ESES: XML 기반의 안전한 전자상거래 서비스

나 중 찬† · 손 승 원†† · 조 현 숙†††

ESES: XML based Secure E-Commerce Services

Jung-Chan Na† · Seung-Won Sohn†† · Hyeun-Sook Cho†††

요 약

최근 XML 문서는 전자상거래 분야에서 표준 전자문서로 자리매김을 하고 있다. 표준화된 전자문서의 정보보호 서비스는 전자상거래의 활성화에 큰 걸림돌로 작용하고 있으며, 안전한 전자상거래를 위해서는 우선적으로 전자문서에 대한 정보보호 서비스 기능을 제공해야만 한다. ESES(ETRI Secure E-commerce Services)는 전자상거래시 교환되는 XML(eXtensible Markup Language) 전자문서 및 기존의 일반 전자문서에 대한 정보보호 서비스를 제공하기 위한 시스템이며, 전자상거래 플랫폼에 절대적으로 필요한 시스템이다. 본고에서는 ESES 시스템의 구조를 제시하며, XML 기반 전자상거래에서의 전자 문서 교환 시 인증, 무결성, 비밀성 등을 지원할 수 있는 안전한 전자상거래 플랫폼을 설계한 내용을 기술한다.

ABSTRACT

Recently, XML(eXtensible Markup Language) Document is widely accepted as the standard for electronic documents in the electronic commerce. Therefore, a security mechanism for XML documents must be provided in the first place. ESES(ETRI Secure E-commerce Services) provides a system designed specifically for securing XML documents and existing non-XML documents that are exchanged in the Electronic Commerce and is essential to various electronic commerce platform as a fundamental system. In this paper, we provide an overview of these aspects of the ESES and designe and implemented the secure E-Commerce Platform to support security services such as authentication, integrity and confidentiality for Electronic Document Interchange.

1. 서 론

최근 제한적인 영역을 갖는 기존 상거래 방식을 탈피하여 시공간을 초월하는 전자상거래는 인터넷의 영향이 커지게 되고, 기업이나 일반 사용자의 인터넷 이용 횟수가 증가하면서 일반적인 거래 형태의 하나로 정착되고 있다. 1996년 국내에 전자상거래 개념이 도입된 이래 경제협력개발기구(OECD)에 따르면 세계 전자상거래 시장규모는 97년 260억 달러에서 2001년에는 3,300억 달러, 2003년에는 1조 달러에 이를 것으로 전망하였고, 한국전자상거래연구조합은 국내 전자상거래 규모가 99년 2,000억원에서 2000년 5,900억원으로 3배 가까이 늘어날 것으로 예상하고 있으며, 특히 기업간 전자상거래는 99년 700억원에서 2000년 3,000억원으로 4.3배 증가할 것으로 예상하였으며, 한국

* 본 논문에서 제안된 연구는 정보통신부의 과제로 지원되었다.

† 한국전자통신연구원 EC정보보호연구팀 팀장

†† 한국전자통신연구원 정보보호응용연구부 부장

††† 한국전자통신연구원 정보보호기술연구본부 본부장

전산원은 국내 전자상거래 규모가 98년 740억원에서 2002년에는 3조7,800억원으로 5배나 늘어날 것으로 전망하는 등 전자상거래가 경제의 틀을 바꾸어 놓고 있는 실정이다. 이러한 사실을 미루어 볼 때 전자상거래는 벤처기업이나 정보통신 산업의 거품론에 관계없이 분명한 하나의 비즈니스 패러다임으로 자리잡아 가고 있음을 보여주는 것이다[1].

그러나 인터넷의 편리성과 효율성을 상거래에 접목하여 출현한 전자상거래는 글로벌 비즈니스를 가능하게 하는 여러 장점에도 불구하고 상거래에 대한 효율성과 안전성 문제가 큰 걸림돌로 작용하여 활성화가 지연되고 있다. 이는 실제 적용에 있어서 메커니즘이 취약하고 표준의 유지보수, 시스템 도입을 위한 과다한 비용과 시간 등과 같은 전자상거래 서비스의 효율성 문제에 대응하지 못하고 있다. 또한, 전자상거래 서비스의 안전성 문제는 외부의 불법적인 침입을 방어하거나, 통신 내용을 보호하는 기능뿐만이 아니라, 사용자 인증, 데이터 무결성 보장, 송수신 부인봉쇄 등 다양하고 복잡한 기능의 제공을 요구받고 있다. 따라서 이러한 전자상거래의 기술적인 문제점을 해결할 수 있는 전자상거래 요소 기술에 대한 연구 개발이 요구된다.

