안전한 전자상거래를 위한 XML 키 정보 서비스 모델링

XML Key Information Service Modeling for Secure Electronic Commerce

박남제(Nam-Je Park)*, 문기영(Ki-Young Moon)*, 송유진(You-Jin Song)**

초 록

XML(eXtensible Markup Language)은 인터넷과 e-비즈니스를 위한 글로벌 표준으로서 전자상거래의 보급 속도에 따라 XML의 활용도가 증가하고 있다. 이러한 환경에서 전자상거래시에 교환되는 전자문서의 보다 안전한 보안서비스를 제공하기 위한 방안이 필요하다. XML 정보보호 기술 중 XML 키 관리 규격(XKMS)은 다양하고 복잡한 기능의 전자상거래 애플리케이션에서 전자문서의 서명을 검증하거나 암호화하는 공개키를 관리하는 프로토콜을 정의한다. 본 논문에서는 XML 기반 보안서비스 특성에 착안하여 안전한 전자상거래를 위한 XML 키 정보 서비스(X-KISS)에 대한 분석과 표준안에 근거한 서비스 참조 모델을 제시하고, 기반되는 서비스 컴포넌트를 구현하여 서비스 모델링을 수행하였다. 본 논문에서 제시된 참조 모델은 식별정보가 주어졌을 때, 필요로 하는 공개키 위치와 식별자 정보, 공개키 연결 기능을 제공한다. 구현한 클라이언트 서비스 컴포넌트의 요청 및 검색 쓰레드의 비율을 제한하여 실시간 키 검색에 대한 컴포넌트의 최소 성능을 분석하였다. 본 논문의 서비스 모델링은 향후 국내 e-비즈니스 프레임워크 구성 시 표준적인 보안 모델을 구현할 수 있는 지침을 제공할 것이다.

ABSTRACT

XML is a global standard for the Internet and e-business, and its use is growing in proportion to the spreading speed of e-Commerce. Thus, a policy for providing more safe security service for exchanging e-documents within e-Commerce is necessary. XKMS, one of XML security specification, defines the protocol for distributing and registering public keys for verifying electronic signatures and enciphering e-documents of e-Commerce applications with various and complicate functions. In this paper, we propose X-KISS service reference model and implement service component based on standard specification. Also describes the analysis and security of XML key information service for safe e-Commerce, paying attention to the features of XML based security service. This reference model supported include public key location by given identifier information, the binding of such keys to identifier information. The client service component controls the number of locate threads and validate threads to analyze the minimum requirements of real-time key retrievals. This service modeling offers the security construction guideline for future domestic e-business frameworks.

키워드 : XKMS, XML보안, XML, 키 관리
XKMS, XML Security, XML, Key Management

* 한국전자통신연구원 정보보호연구본부 능동보안기술연구팀
** 동국대학교 전자상거래대학원

1. 서 론

최근 XML이 인터넷 전자상거래와 데이터 전송 및 검색 부문에서 광범위하게 이용됨에 따라, XML 문서에 대한 보안 문제가 대두되고 있다. 전자문서 및 데이터를 보호하는 일은 전자상거래에서 필수적인 사항이며, XML 문서 보안에 대한 연구개발 또한 활발히 진행되고 있다. XML 환경에서 보안을 위한 핵심 요소 중 하나는 암호키의 안전한 관리이다. 암호에 의해 보호되는 XML 문서 보안은 직접적으로 키에 대한 보호에 달려있다. 따라서 신뢰성 있게 수행되어야 하는 전자상거래 애플리케이션에서 XML 기반의 키 관리에 대한 연구 개발이 중요하다.

PKI(Public Key Infrastructure) 및 공개키 인증서와 XML 애플리케이션의 통합이 용이하도록 Verisign, Microsoft 및 WebMethods는 개방형 XKMS(XML Key Management Specification) 규격을 작성하였다[7]. XML 키 관리 명세는 공개키 관리를 위한 프로토콜을 정의한다. 공개키 기술은 XML 전자서명과 XML 암호화, 기타 여러 보안 응용에 필수적으로 사용되며, 전자서명을 위해 전자문서를 송신 측에서 개인키로 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.

XML 처리가 수행되는 클라이언트상에서 복잡하거나 전문화된 PKI 규칙을 필요로 하지 않고 XML 기반 시스템이 신뢰관계를 구축하는 XML 키 관리 서비스 모델은 PKI 기반의 복잡성으로부터 벗어나 XML 클라이언트의 구현을 용이하게 할 수 있다[7].

현재 W3C(World Wide Web Consortium)에 의해 XKMS 2.0 버전의 Draft 상태로 계속 표준화가 진행 중에 있어 이를 완전히 구현한 제품도 세계적으로 드문 실정이다. Verisign, IBM, MS, RSA Security, Phaos[21] 등의 회사들이 연구 개발을 진행 중이거나 시제품을 개발하고 있다[15]. 국내의 경우는 한국전자통신연구원(ETRI) 정보보호연구본부에서 ESES(ETRI Secure E-Commerce Services) XML 보안 플랫폼을 기반으로 기술 개발이 진행 중에 있다[1,2].

