안전한 전자상거래 플랫폼 개발을 위한 ESES의 구현

이 주 영[†]·김 주 한[†]·이 재 승[††]·문 기 영[†††]

요 약

본 논문에서는 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 필요성을 충족시키기 위해서 ESES(ETRI Secure E-commerce Services) 시스템을 제안한다. ESES는 현재 전자상거래 문서의 표준으로 광범위하게 채택되고 있는 XML(eXtensible Markup Language) 문서 뿐 아니라 전자상거래시 교환되는 디지털 컨텐츠를 위한 보안 서비스를 제공을 목적으로 한다. 본 논문에서는 ESES 시스템에 대한 간략한 소개와 함께 전자상거래시스템에 적용될 보안 서비스를 제공하기 위해 어떻게 설계, 구현되었는지를 기술한다. 마지막으로 ESES를 보완하기 위해 필요한 향후 연구과제를 제시한다.

Implementing the ESES for Secure Electronic Commerce Platform

Joo-Young Lee[†]·Ju-Han Kim[†]·Jae-Seung Lee[††]·Ki-Young Moon[†††]

ABSTRACT

The ESES system has been developed to supply a digital signature function, an encryption function, and a library of cryptographic primitives and algorithm for securing an XML document and the existing non-XML documents that are exchanged in the electronic commerce. In this paper, we will introduce the overview of ESES system and explain how the ESES processes to offer security services Finally we'll conclude our talk by presenting the summary and further works.

키워드 : XML 전자서명(XML Signature), XML 암호화(XML Cipher), 암호 알고리즘 라이브러리(Cryptography Algorithm Library), 전자상거래(Electronic Commerce)

1. 서 론

최근 컴퓨터 시스템의 성능 향상과 더불어 빠른 속도로 확산된 인터넷 사용은 전자상거래에 대한 관심을 고조시키고 있다. 시장전문 조사 기관인 IDC는 전세계적으로 전자상거래 규모가 지난 1998년 504.3억 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 이용자수의 9.7%에 해당하는 17만 명에서, 1999년 17.5%인 58만 명, 그리고 향후 2003년에는 47.6%인 486만 명에 이를 것으로 전망된다.

† 정 회 원 : 한국전자통신연구원 정보보호기술연구본부 EC정보보호연구팀 연구원
†† 정 회 원 : 한국전자통신연구원 정보보호기술연구본부 EC정보보호연구팀 연구원
††† 정 회 원 : 한국전자통신연구원 정보보호기술연구본부 EC정보보호팀장/선임연구원
논문접수 : 2001년 8월 1일, 심사완료 : 2001년 9월 27일

이렇게 인터넷 상에서 전자상거래가 부각됨에 따라 인터넷 사업의 필수 인프라인 정보보호에 대한 요구가 절실하다. Cyber Dialogue의 American Internet User Survey(AIUS)에 따르면 전자상거래를 하는데 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 충족이 되어야 한다. 이를 위한 해결 방안으로 본 논문에서는 ESES(ETRI Secure E-commerce Services) 시스템을 제안한다. ESES는 현재 전자상거래의 표준으로 광범위하게 채택되고 있는 XML(eXtensible Markup Language) 문서 뿐 아니라 전자상거래시 교환되는 디지털 컨텐츠를 위한 보안 서비스를 제공하는 것이 목적이다. 이는 전자서명 서비스를 제공하는 ESES/Signature, 암호화 서비스를 제공하는 ESES/Cipher, 그리고 암호화 알고리즘 라이브러리인

ESES/*j*-Crypto로 구성된다.

본 논문에서는 ESES 시스템에 대한 간략한 소개와 함께 전자상거래 시스템에 적용될 보안 서비스를 제공하기 위해 어떻게 설계, 구현되었는지에 대해 기술한다. 마지막으로 ESES를 보완하기 위해 필요한 향후 연구과제를 제시한다.