이에 따라 전자상거래 서비스의 효율성 문제를 고려하기 위해 전자상거래에서 유통되는 전자문서의 내용에 의미를 부여할 수 있는 XML 기반의 전자상거래가 부각되고 있으며, 최근 XML 기술의 유용성이 인식되기 시작하여 많은 전자상거래 및 EDI 서비스 업체들이 자사의 서비스 플랫폼을 XML 기반으로 바꾸고 있는 실정이다.

이와 더불어 XML 기반의 전자상거래 보안 기술의 중요성이 강조되면서, IETF (Internet Engineering Task Force)와 W3C 등과 같은 인터넷 단체에서 초기 단계부터 보안 기술을 고려하여 시스템을 개발하는 형태로 발전하고 있다. 또한 국내외적으로 보안 분야의 기술력 확보를 위한 연구를 지속적으로 수행해 오고 있다. 특히 안전하고 신뢰할 수 있는 전자상거래 환경 구축에 있어서 반드시 필요한 보안 분야 기술은 모든 보안 기술 개발에 있어서 필수적으로 적용되는 암호 기술, 공개 키 기반 구조, 인증 기술 등 보안 기반 기술과 통신상에서 데이터 기밀성 및 무결성, 사용자 인증, 부인 봉쇄와 같은 네트워크 보안 기술이 있으며, 마지막으로 응용 프로그램에 적용되는 응용계층 보안 기술이 있다. 이와 같은 보안 분야 기술은 서로 밀접한 관계를 맺고 있어 하나의 보안 기술만을 이용해 안전한 전자상거래 환경을 구축할 수 있는 것이 아니라, 다양한 기술들이 결합됨으로써 가능하다.

전자상거래의 효율성과 안전성 보장을 위해 가장 필요한 것은 유통되는 XML 문서에 대한 정보보호이다. 따라서 본고에서는 다양한 보안 기술을 접목하여 효율적인 안전한 전자상거래 서비스를 지원하는 시스템에 대해 설계한 내용을 기술하고자 한다. 2장에서는 응용 계층에서의 XML 문서의 전자서명과 암호 서비스를 기술한다. 3장에서는 ESES 시스템의 전체 구조를 제시하며, 시스템의 각 구성 요소의 기능과 이들간의 관계를 기술한다. 또한 XML 문서에 대한 전자서명 생성 및 검증과 암호문 생성 및 복호를 처리하기 위한 설계 내용을 4장에서 기술하며, 마지막으로 결론을 맺는다.

2. XML 문서의 전자서명 및 암호

본 장은 XML 문서에 대해 효율적인 전자서명과 암호 서비스를 지원하기 위해 응용계층에서의 보안 기술을 살펴본다.

2.1 XML 전자서명

XML 기반의 전자상거래 환경에서 통신을 하는 두 응용 프로그램 사이에 교환되는 XML 문서는 무결성, 메시지 인증, 부인봉쇄 등 기본적인 정보보호 서비스를 요구한다.

현재 널리 사용되고 있는 네트워크 보안 기법인 SSL(Secure Socket Layer)/TLS(Transport Layer Security)는 기밀성, 무결성, 사용자 및 메세지 인증 등의 정보보호 서비스를 제공한다[2, 3]. 그러나 부인봉쇄는 전송되어지는 XML 문서에 대해서 전자서명을 수행함으로써 제공이 가능한데, SSL/TLS는 전송되는 XML 문서의 모든 데이터에 대해서 전자서명을 수행할 경우 많은 연산을 필요로 하여 비효율적이기 때문에 부인봉쇄 서비스를 제공하고 있지 않은 실정이다. 따라서 네트워크 프로토콜 차원이 아닌 응용 차원에서 송수신자(구매자 및 판매자)의 부인봉쇄 서비스를 제공하기 위해 XML 문서에 대한 전자서명 기법이 필요하다.

XML 문서는 문서 자체에 구조적인 정보를 가지고 있으며, XML 문서의 내용에 의미를 부여할 수 있기 때문에 XML 문서 단위 또는 XML 문서의 일부에 대해 전자서명이 가능하다. 따라서 사용자는 전자서명이 필요한 중요한 XML 문서 또는 XML 문서의 일부에 대해서만 전자서명을 수행함으로써 전자서명의 수행 때문에 발생하는 부담을 최소화 할 수 있다.

