XML 정보보호 기술을 적용한 ebXML 보안 시스템의 설계

송준홍[0]* 김동수** 박범대** 윤정희** 신동일* 신동규*
세종대학교 컴퓨터공학과*, 한국전산원**
{song0424[0], dshin, shindk}@gce.sejong.ac.kr, {kimdsoo, parkbd, yunjh}@nca.or.kr

Design of ebXML Security System applying XML Information Security Technologies

Jun-hong Song[0]* Dongsoo Kim** Beomdae Park** Jeonghee Yoon** Dongil Shin* Dongkyoo Shin*
*Dept. of Computer Engineering, Sejong University
**National Computerization Agency

요 약

매년 폭발적 성장률을 유지하고있는 인터넷 기반의 B2B 전자상거래 분야는 현재 그 영역을 기업대 기업, 국가 대 국가의 영역으로 확대하고 있다. ebXML로 대변되는 차세대 XML 기반의 국제적 표준 전자상거래 프레임워크의 활발한 표준화를 통해 이는 더욱 가속화될 전망이다. 그러나 다양한 보안 요소를 만족하는 안전한 거래를 위해 선행되어야 할 XML 기반의 전자상거래 모델에 최적화된 보안 기술에 대한 연구가 다른 분야에 비해 미진한 것이 현실이다. 따라서 본 연구에서는 ebXML 메시징 및 등록기/저장소를 중심으로 보안 요소를 분석하고 XML기반의 보안 기술 적용 시스템을 설계함으로써 신뢰성 있고 안전한 ebXML 거래 모델을 제시한다.

1. 서 론

현재 ebXML[1]로 대변되는 XML 기반의 e-비즈니스 프레임워크 표준에 대한 관심은 그 어느 때 보다 높은 상황이다. 비즈니스의 주 대상인 기업뿐만 아니라 국가적 차원에서도 제도 및 경제적 지원을 아끼지 않고 있다. 이는 기존의 비즈니스 형태를 획기적으로 변화시켜 비즈니스에 대한 공간 및 시간의 제약을 극복하고 최소의 비용으로 최대의 효율을 낼 수 있는 차세대 전자상거래 프레임워크로 기대되기 때문일 것이다.

그러나 현재 대부분의 XML 기반 e-비즈니스 프레임워크의 연구 및 지원은 개별 적인 구성 컴포넌트의 세부 설계 및 구현 기술에만 집중되어 있는 것이 현실이다. 과거와는 달리 국내의 각종 IT 분야에서 보안 요소가 부가적인 요구 사항이 아닌 핵심 개발 요소라는 인식이 확대되어 가는 과정에서 e-비즈니스 프레임워크의 보안에 대한 연구가 미진 한 것은 균형있는 프레임워크 발전에 있어 걸림돌이 될 것이다.

따라서 본 연구에서는 ebXML 프레임워크 및 최근 급 부상하고 있는 차세대 비즈니스 프레임워크인 웹 서비스(Web Service)[2]에 적용될 수 있는 XML 기반의 정보보호 기술을 분석하고 ebXML 프레임워크 내에서 수행 가능한 비즈니스 프로세스 모델을 선택, 각각의 XML 정보보호 기술이 어떻게 보안 요구를 만족하도록 구성될 수 있는지를 논한다.

2. 관련 연구

2.1 ebXML 보안

공개된 네트워크인 인터넷을 사용하는 ebXML 프레임워크는 각종 보안 요구사항의 만족을 위해 모든 구성 요소를 포함하는 방법이 아닌 개별적인 구성요소에 따른 보안 위험 요소의 파악과 대응 기법을 중심으로 개념적인 가이드라인만이 제시되고 있는 실정이다.

ebXML 거래 모델에 있어 확장성 및 상호운용성 보장의 핵심 구성 요소인 메시징 서비스[3]의 보안은 현재 CPP(Collaboration Protocol Profile)를 통해 명시되며 거래 당사자간의 합의된 결과 문서(Collaboration Protocol Agreement)에 이를 포함함으로써 거래 당사자간의 메시지 보안 모델을 제공 할 수 있다[4]. 즉, MSH(Message Service Handler)내에서 메시지의 무결성 및 기밀성, 부인 방지를 위한 XML 기반의 정보보호 기술 적용을 통해 필수 보안 요구를 만족하게된다.