2. 관련 연구

현재 전자서명과 암호화를 수행하기 위해서 IBM의 AlphaWorks, Baltimore의 X/Secure 등 몇 가지의 XML 보안 제품이 개발되어 있다. IBM의 AlphaWorks는 XML 전자서명과 XML 암호를 위한 기능을 제공하고 있으며 상용화된 제품이 아니라 XML 전자서명의 예제 구현을 위하여 개발되었다. AlphaWorks의 전자서명 모듈은 XML 전자서명 표준 초안 따라 개발되었으며, XML 암호 모듈의 경우에는 자체적으로 정의한 규격에 따라 구현하였다[2].

Baltimore의 X/Secure[3, 4] 또한 XML 전자서명과 암호화를 제공한다. X/Secure도 XML 전자서명 표준문서의 초안에 따라 구현하였지만, 현재 발간된 초안에 명시된 기능들 중 많은 부분을 제공하지 못하고 있다.

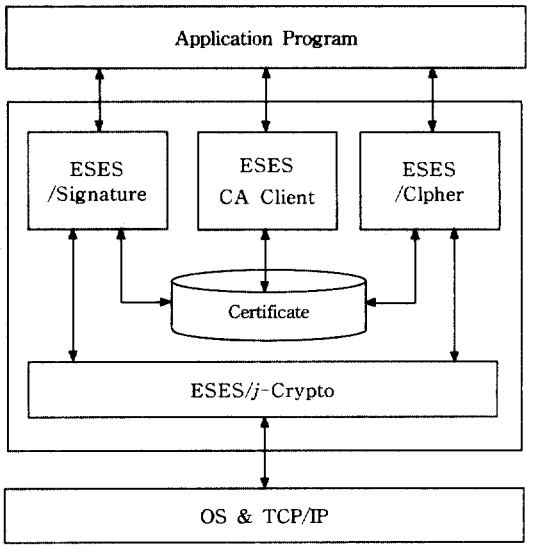
3. ESES의 개요

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

ESES 시스템은 XML Signature 표준(안)[5, 6]과 XML Encryption 표준(안)[7, 8]에 기반하여 각 모듈이 개발되었으며, 실제 응용 프로그램에 적용될 경우, 개발자의 편의성을 향상시킬 수 있도록 각 API를 설계되었다. 이를 위해서 보안 표준(안)에서 정의한 전자서명의 구조를 단순히 생성하는 것뿐 아니라 몇 개의 API들만을 호출함으로써 복잡한 처리절차를 수행할 수 있도록, 많은 부분을 캡슐화 하여 API를 설계하였다. 이는 보안 서비스와 암호 알고리즘에 관련된 지식이 많지 않은 대부분의 응용 프로그램 개발자가 쉽게 사용할 수 있도록 하는데 목적이 있다. 그리고 각 모듈을 기능적으로 분리하여 아직까지 완전하게 표준으로 확정되지 않은 표준(안)이 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 알고리즘을 포함하고 있지 않다는 문제점을 내재하고 있다. 이 문제를 해결하기 위한 방안으로 ESES 시스템은 검증되어진 알고리즘을 제공할 뿐 아니라 국내 표준 알고리즘, 그리고 최근 AES 표준 알고리즘으로 선택된 Rijndael[9]을 지원하고 있으며, 성능이나 강력한 암호 알고리즘으로 알려진 ECC (Elliptic Curve Cryptography) 알고리즘[10]을 개발 중에 있다.

(그림 1)에 ESES 시스템의 구조가 나타나 있다. 이는 ESES/Signature, ESES/Cipher, 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 클라이언트가 포함될 수 있다.



(그림 1) ESES 시스템의 구조

ESES/Signature는 XML 문서를 포함한 임의의 디지털 컨텐츠에 대한 무결성 보장과 인증을 제공하는 것을 목적으로 한다. 이를 위해서 전자서명을 생성하고 검증하는데 필요한 API들과 메시지 다이제스트 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/Cipher는 XML Encryption 초안에 기술된 문서 전체에 대한 암호화와 부분 암호화 기능을 제공한다.

ESES/*j*-Crypto는 암호 알고리즘 라이브러리로 ESES/Signature와 ESES/Cipher에서 필요로 하는 각종 암호 알고리즘을 제공한다.

