 및 메시지 전송 순서 등을 명시 할 수 있는 속성을 가지고 있다. <NonRepudiation> 요소는 ebXML 메시지가 전자서명 된 경우 사용되며, 서명은 XML 전자서명 명세에 따라 생성된다. 이 요소는 비즈니스 트랜잭션 모두에 사용될 수 있다. 이러한 부인 방지에 대한 처리는 MSH내에서 이뤄질 수도 있으며, 별도의 어플리케이션에서 처리 할 수도 있다.

ebXML 명세에서는 자체적으로 전자서명 기법을 제공하지만, ebXML 메시지가 SOAP(Simple Object Access Protocol)[7] 컨테이너 내에 포함되는 것을 고려 할 때 SOAP 자체에서 지원하는 전자서명 방식[8]을 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. ebXML에서는 이때 요구되는 키 관리에 따른 제반 사항을 XKMS를 통해 수행하도록 제안하고 있다.

2.3.3 ebXML 등록기/저장소 보안

ebXML에서 등록기/저장소는 비즈니스를 수행하기 위한 정보의 등록, 발견, 저장 등을 위해 사용된다. 등록기/저장소는 비즈니스 수행을 위한 거래 당사자간의 합의문 및 각종 XML 문서들을 생성 및 저장하는 ebXML 시스템의 핵심 컴포넌트라는 측면에서 보안이 상당히 강조되어야 할 부분이다.

등록기/저장소 보안의 기본 요구사항은 아래와 같다.

- 인증 : 등록된 정보의 소유자 및 권한 인증
- 무결성 : 등록기/저장소 내에서의 등록 정보신뢰성 보장
- 기밀성 : 비인가된 사용자로부터 정보 보호
- 승인 : 사용자의 권한에 따른 정보 획득 제어

ebXML에서는 공개 키 인증서 기반의 전자서명을 통해 사용자 인증을 수행하고, 역할 기반 접근제어를 위해 ContentOwner, RegistryAdministrator, RegistryGuest 로 각 역할을 구분해 적용하며, MSH에서 제공하는 메시지 수준의 기밀성 및 암호화를 사용해 등록기/저장소 보안을 유지하도록 하고 있다.

3. 결론 및 향후 연구방향

ebXML은 규모나 지리적 위치에 제약 없이 인터넷을 통해 최소의 비용으로 비즈니스를 수행 할 수 있게 하는 포괄적인 프레임워크이다. ebXML의 채택 및 지원은 현재 빠른 속도로 증가하고 있으며, 국내에서도 향후 2~3년 내에 가장 유망한 e비즈니스 프레임워크로 전망되고 있다[9]. 하지만, 전자상거래에 있어 요구되어지는 각종 보안 요소를 간과한다면, 아예 비즈니스가 성립될 수 없음으로 보안 요구 사항에 대한 효과적인 대응책이 그 무엇보다 중요하다고 할 수 있다.

이에 본 논문에서는 ebXML의 메시징 서비스와 등록기/저장소를 중심으로 보안 요구 사항 분석을 수행하였고, 현재 적용 가능하거나 향후 개발 및 적용될 XML 기반의 보안 기술을 살펴봄으로써 ebXML 프레임워크에서 제안하는 신뢰성있는 비즈니스 지원 방안을 논의하였다.

향후 연구로는 분석된 요구 사항을 만족하는 실제 ebXML 시스템의 설계 및 구현을 통해 제안된 기법을 검증하고 추가적인 보안 취약 요소의 식별 및 대책에 대한 연구가 요구된다.

4. 참고 문헌

- [1] ebXML
<http://www.ebxml.org>
- [2] XML-Signature Syntax and Processing
<http://www.w3.org/TR/2002/R3C-xmldsig-core-20020212/>
- [3] XML Signature Press Release
<http://www.w3.org/2002/02/xmldsig-release-pressrelease.htm.en>
- [4] XML Encryption
<http://www.w3.org/Encryption/2001/>
- [5] XML Key Management Specification
<http://www.w3.org/2001/XKMS/>
- [6] Security Assertion Markup Language
<http://www.oasis-open.org/committees/security/>
- [7] XML Access Control Markup Language
<http://www.oasis-open.org/committees/xacml/index.shtml>
- [8] Simple Object Access Protocol
<http://www.w3.org/TR/SOAP/>
- [9] SOAP Security Extensions: Digital Signature
<http://www.w3.org/TR/SOAP-dsig/>
- [10] 김채미외 1인, "글로벌 e비즈니스 리더를 위한 ebXML", pp 307-310, 대경, 2001.11.