본 논문에서는 안전한 전자상거래를 위한 XML 정보보호 기술 중 하나인 XML 키 관리 기술에 대해 분석하며, 표준안에 근거한 XML 키 정보 서비스 참조 모델을 제시하고, 표준 컴포넌트를 구현하여 서비스 모델링을 수행하였다. 참조 서비스 모델링을 수행함에 있어 키 정보 서비스 서버의 설계와 동작 프로세스를 기술하고, 키 정보 서비스 모델링 구현에 대해 설명한다. 본 논문의 구성은 다음과 같다. 2장에서 XML 키 정보 서비스에 대해 기술하며, W3C에서 진행 중인 표준안에 근거하여 XML 키 관리의 구조와 처리 절차를 중심으로 설명한 다음, 3장에서 서비스의 요구사항을 분석하고, 이를 바탕으로 4장에서 XML 키 정보 서비스 참조 모델링에 대하여 기술한다. 5장에서는 서비스의 안전성과 기능 및 성능평가를 기술하며, 마지막으로 6장에서 결론을 맺는다.

2. XML 키 정보 서비스

XML 키 관리 명세인 XKMS는 전자서명, 암호화된 XML 문서를 지원할 경우 PKI 기능을 XML 기반 애플리케이션에게 용이하게 지원할 수 있는 공개키의 관리를 위한 프로토콜을 정의한다[7]. XKMS는 X-KISS(XML Key Information Service Specification)와 X-KRSS (XML Key Registration Service Specification)의 두 영역으로 구성되어 있다[7]. 두 프로토콜은 XML SchemaLanguage [13,14], WSDL(Web Services Definition Language)[19]에 의해 정의된 메시지 사이의 관계와 SOAP(Simple Object Access Protocol)을 채택하는 프로토콜 내에서 표현된 구조로 정의된다[10,11]. 또한, 다른 여러 객체 구조에서 XKMS의 적용도 가능하다[11]. 본 장에서는 XML 키 관리 서비스 중 키 정보 처리를 지원하는 X-KISS에 대해 살펴본다.

2.1 XML 키 정보 서비스 규격

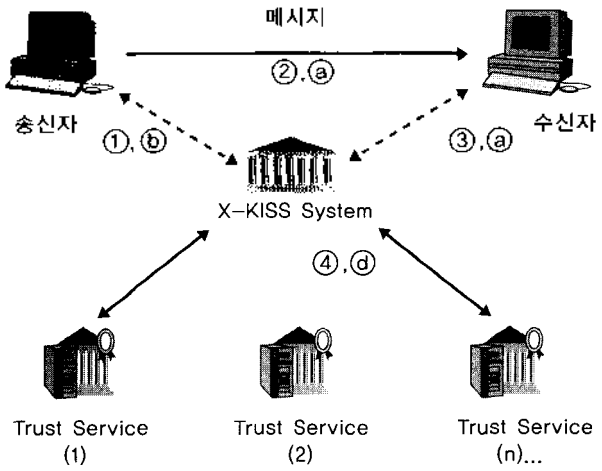
XML 신뢰 기반의 중심인 XML 키 정보 서비스는 XML 기반 애플리케이션에서 신뢰할만한 제 3자에 의해 XML 전자서명, XML 암호화 데이터 또는 기타 공개키 사용과 관련된 키 정보의 처리를 지원하는 프로토콜을 정의한다[7]. 주요 기능은 주어진 식별자 정보에 필요한 공개키의 위치를 부여하고 공개키를 연결하는 것이다.

XML 키 정보 서비스의 규칙에 따른 전자서명 절차는 다음과 같다[6].

① 송신자는 자신의 공개키를 X-KISS 서버에 등록한다.

② 서명된 메시지가 수신자에게 전송된다.

③ 수신자는 공개키를 불러와서 서명을 검증한다.



〈그림 1〉 암호화 및 서명의 XML 키 정보 서비스 절차

④ 키의 정보가 없거나 위의 경우가 아니면, X-KISS 서버가 다른 KISS 혹은 다른 형태의서비스로부터 서명된 키 정보를 가져온다.

XML 키 정보 서비스에서의 메시지 암호화 절차는 다음과 같다[4,6].

ⓐ 수신자가 자신의 공개키를 X-KISS 서버에 등록한다.

ⓑ 송신자는 수신자의 공개키를 불러와 메시지를 암호화한다.

ⓒ 수신자가 메시지를 받아서 복호화한다.

ⓓ 키의 정보가 없거나 위의 경우가 아니면, X-KISS 서버가 다른 KISS 혹은 다른 형태의 서비스로부터 암호화 키 정보를 가져온다.

2.2 XML 키 정보 서비스 프로토콜

X-KISS 프로토콜 설계의 핵심적인 목표는 기본적인 PKI에서의 구문과 응용 구현의 복잡함을 최소로 하기 위한 것이다[7,24]. 기본적인 PKI는 X.509/PKIX, SPKI(Simple PKI) 및 PGP(Pretty Good Privacy)와 같은 다른 명세에 기초를 두고 있다[17,18]. 특정 응용 애플리케이션에서의 강화된 PKI 서비스를 지원하기 위해 X-KISS에서는 계층적 서비스 모델로 세분화시킴으로서, 업무에 따른 정확한 처리 계층을 선택할 수 있도록 정의하고 있다[7].

각각의 계층적인 구조 내부에서 'Trust Service'는 복잡한 구문과 의미의 효율적인 조작, 디렉토리와 데이터 저장 하부 구조로부터의 정보검색, 상태 확인 및 취소, 인증 관계의 생성과 처리와 같은 기능을 클라이언트에게 제공한다.

