안전한 전자상거래를 위한 XML 전자서명의 설계와 구현

이재승*, 문기영*, 손승원*

*한국전자통신연구원 정보보호연구본부 네트워크보안연구부

Design and Implementation of XML Signature for Secure Electronic Commerce

Jae Seung Lee*, Ki Young Moon*, and Seung Won Sohn*

*Information Security Research Division, ETRI

요 약

전자상거래를 위해 가장 중요한 기능은 주문서 등과 같은 전자상거래 당사자간에 교환되는 전자문서 및 메시지에 대한 정보보호이다. XML은 인터넷에서의 데이터 교환의 표준으로 받아들여지고 있으며, 특히 전자상거래 분야에서의 사용이 급속히 확산되고 있다. 그러므로 안전한 전자상거래를 위해서는 XML 전자문서 및 XML 형태의 메시지에 대한 정보보호가 먼저 해결되어야 하며, 또한 기존의 XML 형태가 아닌 전자문서의 정보보호도 함께 해결되어야 한다. XML 전자서명은 이러한 보안 요구사항을 충족시켜 줄 수 있으며, XML 전자문서 및 메시지에 대한 인증, 무결성, 부인봉쇄 등과 같은 정보보호 서비스를 제공해 준다. 본 논문에서는 XML 전자서명에 대한 설계를 제안하며, 이 설계에 따라 XML 전자서명을 구현한 ESES/Signature에 대해 설명한다.

I. 서론

1. ESES/Signature의 개요

인터넷의 보급이 폭발적으로 증가하면서 인터넷의 편리성과 효율성을 기존의 상거래에 접목한 전자상거래가 출현하게 되었으며, 더욱 그 서비스의 종류가 다양해지고 사용자도 크게 확산되고 있다. 전자상거래를 위해 가장 중요한 기능 중의 하나는 주문서 등과 같은 전자상거래 당사자간에 교환되는 전자문서에 대한 정보보호이다.

XML (eXtensible Markup Language) [6] 은 인터넷에서의 데이터 교환의 표준으로 받아들여지고 있으며, 특히 전자상거래 분야에서의 사용이 급속히 확산되고 있다. 그러므로 안전한 전자상거래를 위해서는 XML 전자문서에 대한 정보보호가 먼저 해결되어야 하며, 또한 기존의 XML 형태가 아닌 전자문서의 정보보호도 함께 해결되어야 한다.

ESES/Signature는 ESES (ETRI Secure E-Commerce Services) [16] 의 주요 서브시스템으로, XML 전자문서 및 XML 형태의 메시지에 대한 인증, 무결성, 부인봉쇄 등과 같은 정보보호 서비스를 제공한다.

ESES/Signature는 W3C와 IETF에서 표준화한 XML 전자서명 표준에 의해 개발되었으며, 다수의 XML 기반 응용서비스에 통합되었다.

XML 전자서명은 XML을 비롯한 다양한 형태의 전자문서에 대해 XML 형태의 전자서명을 생성하고 검증할 수 있는 XML 기반의 전자서명 기법이며, 전자문서에 대한 인증, 무결성, 부인봉쇄 등의 정보보호 기능을 제공해 줄 수 있다.

서명 대상이 XML 전자문서인 경우 문서 전체에 대한 전자서명 뿐만 아니라 특정 부분에 대해 선택적으로 전자서명을 할 수 있고 다수의 전자문서에 대한 서명을 한꺼번에 처리할 수 있어 효율적인 전자문서 정보보호 서비스를 제공해 준다. 무엇보다도, ESES/Signature에서 생성된 서명된 결과가 XML 형태이기 때문에, 기존의 XML 기술 및 ebXML, XML/EDI와 같은 XML 기반의 응용서비스에 투명하게 접목이 가능하다는 커다란 장

점을 가지고 있다.

ESES/Signature 는 안전한 전자문서 및 메시지의 교환이 필요한 다양한 서비스에 적용될 수 있다. ESES/Signature는 자바로 구현되었기 때문에 다양한 플랫폼에 쉽게 이식될 수 있다. 또한 ESES/Signature는 XML 전자서명 스펙에 명시된 암호 알고리즘 이외에 국내 표준 알고리즘을 추가로 지원하여 국내외 모두에서 널리 사용 가능하다.

