제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

XKMS 웹 서비스 시스템 설계 및 구현

조영근*, 이재동**, 최정기*
*경남대학교 컴퓨터공학과
**경남대학교 정보통신공학부
e-mail : eaglesjo@hawk.kyungnam.ac.kr

A Design and Implementation of XKMS Web Services System

Cho, Young Keun*, Lee, Jae Dong**, Choi, Jung Gi*
*Division of Computer Engineering, Kyungnam University
**Division of Information & Communication Engineering, Kyungnam University

요 약

최근 XML이 웹 상에서 광범위하게 사용되어지면서 XML 관련 기술들의 눈부신 발전 중에 특히, XML 보안관련 기술들이 대형 벤더들의 활발한 참여로 급속히 발전되어지고 있다. 클라이언트 측면에서 전통적인 PKI 기반 구조의 전문적인 면과 복잡성의 배제가 가능한 XKMS 기술을 이용해 클라이언트 애플리케이션 사이에 신뢰적인 관계구축이 용이해졌다. 본 논문에서는 XML 전자서명/암호화, XKMS 등과 같은 XML 보안관련 기술을 이용하여 XKMS 웹 서비스 시스템을 설계하고 구현하였다.

1. 서론

최근 몇 년 사이에 거대한 네트워크로 구축된 전 세계의 컴퓨터들이, 웹(Web)의 등장으로 이용자와 이용 횟수는 급속히 증가하고 있다. 여기에 디지털 통신망의 급속한 발전과 맞물려 정보화 사회로의 전환이 가속화되어 가고 있다. XML(eXtensible Markup Language)의 활용도가 증가하면서, 전자상거래 시에 교환되는 전자문서의 보다 안전한 보안 서비스를 제공하기 위한 방안의 필요성이 제기되어 왔고, XML 문서 보안에 대한 연구개발 또한 활발히 진행되고 있다. XML 환경에서 보안을 위한 핵심 요소 중 하나는 암호 키의 안전한 관리이다. 암호에 의해 보호되는 XML 문서 보안은 직접적으로 키에 대한 보호에 달려있다. 따라서, 신뢰성 있게 수행되어야 하는 전자거래 애플리케이션에서 XML기반의 키 관리에 대한 연구 개발이 중요하다.

PKI(Public Key Infrastructure) 및 공개키 인증서와 XML 애플리케이션의 통합이 용이하도록 베리사인, 마이크로소프트 및 웹메소드는 개방형 XKMS(XML Key Management Specification) 규격을 작성하였고[1], XKMS는 공개키(Public Key) 관리를 위한 프로토콜을 정의한다. 공개키 기술은 XML 전자서명과 XML 암호화, 기타 여러 보안 응용에 필수적으로 사용되며, 전자서명을 위해 전자문서를 송신 측에서 개인키(Private Key)로 서명하고, 수신측은 상대방의 공개키로 서명을 검증한다. 또, 암호화에서는 공개키로 암호화하고 개인키로 복호화한다. XML 키 관리는 서명을 검증하거나 암호화하는 공개키의 공유를 효율적으로 도와주는 기능을 정의하는 것이다.

웹 서비스 보안 영역에서 XML 전자서명은 핵심 요소 기술로 자리잡고 있으며 이는 XML 보안 관련 기술들과 더불어 안전하고 신뢰성 있는 비즈니스 프레임워크 구축에 있어 핵심 기능을 수행할 것이다.

본 논문에서는 안전한 데이터교환을 위한 XML 정보보호 기술 중 하나인 XKMS를 통해 XKMS 웹 서비스를 설계하고 구현한다.

2. 관련연구

2.1 XML 전자서명

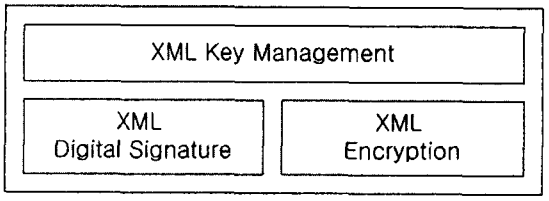
XML 전자서명(XML Signature)은 XML을 포함한 디지털 컨텐츠에 대한 전자서명을 XML 형태로 생성하고 검증하기 위한 표준이다[2].

2.2 XML 암호화

XML 암호화(XML Encryption)는 XML을 포함한 다양한 디지털 컨텐츠에 대한 암호문을 XML 형태로 생성하고 복호화하는 암호화 기법을 말한다[3].