2.2.1 XML 키 위치정보 서비스 (Locate Service)

XML 서명을 포함하는 XML 문서를 검증해야 하는 애플리케이션이 있으면, 이 애플리케이션은 〈ds:Signature〉 엘리먼트를 포함하는 XML 문서를 참조하는 파일이나 스트림(Stream), URI(Uniform Resource Identifier)

〈표 1〉 Tiered Service Model

구 분	서비스명	내 용	비 고
Tier 0	-	애플리케이션에 의한 〈KeyInfo/RetrievalMethod〉 요소 처리	M
Tier 1	Location	애플리케이션에 위임된 서비스에 의해 〈ds:KeyInfo〉 요소 처리	M
Tier 2	Validation	Tier 1에서 추가 이외에 서비스에 기록된 그 이상의 정보에 관한 데이터는 〈ds:KeyInfo〉 블록에서 규정	M
Tier 3	Assertion	장기간 신뢰관계의 설립과 관리	M
Tier 4	Assertion Status	신뢰 확인상태의 관리	M

(M : Mandatory, O : Optional)

값을 받아들인다. 서명의 유효성을 검증하기 위해 클라이언트에 의해 인증 경로를 통해서 유효성을 확인한다[12,25].

2.2.2 XML 키 유효성 검사 서비스 (Validate Service)

키의 검증 서비스는 이름과 공개키 간의 연결에 대한 신뢰를 확인하는 일을 한다. 이 서비스는 앞의 키 검색 서비스를 포함하고 있으므로, 이름과 키 간의 관계를 알아보는 것뿐만 아니라 키의 위치도 알아낸다[12]. 클라이언트는 공개키와 다른 데이터들 사이의 여러 값을 전달받아 공개키와 연계하여 응답받은 데이터의 유효성을 검증한다.

2.2.3 기타 서비스

Tier 3,4의 'Assertion Service'는 장기 신뢰성 관계들이나 신뢰성 확인 상태 등의 서비스를 정의한다. 이는 요청에 의한 부가적인 서비스로 진행하며, XKMS 2.0 규격안에서는 Tier 1,2에 포함되어 정의하고 있다.

3. XML 키 정보 서비스 요구사항 분석

3.1 보안 요구사항

XML 키 정보 서비스를 제공하기 위해서는 상호 운영성(interoperability), 확장성(scalability), 효율성(efficiency), 신뢰성(reliability) 및 보안성(security) 등을 고려하여야 한다. 여기서, XML 정보보호는 기본 보안 요구사항을 고려하면서 전송계층 및 응용계층에서 안전성이 제공되어야 하고, XML 키 정보 서비스로서 안전하게 제공하기 위한 보안 대책도 필수적으로 요구된다. 여기서 XML 기반 응용 서비스에서의 기본 보안 요구사항을 기반으로 키 정보 서비스의 보안 요구사항을 살펴보면 다음과 같다.

이러한 기본 보안 요구사항 외에 부가적으로 요구되는 보안 요구사항은 다음과 같다. XML 키 정보 서비스는 기존의 PKI와 상호 연동되면서 구축된 PKI 시스템 변경을 최소로 하는 등 실용적이어야 하며, 활용성을 높

〈표 2〉 기본 보안 요구사항

내 용	요 구 사 항
개인의 프라이버시 보장 (Privacy)	사용자의 요청이 없으면 키 관리 서버는 사용자의 암호키 분배용 개인키에 접근할 수 없어야 한다.
XML 키 정보 발신처 인증 (User Authentication)	연결 설정 과정에서 서로 간에 신뢰할 수 있도록 클라이언트/서버 간에 상호 인증을 할 수 있도록 해야 한다.
메시지 및 키 검증의 무결성 (Data Integrity)	내부적으로 데이터 전송을 방해할 수 없도록 하거나 재전송 공격에 이용할 수 없도록 메시지의 무결성 및 키 검증 절차에 대한 무결성을 제공해야 한다.
수신 및 발신 부인방지 (Non-Repudiation)	송·수신되는 암호키 정보의 송·수신 부인방지에 대한 기능을 제공해야 한다.

이기 위해 키 백업 기능 외에 키 로밍 서비스 등과 같은 부가 서비스를 제공할 수 있어야 하고, 사용자의 프라이버시를 최대한 보장함으로써, 사용자의 자발적 키 위탁을 유도할 수 있어야 한다.

3.2 XML 전자서명 유효성과 신뢰의 요구사항

XML 키 정보 서비스는 적용된 보안과 키 관리의 많은 부분을 다루고 있다. 암호화의 검증은 X.509 인증서에 포함된 공개키를 사용하고, 서명자에 대한 신뢰 문제는 신뢰 컴포넌트가 수행하지만 서명이 검증하는 것만으로는 충분하지 않기 때문에 다른 사람의 식별자를 사용하여 키를 생성하고 문서에 간단히 서명할 수 있는 식별자와 공개키 사이의 연관관계를 확인할 필요성 있다. 이는 경로의 유효성을 검증하여 확인이 가능하며, 경로 유효성 검사에는 서명 유효성, 유효성 검사, 이름 연결, 인증서 철회 등과 같은 일이 수행되어야 한다. XML 키 관리에서는 XML 키 정보 서비스가 이의 신뢰 컴포넌트 역할을 수행함으로써 공개키의 정보와 신뢰 확인을 얻는 역할을 한다.

3.3 전자서명 기능 요구사항

XML 전자서명 알고리즘은 W3C에서 권고된 알고리즘을 사용하여야 한다. XML 서명 문서의 생성, 검증 처리와 관련하여 XML 전자서명 기능은 XML 전자서명 규격에서 규정되는 모든 표준 알고리즘을 지원해야 한다[8].