등록기 및 저장소[5]의 경우 거래에 필요한 각종 자료 생성 및 공유를 위한 핵심 역할을 수행함으로서 부적절한 접근을 식별하고 권한에 따른 자원 접근을 허용할 수 있어야 한다. 이를 위해 3가지 역할을 정의하고 각 역할에 따른 자원 접근의 정도를 제한하고 있다. 표 1은 각 역할에 따른 권한을 나타낸다.

표 1 등록기/저장소 역할 및 권한

역 할	설 명	권 한
ContentOwner	등록기 컨텐츠 제공자	자신소유의 모든객체 접근
RegistryAdministrator	등록기 관리자	등록기 내의 모든 객체 접근
RegistryGuest	인증되지 않은 사용자	허용된 모든 객체의 읽기 전용 접근

자원에 대한 접근 제어 뿐 아니라 등록/저장되어 있는 자원에 대한 무결성 및 기밀성 보장 또한 고려되어야 할 보안 요구사항이다. 현재 영구적인 무결성 및 인증, 기밀성 보장을 위해 XML 기반의 정보보호 기술 적용이 권장되고 있다.

2.2 XML 정보보호 기술

XML 기반의 거래 프레임워크가 활성화에 따라 기존거래 방식에 적용되었던 보안 기술에 대한 비효율성 대두되고 있다[6]. 이에따라 현재 W3C 및 OASIS를 중심으로 XML 기반의 정보보호 기술 표준화가 활발히 진행 중이다.

2.2.1 XML 전자 서명(XML Digital Signature)

XML 전자서명[7]은 XML의 장점인 구조적 정보 표현 능력 및 확장성을 기반으로 한 전자서명 기술로서 W3C와 IETF의 공동 표준이다. 기존의 전자서명의 경우 단일 홉(Single-hop) 메시지 전송에 적합한 메시지 인증 기능을 제공하지만 XML 전자서명의 경 우 단일 XML 문서에 대한 다수의 전자서명을 포함할 수 있어 다중 홉(Multi-hop) 메시지 전송 모델 적합한 기술이다. 이러한 특징은 전자상거래 관련 메시지가 최종 목적지에 도달하기 전 여러 중간 경유지의 메시지 인증이 필요한 경우 매우 유용하다. 또한 XML 문서 전체에 대한 전자서명 뿐 아니라 개별적인 요소 또는 요소의 내용 자체에 세부적으로 전

자서명을 수행 할 수 있다. 서명 생성을 위한 자원의 제한 역시 없으며 이진 데이터형식이면 무엇이든 전자서명 생성이 가능하다.

XML 전자서명은 현재 ebXML 메시지의 인증 및 무결성을 위한 표준 기술로 적용되고 있다.

2.2.2 XML Encryption

인터넷 상에서 메시지 기밀성 보장 기술로서 폭넓게 사용되고 있는 기술인 IPSec이나 SSL, PGP, S/MIME 등은 전송하려는 데이터 전체에 대한 암호화를 수행함으로써 데이터의 일부만 암호화가 필요한 경우에는 비효율적인 방법이다. 이에 따라 데이터 중 일부분만을 암호화해 중간에 경유하게 되는 제 3자에게 특정 정보를 노출시키지 않으면서 최종 수신자에게 전달할 수 있는 방법으로 현재 W3C에서 XML 기반의 표준화를 추진하고 있는 것이 XML Encryption[8]이다. XML Encryption은 XML 전자서명의 다중 홉 전송에 따른 특징을 그대로 가지며 암호화 수행의 대상에도 제한이 없다. XML 전자서명과 통합 적용을 통해 송수신 메시지에 대한 기본적인 보안 요구를 만족시키기 위해 최적화되어 있다.

XML Encryption은 표준화가 완료되는 시점을 기준으로 ebXML 메시지 기밀성 보장을 위한 표준 기술로 채택될 전망이다.

