XML 기반 안전한 전자상거래를 위한 보안 플랫폼 개발

Development of the XML Security Platform for E-Commerce

문기영(K.Y. Moon) 능동보안기술연구팀 선임연구원
이재승(J.S. Lee) 능동보안기술연구팀 연구원
김주한(J.H. Kim) 능동보안기술연구팀 연구원
이주영(J.Y. Lee) 능동보안기술연구팀 연구원
손승원(S.W. Sohn) 네트워크보안연구부 책임연구원, 부장

XML 전자문서는 전자상거래를 위한 전자문서의 표준으로 받아 들여지고 있으며 안전한 전자상거래를 위해서는 XML 정보보호가 무엇보다도 먼저 해결되어야 한다. 본 논문에서는 인터넷 상에서 XML을 기반으로 하는 전자문서 교환 시스템의 안전한 문서 교환을 위한 정보보호 서비스 구현을 소개한다. XML 기반 전자문서 교환 시스템은 주로 인터넷에서 상거래를 위해 사용자 인증, 데이터 무결성 보장, 송수신에 대한 부인 봉쇄 등 다양한 보안 기능에 대해 필요하다. 또한 본 논문은 이러한 보안 기능을 충족시키는 XML 기반 정보보호 서비스인 ESES(ETRI Secure E-commerce Services)를 제안한다. ESES는 XML 문서 뿐 아니라 전자상거래 시 교환되는 디지털 콘텐츠를 위한 보안 서비스 제공을 목적으로 하며, 자바기반의 암호 구조를 바탕으로 XML 기반 전자서명, XML 기반 암복호, XML 기반 키 복구, 인증서 처리 기능 등을 지원한다.

I. 서 론

인터넷의 보급이 폭발적으로 증가하면서 인터넷의 편리성과 효율성을 기존의 상거래에 접목한 전자상거래가 출현하게 되었으며, 더욱 그 서비스의 종류가 다양해지고 사용자도 폭넓게 확대되고 있다. 상점을 직접 방문하지 않고도 물건을 구매할 수 있으며 글로벌 비즈니스를 가능하게 하고 상거래의 시간적, 공간적 제약을 극복할 수 있는 여러 가지 장점에도 불구하고, 거래에 대한 안전성 문제가 전자상거래의 활성화에 큰 걸림돌로 작용하고 있다. 전자상거래의 안전성 보장을 위해 가장 필요한 것 중의 하나는 주문서 등의 전자상거래 시에 교환되는 전자문서에 대한 정보보호이다.

XML(eXtensible Markup Language)은 SGML(Standard Generalized Markup Language)의 간략화된 버전으로 SGML의 확장성, 구조, 검증의 특성을 계승하고 있다. 이런 장점으로 인해 XML은 발표된 이래로 인터넷 상의 자료 표현의 표준으로 각광을 받았다. 기술의 발전으로 인해 인터넷은 문서 교류의 장에서 사이버 뱅킹 등을 거쳐 상거래의 장으로 발전되었고, XML 또한 단순한 문서 교환이 아니라 여러 형태의 문서를 통합하고 전달하는 전자상거래 문서 표준으로 자리 잡고 있다.

경제협력개발기구(OECD)에 따르면 전세계 전자상거래 규모가 지난 2001년 3,300억 달러에서

2003년에는 1조 3,173억 달러에 달할 것으로 전망하고 있다. 특히 국내 인터넷 및 전자상거래 현황에 대한 IDC의 조사를 살펴보면 인터넷 이용자 중에서 최근 3개월 동안 인터넷을 통해 물건을 구입한 경험이 있는 전자상거래 이용자 수는 지난 1998년 국내 인터넷 이용자 수의 9.7%에 해당하는 17만 명에서, 1999년 17.5%인 58만 명, 그리고 향후 2003년에는 47.6%인 486만 명에 이를 것으로 전망된다.

이렇게 인터넷 상에서 전자상거래가 부각됨에 따라 인터넷 사업의 필수 인프라인 정보보호에 대한 요구가 절실하다. Cyber Dialogue의 AIUS (American Internet User Survey)에 따르면 전자상거래를 하는 데 있어서 가장 큰 장애요인은 정보보호에 대한 불신과 프라이버시의 침해 문제이며 전자상거래 사이트에 개인정보보장 정책의 공표가 온라인 쇼핑몰 재방문 결정에 중요한 요인이 되는 것으로 나타났다[1].

따라서 전자상거래의 활성화를 위해 네트워크를 통해 전달되는 내용에 대한 보호 뿐 아니라 사용자 인증, 데이터 무결성 보장, 송수신에 대한 부인 봉쇄 등 다양한 보안 기능에 대한 요구가 충족되어야 한다. 이를 위한 해결방안으로 본 논문에서는 ESES(ETRI Secure E-commerce Services) 시스템을 제안한다[2],[3]. ESES는 현재 전자상거래의 표준으로 광범위하게 채택되고 있는 XML 문서 뿐 아니라 전자상거래 시 교환되는 디지털 콘텐츠를 위한 보안 서비스를 제공하는 것이 목적이다. 이는 전자서명 서비스를 제공하는 ESES/Signature, 암호화 서비스를 제공하는 ESES/Cipher, 회사 규모의 암호 키 관리를 위한 키 복구 시스템인 ESES/XKRS 그리고 암호화 알고리듬 라이브러리인 ESES/j-Crypto로 구성되고 보조기능으로 자바기반 인증서 처리와 자바카드 연동기능을 가진다.