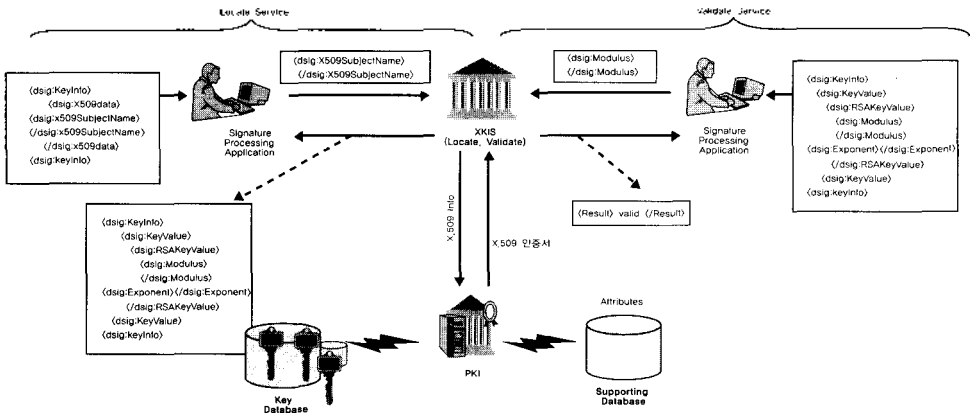
4. XML 키 정보 서비스 모델링

4.1 모델링 환경

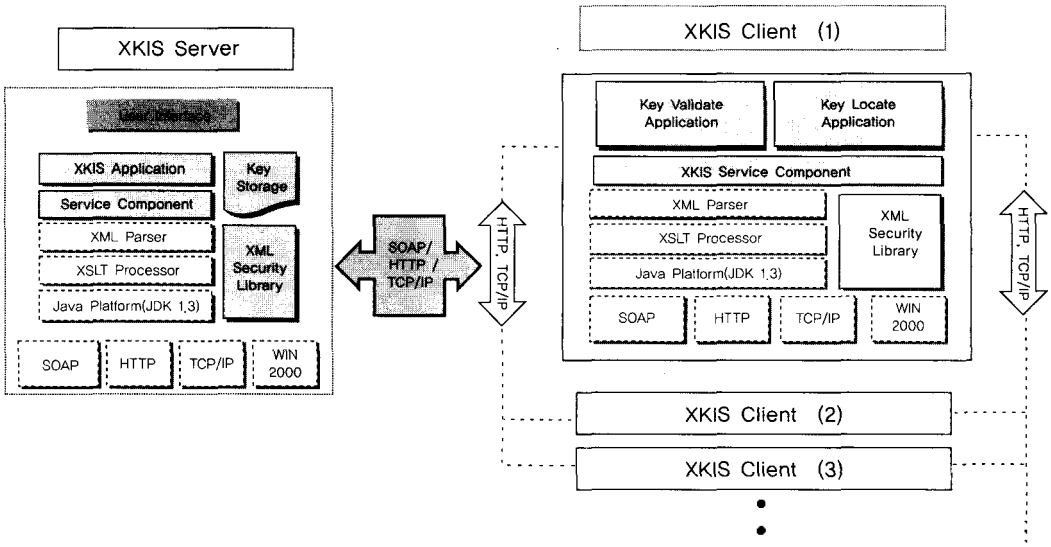
본 논문에서 구현한 참조 서비스 모델의 환경은 펜티엄 Ⅲ 사양에서 TCP/IP 환경을 기반으로 아파치 웹 서버를 사용하였다. 운영체제는 Windows 2000 서버에서 개발되었으며, 자바 환경을 통하여 네트워킹 프로그램이 운용되도록 하였다. 웹 서버와 데이터베이스 시스템은 본 논문의 구현 애플리케이션에 적용되지 않았지만, 향후 업그레이드 버전으로 구성될 예정이므로 기반 환경으로 설정하였다.

XML 키 정보 서비스를 수행하기 위한 메시지 처리와 처리 후의 메시지 처리는 메시지 처리 클래스에서 수행한다. 웹 서비스를 전제로 하고 있으므로 클라이언트에서 키 정보 서비스로의 요청 메시지는 SOAP 메시지 형태이며, 사용자 서명과 함께 암호화되어 있다. 반대로 클라이언트로의 응답 메시지는 메시지를 서명해서 암호화하는 과정을 거쳐야 한다〈그림 2 참조〉.

X-KISS 서버 컴포넌트는 윈도우 환경의 자바 플랫폼을 기반으로 하며, XML 보안 라이브러리를 이용해 구현하였다. 클라이언트는 XML 보안 라이브러리를 기반으로 여러 가지 모듈들을 운용한다. 〈그림 3〉은 본 논문에서 개발된 서비스 참조 시스템의 구조를 나타낸 것으로, 음영부분의 서비스 컴포넌트 팩키지 부분이 서비스 모델링을 위해 개발된 영역이다.



〈그림 2〉 XML 키 정보 서비스 모델 구성



〈그림 3〉 X-KISS 서비스 참조 시스템 구조

4.2 구현 라이브러리 플랫폼 구조

본 논문에서 구현된 라이브러리 플랫폼은 자바 플랫폼에서 참조 모델 구현 기능을 제공하는 프레임워크이다. XML Security API는 암호화와 관련된 보안 플랫폼 API이고, 다중, 교차연산 가능한 암호화 작용을 허용하는 프로바이더 구조로 표현된다. SOAP Security API는 XML 웹 서비스 상의 보안을 제공하며 키 교환과 암호화를 지원한다. XML