2. 연구 필요성

최근, XML 기술의 유용성이 널리 인식되기 시작하면서 XML 기반 응용 서비스의 개발이 크게 늘어나고 있다. 하지만, 대부분의 경우 XML 환경에 적합한 보안 메커니즘을 제공하고 있지 않다. XML 기반의 어플리케이션은 XML 형태의 데이터를 입력으로 요구한다. 하지만, XML 데이터에 기존의 전자서명 방식을 적용한다면, 서명결과는 바이너리 객체 형태가 되어버리고 이것은 XML 기반 어플리케이션이 처리하기에 적합하지 않은 형태이다. 반면에 XML 데이터에 XML 전자서명을 적용하면 그 결과도 또한 XML 형태가 되며, XML 전자서명은 XML 기반 어플리케이션에 적합한 보안 메커니즘이다. 따라서, 안전한 XML 기반의 응용서비스를 위해 XML 전자서명에 대한 연구개발이 필요하다.

한편, XML 전자서명을 국내 서비스에 적용하기 위해서는 다른 정보보호 제품과 마찬가지로 국내에서 개발된 제품 사용이 바람직하며, XML 전자서명 국제 표준에서 권고하는 암호 알고리즘 이외에 KCDSA [10] 등의 국내 표준 암호 알고리즘의 추가 지원이 필요하다.

위와 같은 상황들을 볼 때, XML 전자서명에 대한 더 많은 연구와 개발이 필요하다.

본 논문에서는 XML 전자서명에 대한 설계를 제안하며, 이 설계에 따라 XML 전자서명을 구현한 ESES/Signature에 대해 설명한다.

본 논문의 2절에서는 XML 전자서명과 관련된 연구동향에 대해 간략히 설명하고, 3절에서는 ESES의 구조 및 처리절차에 대해 설명한다. 4절에서는 XML 전자서명에 대한 설계를 제안하며, 5절에서는 이 설계에 따라 XML 전자서명을 구현한 ESES/Signature에 대해 설명하고, 6절에서 결론을 맺는다.

II. 관련 연구동향

이 절에서는 XML 전자서명과 관련된 표준화 동향 및 관련 제품 동향을 설명한다.

1. XML 전자서명 표준화 동향

현재 W3C XML Signature Working Group과 IETF에서 공동으로 XML 전자서명을 표준화 하고 있다. XML 전자서명 구문과 처리 (XML Signature Syntax and Processing) [2], 정규 XML 버전 1.0 (Canonical XML Version 1.0) [3], 배제 정규 XML 버전 1.0 (Exclusive Canonical XML Version 1.0) [13], XML 전자서명 XPath 필터 2.0 (XML Signature XPath Filter 2.0) [14] 등이 W3C 권고안 상태에 있으며, XML 전자서명 요구사항 (XML Signature Requirements) [1] 이 워킹 드래프트 상태이다. XML 전자서명 스펙이 최근에 표준화가 마무리되었기 때문에 스펙 구현을 통한 검증이 필요하다.

2. XML 전자서명 제품 동향

볼티모어, 인트러스트, HP, IAIK, IBM, MS, RSA, 베리사인 등 다수의 기업체에서 XML 전자서명 표준을 구현하고 있다. IBM의 'XML Security Suite' [5] 은 XML 전자서명, XML 암호 및 XML 접근제어 언어의 구현을 제공한다. 볼티모어의 'KeyTools XML' [4] 도 XML 전자서명과 XML 암호의 구현을 제공한다. 아파치에서도 최근 XML 전자서명을 구현한 'Apache XML Security for Java' [15] 를 공개 소스로 릴리즈하였다.

XML 전자서명 표준화가 비교적 최근에 완료되었기 때문에 아직 각 제품간의 충분한 호환성이 보장되지 않고 있다. XML 전자서명 제품간의 호환을 위해서는 더 많은 구현 경험과 노력이 필요하다.