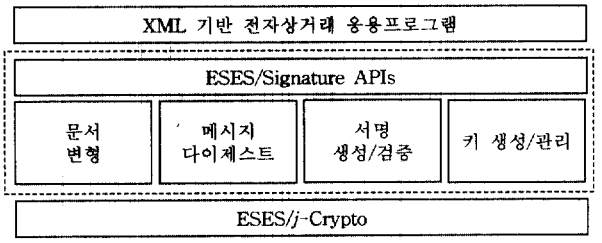
ESES에 의해서 서명이 되거나 암호화가 된 문서의 결과는 XML 형식으로 표현되어 기존의 XML 문서, XML 기반의 전자상거래 플랫폼과 쉽게 통합될 수 있다. 또한 앞서 언급했듯이 ESES는 자바언어를 이용해 API 형태로 개발되었으며, 국제 표준에 따르기 때문에 플랫폼에 독립적이고 B2C(Business to Customer) EC, B2B(Business to Business) EC 그리고 XML/EDI를 위한 다양한 서비스를 개발하는데 있어서 쉽게 사용될 수 있다는 장점을 지닌다.

4. ESES의 설계와 구현

4.1 ESES/Signature

ESES/Signature는 XML 문서뿐 아니라 임의의 디지털 컨텐츠에 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.

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.

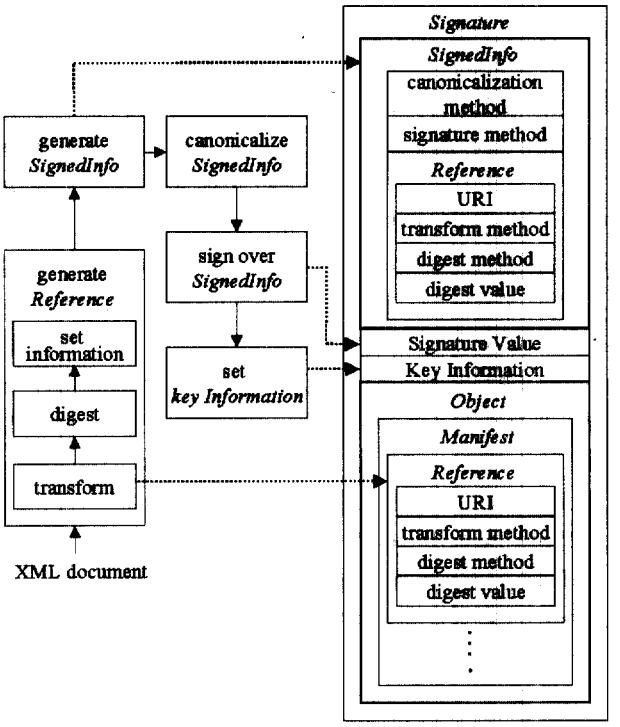


(그림 2) ESES/Signature의 구조

ESES/Signature는 IETF/W3C의 XML Signature 초안을 따르도록 설계되었다. 초안에 명시된 문서의 변형 방법은 Canonical XML[11], Canonical XML with Comments, Base 64 Encoding, XSLT Transform[12], XPath Transform[13] 그리고 Enveloped Signature Transform 등이 있다. 메시지 다이제스트는 ESES/*j*-Crypto를 이용해 서명될 리소스에 대한 다이제스트 값을 얻는 과정으로 SHA1, MD5, 그리고 HAS 160 알고리즘 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 변형알고리즘을 사용하여 적절히 변형한다. 다음으로, 서명대상에 대한 메시지 다이제스트를 수행하고 서명 대상에 대한 URI, 사용한 변형 알고리즘, 다이제스트 알고리즘, 다이제스트 값을 포함하는 *Reference* 라는 이름을 갖는 엘리먼트를 생성한다. 다수의 자원을 한꺼번에 서명하는 경우 각 자원에 대한 *Reference* 엘리먼트들이 직접 *SignedInfo* 라는 이름의 엘리먼트에 포함되거나 혹은 *Manifest* 라는 이름의 엘리먼트에 포함되도록 한다. 후자의 경우, *Manifest* 엘리먼트에 대한 *Reference* 엘리먼트가 생성되어 이 *Reference* 만 *SignedInfo* 구조에 포함되게 된다.