이와 같이 XML 전자서명 기술의 중요성이 강조되면서, IETF Security Area의 XML-DSIG Working Group과 W3C가 공동으로 XML-Signature Syntax and Processing, Canonical XML Version 1.0 등 XML 문서에 대한 전자서명 기술의 표준화를 추진중이다. 현재는 각각이 작업 등급의 표준 상태로서 구현을 통한 검증과정을 거쳐야 하는 단계이며, 2001년 5월 이후에 권고 등급의 표준이 제정될 예정이다[4, 5].

현재 W3C의 표준에 따른 XML 전자서명 기술은 크게 활성화되고 있지 못하고 있는 것이 사실이나, XML 기반의 전자상거래의 움직임이 활발해짐과 동시에 XML 문서에 대해 전자서명된 결과가 XML 문서 형태가 되어 기존의 XML 응용 및 XML 기반 전자상거래 플랫폼에 투명하게 접목 가능함에 따라 매우 활용의 폭이 크기 때문에 지속적인 관심을 가질 것이다.

따라서 본고에서는 W3C에서 표준으로 제정하고 있는 XML-Signature 작업 등급의 표준 규격을 구현하고자 한다.

2.2 XML 암호 및 복호

XML 기반의 전자상거래 환경에서 통신을 하는 두 응용 프로그램 사이에 상거래 관련 XML 문서를 암호화하고 제삼자가 그 문서를 도청하더라도 그 내용을 판별할 수 없도록 하는 XML 문서에 대한 기밀성이 요구된다.

XML 전자서명과 마찬가지로, XML 암호는 XML 문서 단위 또는 XML 문서의 일부에 대해 암호가 가능하다. 따라서 사용자는 암호가 필요한 중요한 XML 문서 또는 XML 문서의 일부에 대해서만 암호를 수행함으로써 암호화 때문에 발생하는 부담을 최소화 할 수 있다.

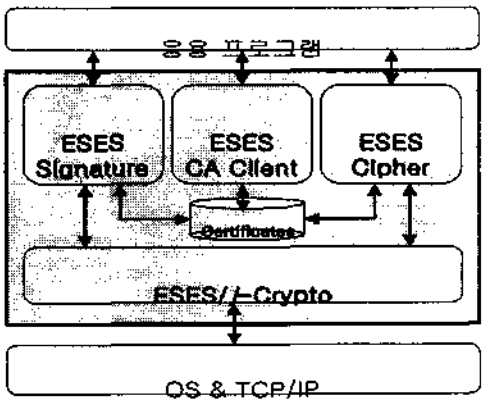
XML 문서에 대한 암호는 아직 IETF나 W3C에서 공식적으로 뚜렷한 표준이 없는 실정이며, 메일링 리스트를 통해 XML 암호에 대한 제안이 되고 있는 상황이다. 그러나 최근 2001년 1월에 표준을 제정하기 위해 XML-Encryption 표준 작업그룹을 형성하였다[6].

따라서 본고에서는 XML-Signature 표준과 마찬가지로 XML 문서에 대한 암호문은 XML 문서 형태가 되어 기존의 XML 응용 및 XML 기반 전자상거래 플랫폼에 투명하게 접목 가능하도록 하였다.

3. ESES 시스템 구조

ESES 시스템의 구조는 (그림 1)와 같다.

ESES/Signature와 ESES/Cipher는 동일한 수행환경을 가지며, ESES CA Client와 ESES/j-Crypto는 서로 각각 다른 수행환경을 갖는다. ESES/Signature와 ESES/Cipher는 응용 프로그램과 암호 기반을 제공하는 하부구조인 ESES/j-Crypto와 상호관계를 갖는다. 또한 ESES CA Client는 응용 프로그램과 전자상거래 환경에 있는 CA 서버로부터 발급받은 인증서를 저장하는 데이터베이스와 상호관계를 갖는다. 마지막으로 ESES/j-Crypto는 ESES/Signature와 ESES/Cipher와 상호관계를 갖는다.