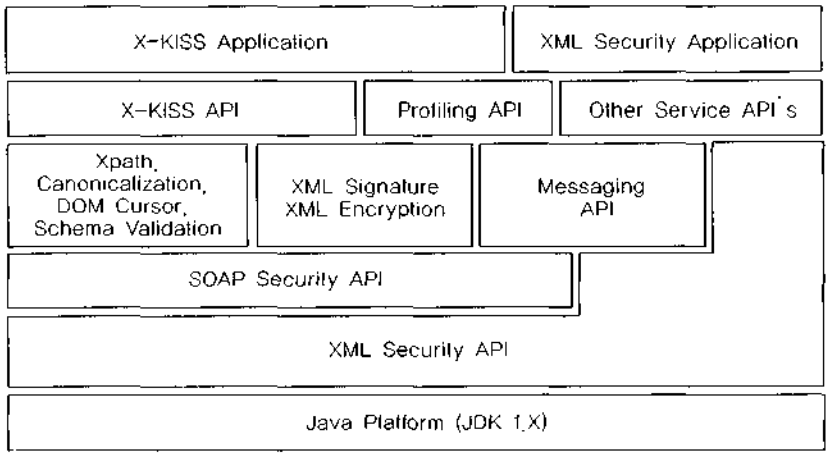
Security API와 SOAP Security API는 완전한 플랫폼 독립적인 암호 API를 제공한다.

XML Security API에서 제공되어지는 기반 암호 알고리즘으로 XML 관련 전자서명 및 암,복호화 기능을 지원하며, 이를 기반으로 X-KISS 서비스 컴포넌트들이 구성된다. 이렇게 각 기능별로 이뤄진 컴포넌트들을 중심으로 참조 모델이 구현된다.

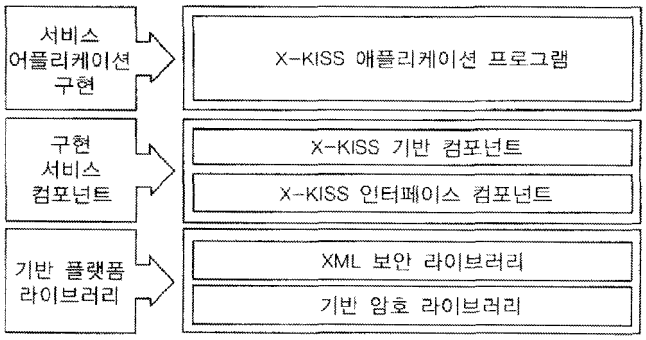
서비스 애플리케이션 이외에도 XML Security API 및 기반 암호 API에서 제공되어지는 라이브러리를 응용하여 여러 XML 관련 애플리케이션의 보안을 제공할 수 있다. 다음의 〈그림 4〉는 본 논문에서 개발된 서비스 컴포넌트를 구성하고 있는 라이브러리 플랫폼 구조를 나타내고 있다.

서비스 컴포넌트의 기반이 되는 자바 암호 라이브러리는 암호화 알고리즘과 그에 관련한 매개 변수들을 CAPI(Cryptographic Application Programming Interface) 기반으로 구성하고 있다. CAPI란 개발자들이 구현된 라이브러리의 함수나 메소드에 대한 일반 정보만으로도 쉽게 보안 시스템을 구축할 수 있도록 하기 위한 보안 서비스 API를 말한다. 〈그림 5〉는 시스템 개발자들이 참조 모델 구현 시 CAPI를 통해서 구현 라이브러리를 사용하는 구조를 나타낸 것이다.앞서 살펴본 라이브러리 플랫폼을 기반으로 본 논문을 통해 개발한 서비스 컴포넌트의 각 모듈을 살펴보면 다음 〈그림 6〉과 같다.

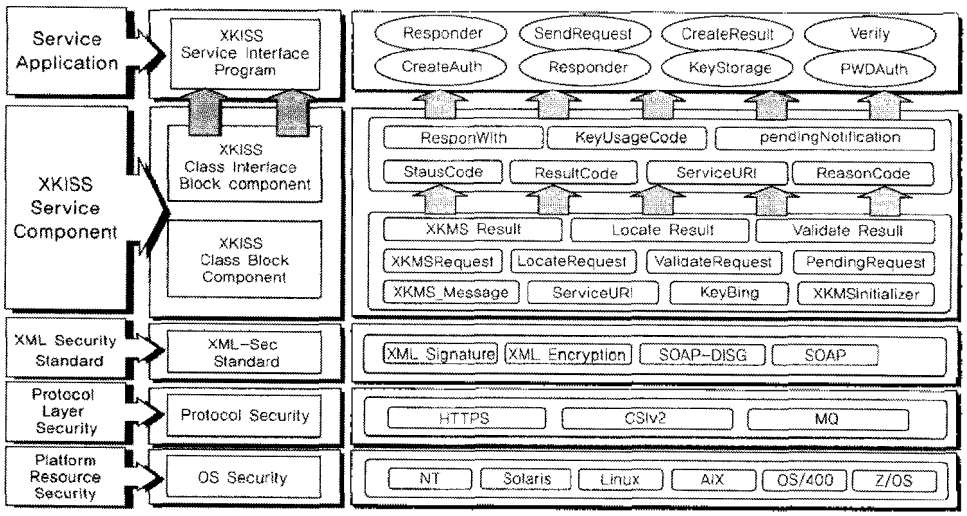
구현 서비스 컴포넌트를 이용하여 시스템 개발자들이 실제 XML 키 관리 시스템을 구축하고자 할 때, 기반 암호 모듈 및 암호 알고리즘 및 W3C의 표준에 적합한 키 연결요소, 메시지 속성값, 프로토콜 처리 결과 값 등에 관련된 내부 함수에 대한 자세한 지식 없이도 용이하게 구축할 수 있도록 함수 내부와의 인터페이스를 제공 해주는 모듈을 별도로 만들었다. 그리고, CAPI에 기반한 플랫폼 제공으로 시스템 개발자 편의성을 제공하고 있다.