(그림 3) 서명의 생성 과정과 서명의 구조

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

SignedInfo 엘리먼트는 *SignedInfo* 그 자체에 대한 정규화 알고리즘에 대한 정보(*CanonicalizationMethod*), 전자서명 알고리즘에 대한 정보(*SignatureMethod*), *Manifest*에 대한 *Reference*, 기타 다른 자원들을 위한 *Reference* 등을 포함하도록 구성된다.

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

마지막으로 XML 전자서명의 루트 엘리먼트인 *Signature* 엘리먼트는 *SignedInfo* 엘리먼트, *SignedInfo*에 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 *SignedInfo*에 대한 전자서명 검증과 *SignedInfo*에 포함되어 있는 각 *Reference* 의 검증이 이루어져야 한다. XML 전자서명의 구

체적인 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 알고리즘을 사용해서 다이제스트 값을 계산한다. 계산된 다이제스트 값은 해당 *Reference* 엘리먼트에 들어있는 다이제스트 값과 같은지 비교된다. 메시지 다이제스트 알고리즘의 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 *Reference* 들은 이와 같은 방식으로 검증된다.

*SignedInfo*는 우선 *SignedInfo*에 지정되어 있는 문서의 정규화 방법을 이용해 정규화된다. 서명 검증을 위해 *KeyInfo* 엘리먼트로부터 공개키 정보를 가져와 이 정보와 *SignatureMethod* 엘리먼트에서 지정한 서명 알고리즘을 이용하여 *SignedInfo*에 대한 전자서명 값을 검증한다.

Manifest 검증을 위해서는 *Manifest*가 포함하고 있는 각 *Reference*를 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.

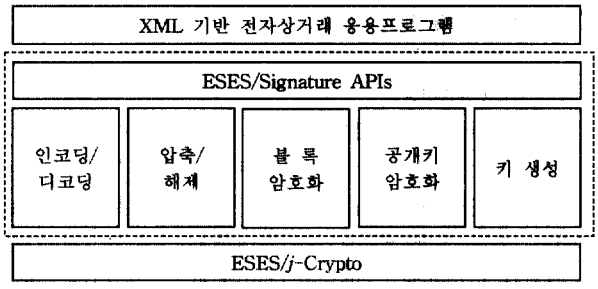
4.2 The ESES/Cipher

XML/Cipher는 XML 문서를 포함한 디지털 컨텐츠를 암호화 하는데 필요한 구문과 처리 방법을 제공하며 XML 문서의 전체 또는 부분에 대한 암호화 방법을 제공한다[19].

(그림 4)는 ESES/Cipher의 구조를 보여준다. 이는 인코딩/디코딩 처리 클래스, 암호 알고리즘 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 암호화하기 위해서 두 단계의 암호화 과정이 필요하다. 첫 번째는 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 알고리즘을 이용해서 암호화된다. 그리고 나서 암호화된 바이트는 XML 노드의 형태로 인코딩 된다.



(그림 4) ESES/Cipher의 구조

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

다음의 <표 1>은 지금까지 기술한 암호화 과정을 정리한 것이다. 암호화된 문서를 풀기 위해서는 먼저 XML 노드로 인코딩 된 부가정보를 디코딩해서 암호화하는데 어떤 알고리즘이 사용되었는지를 점검해야 한다. 수신자의 개인키를 이용해서 XML 문서에 포함된 비밀키를 복호화한다. 그 후 XML 암호문은 선택된 대칭키 암호 알고리즘과 바로 전에 복호화 된 개인키를 이용해서 복호화된다. 그리고 압축된 바이트 스트림의 압축을 풀고, 마지막으로 이 바이트 스트림을 원래의 XML 구조로 복원한다.