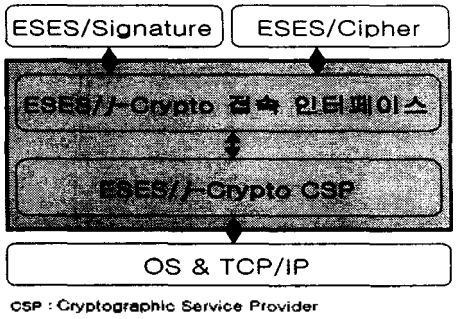
(그림 1) ESES 시스템 구조

3.1 응용 프로그램

응용 프로그램은 XML 문서의 전자서명 생성 및 검증, 암호화 및 복호화, 인증서 요구를 발생시키는 역할을 한다. 예를 들면 전자상거래 플랫폼을 구성하는 응용 또는 전자상거래를 위한 응용들을 가리킨다.

3.2 ESES/j-Crypto

ESES/j-Crypto는 XML 기반 전자상거래에서 교환되는 XML 문서에 대해 전자서명 생성 및 검증, 암호화 및 복호화 기능을 지원하는 보안 기반 기능을 제공한다.



(그림 2) ESES/j-Crypto 구조

ESES/j-Crypto 구조는 (그림 2)와 같이 Sun 사의 JDK 1.2에서 제시한 응용 프로그래머들을 위한 API와 API에서 이용할 수 있는 암호 알고리즘을 지원하는 공급자를 위한 SPI(Service Provider Interface)를 구조를 갖는 보안 모델을 기반으로 하였다[7].

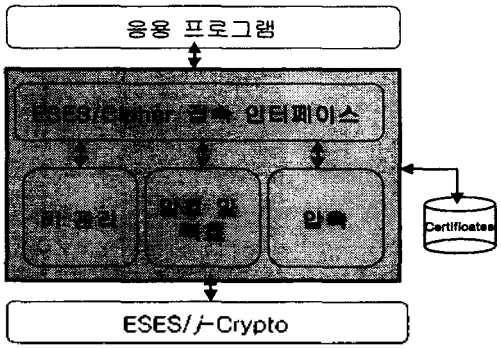
ESES/j-Crypto 접속 인터페이스는 응용 개발자가 자바의 보안기술을 사용할 수 있도록 하는 API를 제공한다. ESES/j-Crypto CSP는 자바로 구현된 암호 알고리즘에 해당된다. 구현된 알고리즘들은 고유한 암호 서비스 제공자 이름을 가지게 되며, 응용 개발자는 이 이름을 통해 특정 제공자에서 제공한 암호 알고리즘을 접근할 수 있다.

3.3 ESES/Signature

ESES/Signature는 XML 문서에 대해 전체적으로 또는 부분적으로 전자서명 생성 및 검증 기능을 지원하며, 구조는 (그림 3)과 같다.

ESES/Signature 접속 인터페이스는 응용 프로그램으로부터 서명 및 검증 요구를 받아 처리하는 창구 역할을 한다.

정규화는 XML 문서에 대한 전자서명 생성 및 검증 시 DOM 또는 SAX를 사용하는 경우에 SAX event 순서나 DOM Tree의 관계된 부분을 처리한다.



(그림 3) ESES/Signature 구조

키 관리는 XML 문서에 대한 전자서명 시 필요한 키 생성을 요구하며, 생성된 키를 ESES/Signature 접속 인터페이스에 반환한다. 여기서 반환되는 키는 ESES/j-Crypto를 이용하여 얻을 수 있고, 또는 CA Client에 의해 얻어진 인증서를 이용하여 얻을 수 있다.

메시지 다이제스트는 ESES/j-Crypto를 이용하여 서명 대상의 XML 문서에 대한 다이제스트 값을 얻는다.

서명 값은 ESES/j-Crypto를 이용하여 서명 대상의 XML 문서에 대한 서명 값을 얻는다.

3.4 ESES/Cipher

XML 문서에 대해 전체적으로 암호 또는 부분적으로 암호 및 복호 기능을 지원한다.

ESES/Cipher 접속 인터페이스 응용 프로그램으로부터 XML 문서의 암호 및 복호 요구를 받아 처리하는 창구 역할을 한다.

키 관리는 XML 문서에 대한 암호 및 복호 시 필요한 키 생성을 요구하며, 생성된 키를 ESES/Cipher 접속 인터페이스에 반환한다. 여기서 반환되는 키는 ESES/Signature와 마찬가지로 ESES/j-Crypto를 이용하여 얻을 수 있고, 또는 CA Client에 의해 얻어진 인증서를 이용하여 얻을 수 있다.

