XML 보안을 위한 암호 API 설계

반용호[0] 서철우 김종훈
동아대학교 컴퓨터공학과
우 부경대학교 전자계산학과

gaussian@donga.ac.kr

Design of Crypto API for XML Security

Yong-Ho Ban[0] Sur Chul우 Jong Hoon Kim
Dept. of Computer Engineering, Dong-A University
우 Dept. of Computer Science, Pukyong University

요 약

최근 XML에 관련된 여러 가지 보안기술에 관한 연구가 진행되고 있다. 본 본문에서는 XML 표준화 단체에서 규정한 XML 전자서명과 XML 암호화 표준 명세서를 준수하는 XML 보안 API를 설계하고 구현한다. 본 논문에서 제안된 시스템은 표준 명세서에서 요구하는 암호 알고리즘 및 국내 표준 암호알고리즘과 공개키 인증서를 처리 할 수 있도록 설계하였다.

1. 서 론

인터넷 e-비즈니스 시스템들의 상호 운영성을 확보하기 위하여 e-비즈니스 시스템 개발 회사들과 이용자 회사들은 UN산하 CEFECT와 XML 관련 표준화 단체인 OASIS가 공동으로 e-비즈니스 공용 프레임워크에 관한 국제 표준인 ebXML 명세서들을 제정하여 발표하였다. 표준 명세서는 공용 프레임워크의 기반 기술로 XML 기반의 통합 기술을 채택, 즉 e-비즈니스 시스템들은 비즈니스 문서와 비즈니스 연산(operations)들을 XML로 표현한 메시지들의 교환을 통하여 비즈니스를 수행하도록 하고 있다. 또한 표준 명세서에서는 상호 교환하는 XML 비즈니스 문서에 XML 디지털 서명을 반드시 포함시키도록 권고하고 있으며, 이는 e-비즈니스 시스템들이 XML 디지털 서명을 작성하거나 검증할 때 XML 디지털 서명의 구문과 처리 과정을 기술하고 있는 국제 표준인 W3C/IETF의 "XML digital signature Syntax & Processing" 명세서에서 정의한 규칙과 절차를 따르도록 권고하고 있다. 따라서 향후 XML을 채택하는 *e-Biz* 시스템은 기본적으로 XML 디지털 서명기술 및 XML 암호 기술을 기본적으로 고려 할 것으로 예상되어지며, 이에 대한 연구의 필요성의 인식과 함께 국·내외에서 XML 보안 기술에 대한 활발한 연구가 진행되고 있다.[1][2][3][7][8][9][10] 본 논문에서는 XML 표준화 단체에서 정의한 XML 전자서명 표준 명세서와 XML 암호화 표준 명세서를 준수하는 XML 보안 API인 XCrypto를 설계하고 구현한다. 본 논문에서 제안된 시스템은 표준 명세서에서 요구하는 암호 알고리즘 및 국내 표준 암호알고리즘과 공인인증서를 처리 할 수 있도록 설계하였다.

2. 관련 연구

2.1 XML 문서의 보안 요구 사항

최근 XML은 B2B 와 B2C와 같은 기본적인 응용뿐만 아니라 XML-EDI, eBX, 전자 금융 서비스를 위한 OFX, IFX 등에 모두 적용할 수 있는 기술로 각광 받고 있다. 그러나 이와 같은 전자 응용 서비스에 XML 기술을 적용하기 위해서는 기존의 전자상거래 시스템과 마찬가지로 XML 기술에 대하여, 다음과 같은 보안성의 고려가 필요하다.