2.2.3 XKMS(XML Key Management Specification)

XML 전자서명 및 XML Encryption을 이용하는 클라이언트 어플리케이션은 전자서명 검증이나 암복호화를 위한 공개키 정보의 처리를 위해 기존 PKI(Public Key Infrastructure) 시스템과의 연동이 필수적이다. 하지만 이는 클라이언트 시스템의 복잡도를 높여 구현에 대한 부담을 가중 시킨다. 이에 PKI 시스템을 클라이언트에게 숨겨 키 관리 부담을 트러스트 서비스(trust service)에 위임함으로써 그 구현을 용이하게 하기 위해 등장한 것이 XKMS[9]이다. XKMS는 X-KISS(XML Key Information Service Specification)과 X-KRSS(XML Key Registration Service Specification) 두 부분으로 구성된다.

X-KISS는 공개키의 획득 및 검증 서비스를 제공하는 티어 서비스 모델(tiered service model)로 구성되어 각각의 필요에 맞는 서비스를 구분해 구현 할 수 있다. 공개 키 쌍에 대한 관리는 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[10]은 OASIS의 STTC(Security Services Technical Committee)에서 표준화가 진행 중인 XML 기반의 인증(authentication) 및 승인(authorization) 정보를 안전하게 교환하기 위한 명세이다. SAML은 현재 SSO(Single sign-on) 처리 및 e-비즈니스 프로세스내의 사용자의 인증 및 승인 정보 전달을 가능케 하는 표준적인 기술로서 WS-Security[11] 및 Liberty Alliance 프로젝트[12]에서 표준으로서 채택했다. 현재 버전 1.0이 OASIS Committee 명세 단계이다.

2.2.5 XACML(XML Access Control Markup Language)

지속적으로 증가하는 XML 기반의 데이터들에 대한 접근 제어는 기업 및 서비스 제공자에게 있어 필수 보안 요구 사항이다. XACML[13]은 접근제어 정책을 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공 할 수 있는 XML 기반의 언어이다. XACML은 SAML PDP(Policy Decision Point)의 일부로서 역할을 수행 해 최종적인 자원 접근 요청에 대한 결과를 생성한다. 할 수 있다. XACML의 정의에 따라 각각의 사용자 별 XML 데이터 접근 정책을 수립하고 적용 할 수 있다.

XACML 명세는 현재 OASIS에서 개발 중에 있으며 Draft상태이다.

3. ebXML 보안 시스템의 구조

본 연구에서 설계한 시스템은 기본적인 ebXML 시스템의 비즈니스 시나리오를 신뢰성 있는 환경에서 수행 할 수 있는 시스템을 목표로 하며, 등록기/저장소 및 메시지 보안 측면에 중점을 두어 설계하였다. 시스템의 대략적인 구조는 아래의 그림 1과 같다.

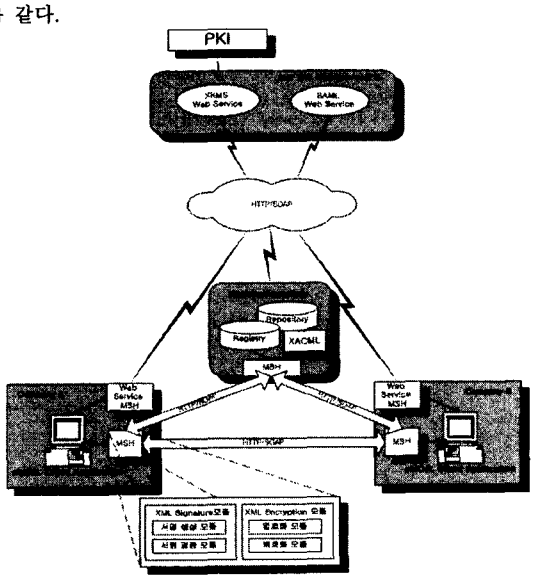

그림 1 ebXML 보안 시스템 전체 구조

XML 전자서명 및 암복호화 기능은 클라이언트 어플리케이션 및 Reg/Rep, XKMS 및 SAML 웹 서비스의 MSH(Message Service Handler)에 위치해 송수신 메시지에 대한 인증 및 암복호화 작업을 수행하게된다. 이때 서명 생성 및 검증, 암복호화 시 필요한 PKI 서비스는 XKMS 웹서비스에서 처리하게된다. XKMS 웹 서비스를 ebXML 시스템과 별도의 웹 서비스 모델로 구현함으로써 기존의 웹 서비스 어플리케이션에도 호환성 있는 PKI 서비스를 제공해 줄 수 있다. SAML 웹 서비스는 등록기/저장소의 정보 저장 및 변경 등의 작업 요청 시 요구자의 인증 및 승인을 위한 정보를 제공해 자원 접근제어를 수행하게된다. 이때 실제적인 접근 제어 정보는 XACML에 정의되며 XML 요소에 대한 세부 접근 제한을 가능하게 한다.