본 논문에서는 ESES 시스템에 대한 간략한 소개와 함께 전자상거래 시스템에 적용될 보안 서비스를 제공하기 위해 어떻게 설계, 구현되었는지에 대해 기술한다.

II. 관련 연구

1. 연구동향 및 추세

현재 전자서명과 암호화를 수행하기 위해서 IBM의 AlphaWorks, Baltimore의 X/Secure 등 몇 가지의 XML 보안 제품이 개발되어 있다. IBM의 Alpha Works는 XML 전자서명과 XML 암호를 위한 기능을 제공하고 있으며 상용화된 제품이 아니라 XML 전자서명의 예제 구현을 위하여 개발되었다. Alpha Works의 전자서명 모듈은 XML 전자서명 표준 초안에 따라 개발되었으며, XML 암호 모듈의 경우에는 자체적으로 정의한 규격에 따라 구현하였다[4]. 최근 Apache에서도 Apache-XML-Security 라는 XML 전자서명 구현 패키지를 개발하였으며, MS에서도 자사의 .NET 프레임워크에 XML 전자서명 기능을 통합해 넣었다. 이외에도 DSTC, HP, Entrust, NEC, Verisign에서도 각각 자사의 XML 전자서명 패키지를 개발하였다.

Baltimore의 X/Secure[5],[6] 또한 XML 전자서명과 암호화를 제공한다. X/Secure도 XML 전자서명 표준문서의 초안에 따라 구현하였지만, 현재 발간된 초안에 명시된 기능들 중 많은 부분을 제공하지 못하고 있다[4].

2. 표준화 동향

XML 전자서명은 W3C의 XML-Signature 워킹그룹이 IETF와 공동으로 XML 전자서명에 대한 표준화 작업을 진행중이며, 표준화의 핵심인 XML 전자서명 구문 및 처리절차(XML-Signature Syntax and Processing)[7]가 올해 2월 W3C의 권고안(recommendation)으로 채택되었다.

XML 암호화는 W3C의 XML Encryption 워킹그룹에서 표준화 작업을 수행중이며, 2002년 8월에 후보 권고안(candidate recommendation)이 제안되었다[8].

III. ESES 개요

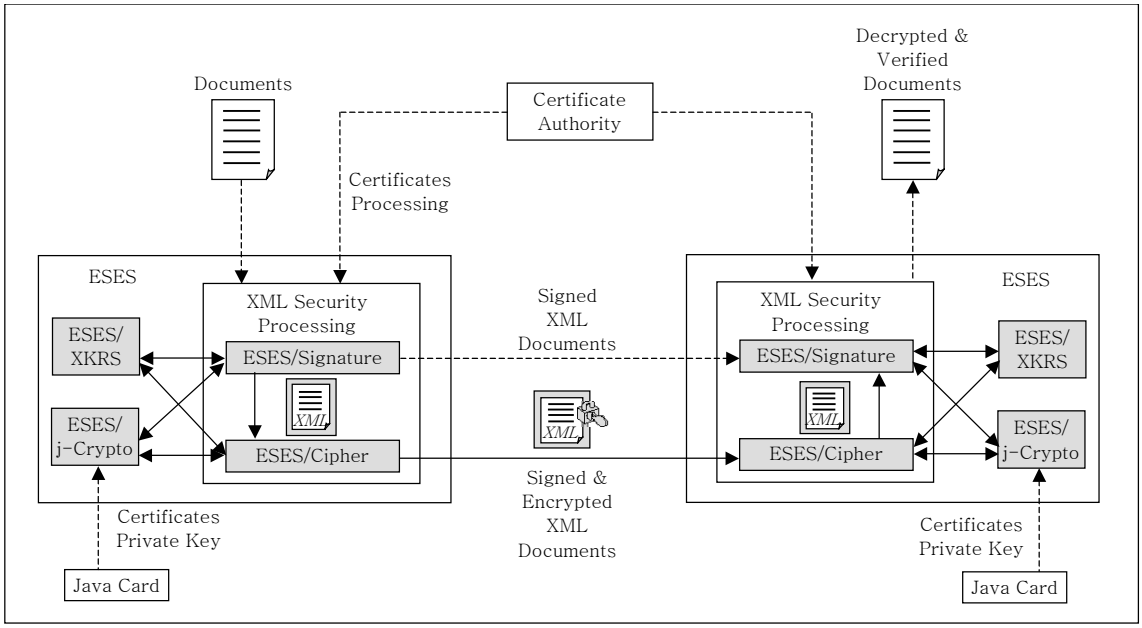
ESES는 XML 문서 및 전자상거래를 수행할 때 교환되는 디지털 데이터들을 보호하기 위해 전자서명, 암호화 등의 보안 서비스들과 암호 알고리듬 라이브러리를 통합한 시스템이다.

ESES 시스템은 XML Signature 표준(안)[7], [9]과 XML Encryption 표준(안)[8],[10]에 기반하여 각 모듈이 개발되었으며, 실제 응용 프로그램에 적용될 경우, 개발자의 편의성을 향상시킬 수 있도록 각 API가 설계되었다. 이를 위해서 보안 표준(안)에서 정의한 전자서명의 구조를 단순히 생성하는 것 뿐 아니라 몇 개의 API들만을 호출함으로써 복잡한 처리절차를 수행할 수 있도록, 많은 부분을 캡슐화하여 API를 설계하였다. 이는 보안 서비스와 암호 알고리듬에 관련된 지식이 많지 않은 대부분의 응용 프로그램 개발자가 쉽게 사용할 수 있도록 하는 데 목적이 있다. 그리고 각 모듈을 기능적으로 분리하여 아직까지 완전하게 표준으로 확정되지 않은 표준(안)의 변경에 따라 ESES 또한 쉽게 추가, 삭제, 변경할 수 있도록 하였다.