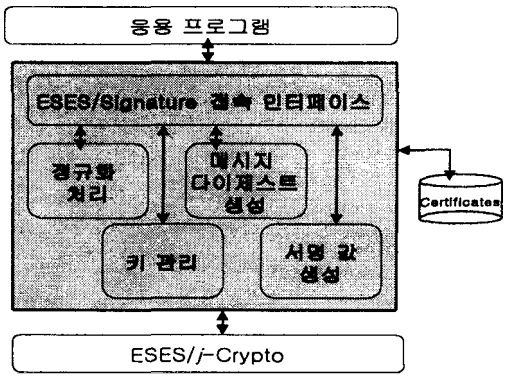
암호 및 복호는 크게 두 부류로 처리한다. 하나는 XML 문서에 대해 암호문 생성 시 사용된 비밀키를 암호 및 복호 처리하는 것이며, 다른 하나는 대칭 키 방식으로 XML 문서에 대해 암호 및 복호 처리한다.

압축은 암호문의 크기를 줄일 수 있고, 공격자에게 유용한 평문 정보가 숨겨질 수 있도록 XML 문서를 암호하기

전에 인코딩된 바이트 스트림에 대해 불필요한 부분을 제거한다.

3.5 ESES/CA 클라이언트

ESES/CA 클라이언트는 X.509 기반의 인증서를 이용하여 ESES 서비스를 제공하고자 할 때에 CA 서버로부터 인증서를 요구하는 클라이언트 응용이다.



(그림 4) ESES/Cipher 구조

4. ESES 설계 및 구현

본 장은 ESES 시스템 설계 및 구현에 있어 일반적인 요구사항과 이를 반영한 설계 및 구현 내용을 기술하기로 한다.

ESES 설계시 일반적인 요구사항은 다음과 같다.

i) 다양한 플랫폼에 이식 가능하여 기술 보급이 용이

ii) 기존의 XML 기술 및 XML 기반 전자상거래 플랫폼에 투명하게 접목 가능하도록 기술 개발

iii) 국제 표준 준수로 상호호환성 제공

iv) 기존의 XML 기술 및 XML 기반 전자상거래 플랫폼에 투명하게 접목 가능하도록 기술 개발

v) SEED, KCDSA 등 국내 표준 암호 알고리즘을 추가하여 국내외 어디에서나 널리 쓰일 수 있게 함

vi) SEED, KCDSA 등 국내 표준 암호 알고리즘을 추가하여 국내외 어디에서나 널리 쓰일 수 있게 함

vii) 국가 표준 CA와 연동 가능하여 글로벌한 전자상거래에 적용 가능

4.1 ESES/j-Crypto

ESES/j-Crypto는 JCA와 JCE1.2 표준 규격에 따라 설계하였다. 또한 ESES/j-Crypto CSP가 지원하는 알고리즘은 (표 1)에 나타나 있다.

(표 1)에서 제시한 암호 알고리즘은 XML전자서명 모듈과 XML 암호화 모듈에서 필요로 하는 알고리즘과 국내

(표 1) ESES/j-Crypto CSP가 지원하는 알고리즘

보안 기술	암호 알고리즘
Message Digest	MD5, SHA1, HAS160
Block Cipher	DES, DESede, SEED, Rijndael, Twofish
Cipher(Asymmetric)	RSA, ElGamal
Signature	DSA, ECDSA, KCDSA, ElGamal Signature, ECKCDSA
MAC	HMACwithMD5, HMACwithSHA1

표준으로 선정된 알고리즘, 그리고 최근 AES(Advanced Encryption Standard)의 표준으로 선정된 알고리즘을 선정하였다.

설계한 ESES/j-Crypto의 주요 패캐지는 다음과 같다.

i) javax.crypto

Cipher, SecretKeyFactory, KeyAgreement, MAC, KeyGenerator 등 JCE에 포함된 보안기술을 제공하기 위해

필요한 핵심 엔진클래스와 그에 대응하는 SPI 클래스, 그리고 각 클래스에서 발생하는 예외상황을 처리하기 위한 클래스들로 총 19개로 구성된다.

ii) javax.crypto.interface

JCE 암호라이브러리에 포함될 암호 알고리즘에서 사용되는 Key에 대한 인터페이스를 포함한다.

iii) javax.crypto.spec

각 알고리즘에서 사용되는 키와 매개변수들에 대한 규격을 포함한다.

iv) eses.jcrypto.security.provider

ESES/j-Crypto에서 제공하는 암호 알고리즘을 지원하는 클래스들로 구성된다.