- 기밀성(*Confidentiality*) - 전송되는 거래전문의 일부 또는 전부를 송신자 및 적법한 수신자를 제외한 제3자는 볼 수 없도록 하는 기능을 의미한다. B2B 또는 B2C 서비스에서 은행으로 전송되는 사용자 계좌번호, 계좌이체 승인번호 등에 대해서는 반드시 기밀성이 보장되어야 한다.
- 인증, 무결성(Authentication, Integrity) - 전자 응용 서비스에서 사용자 인증은 원격지에서 접속한 사용자가 정당한 사용자임을 증명하는 것을 말하고, 메시지 인증은 원격지에서 전송된 거래전문이 위, 변조되지 않았음을 증명하는 것을 말한다. 일반적으로 인증이라 함은 사용자 인증을 말하는 것이며, 거래전문에 대한 인증은 무결성으로 대치될 수 있다. B2B와 B2C 같은 서비스에서는 공개키 인증서와 전자서명을 통하여 사용자와 전송되는 전문에 대한 인증 및 무결성을 보장하게 된다.
- 승인(Authorization) - 거래요청에 대하여 상대방의 거래를 인증하고 이에 대한 처리 결과를 거래 요청자에게 통보하는 것을 의미한다. 승인에 대한 유효성 확보는 권한을 가진 승인자가 거래 사실의 결과를 전자서명 후, 거래 요청자에게 통보함으로서 이루어진다.
- 부인방지(Non-Repudiation) - 부인방지는 메시지를 송, 수신하는 경우 해당자가 송, 수신에 대한 행위를 부인할 수 없도록 하는 기능을 말한다. 송신자의 부인방지를 위해서는 송신자가 생성한 거래전문에 대한 전자서명을 요구함으로서 가능하나, 수신자 측의 전문 수신 후 부인방지를 위한 기법에 대한 연구는 향후에 더 이루어져야 할 것으로 보여진다.

앞에서 언급한 바와 같이 B2B 또는 B2C와 같은 전자거래에서 거래 내용의 기밀성을 보장하기 위한 기술은 암호화로 귀결되며, 거래 상대방의 신원확인, 거래내용의 위, 변조방지, 승인, 거래사실의 부인방지 등을 보장해 주는 기술은 전자 서명으로 귀결된다. 현재 XML 문서 보호를 위한 W3C 표준은 전자서명, XML 암호화, 키 관리 등으로 각기 분리되어 제안 혹은 표준화 단계에 있으나, 실제적인 응용 서비스 구현을 위해서는 각 표준 명세서를 통합한 시스템에 관한 연구가 이루어져야 한다.

2.2 XML 전자서명 표준 명세서의 요구사항

W3C/IETF의 "XML digital signature Syntax and Processing" 명세서에는 XML문서에 대한 전자서명을 표현하고 생성하기 위한 XML 문법과 처리 규정을 정의하고 있다. XML 전자서명은 XML 형태로 표현된 문서에 대한 무결성, 메시지 인증, 서명자의 인증 등 XML 문서의 보안 요구 사항 중 기밀성을 제외한 인증, 무결성, 승인, 부인방지 서비스를 제공한다. 명세서에서 정의한 XML 전자서명 문서의 구조는 <Signature> 요소가 전송 문서의 최상위 요소로 되는 Enveloping Signature, <Signature> 요소가 XML 문서 내부에 포함되어 하위 요소로 구성되는 Enveloped signature, XML 문서가 전자서명 된 문서와 따로 분리되어 전송되는 Detached Signature등이 존재한다. XML 문서의 정규화는 W3C에서 규정한 "Canonical XML version 1.0" 명세서에 정의한 방법에 따라 이루어진다.[5] 또한 XML 전자서명 명세서는 전자서명에 사용되는 다양한 알고리즘을 정의하고 있는데, 메시지 다이제스트를 위해서 SHA-1 해쉬 알고리즘의 구현을 요구한다. 인코딩 방식은 Base-64 방식을 요구하며, 메시지 인증을 위한 MAC 은 HMAC-SHA1의 구현을 필요로 한다. <SignatureMethod>에서 사용하는 서명 알고리즘은 DSAwithSHA1의 구현을 필수적으로 요구하며, RSAwithSHA1이 권고되고 있다. XML 문서의 정규화를 위한 정규화 방식은 Canonical XML(omits command)의 구현을 요구하며 문서 변환 방식은 Enveloped Signature의 구현을 필수적으로 요구한다. 표 1은 XML 전자서명 명세서에 정의된 알고리즘 및 구현 요구사항을 보여준다.[1][2][4][5][6]