또한 기존에 오픈 소스형태로 인터넷 상에서 제공되는 암호 라이브러리들은 그 동작의 정확성이 검증되어 있지 않을 뿐 아니라 국내 표준 알고리듬을 포함하고 있지 않다는 문제점을 내제하고 있다. 이 문제를 해결하기 위한 방안으로 ESES 시스템은 검증되어진 알고리듬을 제공할 뿐 아니라 국내 표준 알고리듬, 그리고 최근 AES 표준 알고리듬으로 선택된 Rijndael[11]을 지원하고 있으며, 성능이나 강력한 암호 알고리듬으로 알려진 ECC(Elliptic Curve Cryptography) 알고리듬[12]을 개발중에 있다.

(그림 1)에 ESES 시스템의 구조가 나타나 있다. 이는 ESES/Signature, ESES/Cipher, ESES/XKRS 그리고 ESES/j-Crypto라는 세 개의 모듈을 통합한 시스템이며, 이 외에 부가적으로 인증 서버로부터 인증서에 대한 발급 요청을 하고, 발급된 인증서를 저장, 관리하기 위한 인증 클라이언트와 자바카드 연동 API가 포함될 수 있다.

ESES/Signature는 XML 문서를 포함한 임의의 디지털 콘텐츠에 대한 무결성 보장과 인증을 제공하는 것을 목적으로 한다. 이를 위해서 전자서명을 생성하고 검증하는 데 필요한 API들과 메시지 다이제



(그림 1) ESES 구조도

스트 기능, 문서에 대한 변환 기능 등을 포함한다. 전자 서명은 XML 문서의 전체에 대해서 혹은 원하는 일부분에 대해서만 부분적으로 수행할 수 있다.

ESES/Cipher는 암호화와 복호화에 필요한 API들과 암호화된 문서와 부가 정보들을 표현하기 위한 XML 구문을 제공한다. ESES/XKRS는 회사 업무 수행을 목적으로 암호문을 복호해야 한다거나, 암호문의 소유자가 암호문에 사용된 키를 분실해서 중요 데이터를 복호할 수 없을 경우 등에 한해 허가된 사람에게 해당하는 암호문에 한해서 복호화가 가능한 능력을 제공하는 암호 시스템이다. ESES/Cipher는 XML Encryption 초안에 기술된 문서 전체에 대한 암호화와 부분 암호화 기능을 제공한다.

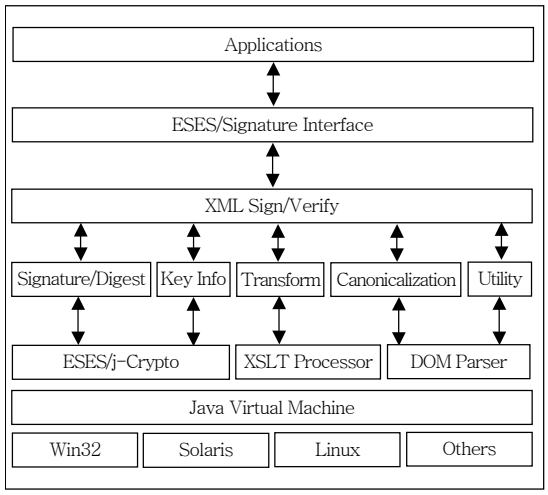
ESES/j-Crypto는 암호 알고리듬 라이브러리로 ESES/Signature와 ESES/Cipher에서 필요로 하는 각종 암호 알고리듬을 제공한다.

ESES에 의해서 서명이 되거나 암호화가 된 문서의 결과는 XML 형식으로 표현되어 기존의 XML 문서, XML 기반의 전자상거래 플랫폼과 쉽게 통합될 수 있다. 또한 앞서 언급했듯이 ESES는 자바언어를 이용해 API 형태로 개발되었으며, 국제 표준에 따르기 때문에 플랫폼에 독립적이고 B2C(Business to Customer) EC, B2B(Business to Business) EC 그리고 XML/EDI를 위한 다양한 서비스를 개발하는 데 있어서 쉽게 사용될 수 있다는 장점을 지닌다.

IV. ESES 설계와 구현

1. ESES/Signature

ESES/Signature는 XML 문서 뿐만 아니라 임의의 디지털 콘텐츠에 대한 무결성 보장과 인증, 부인봉쇄 기능 등을 제공한다[4]. ESES/Signature는 XML 문서 전체 혹은 특정 부분, XML이 아닌 일반 전자문서에 대해 XML 형태의 전자서명을 생성하고 검증할 수 있으며 다수의 리소스에 대한 서명을 하나의 XML 전자서명으로 처리할 수도 있다. ESES/Signature의 구조는 (그림 2)와 같다.