주요 보안 모듈의 내부 구성은 다음과 같다.

- ebXML Client MSH
  ebXML의 메시지 처리기 역할을 수행하며 본 시스템에서는 메시지 보안을 위한 XML 전자서명 및 암복호화 기능을 포함한다.
- XKMS 웹 서비스 모듈
  웹 환경에서 클라이언트가 처리해야할 PKI 관련 프로세스를 별로의 독립적인 웹 서비스로 제공함으로써 클라이언트의 PKI 요구 처리 부하를 최소화하는 역할을 수행한다.
- SAML 웹서비스 모듈
  등록기/저장소의 각 이용자에 따른 인증 및 권한에 따른 작업 허용 여부를 결정하는 역할을 수행 한다. 아래 각각의 모듈은 SAML 주장을 생성, 처리한다.
- ebXML Reg/Rep MSH 모듈
  ebXML을 기반으로한 거래 당사자들의 인증 정보 및 CPP를 저장, 관리하며 Reg/Rep내의 자원에 대해 XACML 문서에 기반 한 접근 제어를 수행한다.

• XACML 처리 모듈
클라이언트로부터 제한된 자원에 접근하기 위한 요청이 수신된 경우 Reg/Rep모듈이 XACML로 SAML 주장 처리 요청을 전달한다. SAML 처리 결과에 따라 최종 승인 주장을 생성해 낸다.

4. 시스템 수행 시나리오

ebXML 클라이언트가 ebXML Reg/Rep에 등록된 자신의 CPP를 수정하기 위한 과정을 수행한다. 이때 각 메시지 송수신 단계에 따라 위에서 정의한 보안 모듈을 적용하여 보안 요구를 만족하는 비즈니스 프로세스를 구현한다.

각 구성 모듈 별 메시지의 흐름 및 역할은 그림 2를 통해 설명한다.