2.3 XKMS

XKMS는 암호 기능이 있는 XML 애플리케이션을 인증하기 위한 포괄적이고 개방이며 표준적인 접근 방식을 취하는 구조를 가진다. 구조는 XML 전자서명과 XML 암호화 워킹그룹내의 W3C(World Wide Web Consortium) 표준화 활동과 호환성이 있도록 설계된다[1,4]. [그림 1]은 XKMS의 전체 구조에서 XML 전자서명과 XML 암/복호화 사이의 관계를 나타낸 것이다.



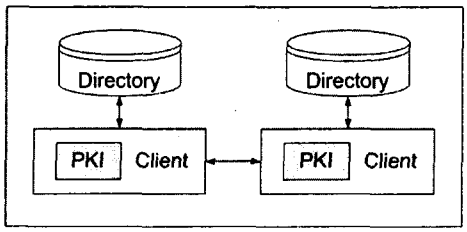
[그림 1] XML 전자서명/암호화와 XKMS의 관계

XKMS는 전자서명, 암호화된 XML 문서를 지원할 경우 PKI 기능을 XML 기반 애플리케이션에게 용이하게 지원할 수 있는 공개키의 관리를 위한 프로토콜을 정의한다. 최초 설계 목적은 XML 전자서명과의 연동 시, 기존 PKI 시스템에 대한 복잡성을 클라이언트에게 숨겨 키 관리 부담을 신뢰 서비스(Trust Service)에 위임해 그 구현을 용이하게 하기 위함이다. 주요목적은 전자서명을 검증하거나 데이터를 암호화하기 위해 사용되는 공개키 사용자에게 필요한 키의 위치를 명시하고, 이름이나 속성 정보를 해당 개인키 소유자와 관련지어 주는 것이다. XKMS는 인증서 정보를 제공하는 X-KISS(XML Key Information Service Specification)와 인증서 관리를 위한 X-KRSS(XML Key Registration Service Specification)의 두 부분으로 구성된다.

2.4 PKI

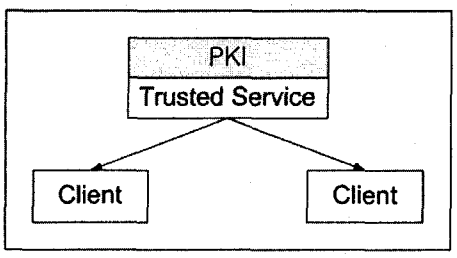
PKI는 기본적으로 인터넷과 같이 안전이 보장되지 않은 공중망 사용자들이, 신뢰할 수 있는 기관에서 부여된 한 쌍의 공개키와 개인키를 사용함으로써, 안전하고 은밀하게 데이터나 자금을 교환할 수 있게 해준다[6]. PKI는 한 개인이나 기관을 식별할 수 있는 디지털 인증서와, 인증서를 저장했다가 필요할 때 불러다 쓸 수 있는 디렉토리 서비스를 제공한다.

PKI는 [그림 2]와 같은 구조를 가진다.



[그림 2] 전통적인 PKI 구조

전통적인 PKI 구현의 복잡성에 비해 XML의 단순성은 비즈니스 시스템 간 데이터의 간편한 응용성을 제공한다. XKMS와 XML 신뢰 서비스의 주요목적은 XML 애플리케이션을 전통적인 PKI 구현의 복잡성으로부터 분리하자는 것이다. XKMS는 XML 처리가 수행되는 클라이언트 플랫폼 상에서 복잡하거나 전문화된 PKI 애플리케이션 도움 없이 XML 기반 시스템이 신뢰적 관계를 구축한다.



[그림 3] PKI에 XKMS를 적용한 구조

XKMS는 애플리케이션을 공개키 기반 구조에 결부시킴으로써 소프트웨어 개발자들이 [그림 3]과 같이 PKI를 좀더 저렴하고 쉽게 사용할 수 있도록 하기 위한 방식이며, 사용자 측면에서 PKI를 단순화시키는 것이다.