〈그림 4〉 X-KISS 라이브러리 플랫폼 구성도



〈그림 5〉 CAPI를 이용한 X-KISS 플랫폼 구조



〈그림 6〉 구현한 각 서비스 컴포넌트별 모듈 구성도

4.3 참조 서비스 모델 구현

본 논문에서 개발된 서비스 모델링은 XKMS 전체 기능 중에서 키 위치정보 서비스 및 키 검증 서비스를 중심으로 이뤄진다. XML 키 정보 서비스를 하기 위한 인증서 및 키 쌍의 생성은 사전에 XML 키 등록 서비스를 받은 상태로 전제하며, 인증서 디렉토리에 서버의 인증서 및 각각의 클라이언트 관련 중요 정보들을 두어 저장소로서 기능을 한다. XML 키 정보 서비스 컴포넌트들의 사용을 시나리오를 통해서 알아보면 다음과 같은 순서로 처리된다.

① 클라이언트가 X-KISS 서버에 인증서 정보의 타당성 검사를 요청한다.

② Locate Service의 Request 모듈에서 전자서명 값을 가진 XML 문서를 인식하여 키의 검증과정을 진행시킨다. 〈ds:Signature〉 엘리먼트를 포함하는 XML 파일을 통해 서명을 검증하고, 유효성을 검증한다.

③ Request 명령을 통해 키 식별자에 부합하는 X.509 인증서를 찾는 키 위치검색 서비스(Locate Service)를 진행한다.

④ 키 위치검색 서비스를 통해 인증서를 분석하여 실제 공개키 값을 〈ds:RSAKeyValue〉이나 〈ds:DSAKeyValue〉 엘리먼트로 만들어 클라이언트에 결과값을 반환한다.

⑤ Validate Service의 검증 클래스의 실행을 통해 이름과 공개키간의 연결에 대한 신뢰를 확인하는 유효성 검사를 시행한다.

⑥ 〈ds:X509Data〉 엘리먼트를 상태 결과와 키 연결 지시의 문의를 X-KISS 서버에 하면, 서버는 질의한 인증서를 가지고 이름과 공개키 간의 연결에 대한 확인을 하고, 이름과 공개키를 찾아 반환한다.

⑦ 'Validate' 요청 메시지는 요청 메시지의 인증서에 따른 공개키를 반환함에 따라 그것이 믿을 수 있다는 것을 검증한다.

위의 과정은 키 등록 서비스의 과정이 선행되었음을 전제로 한 상황이다. 즉, 사용자는 이미 자신의 공개키를 X-KISS 서버에 저장해 놓은 상태이다. 그리고 위의 과정은 X-KISS 서비스 중 Tier 0에서 Tier 2의 모든 과정을 지원하고 있다. 즉, Tier 0 은 Trust Service 없이 요청 문서를 전달하는 서비스이며, Tier 1은 〈ds:KeyInfo〉가 포함하는 데이터의 처리는 Trust Service에 위임되며, 공개키를 가진 〈ds:KeyInfo〉를 반환하고, 〈ds:KeyInfo〉의 유효성은 클라이언트에 의해 수행된다. Tier 2에서는 클라이언트는 공개키와 다른 데이터들 사이의 조합 상태에 대한 정보들을 획득할 수 있고 공개키와 연계하여 응답받은 데이터의 유효성을 확인할 수 있다.

5. 안전성 및 시험평가

본 장에서는 논문에서 구현한 서비스 컴포넌트와 표준 규격안에 근거하여 기능과 안전성에 대한 분석을 하였다. 2장에서 설명한 표준 규격과 3장에서 설명한 기능 요구사항에 대비하여 실행한 기능 평가와 프로토콜에 대한 안전성을 설명한다. 검증 과정은 서버 환경에서 각 모듈에 대해 올바른 결과 값이 나오는지를 검증하는 것과 실제 구현에서의 올바른 작동 여부를 테스트 하였다. 그리고, 전체 프로토콜이 올바르게 수행하는지를 검증하였다.

5.1 기능평가

아래의 〈표 3〉은 2장에서 분석된 키 정보 서비스 규격과 3장에서 설명한 기능 요구사항에 대비하여 본 논문에서 개발된 참조 시스템에 대한 기능 평가 분석표이다.

본 논문의 참조 시스템은 W3C에서 권고된 아래의 알고리즘을 사용하였다. XML 서명 문서의 생성, 검증 처리에 관련하여 XML 전자서명 기능에서는 〈표 4〉와 같은 알고리즘을 지원한다.

국외의 XKMS 표준 규격안의 참조 모델로 구현된 Verisign의 XKMS 웹 서비스[22]와 Baltimore UniCert 서비스[16], Microsoft의 ASP.NET 기반 XKMS 서비스[9] 및 Entrust의 XKMS 참조 시스템[15]들과 표준 규격안의 기능 수용을 기준으로 본 논문에서 구현된 X-KISS 참조 모델의 공용적인 특징을 비교 및 분석해보면 다음 〈표 5〉와 같다.

제안 모델에서 사용자의 개인키는 사용자만이 아는 패스워드로 암호화되고, 이것은 다시 서버의 공개키로 재 암호화되어 전송되므로, 사용자의 프라이버시가 보장되고, 키의 은닉성을 제공한다. 하위 단위 컴포넌트의 독립적인 구조로 구성되어 개별적인 컴포넌트 분리 구조를 이룰 수 있으며, 각종 부가 서비스의 지원의 확장이 가능하다.