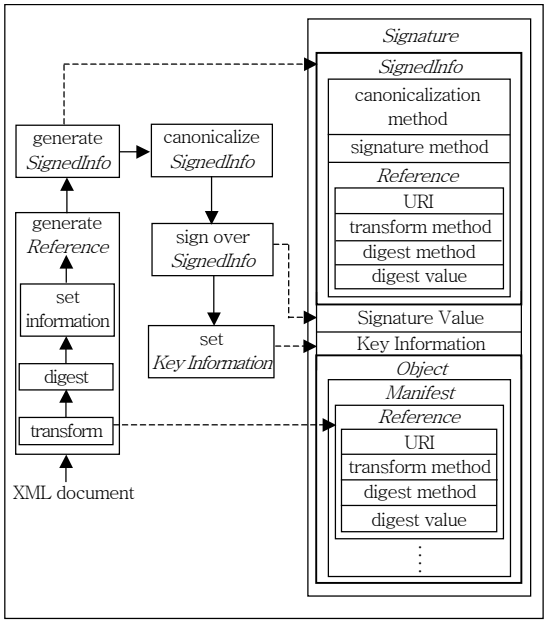
(그림 2) ESES/Signature 구조

ESES/Signature API는 응용 프로그램으로부터 XML 문서에 대한 전자서명을 생성하거나 검증하도록 요청을 받고 그 처리 결과를 반환하는 창구의 역할을 수행한다. ESES/Signature는 문서에 대한 변형(transform), 메시지 다이제스트, 전자서명을 생성, 검증하는 모듈을 포함하고 있다.

ESES/Signature는 IETF/W3C의 XML Signature 초안을 따르도록 설계되었다. 초안에 명시된 문서의 변형 방법은 Canonical XML[13], Canonical XML with Comments, Base64 Encoding, XSLT Transform[14], XPath Transform[15] 그리고 Enveloped Signature Transform 등이 있다. 메시지 다이제스트는 ESES/j-Crypto를 이용해 서명될 리소스에 대한 다이제스트 값을 얻는 과정으로 SHA1, MD5, 그리고 HAS160 알고리듬 등을 사용할 수 있다. ESES는 서명을 생성하기 위해 DSA, RSA 그리고 KCDSA를 지원한다.

XML Signature 초안은 XML 전자서명의 구조만을 정의하였으며, ESES/Signature는 이 구조를 만족하는 XML 전자서명을 생성하기 위해 (그림 3)과 같은 처리절차를 따르도록 설계되었다. 처리절차에서 사용된 엘리먼트 이름은 모두 XML Signature 초안에서 지정한 이름들이다.

서명을 생성하기 위해서 먼저 서명할 문서를 변,



(그림 3) 서명의 생성 과정과 서명의 구조

형알고리듬을 사용하여 적절히 변형한다. 다음으로 서명대상에 대한 메시지 다이제스트를 수행하고 서명 대상에 대한 URI, 사용한 변형 알고리듬, 다이제스트 알고리듬, 다이제스트 값을 포함하는 Reference라는 이름을 갖는 엘리먼트를 생성한다. 다수의 자원을 한꺼번에 서명하는 경우 각 자원에 대한 Reference 엘리먼트들이 직접 SignedInfo라는 이름의 엘리먼트에 포함되거나 혹은 Manifest라는 이름의 엘리먼트에 포함되도록 한다. 후자의 경우, Manifest 엘리먼트에 대한 Reference 엘리먼트가 생성되어 이 Reference만 SignedInfo 구조에 포함되게 된다.

Manifest 엘리먼트는 각 서명 대상들에 대한 Reference 엘리먼트들의 리스트로 구성되고 이 Manifest는 XML 전자서명의 루트 엘리먼트인 Signature 구조에 포함되며 SignedInfo 내에는 Manifest에 대한 Reference 엘리먼트만 포함된다. 서명의 수신자는 필요에 따라 검증 시 Manifest 내의 Reference 엘리먼트들을 검증할 수도 있고 검증을 생략할 수도 있다.

SignedInfo 엘리먼트는 SignedInfo 그 자체에 대한 정규화 알고리듬에 대한 정보(CanonicalizationMethod), 전자서명 알고리듬에 대한 정보(SignatureMethod), Manifest에 대한 Reference, 기타 다른 자원들을 위한 Reference 등을 포함하도록 구성된다.

그 다음 SignedInfo 내의 Signature-Method 엘리먼트에 지정된 전자서명 알고리듬을 이용하여 SignedInfo에 대해 전자서명을 수행하여 그 결과 값을 SignatureValue 라는 이름의 엘리먼트에 인코딩하여 저장한다.

마지막으로 XML 전자서명의 루트 엘리먼트인 Signature 엘리먼트는 SignedInfo 엘리먼트, SignedInfo에 대한 전자서명 값(SignatureValue)과 서명자의 키 정보(KeyInfo), Manifest 엘리먼트 등을 포함하는 Object 엘리먼트와 같은 다양한 부가적인 정보를 포함하여 생성된다.

XML 전자서명에 대한 검증을 하기 위해서는 SignedInfo에 대한 전자서명 검증과 SignedInfo에 포함되어 있는 각 Reference의 검증이 이루어져야 한다. XML 전자서명의 구체적인 검증절차는 다음과 같다.