표 1. XML 전자서명 알고리즘 식별자 및 구현 요구사항

알고리즘 유형	세부 알고리즘	구현 여부
Digest	SHA1	필수
Encoding	base64	필수
MAC	HMAC-SHA1	필수
Signature	DSAwithSHA1(DSS)	필수
	RSAwithSHA1	권고
Canonicalization	Canonical XML (omits comments)	필수
	Canonical XML with Comments	권고
Transform	XSLT	선택
	XPath	권고
	Enveloped Signature	필수

2.3 XML 암호화 표준 명세서의 요구사항

XML 암호화에 관련된 표준화를 위해 W3C/IETF의 "Encryption Syntax and Processing" 명세서에는 평문으로 구성된 XML문서를 암호화하여 암호문을 생성하고, 암호문을 평문 데이터로 복구하기 위한 문법과 처리 규정 및 지정된 수신자가 암호문을 복호화 하기 위해 필요로 하는 정보를 표현하기 위한 XML 문법을 정의하고 있다. 또한 암호화된 XML 문서의 표현 방법에 대한 규정, 암호화된 정보의 전송문제, XML의 암호화를 위해 필요한 알고리즘 등을 규정하고 있다.[6][7][8] 그림 1은 XML 문서의 암호화 과정을 보여준다.

3. XML 보안을 위한 암호 API 설계

3.1 시스템 설계 및 구현상의 주요 특징

본 논문에서는 XML 표준화 단체에서 정의한 XML 전자서명 표준 명세서와 XML 암호화 표준 명세서를 준수하는 XML 보안 API를 설계하고 구현한다. 본 논문에서 제안된 시스템은 표준 명세서에서 요구하는 암호 알고리즘을 지원할 수 있도록 할 뿐만 아니라 국내 표준 암호알고리즘인 SEED, 전자서명 알고리즘인 KCDSA, 그리고 국내 공인인증기관에서 발행하는 공인인증서를 기반으로 전자서명을 수행 할 수 있도록 각 모듈을 패키지화하여 전체적인 모듈로 설계 및 구현하였다. 또한 본 논문에서 제안된 시스템은 향후에 추가되는 암호알고리즘 및 전자서명 알고리즘을 수용할 수 있는 SPI(Service Provider Interface) 개념을 도입하여 시스템이 충분한 확장성을 가질 수 있도록 설계하였다. XML 전자서명(XML-DSIG) 모듈의 설계에서 W3C 명세서의 규정 중 고려된 주요 요소들 중 Detached, enveloping, enveloped 유형의 전자서명 생성, Canonical XML 1.0 (XML-C14N)을 지원하고, SHA-1 및 HAS-160 메시지 다이제스트 알고리즘을 사용 가능하도록 설계하였다. 전자서명 알고리즘은 RSA withSHA1과 DSAwithSHA1 및 KCDSA를 지원 가능하다. <KeyInfo> 요소에 사용 가능하도록 RSAKeyValue, DSAKeyValue, X509Data, rawX509Certificate를 지원하도록 하였다. XML 문서의 효율적인 변환을 위한 XSLT 및 XPath를 위한 모듈을 별도로 구성한다. XML 문서의 전송에서 처리의 효율성을 위하여 Base64 인코딩/디코딩이 기본적으로 가능하도록 하였다. XML 암호화를 처리하기 위한 모듈에서 고려된 부분은 다음과 같다. XML 문서의 암호화와 이를 복호화하고 (임의의 데이터, XML 엘리먼트, XML 엘리먼트의 내용), 이를 XML 형태로 그 결과를 표현할 수 있도록 시스템을 구성하였다. 또한 지정된 수신자에 암호화에 필요한 키와 이를 전할 전달 할 수 있는, 키 생성 및 키 암호화에 필요한 알고리즘을 지원할 수 있도록 하였다. 본 시스템은 대칭키 암호 알고리즘으로 Triple-DES, AES-128-256, SEED를 지원하고, 키 전송을 위한 RSA1.5 알고리즘과 RSA-OAEP를 지원한다. 또한 SHA1, SHA256, SHA512, HAS-160 메시지 다이제스트 알고리즘을 수용할 수 있도록 설계하였