〈표 1〉 암호화된 XML 문서를 생성하기 위한 절차

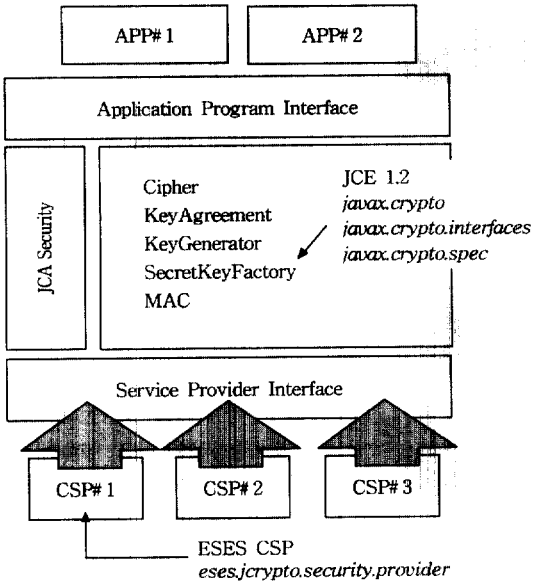
단계	작 업 내 용
1	비밀키를 생성
2	XML 문서를 바이트 스트림으로 변경
3	바이트 스트림을 압축
4	압축된 바이트 스트림을 암호화
5	암호문을 Base64를 이용해 인코딩
6	공개키를 이용해서 비밀키를 암호화
7	Base64를 이용해서 암호화된 비밀키를 인코딩
8	부가정보를 인코딩

4.3 The ESES/j-Crypto

ESES/*j*-Crypto는 두 개의 소프트웨어 컴포넌트를 포함한다. 하나는 암호 서비스를 정의하고 자바에서 지원하기 위한 JCE 1.2 규격서[14, 15]를 구현한 다른 하나는 (그림 5)에 나타난 것처럼 CSP(Cryptographic Service Provider)라고 불리는 암호 알고리즘 라이브러리이다. JCE와 ESES CSP는 각각 세 개의 패키지와 하나의 패키지로 구성된다.

ESES CSP는 암호화 알고리즘과 그에 관련된 매개변수들을 실제 구현하여 공급하는 부분으로서 JCE에 플러그 인 되어 사용된다. 현재 몇 가지의 CSP들이 개발되어 있을지라도 ESES CSP는 일반적으로 사용되는 알고리즘 뿐 아니라 국내 표준으로 채택된 알고리즘을 지원한다. 또한 다른 CSP들

과 쉽게 접목되어 사용되며 새로운 알고리즘의 추가, 삭제 또한 용이하다. 각 CSP를 구성하는 각 알고리즘들은 JCE로부터 해당하는 SPI를 상속받아 구현한다[16, 17].



(그림 5) ESES/j-Crypto의 소프트웨어 컴포넌트

이는 JCE API와 ESES CSP로 구성된다.

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

〈표 2〉 ESES/j-Crypto에서 지원하는 보안 서비스와 알고리즘

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

5. 결 론

지금까지 본 논문에서 전자상거래를 수행하는 중에 발생할수 있는 보안 문제를 해결하기 위해 개발된 ESES 시스템을 간략하게 소개했다. ESES 시스템은 ESES/Signature, ESES/Cipher, 그리고 ESES/j-Crypto의 세 개 모듈로 구성이 된다. 이 모듈은 각각 전자 서명 기능, 암호화 기능, 그리고 암호 알고리즘의 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 처리절차 따르도록 설계하여 개발자의 편의성을 도모하였다.

본 연구의 결과는 잠재적으로 매우 다양한 분야에 적용될 수 있다. 주식 거래 정보, 개발 중인 신제품이나 회사에 대한 중요한 기밀 정보, 입찰, 주문, 결제 내역서 등이 인터넷을 통하여 전송되는 경우 ESES에서 제공하는 전자서명과 암호 기능이 적용될 수 있다[18]. ESES는 XML 문서 뿐 아니라 네트웍을 통해 교환되는 모든 종류의 디지털 컨텐츠와 XML형태로 로컬에 저장되는 데이터에 적용될 수 있고, 그 적용 결과로 XML 형태의 전자서명과 암호문을 생성하기 때문에 기존에 개발되어 사용 중인 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.