우선 검증할 자원을 해당되는 Reference 엘리먼트에 있는 URI 정보를 사용해 접근한다. 그리고 Reference 엘리먼트에서 지정한 변형 방법을 사용해서 획득한 자원을 변형한 후 지정된 다이제스트 알고리듬을 사용해서 다이제스트 값을 계산한다. 계산된 다이제스트 값은 해당 Reference 엘리먼트에 들어 있는 다이제스트 값과 같은지 비교된다. 메시지 다이제스트 알고리듬의 특성에 의해 만일 해당 자원이 변경되었을 경우, Reference 내의 원본에 대한 메시지 다이제스트 값과 변경된 자원의 메시지 다이제스트 값이 다르게 되고, 데이터의 변경 유무를 판단할 수 있는 근거가 된다. 각 Reference들은 이와 같은 방식으로 검증된다.

SignedInfo는 우선 SignedInfo에 지정되어 있는 문서의 정규화 방법을 이용해 정규화된다. 서명 검증을 위해 KeyInfo 엘리먼트로부터 공개키 정보를 가져와 이 정보와 SignatureMethod 엘리먼트에서

지정한 서명 알고리듬을 이용하여 SignedInfo에 대한 전자서명 값을 검증한다.

Manifest 검증을 위해서는 Manifest가 포함하고 있는 각 Reference를 검증해야 하며, 이 과정은 응용프로그램의 결정에 따라 생략할 수도 있다.

위와 같이 검증된 XML 전자서명은 각 리소스가 변경되지 않았음을 보장하며 송신자 인증, 송신 부인 방지를 제공해 준다[1],[2].

2. ESES/Cipher

XML/Cipher는 XML 문서를 포함한 디지털 콘텐츠를 암호화 하는 데 필요한 구문과 처리 방법을 제공하며 XML 문서의 전체 또는 부분에 대한 암호화 방법을 제공한다[7].

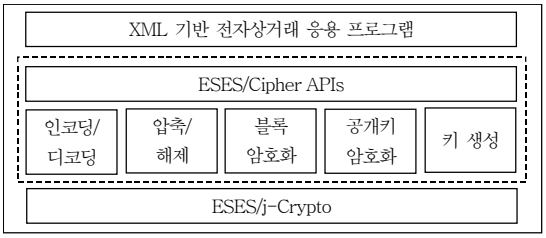
(그림 4)는 ESES/Cipher의 구조를 보여준다. 이는 인코딩/디코딩 처리 클래스, 암호 알고리듬 매개변수를 위한 클래스, 키 매개변수 클래스, XML 인스턴스를 위한 DOM 클래스 등으로 구성된다.

ESES/Cipher API는 응용 프로그램으로부터 암호화 혹은 복호화 요청을 받고 이를 처리한 후 그 결과를 반환하는 역할을 수행한다.

XML 문서를 암호화 하기 위해서 두 단계의 암호화 과정이 필요하다. 첫번째는 암호화될 문서를 위한 것이고 다른 하나는 문서를 암호화하기 위해 사용된 비밀키를 위한 것이다. 첫 단계의 암호화를 수행하기 위해서는 먼저 랜덤 값 생성기를 사용해서 비밀키를 생성할 필요가 있다. 다른 한편으로 XML 문서는 바이트 스트림으로 인코딩되고 압축된다. 이는 생성될 암호문의 크기를 줄일 수 있을 뿐 아니라 암호문에 대한 공격자들에게 평문에 관련된 정보를 적게 노출시킨다는 장점을 지닌다. 다음으로 암호화된 바이트 스트림은 방금 전에 생성된 비밀키와 대칭키 암호 알고리듬을 이용해서 암호화된다. 그리고 나서 암호화된 바이트는 XML 노드의 형태로 인코딩 된다.

암호화의 두번째 단계는 앞서 언급했듯이 문서를 암호화하기 위해 사용된 비밀키를 안전하게 전송하기 위해 암호화 하는 단계이다. 이는 암호문을 받을 수신자의 공개키를 사용해서 암호화된다. 암호화된 비밀키와 사용된 알고리듬 종류 등과 같이 부가적인 정보 또한 XML 노드로 인코딩 된다. 이렇게 생성된 XML 노드들은 DTD-defined XML 형태로 구조화된다.

<표 1>은 지금까지 기술한 암호화 과정을 정리한 것이다. 암호화된 문서를 풀기 위해서는 먼저 XML 노드로 인코딩된 부가정보를 디코딩 해서 암호화하는 데 어떤 알고리듬이 사용되었는지를 점검해야 한다. 수신자의 개인키를 이용해서 XML 문서에 포함된 비밀키를 복호화한다. 그 후 XML 암호문은 선택된 대칭키 암호 알고리듬과 바로 전에 복호화된 개인키를 이용해서 복호화된다. 그리고 압축된 바이트 스트림의 압축을 풀고, 마지막으로 이 바이트 스트림을 원래의 XML 구조로 복원한다[1],[2].