III. ESES의 구조 및 처리 절차

이 절에서는 ESES (ETRI Secure E-Commerce Services) [16] 의 구조 및 처리 절차를 설명한다. ESES는 전자문서 보호를 위하여 XML 전자서명 [2], XML 암호 [9], 자바 암호 라이브러리 [11, 12]와 PKI 기반의 정보보호 기능을 제공한다.

ESES의 주요 구성요소 중의 하나는 XML 정보보호처리 서브시스템으로, 여기에는 XML 전자서명을 구현한 ESES/Signature 와 XML 암호를 구

현한 ESES/Cipher가 포함되어 있다. ESES의 나머지 주요 구성요소로는 SUN JCE [12] 와 호환되는 자바 암호 라이브러리인 ESES/j-Crypto 가 있다. ESES는 또한 인증서 처리를 위한 CA (Certificate Authority) 클라이언트 모듈 및 사용자의 개인키와 인증서를 저장하고 검색할 수 있는 IC 카드 인터페이스도 포함하고 있다. 그림 1은 ESES의 구조를 간략하게 도식화한 것이다.

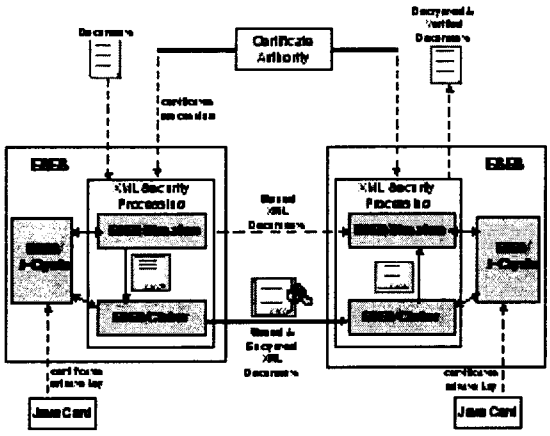

그림 1: ESES의 구조

XML 정보보호처리 (XML Security Processing) 서브시스템은 보호해야 하는 입력 문서를 처리하며, ESES/Signature와 ESES/Cipher로 구성되어 있다.

ESES/Signature는 XML 전자문서 혹은 비 XML 전자문서에 대한 전자서명 생성과 검증을 수행한다. 전자서명을 한 결과는 모두 XML 문서 형태가 된다. ESES/Cipher는 XML 전자문서 혹은 비 XML 전자문서를 암호화하고 복호화 한다. 암호화된 문서도 XML 문서 형태가 된다. ESES/j-Crypto는 자바 기반의 암호 알고리즘 라이브러리로서 암호 처리를 위해 XML 정보보호처리 서브시스템에서 호출하여 사용한다.

XML 정보보호처리 서브시스템은 전자서명을 위해 CA에서 발행한 X.509 인증서를 사용하며, 이때 인증서 처리를 위해 CA 클라이언트 모듈이 사용된다. 또한 XML 정보보호처리 서브시스템은 IC 카드 인터페이스를 사용해 사용자의 IC 카드에서 개인키와 인증서를 억세스 할 수 있다.

전자문서가 ESES에 의해 처리될 때 먼저 ESES/Signature 에 의해 전자서명이 이루어지며 서명된 문서는 상대방 시스템에 전달된 후에 상대방 시스템의 ESES/Signature에 의해 전자서명이 검증된다. 이 경우, 해당 전자문서에 대한 부인봉쇄, 무결성, 인증이 보장된다.

기밀성을 추가로 제공하기 위해서 ESES/Signature에 의해 서명된 문서는 ESES/Cipher에 의해 XML 형태로 암호화 될 수 있다. 서명되고 암호화된 결과는 상대방 시스템에 전달된 후 먼저 ESES/Cipher를 이용해 복호화가 이루어지고, ESES/Signature에 의해 복호화된 문서에 대한 전자서명이 검증되게 되며, 이 경우 해당 전자문서에 대한 부인봉쇄, 무결성, 인증, 기밀성이 모두 보장되게 된다.