지금까지 소개한 ESES가 안전한 전자상거래를 수행하기 위한 보안 서비스를 구현하는데 편리하고 적합한 방법을 제공한다고 할지라도 시스템의 기능을 향상시키기 위해 해야할 과제들이 남아있다. 첫째로, 신뢰성과 안전성을 요구하는 공공기관의 실제 업무에 적용해 볼 필요가 있다는 점이다. 둘째로 온, 오프라인 상거래에서 유용하게 사용될 IC 카드와 연동하기 위한 방법을 포함하는 등 XML 기반의 전자상거래 플랫폼에서 사용하는데 필요한 기능들을 추가할 필요가 있다. 마지막으로 지속적으로 개발되고 있는 새로운 암호 알고리즘의 추가를 통해 더욱 강력한 보안 기능을 제공할 수 있을 것이다.

참 고 문 헌

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

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

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

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

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

[6] IETF/W3C, "XML-Signature Requirements (Working Draft)," http : //www.w3.org/TR/1999/WD-xmldsig-require-ments-19991014.html, October, 1999.

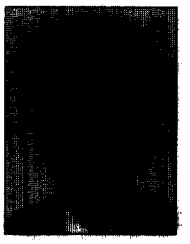
[7] W3C XML Encryption WG, "XML Encryption Charter," http : // www.w3.org, 2001.

[8] xml-encryption@w3.org Mail Archives, http : //lists.w3.

org/Archives/Public/xmlencryption/.
[9] J. Daemen and V. Rijmen, "AES Proposeal : Rijnael," http : //csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1999.
[10] A. J. Menezes, P. C. vanOorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC.
[11] W3C, "Canonical XML Version1.0 (Working Draft)," http : //www.w3.org/TR/2000/WD-xml-c14n-20000907, 2000.
[12] W3C, "XSL Transformations (XSLT) Version 1.0," November, 1999.
[13] W3C, "XML Path Language (XPath) Version 1.0," November, 1999.
[14] Sun, Java™ Cryptography Extension 1.2 API Specification and Reference, Sun micro systems, 1999.
[15] Sun, "Java™ Cryptography Architecture API Specification and Reference," Oct. 1999.
[16] J. Knudsen, *Java Cryptography*, O'Reilly, May, 1998.
[17] S. Oaks, *Java Security*, O'Reilly, May, 1998.
[18] Frank Boumphrey, *Professional XML Applications*, WROX, 1999.
[19] J-H Kim, J-Y Lee, J-C Na, and S-W Sohn, "ESES / Cipher : A Design of XML Encryption System," *Proceeding of the int'l conference in Internet Computing*, Vol.1. pp.206 -212, 2001.

이 주 영

e-mail : joolee@etri.re.kr
1997년 덕성여자대학교 전산학과 졸업 (이학사)
1999년 연세대학교 컴퓨터과학과 석사 (공학석사)
2000년~현재 한국전자통신연구원 정보보호기술연구본부 EC정보보호연구팀 연구원
관심분야 : 전자상거래 보안, 정보보호기술

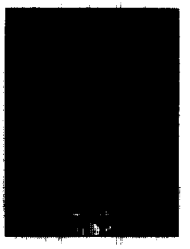


김 주 한

e-mail : juhankim@etri.re.kr
1997년 충남대학교 컴퓨터과학과 졸업 (이학사)
1999년 충남대학교 컴퓨터과학과 정보과학 전공 졸업(이학석사)
2000년~현재 한국전자통신연구원 정보보호기술연구본부 EC정보보호연구팀 연구원
관심분야 : 전자상거래 보안, XML, 정보보호, 워터마킹

이 재 승

e-mail : jasonlee@etri.re.kr
1993년 서강대학교 수학과 졸업(이학사)
1997년 포항공과대학교 정보통신대학원 졸업 (정보통신공학 전공, 공학석사)
1997년~1999년 데이콤 정보통신연구소 인터넷 개발팀, EC기술팀 연구원
1999년~현재 한국전자통신연구원 정보보호기술연구본부 EC정보보호연구팀 연구원
관심분야 : 전자상거래 정보보호, 네트워크 정보보호, 불확정 전송, 보안관리



문 기 영

e-mail : kymoon@etri.re.kr
1986년 경북대학교 전자공학과 졸업(공학사)
1989년 경북대학교 전자공학과 전산전공 졸업(공학석사)
1992년~1994년 (주)대우정보시스템 기술연구소 대리
1994년~현재 한국전자통신연구원 정보보호기술연구본부 EC정보보호팀장/선임연구원