〈표 3〉 참조 시스템의 기능 평가

X-KISS 규격 / 키 서비스 기능	KISS					비 고
	Tier 0	Tier 1	Tier 2	Tier 3	Tier 4	
서명 키 쌍의 등록(Register)	*	*	*	*	*	KRSS
공개키의 검색(Locate)	M	M	*	O	O	·
공개키의 검증(Validate)	M	M	M	O	O	·
키 복구/취소(Recovery/Revoke)	*	*	*	*	*	KRSS

(M : Mandatory, O : Optional, * : No Recommendation)

〈표 5〉 국외 참조 시스템들과 비교

	V사 모델	B사 모델	M사 모델	E사 모델	제안 모델
사용자 프라이버시 보장	×	×	×	×	○
키의 은닉성	×	×	×	×	○
개별 컴포넌트 분리구조	×	×	×	×	○
SW 구현 가능성	○	○	○	○	○
부가서비스 지원	○	○	○	×	○

〈표 4〉 지원 알고리즘 평가

구 분	알고리즘 형태	지원 알고리즘	지원여부
XML 전자서명 알고리즘	Digest	SHA1	○
	Encoding	Base64	○
	MAC	HMAC-SHA1	○
	Signature	DSAwithSHA1(DSS)	○
		RSAwithSHA1	△
	Canonicalization	Canonical XML	△
		Canonical XML with Comments	○
	Transform	XSLT	◈
		Xpath	△
		Enveloped Signature	○
XML 암호화 알고리즘	Block Encryption	3-DES	○
		AES-128	○
		AES-256	○
		AES-192	◈
	Key Transport	RSA-v1.5	○
		RSA-OAEP	○
	Key Agreement	Diffie-Hellman	◈
	Symmetric Key Wrap	3-DES KeyWrap	○
		AES-128 KeyWrap	○
		AES-256 KeyWrap	○
		AES-192 KeyWrap	◈
	Message Digest	SHA1	○
	Message Authentication	XML Digital Signature	△
	Canonicalization	Canonical XML (omits comments)	◈
		Canonical XML with Comments	◈
		Exclusive XML Canonicalization	◈
		Exclusive XML Canonicalization with Comments	◈
	Encoding	base64	○

[REQUIRED(○), RECOMMENDED(△), OPTIONAL(◈)]

5.2 안전성

3장에서 설명된 보안 요구사항에 대비하여 여러가지 공격 방법들로부터 구현된 참조 모델의 보안 요구사항 평가는 다음 〈표 6〉과 같다.

X-KISS 메시지와 엘리먼트는 전송에 따른 보안요소를 가지고 있지 않아 전송 시에 보안 문제인 요청과 응답 메시지의 무결성, 기밀성, 신뢰성 문제를 안고 있다. 클라이언트가 키 정보 서비스에서 'Locate'나 'Validate' 메시지를 보낸다고 할 때 메시지의 위·변조나 방해가 있을 수 있다. 또한 서버에서 오는 응답을 신뢰할 수도 없으며, 클라이언트 측에서는 서비스를 신뢰할 방법이 없다. 이러한 전송상의 보안 문제를 해결할 두 가지 방안 중 첫째는 연결된 전송 프로토콜을 보안 서비스에 사용하는 것이고, 두 번째 방안은 보안 특성이 없는 전송 프로토콜을 사용하는 것이다. 두 번째 방법을 사용하면, X-KISS 메시지를 보호하기 위해 소켓 레벨 보안이나 패킷 레벨의 보안을 사용해야 하고, TLS(Transport Layer Security)를 사용하여 소켓 레벨 보안을 유지할 수 있으며, 패킷 레벨보안은 IPSEC(IP Security)을 주로 사용한다[3].

본 논문에서 개발된 X-KISS 참조 모델은 X-KISS 메시지를 둘러싸서 해당 정보를 보호하는 XML 기반 보안기술인 SOAP 프로토콜을 사용하여 전송상의 보안 문제를 해결하며, 여러가지 신뢰 및 검증 서비스를 지원한다.

5.3 시험평가

클라이언트가 포함된 전체 서비스 컴포넌트의 통합 테스트 및 성능평가는 동시 처리능력 및 처리시간 평가에 초점을 두어 실행하였다. 구현한 컴포넌트들을 테스트하기 위해 가상 클라이언트 모듈과 시험용 프로토콜 모듈

〈표 6〉 보안 요구사항 평가

요구사항	내 용
사용자의 프라이버시 보장	사용자의 개인키는 패스워드로 암호화되고, 다시 X-KISS의 공개키로 재암호화되어 전송되므로, 사용자의 프라이버시가 보장된다.
사용자의 프라이버시 보장	X-KISS 서버가 보낸 임의의 난수에 서버가 서명을 하게 되므로 검증자인 서버는 클라이언트를 인증할 수 있다. 또한 클라이언트도 서버의 인증서에 기반한 공개키를 이용해 세션키를 생성함으로써 서버를 인증할 수 있다.
메시지 및 키 검증의 무결성	정규화된 XML 전자문서의 검증으로 암,복호화 작업 후의 문서의 무결성 및 XML 전자서명 기능을 통한 키 검증의 무결성을 지원한다.
수신 및 발신 부인방지	X-KISS 클라이언트에서 X-KISS 서버로 가는 정보에 XML 전자서명을 하므로 클라이언트는 서버에게 보낸 정보를 부인할 수 없게 된다.
전자서명 유효성과 신뢰성	경로의 유효성 검증으로 서명의 유효성, 유효성 검사, 이름 연결, 인증서 철회 등이 실행되며, 이는 KISS가 신뢰엔진의 기능으로 공개키의 정보와 신뢰 확인을 얻는다.