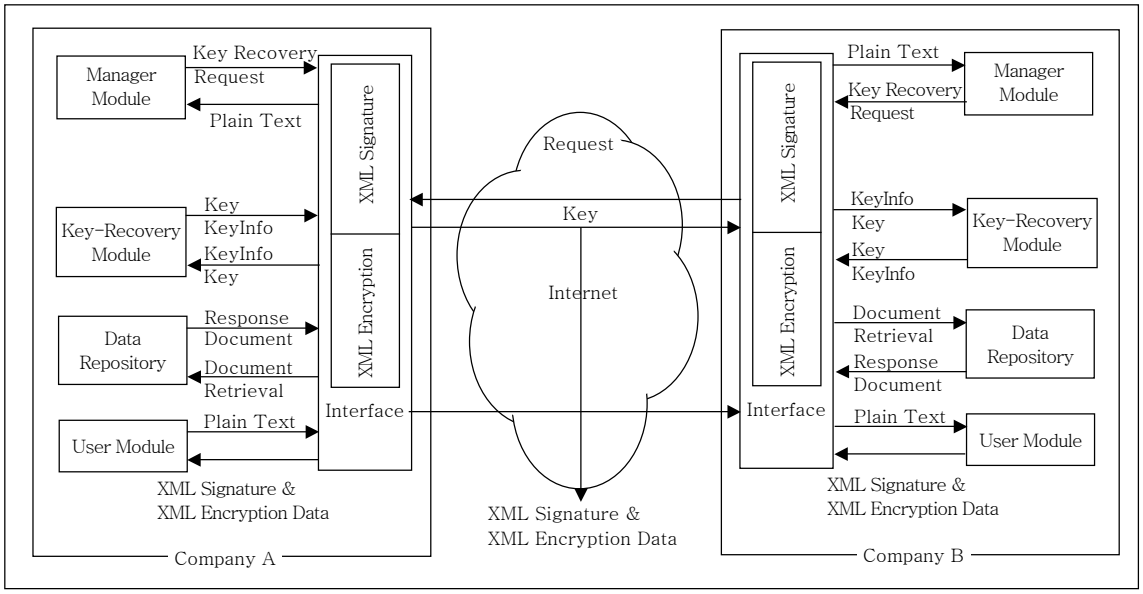
(그림 4) ESES/Cipher의 구조

<표 1> 암호화된 XML 문서 생성 절차

단계	작 업 내 용
1	비밀키를 생성
2	XML 문서를 바이트 스트림으로 변경
3	바이트 스트림을 압축
4	압축된 바이트 스트림을 암호화
5	암호문을 Base64를 이용해 인코딩
6	공개키를 이용해서 비밀키를 암호화
7	Base64를 이용해서 암호화된 비밀키를 인코딩
8	부가정보를 인코딩

3. ESES/XKRS

ESES/XKRS는 B2B를 위한 키 복구 모델은 위와 같이 암호 라이브러리와 그를 기반으로 한 XML



(그림 5) ESES/XKRS 시스템 운영도

전자서명과 XML 암호화가 서브 시스템을 구성한다. 또한, 실제적인 키 복구 시스템 구성을 위해 필요한 데이터 저장소, 사용자 및 관리자 모듈 및 키 복구 모듈 등으로 구성된 키 복구 모듈 등이 키 복구 서브 시스템으로 구성된다. 이 서브 시스템들 위로 응용 프로그램과의 인터페이스를 제공하는 XML 기반 키 복구 인터페이스 서브시스템이 존재한다. 이 인터페이스 서브시스템은 XML 전자서명, XML 암호화, 키 복구 모듈들 및 암호 라이브러리 등의 각각의 서브 시스템들에 대한 구성의 융통성을 제공한다.

각각의 서브시스템들은 응용 프로그램에서 직접 호출할 수 없으며 인터페이스를 통해서만 가능하다. 인터페이스를 통하지 않고 직접 호출이 가능하게 되면, 암호 문서를 만드는 사용자가 임의로 암호화나 서명이 가능하게 되어 문서가 조작될 가능성이 있기 때문이다.

위에서 언급한 바와 같이, XML 전자서명과 XML 암호화는 W3C의 XML 전자서명 그룹과 XML 암호화 그룹에서 각기 정의하고 있는 표준을 따른다. 이렇게 함으로써 내부적으로 암호화해서 데이터 저장소에 저장되는 문서나 그 문서에 대한 키를 저장하는 키 저장소에 대해 보다 편리하고 안전하게 문서나 키를 저장할 수 있다. 또한, 인터넷을 통한 문서의 교환에도 표준을 따르므로 별도의 데이터 통합 작업 등이 필요하지 않게 된다.

(그림 5)는 키 복구 모듈, 데이터 저장소, 사용자 및 관리자 모듈 그리고 그것들 간의 인터페이스 등이 각각 있는 두 기업의 키 복구 시스템들의 운영을 보여주고 있다. 두 기업의 시스템은 모두 동일한 시스템이다.

(그림 5)에서처럼 모든 모듈간의 인터페이스는 논리적으로 한곳에서 관리되고 있으며, 다른 회사와의 인터페이스도 역시 같은 곳에서 관리한다. 그러나, 이 인터페이스들은 물리적으로 모든 모듈에 대해 같은 기능을 하지 않으며 각각의 모듈별로 기능별로 분리된 세부 인터페이스들을 조합하여 사용한다. 예를 들어, 사용자 모듈의 인터페이스에는 XML 전자서명 기능, XML 암호화 기능, 키 생성 기능, 키 복구 모듈에게 생성한 키를 전달하는 기능, 키 복구 모듈로부터 키 정보를 담은 KeyRecoveryInfo 엘리먼트(XML 문서의 한 노드)를 받는 기능, 서명되고 암호화된 결과에 위에서 생성된 엘리먼트를 붙여 최종 암호문을 만드는 기능, 데이터 저장소에 생성된

암호문을 저장하는 기능 등이 포함된다.