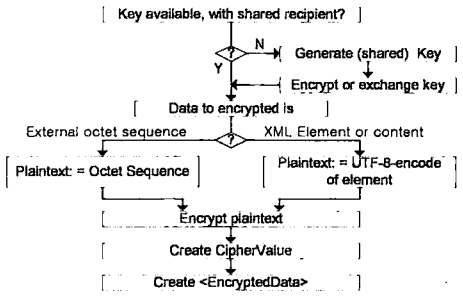

그림 1. XML 문서의 암호화 과정

표 2. 시스템 모듈별 구성

수행모듈 구분	주요 기능	명세서
Signature Generator	XML 문서에 대한 전자서명 생성 기능 수행 모듈	DSIG
Signature Verifier	전자서명 된 XML 문서에 대한 전자서명 검증 기능 수행 모듈	DSIG
Encryption Generator	XML 문서에 대한 암호화를 수행하는 모듈	XER
Decryption Processing Module	암호화 된 XML 문서에 대한 복호화를 수행하는 모듈	XER
Canonicalization Processing Module	전자서명 또는 암호화 수행 이전·이후 XML 문서의 정규화 수행	Canonical
Transform Processing Module	문서의 암호화·복호화 또는 전자서명 생성·검증 후, 처리 결과를 외부의 요구 사항에 따라 변환기능 수행	common
Certificate Handling Module	전자서명 또는 암호화 모듈 수행 시 요구되는 공개키 인증서의 정보를 추출하고 인증서를 검증하는 기능을 수행하는 모듈	--

으며, Diffie-Hellman 키 교환 프로토콜을 지원 할 수 있도록 하였다. 표2는 제안된 시스템의 모듈별 구성을 보여준다.

3.2 시스템 구성 및 운영 환경

본 논문에서 제안된 시스템은 windows2000 환경에서 J2SDK 1.3 및 JSDK1.4를 기반으로 구현하였다. 본 논문에서 DISG와 XML 암호화를 위한 API(XCrypto AIP)는 그림 2와 같이 구성된다. 본 논문에서 구현된 시스템은 Toolkit 형태의 API로 작성되어 있기 때문에 XML을 기반으로 하는 B2B 와 B2C 응용서비스를 위하여 기존의 B2B 업무 처리 트랜잭션 내부에 기밀성과 전자서명과 같은 보안 서비스를 요구하는 부분에서 해당 서비스를 제공하는 API를 호출함으로 해당 서비스를 제공받을 수 있다. 그림 2는 제안된 시스템의 구현 환경을 보여준다.

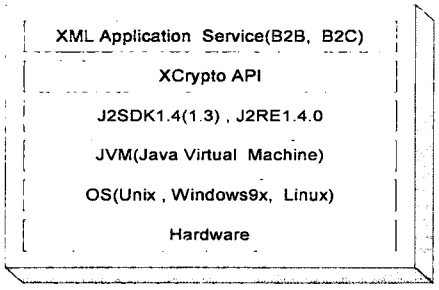

그림 2. 시스템 구성 및 운영 환경

그림3은 제안된 시스템의 전체적인 패키지의 계층도를 보여준다. 제안된 시스템은 xcrypto 모듈하부에 전자서명을 위한 dsig 모듈과 암호화를 위한 enc 모듈, 키를 생성하고 관리하기 위한 key 모듈, JCE(Java Cryptography Extension)와 연동을 위한 provider 모듈로 구성된다.