서명되거나 암호화된 결과는 모두 XML 형태로, XML 기반 응용에서 투명하게 처리될 수 있다.

IV. ESES/Signature의 설계

이번 절에서는 ESES의 주요 구성요소인 ESES/Signature의 설계에 대하여 설명한다. 먼저 XML 전자서명에 대해 간단히 설명하고, ESES/Signature의 구조 및 각 모듈의 기능 그리고 자세한 처리 절차에 대해 설명한다.

1. XML 전자서명 개요

XML은 인터넷과 전자상거래 분야에서 데이터 교환의 표준 형식으로 널리 받아들여지고 있다. XML 전자서명은 이러한 XML 문서를 비롯한 다양한 형태의 전자문서에 대해 XML 형태의 전자서명을 생성하고 검증하여, 전자문서의 인증, 무결성, 부인봉쇄 등의 정보보호 기능을 제공해 준다.

기존의 전자서명 방식은 전자서명 결과가 바이너리 객체 형식으로 생성되어 XML 기반의 응용에서 처리하기에 적합하지가 않다. 사용한 알고리즘 등 전자서명과 관련된 정보가 사용자와 어플리케이션에서 이해하기 힘든 OID (Object Identifier)로 표시되며, 전자서명 검증을 위해서는 서명된 문서에 대한 정보, 알고리즘에 관한 정보, 키에 관한 정보, 인증서에 관한 정보 등을 처리해야 하는데 이에 대한 처리가 특정 어플리케이션에 종속적이며 처리가 복잡하다.

XML 전자서명은 기존의 이러한 문제점을 해결해 준다. 전자서명 결과가 XML 형태로 생성되어 XML 기반 어플리케이션에 통합이 용이하고, 알고리즘 식별자가 사용자와 어플리케이션에서 이해하고 처리하기 쉬운 URI (Uniform Resource

Identifiers) 형식으로 저장된다. 또한 전자서명과 관련된 정보가 사용자와 어플리케이션에서 처리하기 쉬운 텍스트 형태의 XML 노드 형태로 생성되어 이에 대한 처리가 쉽다.

그림 2는 XML 전자서명 생성 절차를 간략하게 나타낸 그림이다. XML 전자서명 생성시 먼저 서명대상인 리소스들에 대한 다이제스트 값을 구하여, 그 값을 알고리즘 이름, 리소스에 대한 URI 등의 정보들과 함께 Reference 라는 이름의 특정 엘리먼트 내부에 삽입하고, 이들 Reference 들을 포함하고 있는 SignedInfo 라는 이름의 엘리먼트에 대해 전자서명 값을 구한 후, 이들과 키 정보 등의 부가적인 정보를 XML 문서 형태로 구성하여 저장한다. 전자서명 검증시 XML 전자서명은 URI 정보를 이용해 각 리소스를 억세스하여 전자서명이 유효한지 검증한다.

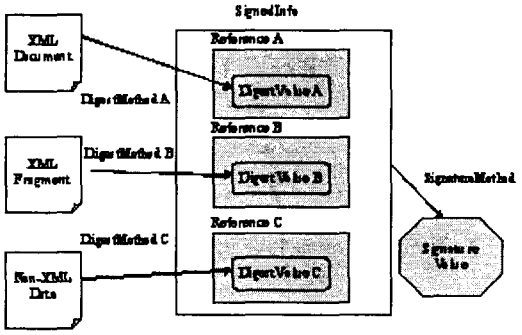

그림 2: XML 전자서명 생성절차

XML 전자서명은 XML 데이터 뿐만 아니라 어떠한 디지털 컨텐츠에도 적용이 가능하다. XML 전자서명은 다수의 리소스에 대한 전자서명을 한꺼번에 처리하여 하나의 전자서명 문서로 나타낼 수 있으며, XML 전자문서에 대해서는 문서 전체에 대한 전자서명뿐만 아니라 XML 문서의 특정 부분에 대해서도 전자서명을 할 수 있어 효율적인 전자서명 처리가 가능하다 [2].