데이터 저장소의 인터페이스는 검색 요청에 따른 문서 반환 기능과 문서에 대한 저장 기능 등이 포함된다. 그리고, 키 복구 모듈은 키를 받아 키 정보를 생성하는 기능과 키 정보를 받아 키 복구를 하는 기능이 있다. 관리자 모듈은 문서를 검색 요청하는 기능, 받은 문서에 대한 키 복구 요청 기능 및 복호화된 문서를 표시하는 기능 등을 갖는 인터페이스들이 있다. 이들 세분화되어 있는 인터페이스들은 각각의 모듈에 조합되어 같이 포함되어 있다.

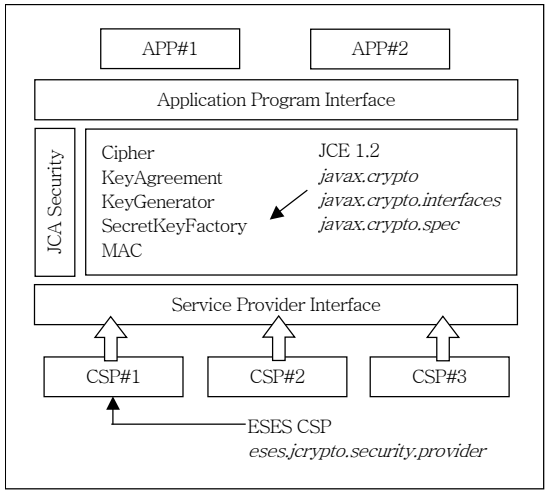
키 복구 대상 문서는 한 회사 내부에서 생성하고 내부에서 사용하는 문서, 내부에서 생성해서 외부 즉, 다른 회사로 보내는 문서, 그리고 외부에서 생성되어 내부로 들어오는 문서로 나뉜다.

내부에서 생성 시에는 XML 암호화 시에 키가 키 복구 모듈에 저장된다. 외부에서 생성된 문서는 복호화 시에 키가 저장되므로, 내부와 외부의 문서에 상관없이 특정 암호문에 관련된 키가 키 복구 모듈에 저장된다. 따라서 한 키 복구 모듈은 내부에서 생성되거나 혹은 외부에서 생성되어 내부로 들어온 문서에 대해서도 모든 키를 저장하고 있게 된다. 물론, 데이터 저장소에는 위의 암호문이 모두 별도로 저장된다. 따라서, 외부에 키 복구 요청을 하지 않아도 자신과 관련된 모든 문서에 대한 키 복구가 가능하다. 물론, 상대 회사도 마찬가지로 자체 내의 문서와 상대 회사에서 생성해서 보낸 문서들을 모두 가지고 있다.

키가 복구되는 지역에 따라 내부 키 복구와 외부 키 복구로 나눌 수 있다. 내부 키 복구는 위에서처럼 한 기업의 내부에 있는 키 복구 모듈을 통해 키 복구를 하는 것이고 외부 키 복구는 다른 기업에 속한 키 복구 모듈에게 키 복구를 요청하는 것이다.

4. ESES/j-Crypto

ESES/j-Crypto는 두 개의 소프트웨어 컴포넌트를 포함한다. 하나는 암호 서비스를 정의하고 자바에서 지원하기 위한 JCE 1.2 규격서[16],[17]



(그림 6) ESES/j-Crypto 컴포넌트

를 구현한 것이고 다른 하나는 (그림 6)에 나타난 것처럼 CSP(Cryptographic Service Provider)라고 불리는 암호 알고리듬 라이브러리 이다. JCE와 ESES CSP는 각각 세 개의 패키지와 하나의 패키지로 구성된다.

ESES CSP는 암호화 알고리듬과 그에 관련된 매개변수들을 실제 구현하여 공급하는 부분으로서 JCE에 플러그 인 되어 사용된다. 현재 몇 가지의 CSP들이 개발되어 있을지라도 ESES CSP는 일반적으로 사용되는 알고리듬 뿐 아니라 국내 표준으로 채택된 알고리듬을 지원한다. 또한 다른 CSP들과 쉽게 접목되어 사용되며 새로운 알고리듬의 추가, 삭제 또한 용이하다. 각 CSP를 구성하는 각 알고리듬들은 JCE로부터 해당하는 SPI를 상속 받아 구현한다[18],[19].

ESES CSP는 대칭키 암호 알고리듬, 비대칭키 암호 알고리듬, 전자서명 알고리듬, 메시지 인증 코드(MAC) 알고리듬, 메시지 다이제스트 알고리듬 등을 포함한다. ESES/j-Crypto에서 지원하는 보안 서비스와 알고리듬이 <표 2>에 나타나 있다. 이는 DSA, RSA, DES, SHA1, 그리고 HMAC처럼 일반적으로 많이 사용되는 알고리듬 뿐 아니라 SEED와 KCDSA와 같이 국내 표준으로 채택된 알고리듬을 포함한다[1],[2].

<표 2> 지원하는 보안 서비스와 알고리듬

보안 서비스	알고리듬
메시지 다이제스트	MD2, MD5, SHA1, HAS160, RIPEMD160
블록 암호 알고리듬	DES, DESede, SEED, RC2, RC4, RC5, Blowfish, IDEA, Rijndael
공개키 암호 알고리듬	RSA, ElGamal
전자 서명	DSA, ElGamal Signature, KCDSA
MAC	HMACwithMD5, HMACwithSHA1
키 동의 알고리듬	Diffie-Hellman

V. 결 론

본 논문에서 전자상거래를 수행하는 중에 발생할 수 있는 보안 문제를 해결하기 위해 개발된 ESES 시스템을 간략하게 소개하였다. ESES 시스템은 ESES/Signature, ESES/Cipher, ESES/XKRS 그리고 ESES/j-Crypto의 네 개 모듈로 구성이 된다. 이 모듈들은 각각 전자서명 기능, 암호화 기능, 키 복구 기능 그리고 암호 알고리듬의 라이브러리를 공급한다.