2.5 웹 서비스 보안

웹 서비스는 표준화된 XML 기반의 메시지 및 전송 프로토콜을 통해 인터넷 상에 존재하는 실행 가능한 애플리케이션에 접근하는 표준적인 기술들의 통합을 의미한다[7]. 구성요소는 SOAP, WSDL(Web Service Description Language), UDDI(Universal Description, Discovery, and Integration)가 있다. 최초 SOAP 명세는 어떠한 보안 요소도 포함하고 있지 않았으나, 최근 마이크로소프트와 IBM, 베리사인을 중심으로 웹 서비스 보안(WS-Security) 명세가 제안됨으로써 새로운 SOAP 메시지의 인증, 무결성 보장, 부인 방지 등을 위한 보안 모델을 제시하고 있다. 이 명세는 기존의 SOAP-SEC : 전자서명 명세를 대체하는 역할을 수행함으로써 향후 웹 서비스 메시지 보안 모델의 표준 기술로 채택될 전망이다.

웹 서비스 보안 명세에서는 SOAP 헤더 내에 엘리먼트를 새롭게 정의해 수신측에서 요구하는 보안 정보를 포함시킨다. 엘리먼트를 통해 메시지 송신자를 식별하며 엘리먼트로 XML 전자서명을 검증하는데 필요한 서명 정보를 포함하도록 규정하고 있다.

3. 설계 및 구현

3.1 개발환경

본 논문은 XKMS 웹 서비스의 구현 시 개발환경은 [표 1]과 같다.

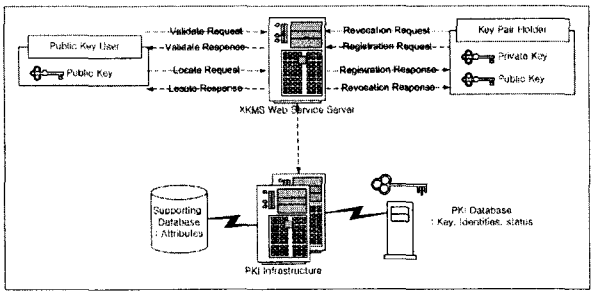
환경	개발 툴
언어	J2SE
웹 서비스, JSP 엔진	Apache Tomcat
XML Signature/Encryption	IBM XML Security Suite (XSS4J)
SOAP RPC/Message	Apache SOAP을 활용해서 SecureSOAP 구현
XML 파서	Xalan-Java, Xerces-Java

[표 1] XKMS 웹 서비스 개발환경

3.2 시스템 구성

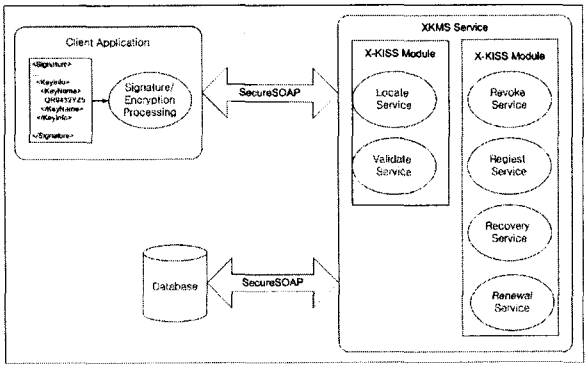
XKMS 웹 서비스는 PKI와 애플리케이션 사이의 인터페이스를 제공하므로, 애플리케이션은 XKMS 웹 서비스를 통해 복잡하고 전문화된 PKI 애플리케이션의 도움 없이 PKI 시스템과 신뢰적 관계가 구축가능하다.

[그림 4]에서는 XKMS 웹 서비스의 흐름을 나타내고 있다.



[그림 4] XKMS 웹 서비스 흐름도.

본 논문에서는 [그림 5]과 같이 XKMS 웹 서비스 시스템을 구현하였다. 현재 PKI 기반 시스템은 설계 중에 있다.



[그림 5] XKMS 웹 서비스 시스템 구성도

3.3 XKMS 웹 서비스 서버

각 서비스들은 다음과 같은 과정으로 동작한다.

3.3.1 Locate 서비스

XML 서명을 포함하는 XML 문서를 검증해야 하는 애플리케이션이 있다.

1. 이 애플리케이션은 <ds:Signature> 엘리먼트를 포함하는 XML 문서를 XKMS 서버에 전송한다.
2. <ds:Signature> 엘리먼트에서 <ds:KeyName>을 포함한 <ds:KeyInfo> 엘리먼트를 추출하여 Locate 서비스에 전송한다.
3. KeyName에 부합하는 X.509 인증서를 키 저장소에서 검색한다.
4. 인증서를 찾아서 <ds:KeyInfo> 엘리먼트 형태로 만들어 애플리케이션에 반환한다.