2. ESES/Signature의 구조 및 기능

그림 3은 ESES/Signature의 구조를 도식화한 것이다. ESES/Signature의 주요 구성요소로는 ESES/Signature 인터페이스, XML 서명 및 검증 (Sign/Verify) 모듈, 서명 및 다이제스트 (Signature/Digest) 모듈, 키 정보 (Key Info) 모듈, 변환 (Transform) 모듈, 정규화 (Canonicalization) 모듈 및 유틸리티 (Utility) 모듈 등이 있다.

ESES/Signature 인터페이스는 어플리케이션에게 API 를 제공해 준다. 어플리케이션은 이 인터페이스 모듈을 사용해 XML 전자서명을 위한 파라미터를 설정한다. 어플리케이션에서 인터페이스 모듈을 통해 파라미터를 설정해 XML 서명 및 검증 모듈에 넘겨주기만 하면, 다른 모듈들이 호출되어 XML 전자서명이나 검증이 수행된다. 어플리케이션에서는 ESES/Signature 인터페이스 모듈 이외의 다른 모듈이나 내부 처리에 대해 신경을 쓸 필요가 없다. 즉, ESES/Signature 인터페이스는 응용 프로그램으로부터 XML 전자서명 생성이나 검증의 복잡한 처리 절차를 감춰주는 역할을 해준다.

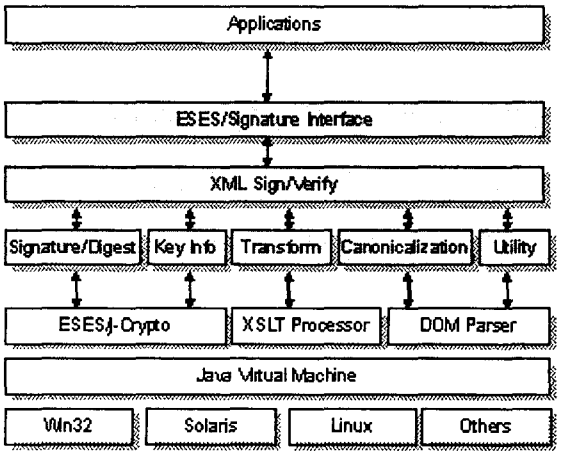

그림 3: ESES/Signature의 구조

XML 서명 및 검증 모듈은 XML 전자서명 생성과 검증을 수행한다. 이 모듈은 메인 모듈과 같은 역할을 하며, XML 전자서명 처리를 할 때 필요한 다른 모듈들을 호출한다.

서명 및 다이제스트 모듈은 XML 전자서명 및 검증에 필요한 전자서명과 메시지 다이제스트를 수행한다. 이 모듈은 ESES/j-Crypto 모듈을 호출하여 특정한 전자서명이나 다이제스트 알고리즘을 사용하여 XML 전자서명이나 검증을 수행한다.

키 정보 모듈은 키와 관련된 처리를 수행한다. 이 모듈을 통해 XML 전자서명 생성이나 검증시에 필요한 비밀키, 공개키 및 인증서에 대한 처리를 할 수 있다. 이 모듈은 또한 KeyInfo 엘리먼트 생성과 검증을 위해 필요한 공개키와 인증서 정보의 인코딩 및 디코딩 기능도 수행한다.

변환 모듈은 XML 전자서명을 위해 필요한 다

양한 변환처리 기능을 제공한다. Base64 Transform, XPath Transform, XSLT Transform, Enveloped Signature Transform [2] 등의 변환처리 기능이 이 모듈에서 제공된다.

정규화 모듈은 XML 데이터를 정규화하는데 필요한 정규 XML (Canonical XML) [3] 과 배제 정규 XML (Exclusive Canonical XML) [13] 알고리즘을 제공한다.

유틸리티 모듈은 ESES/Signature의 다른 모듈들에서 필요로 하는 다양한 함수를 제공한다. 이 모듈에서 Base64 인코딩/디코딩 알고리즘, DOM 파서를 이용한 XML 문서처리 기능, 예외 처리 기능 및 기타 다양한 기능이 제공된다.