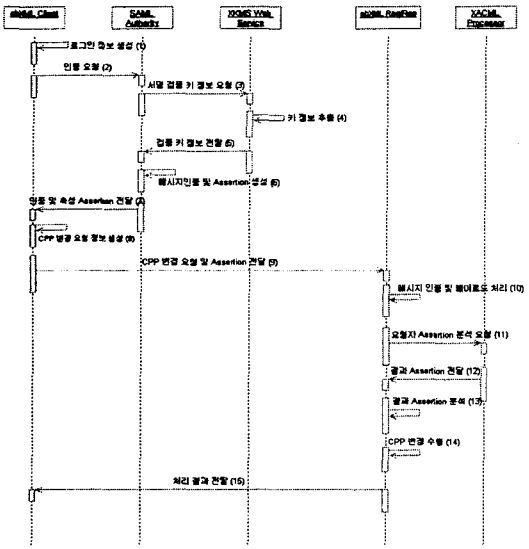

그림 2 시스템 수행 시나리오

(1) 로그인 정보 생성 : 클라이언트는 패스워드 기반의 인증을 위해 사용자로부터 ID와 패스워드를 입력받아 로그인 메시지를 생성.
(2) 인증 요청 : 생성된 로그인 메시지를 SAML 웹 서비스에 전달.
(3) 서명 검증 키 정보 요청 : XKMS 웹 서비스에 클라이언트 공개키 정보를 XML 요청 프로토콜에 따라 요청.
(4) 키 정보 추출 : 수신한 클라이언트 정보를 통해 공개키 정보를 PKI 역할을 수행하는 키 저장소에서 추출.
(5) 검증 키 정보 전달 : 추출된 클라이언트의 공개키 정보는 XKMS 응답에 따라 SAML 웹 서비스에 전달.
(6) 메시지 인증 및 Assertion 생성 : 전달받은 공개 키 정보를 이용해 클라이언트의 메시지를 인증하고 로그인 정보를 복호화해 해당 사용자가 있을 경우 적절한 인증 및 속성에 대한 Assertion을 생성.
(7) 인증 및 속성 Assertion 전달 : 생성된 Assertion을 클라이언트로 전달.
(8) CPP 변경 요청 정보 생성 : 수신한 Assertion과 변경할 CPP 문서 및 변경 요청을 결합하여 메시지를 구성.
(9) CPP 변경 요청 및 Assertion 전달 : 재구성한 메시지를 Reg/Rep로 전달한다
(10) 메시지 인증 및 페이로드 처리 : 수신한 메시지의 Assertion을 분석 처리 후 요청 분석. CPP 변경 요청이 Reg/Rep의 컨텐츠 소유주(ContentOwner)역할 만이 가능한 작업이므로 XACML 처리기의 결과를 얻은 후 작업을 수행.
(11) 요청자 Assertion 분석 요청 : 클라이언트의 속성 Assertion을 XACML 처리기에 분석을 요청.
(12) 결과 Assertion 전달 : XACML 처리기는 입력으로 받아들인 Assertion의 속성을 Policy 문서와 비교해 승인 Assertion을 생성 후 전달.
(13) 결과 Assertion 분석 : Reg/Rep는 XACML 처리기로부터 얻은 승인 Assertion을 분석 후 작업을 진행.
(14) CPP 변경 수행 : Assertion 분석 결과에 따라 기존 CPP 문서를 변경.
(15) 처리 결과 전달 : CPP 변경 작업의 성공/실패 메시지를 클라이언트에 전송.

수행 단계 별로 적용된 각각의 보안 모듈은 CPP변경 수행 업무 뿐 아니라 ebXML 메시징 서비스를 이용하는 기타 비즈니스 프로세스에도 그대로 적용 할 수 있다.

5. 결론

ebXML은 기존의 EDI 방식의 거래 모델의 비효율성을 개선하고 상호운용성을 극대화하기 위해 기업 및 정부 차원에서 표준화 및 관련 기술의 개발이 활발히 진행되고 있다.

하지만 현재의 ebXML 적용 연구 및 개발은 주로 실제 거래를 수행하는데 필요한 컴포넌트에 집중되어 있어 상대적으로 기본 전제가 되어야 할 보안 기술에 대한 관심이 부족한 상태이다.

이에 따라 본 연구에서는 ebXML에 적용될 수 있는 XML 기반 정보보호 기술에 대한 분석을 수행했으며 ebXML 거래 모델을 따르는 시나리오를 구성하여 각 거래 단계별로 요구되는 보안 기법을 분석하고, 이에 따라 XML 기반 정보보호 기술을 적용한 ebXML 시스템을 설계하였다.

향후 연구로는 기 설계된 ebXML 기반의 거래 시스템 S/W를 구현해 실제 시스템 운용에 있어 적용 가능한 보안 모델을 제시하고 평가함으로써 ebXML 프레임워크에 최적화된 보안 시스템 구조를 제안하는 것이다.

참고문헌

[1] ebXML, http://www.ebxml.org
[2] Web Service, http://www.w3.org/2002/ws/
[3] ebXML Message Service Specification v1.0, http://www.ebxml.org/specs/ebMS.pdf
[4] 송준홍, 차석일, 김현희, 성백호, 신동일, 신동규 "ebXML에서의 XML보안기술 적용 연구" 한국정보과학회 학술발표논문집(B), 제29권, 제 1호, pp796~798, 2002.
[5] ebXML Registry Services Specification v1.0, http://www.ebxml.org/specs/ebRS.pdf
[6] Getting Started With XML Security, http://home.earthlink.net/~fjhirsch/xml/xmlsec/starting-xml-security.html
[7] XML Signature Specification, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
[8] XML Encryption, http://www.w3.org/Encryption/2001
[9] XML Key Management Specification, http://www.w3.org/2001/XKMS/
[10]SAML, http://www.oasis-open.org/committees/security
[11]WebServiceSecurity(WS-Security), www.verisign.com/wss/wss.pdf
[12] Liberty Alliance Project, http://www.projectliberty.org
[13] XML Access Control Markup Language, http://www.oasis-open.org/committees/xacml/index.shtml.