ESES를 사용하여 전자상거래 응용프로그램 개발자는 XML 문서의 전체 혹은 특정하게 지정된 부분만을 선택하여 서명하거나 암호화 할 수 있다. 이 특징은 연산을 수행하기 위해 필요한 계산 시간을 줄이고 시스템 자원을 적게 사용하는 등 효율성을 높일 수 있도록 한다. 특히 단순히 XML 보안 표준(안)을 구현하는 것이 아니라 표준(안)에서 제공하는 구조를 만족하는 XML 전자서명과 암호문을 생성하기 위한 처리절차를 따르도록 설계하여 개발자의 편의성을 도모하였다.

본 연구의 결과는 잠재적으로 매우 다양한 분야에 적용될 수 있다. 주식 거래 정보, 개발중인 신제품이나 회사에 대한 중요한 기밀 정보, 입찰, 주문, 결제 내역서 등이 인터넷을 통하여 전송되는 경우 ESES에서 제공하는 전자서명과 암호 기능이 적용될 수 있다[20]. ESES는 XML 문서 뿐 아니라 네트워크를 통해 교환되는 모든 종류의 디지털 콘텐츠와 XML 형태로 로컬에 저장되는 데이터에 적용될 수 있고, 그 적용 결과로 XML 형태의 전자서명과 암호문을 생성하기 때문에 기존에 개발되어 사용중인 XML 응용 프로그램과 쉽게 연동할 수 있을 뿐 아니라 정부 정책에 의해 XML이 전자상거래에서 사용되는 문서의 표준 형식으로 채택됨에 따라 그 활용의 범위가 더욱 넓어지고 다양해 질 것이다.

향후 XML 정보보호 기술은 전자상거래의 발전 추이에 따라 요구되는 기술이 다양화 될 것으로 예상된다. 가까운 장래에 전자상거래 형태는 XML을 기반으로 하는 ebXML(e-business XML)과 웹 서비스로 변화할 것이다. 특히 기존 웹을 확장하여, 보여지는 웹에서 업무와 연결되어 수행되고 웹 문서에 의미를 삽입할 수 있는 시맨틱 웹이 ebXML이나 웹 서비스 등의 전자상거래 플랫폼과 결합하여 개인, 회사, 공장, 정부 등 전자상거래 주체들 간이나 상호간의 거래 업무를 유기적으로 분산, 통합되는 형태로 발전할 것으로 전망된다. 이에 따라 시맨틱 웹, ebXML, 웹 서비스를 위한 정보보호 기술로 기존의 ESES 기술을 기반으로 XML 기반의 통신 프로토콜 보안, XML 기반 키 관리, XML 기반 접근 제어, XML 기반 보안정보 교환 기술 등이 필요하다.

참 고 문 헌

[1] M. Mooney and T. Pozil, American Internet user survey, http://www.cyberdialogue.com, 1998.

[2] Joo-Young Lee, Ju-Han Kim, Jae-Seung Lee, Ki-Young Moon, and Hyun-Sook Cho, "ESES: XML Security for Secure Electronic Commerce," *Proceedings of WISA 2001*, Sep. 2001.

[3] 문기영, 이주영, 박치항, "XML 기반 정보보호 서비스 구현," *Proceedings of NCS2001*, 2001. 12.

[4] IBM AlphaWorks Homepage, http://www.alphaworks.ibm.com/tech/xmlsecuritysuite

[5] Baltimore, "X/Secure White Paper," http://www.baltimoreinc.com/library/whitepapers/xsecure.html

[6] Baltimore, "X/Secure Developer's Guide," 1999.

[9] IETF/W3C, XML-Signature Syntax and Processing (Working Draft), Oct. 2000, http://www.w3.org/TR/2000/WD-xmldsig-core-20001012/

[7] IETF/W3C, "XML-Signature Requirements(Working

Draft)," Oct. 1999, http://www.w3.org/TR/1999/WD-xmldsig-requirements-19991014.html
[8] W3C XML Encryption WG, "XML Encryption Charter," http://www.w3.org, 2001.
[10] xml-encryption@w3.org Mail Archives, http://lists.w3.org/Archives/Public/xmlencryption/
[11] J. Daemen and V. Rijmen, "AES Proposeal: Rijnael," http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1999.
[12] A.J. Menezes, P.C. vanOorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC.
[13] W3C, "Canonical XML Version1.0(Working Draft), 2000, http://www.w3.org/TR/2000/WD-xml-c14n-20000907
[14] W3C, "XSL Transformations(XSLT) Version 1.0," Nov. 1999.
[15] W3C, "XML Path Language(XPath) Version 1.0," Nov. 1999.
[16] Sun, Java™ Cryptography Extension 1.2 API Specification and Reference, Sun micro systems, 1999.
[17] Sun, "Java™ Cryptography Architecture API Specification and Reference," Oct. 1999.
[18] J. Knudsen, *Java Cryptography*, O'Reilly, May 1998.
[19] S. Oaks, *Java Security*, O'Reilly, May 1998.
[20] Frank Boumphrey, *Professional XML Applications*, WROX, 1999.