4.2 ESES/Signature

ESES/Signature는 2.1절에서 언급하였듯이, XML 문서 단위인 전문에 대한 전자사명 생성 및 검증뿐만이 아니라 XML 문서의 일부에 대해 부분 서명이 가능하도록 하였으며, XML 문서에 대한 전자서명 생성 그 자체가 XML 문서 형태가 되어 기존의 XML 응용 및 XML 기반 전자상거래 플랫폼에 투명하게 접목 가능하도록 설계하였다.

설계한 ESES/j-Crypto의 주요 패캐지는 다음과 같다.

i) eses.xml.xsignature

XML 문서의 다이제스트, 전자서명 생성 및 복호 기능을 지원한다

ii) eses.xml.xsignature.spec

XML 문서의 다이제스트, 전자서명을 위한 알고리즘 매개변수를 지원한다.

4.3 ESES/Cipher

ESES/Cipher는 2.2절에서 언급하였듯이, XML 문서 단위인 전문 암호화뿐만이 아니라 XML 문서의 일부에 대해 부분 암호화가 가능하도록 하였으며, XML 문서에 대한 암호문은 그 자체가 XML 문서 형태가 되어 기존의 XML 응용 및 XML 기반 전자상거래 플랫폼에 투명하게 접목 가능하도록 설계하였다.

설계한 ESES/Cipher의 주요 패캐지는 다음과 같다.

i) eses.xml.xcipher

XML 문서의 암호 및 복호 기능을 지원한다.

ii) eses.xml.xcipher.spec

XML 문서의 암호 알고리즘 매개변수를 정의한다.

4.4 구현환경

구현 환경은 Pentium III의 Window2000 운영체제와 JDK 1.2.2 자바 플랫폼에서 수행하였으며, XML 문서에 대한 부분 서명 및 암호를 위해 요구되는 XML 파서는 DOM을 지원하는 IBM의 xml4j를 이용하였다. 그리고 ESES 시스템을 구현하기 위한 언어는 Java 언어를 사용하였다.

5. 결론

본고에서는 인터넷을 통한 XML 기반의 전자상거래 안전성 문제를 해결하기 위하여 유통되는 XML 문서의 정보보호 서비스를 지원할 수 있도록 하였다.

시스템의 주요 특성은 사용자가 XML 문서에 대해 전자서명 및 암호화를 하는데 있어 중요한 XML 문서 또는

XML 문서의 일부에 대해서만 전자서명 생성 및 암호화를 수행함으로써 전자서명 생성 및 암호화 수행 때문에 발생하는 부담을 최소화하였다. 그리고 XML 기반 전자상거래에서 교환되는 XML 문서에 대해 전자서명 생성 및 검증, 암호화 및 복호화 기능을 지원하는 보안 기반 서비스를 지원하였다.

ESES는 통합된 환경에서의 모든 형태의 안전한 전자상거래 및 EDI 서비스, B2B, B2C, M2M 등의 전자상거래에서의 안전한 주문서 교환에 활용될 것으로 기대된다.

향후 신뢰성을 요구하는 공공기관의 실제 업무와 연동하거나 또는 XML 기반의 전자상거래 플랫폼과 연동하는 기능을 앞으로 추가되어져야 한다.

참 고 문 헌

[1] 한국전자통신연구원, "정보기술 표준화 핵심기술 동향", 2000. 12.

[2] A. Freier, P. Karton, P. Kocher, "The SSL Protocol Version 3.0", http://www.netscape.com/engrmn/ssl3/draft302.txt

[3] T. Dierk, C.Allen, "The TLS Protocol Version 1.0", IETF RFC2246, 1999. 1.

[4] M. Bartel, J. Boyer, B. Fox, E. Simon, "XML-Signature Syntax and Processing", http://www.w3.org/TR/xmldsig-core/, 2000. 10.

[5] J. Boyer, PureEdge Solutions Inc, "Canonical XML Version 1.0", http://www.w3.org/TR/xml-c14n, 2001. 1.

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

[7] sun, "Java Cryptography Extension 1.2 API Specification and Reference", http://java.sun.com/products/jce/index.html