3.3.2 Validate 서비스

1. Locate 서비스를 실행한다.
2. 애플리케이션은 <ds:KeyInfo> 엘리먼트 형태의 인증서를 Validate 서비스에 전송한다.
3. KeyName과 공개키 간의 바인드를 확인한다.
4. KeyName과 공개키를 애플리케이션에 반환한다.

<xkms:Status>의 값으로 유효성 검사결과를 확인가능하다.

3.3.3 Registration 서비스

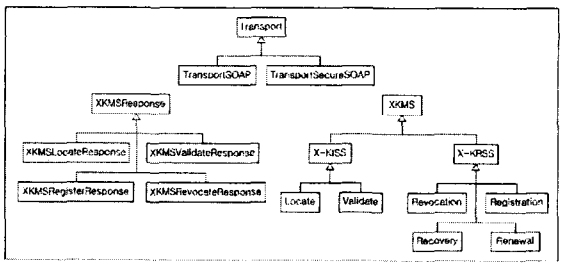
Key Pair Holder의 경우는 먼저 키쌍을 생성한다.

1. KeyName, 공개키, 개인키 소유증명을 포함해서 등록을 요청한다.
2. Registration 서비스는 1의 정보를 가지고 소유증명을 확인한다.
3. 등록 결과를 애플리케이션에 반환한다.

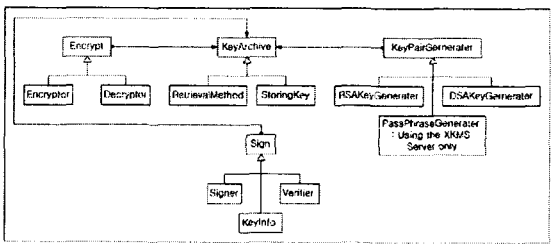
Public Key User의 경우는 소유 증명이 필요하지 않고, 서버에서 생성된 키쌍과 등록결과를 반환받는다.

3.3.4 Revocation 서비스

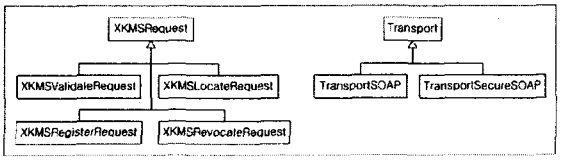
Registration 서비스에서 등록된 <xkms:Status> 엘리먼트의 값이 Invalid로 바뀐다. 개인키 소유를 증명하는 서명이 필요하다.



[그림 6] XKMS 서버 SDK 구성도



[그림 7] Utilities SDK 구성도



[그림 8] XKMS 애플리케이션 SDK 구성도

[그림 6], [그림 7], [그림 8]은 XKMS 웹 서비스 시스템의 SDK를 도식화한 것이다.

4. 결론

본 논문에서는 PKI의 차세대 모델이라고 할 수 있는 XKMS를 통해서 개발자들이 다른 애플리케이션에 쉽게 접목시킬 수 있는 XKMS 웹 서비스 및 XKMS SDK를 설계하고 이를 구현하였다.

XKMS 웹 서비스를 통해서 애플리케이션 상에서 복잡하거나 전문화된 PKI 애플리케이션과의 연동 없이 XML 기반 시스템이 신뢰적 관계를 구축 가능하다.

SOAP에 XML 전자서명과 암호화 기술을 적용해서 SecureSOAP을 구현함으로써 더욱 확고한 보안성을 부여하였다.

참고문헌

[1] XML Key Management Specification (XKMS) Version 2.0, W3C Working Draft 18 April 2003.

[2] W3C. "XML-Signature Syntax and Processing", 12 February 2002

[3] W3C, "XML Encryption Syntax and Processing", 10 December 2002.

[4] Blake Dournaee, "XML Security", RSA Press, 2002.

[5] Kitty Niles, 외 1명, "Secure XML", Addison-Wesley, 2002.

[6] Andrew Nash 외 3명, "PKI", McGraw-Hill, 2001.

[7] Mark O'Neill, "Web Services Security", McGraw-Hill, 2003.

[8] W3C. "SOAP Version 1.2 Part 0, Part 1 Part 2", 24 June 2003.

[9] Ben Galbraith외 7명 공저. "Professional Java Web Services", Wrox Press, 2002.

[10] Jess Garms, Daniel Somerfield. "Professional Java Security", Wrox Press, 2001