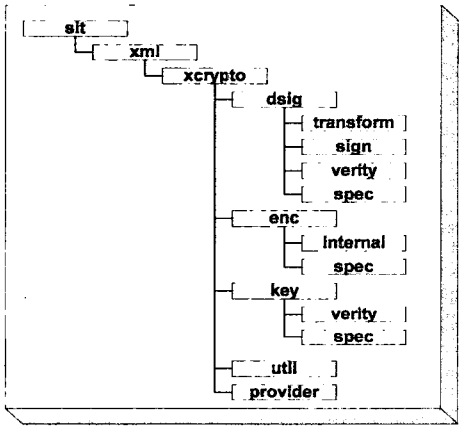

그림 3. XCrypto 시스템 모듈 계층도

3.3 XCrypto의 XML 문서 처리절차(XML 전문의 암호화)

XCrypto 기반 XML문서 처리절차는 다음과 같은 형태로 이루어진다. 먼저 응용 프로그램에서 XML 문서를 생성하고, 계좌번호, 계좌비밀번호와 같은 기밀성을 요구하는 엘리먼트를 암호화하기 위하여 XML 문서를 직렬화(serialization) 하고, 직렬화 된 XML 문서를 비밀키 암호 알고리즘으로 암호화를 수행후, 암호화에 사용된 키를 수신자의 공개키로 암호화하여, 이들 정보를 취합하여 <EncryptedData>를 생성하여 암호화된 XML 문서를 생성한다. 그림 4는 앞에서 설명한 XML 형태의 전문을 암호화하는 과정을 보여준다.

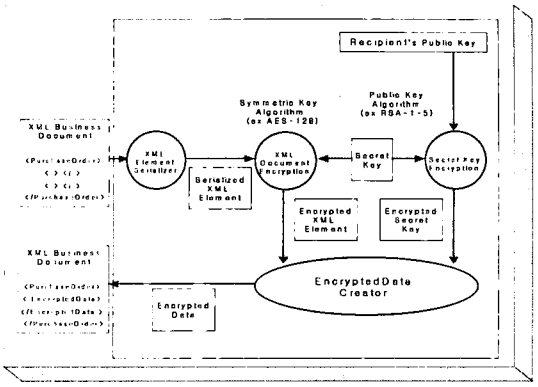

그림 4. Xcrypto 기반 암호화 처리절차

4. 결 론

본 논문에서는 XML 표준화 단체에서 정의한 XML 전자서명 표준 명세서와 XML 암호화 표준 명세서를 준수하는 XML 보안 API를 설계하고 구현하였다. 본 논문에서 제안된 시스템은 표준 명세서에서 요구하는 암호 알고리즘을 지원할 수 있도록 할 뿐만 아니라 국내 표준 암호알고리즘인 SEED, 전자서명 알고리즘인 KCDSA, 그리고 인증기관에서 발행하는 공개키 인증서를 기반으로 전자서명을 수행 할 수 있도록 각 모듈을 패키지화하여 전체적인 모듈로 설계 및 구현하였다. 또한 본 논문에서 제안된 시스템은 향후에 추가되는 암호알고리즘 및 전자서명 알고리즘을 수용할 수 있도록 SPI(Service Provider Interface) 개념을 도입하여 시스템이 충분한 확장성을 가질 수 있도록 설계하였다. 본 논문에서 제안된 시스템은 B2B, B2C와 같은 기본적인 응용에 적용 가능할 뿐만 아니라, XKMS, XACL(XML Access Control Language), XML 보안 프로토콜 등의 연구에 많은 도움을 줄 수 있을 것으로 예상된다. 향후 연구 과제로는 본 논문에서 제안된 시스템을 기반으로 XML 문서의 안전한 전송을 위한 XML 보안 프로토콜, XACL 등에 관한 연구가 추가로 이루어져야 할 것이다.

참고문헌

[1] www.w3.org "XML Signature Requirements WD", W3C Working Draft 14-October-1999
[2] www.w3c.org "XML-Signature Syntax and Processing" W3C Recommendation 12 February 2002
[3] http://xml.apache.org/security/index.html "
[4] www.w3c.org "Canonical XML Version 1.0" W3C Recommendation 15 March 2001
[5] www.w3c.org "Exclusive XML Canonicalization Version 1.0", W3C Candidate Recommendation 12 February 2002
[6] www.w3c.org "XML Encryption Requirements", W3C Working Draft 18 October 2001
[7] www.w3c.org "XML Encryption Syntax and Processing", W3C Working Draft 18 October 2001
[8] www.w3c.org "Decryption Transform for XML Signature" W3C Working Draft 18 October 2001
[9] http://www.alphaworks.ibm.com "XML Security Suite"
[10] E. Damiani 외 3인, "Secureing XML Document"