서명 및 다이제스트 모듈과 키 정보 모듈은 암호 처리를 위해 ESES/j-Crypto를 호출하여 사용한다. ESES/j-Crypto는 SUN JCE [12] 표준을 준수하며, 다양한 국제 표준 암호 알고리즘을 제공해 주고 KCDSA [10]와 같은 국내 표준 암호 알고리즘도 추가로 제공한다. ESES/j-Crypto는 인증, 전자서명, 메시지 다이제스트, 암호, 키 생성 및 처리, MAC 등을 위한 표준화된 API를 제공한다.

정규화 모듈과 유틸리티 모듈은 DOM 파서를 사용하여 XML 문서의 노드를 억세스하고 변경한다. 변환 모듈은 XSLT 프로세서를 사용해 XSLT [7] 와 XPath [8] 연산을 수행한다.

ESES/Signature의 모든 모듈은 자바로 구현되었기 때문에 JVM (Java Virtual Machine) 이 탑재된 다양한 플랫폼에서 수행될 수 있다.

V. ESES/Signature의 구현

이번 절에서는 ESES/Signature의 구현에 대해 설명한다. ESES/Signature는 앞 절에서 제시한 설계에 기반하여 구현되었다. ESES/Signature의 패키지 구조는 그림 4와 같다.

eses.xml.xsignature 패키지는 XML 생성 및 검증 모듈을 구현한 것이며 XML 전자서명 생성 및 검증 기능을 수행한다.

eses.xml.xsignature.spec 패키지는 ESES/Signature 인터페이스를 구현한 패키지이며 응용 프로그램을 위한 API를 제공해 준다.

eses.xml.xsignature.canonical 패키지는 정규화 모듈을 구현한 것이며 정규 XML [3] 과 배제 정규 XML [13] 표준에 대한 구현이 제공된다.

eses.xml.xsignature.transform 패키지는 변환 모듈을 구현한 패키지이다. XML 전자서명 표준에서 제시한 Base64 Transform, XPath Transform, XSLT Transform, Enveloped Signature Transform [2] 등의 구현이 이 패키지에서 제공된다.

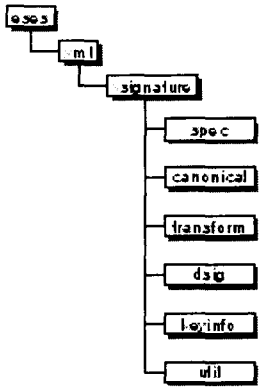

그림 4 패키지 구조

eses.xml.xsignature.dsig 패키지는 전자서명 및 다이제스트 모듈을 구현한 패키지이며 전자서명과 메시지 다이제스트 기능을 수행한다. XML 전자서명 표준에서 명시한 SHA1, HMAC, DSA, RSA 등의 알고리즘을 사용한 XML 전자서명 생성 및 검증 기능이 지원되며, 국내 사용을 위해 KCDSA [10] 에 대한 지원이 추가되었다.

eses.xml.xsignature.keyinfo는 키 정보 모듈을 구현한 패키지이며, 비밀키, 공개키, 인증서 처리 등과 관련된 기능이 구현되었다.

eses.xml.xsignature.util은 유틸리티 모듈을 구현한 패키지이며, 다른 모듈들이 필요로 하는 다양한 함수들을 제공한다.

ESES/Signature는 자바로 구현되었으며 JDK 1.3 이상에서 수행이 가능하다. 암호 라이브러리로는 ETRI에서 개발한 ESES/j-Crypto를 사용하였다. 하지만, KCDSA와 같은 국내 표준 암호 알고리즘의 사용이 필요 없는 경우에 한해서 SUN JCA [11] 및 JCE [12] 표준을 따르는 다른 자바 암호 라이브러리도 적용 가능하다.

XML 문서의 파싱 및 처리를 위해서 Apache Xerces-J 1.4.3 을 사용하였으며, XPath [8] 와 XSLT [7] 연산을 위해 Apache Xalan-J 2.3.1을 사용하였다.

ESES/Signature는 펜티엄 III 와 펜티엄 IV PC

를 사용해 Windows 2000, Windows XP, Windows 98, Windows NT 및 리눅스 2.4.3 환경에서 테스트되었다.

ESES/Signature에서 지원되는 알고리즘들을 표 1 에 요약하였다. ESES/Signature는 XML 전자서명 구문 및 처리절차 [2] 표준 문서에서 권고한 모든 알고리즘들을 지원하며, 추가로 국내 환경을 위해 KCDSA [10] 를 지원한다.

알고리즘 형태	알고리즘	요구사항
Digest	SHA1	Required
Encoding	Base64	Required
MAC	HMAC-SHA1	Required
Signature	DSAwithSHA1 (DSS)	Required
	RSAwithSHA1	Recommended
	KCDSA	추가됨
Canonicalization	Canonical XML	Required
	Canonical XML with Comments	Recommended
Transform	XSLT	Optional
	XPath	Recommended
	Enveloped Signature	Required

표 1: ESES/Signature가 지원하는 알고리즘

VI. 결론

본 논문에서는 XML 전자서명의 연구 동향에 대해 알아보고 안전한 전자상거래를 위한 XML 전자서명에 대한 설계를 제안하였으며, 이를 바탕으로 구현된 ESES/Signature에 대해 설명하였다.

ESES/Signature는 XML 문서를 포함한 다양한 형태의 전자문서에 대해 인증, 무결성, 부인봉쇄 등의 정보보호 기능을 제공한다. 전자서명된 결과가 XML 형태로 생성되기 때문에 ebXML 및 XML/EDI 와 같은 XML 기반의 어플리케이션에 투명하게 접목이 가능하다. ESES/Signature는 안전한 전자문서의 교환이 필요한 다양한 응용 프로그램에 적용될 수 있다.

자바로 개발되어 다양한 플랫폼에 쉽게 이식될 수 있으며, 국제적으로 널리 쓰이는 암호 알고리즘 이외에 국내 환경을 위한 국내 표준 알고리즘에 대한 지원이 추가되었다.

ESES/Signature는 전자상거래를 포함한 다양한 어플리케이션에서 안전한 데이터 교환을 할 수 있도록 해주는 주요 구성요소이며, 다양한 XML 기반 어플리케이션에 대한 적용이 필요하다. 이를 위해서는 보다 많은 연구개발과 통합시도가 필요하다.

참고문헌

[1] IETF/W3C, "XML-Signature Requirements (W3C Working Draft)", October 1999.

[2] IETF/W3C, "XML-Signature Syntax and Processing (W3C Recommendation)", February 2002.

[3] IETF/W3C, "Canonical XML Version 1.0 (W3C Recommendation)",March 2001.

[4] Baltimore, Baltimore KeyTools XML Homepage, http://www.baltimore.com/keytools/xml/.

[5] IBM, alphaWorks XML Security Suite Homepage, http://www.alphaworks.ibm.com/tech/xmlsecuritysuite.

[6] W3C, "XML 1.0 Recommendation", February 1998.

[7] W3C, "XSL Transformations (XSLT) Version 1.0", November 1999.

[8] W3C, "XML Path Language (XPath) Version 1.0", November 1999.

[9] W3C, "XML Encryption Syntax and Processing (W3C Recommendation)", December 2002.

[10] KCDSA Task Force Team, "The Korean Certificate-based Digital Signature Algorithm", August 1998.

[11] Sun, "Java Cryptography Architecture API Specification and Reference", October 1999.

[12] Sun, "Java Cryptography Extension 1.2 API Specification and Reference", March 1999.

[13] W3C, "Exclusive XML Canonicalization Version 1.0 (W3C Recommendation)", July 2002.

[14] W3C, "XML-Signature XPath Filter 2.0 (W3C Candidate Recommendation)", July 2002.

[15] Apache, Apache XML Security for Java Homepage, http://xml.apache.org/security/index.html.

[16] J.Y. Lee, J.H. Kim, J.S. Lee, K.Y. Moon, and H.S. Cho, "ESES: XML Security for Secure Electronic Commerce", Proceedings of WISA 2001, Seoul, Korea, 2001, 165-174.