을 작성하여 메인 서버와 클라이언트 환경을 구성하였다. 서버의 성능분석을 위한 것이므로 클라이언트의 사양은 중요하지 않아서 기본 구성되어 있는 사양과 운영체제를 그대로 사용하였다. 본 시험은 서버 기반의 트래픽 발생 모듈 생성하여 가상 클라이언트 모듈을 통해 약 1000회 이상 트래픽 발생시켜 분당 처리능력 및 건당 처리능력 평가의 기준으로 클라이언트 접속 테스트를 하였다. 전체 프로토콜 실행시간은 사용자의 요청메시지를 서버측으로 보내는 곳부터 최종적으로 서버로부터 인증 성공, 실패 메시지를 받는 것까지 측정한다. 각 실행횟수는 트래픽 1000회의 반복 테스트를 통한 평균값을 기록하였다.

X-KISS 서버와 클라이언트 사이의 통신은 안전한 SOAP 프로토콜을 기반으로 하며, 〈표 7〉은 X-KISS 기반 전자서명에 따른 XML 암·복호화 기능의 서버/클라이언트간 평균 전송 시간을 비교한 것으로 평균적으로 0.2초간의 차이를 보였다. 전체적으로는 클라이언트 수를 늘려감에 따라 0.3초까지 증가하는 현상을 보였다.

〈표 8〉은 전체 프로토콜 수행에서 클라이언트 수를 증가함에 따라 평균전송 시간의 변이를 나타낸 것이다. 클라이언트 수를 늘려가면 대체로 평균 전송시간이 증가하는 것을 볼 수 있다. 그리고, 클라이언트수가 45대 이상일 경우에 평균 전송 시간이 급격히 증가하는 현상을 보였다. 따라서 테스트 환경상의 Windows 2000 서버를 탑재한 Pentium Ⅲ에서 안정적으로 처리할 수 있는 클라이언트 수는 40대 정도로 파악되었다.

〈표 7〉과 〈표 8〉의 차이점을 비교해 볼 때 XML 전자서명 모듈의 수행시간이 전체 수행프로토콜 수행시간의 60% 정도를 차지하고 있어 XML 전자서명 모듈의 중요성을 보여준다.

6. 결 론

차세대 e-Business 기반은 웹 서비스로 구축될 것이라는 전망이 제기되고 있는 가운데, XML이 전자상거래와 B2B 거래의 문서교환 표준이 되면서 XML 문서를 보호하기 위한 암호화, 전자서명에 대한 필요성이 대두되었고 이를 위한 표준화 작업이 진행되고 있다. 현재 차세대 인터넷 환경에서 XML 기반의 정보보호 서비스를 처리할 수 있는 적합한 방

〈표 7〉 성능측정 시험결과 (1)

구분 (클라이언트 수)	1	10	35	50
전자서명 시간 (초)	0.41	0.56	0.78	1.23

〈표 8〉 성능측정 시험결과 (2)

구분 (클라이언트 수)	1	5	10	15	25	35	45	50
프로토콜 수행 시간 (초)	0.7	0.74	0.83	0.91	1.16	1.23	1.92	2.53

식이 제공되고 있지 않은 시점에서 XML 보안 플랫폼 기반인 XML 키 정보 서비스 시스템의 연구는 국제 표준적인 XML 키 관리 시스템에 대한 기술 개발과 상업용 모델의 도입을 위한 연구 기반으로 필요하다.

XML 키 관리 기술은 B2B와 B2C 애플리케이션의 신뢰도 확보에 혁신을 불러일으킬 수 있을 것으로 전망되고 있으며, 어떤 개발자들이라도 PKI 제품 및 서비스를 활용한 애플리케이션 개발에 보다 용이하게 접근하게 할 수 있을 것으로 예상하고 있다. 또한, 이 기술을 통해 개발자들은 전자서명과 암호화 같은 진보적 기술들을 그들의 웹 기반 애플리케이션에 통합할 수 있게 됐으며, 특히 이 기술이 애플리케이션 개발에 있어서의 표준으로 빠르게 자리 잡고 있는 XML을 기반으로 하고 있기 때문에 이러한 진보적 기술들의 상호 호환성 확보를 촉진시킬 수 있을 것으로 예상된다.

이에, 암호화나 전자서명을 사용하기 위해서는 암호키를 교환하기 위해 PKI와 같은 신뢰기반이 필요하게 되었고, 클라이언트 플랫폼 상에서 복잡하거나 전문화된 PKI 애플리케이션을 필요로 하지 않고 XML기반 시스템의 신뢰 관계를 구축하는 XML 키 정보 서비스의 모델 분석 및 서비스 컴포넌트를 구현하였다. 본 논문의 참조 모델은 향후 국내 e-비즈니스 프레임워크 구성 시 표준적인 보안 모델을 구현할 수 있는 지침으로 활용될 수 있을 것이다.

앞으로 XML 키 관리 시스템을 위한 상업용 검토 모델 중 하나로 사용자에게 편리함과 안전성 보장을 위해 보다 효율적인 기존 PKI 시스템과 연동하는 방안이 과제로 남아 있다. 그리고, 차세대 전자상거래 환경인 유·무선 통합 웹 서비스를 지원하기 위해 모바일 플랫폼에서의 XML 전자서명 및 XML 암, 복호화 기술개발과 유선상의 XML 키 관리 시스템 연동 및 다양한 신뢰 서비스 시스템과의 연동을 위한 지속적인 연구가 필요하다.

참 고 문 헌

[1] 문기영 외 4명, "XML 기반 안전한 전자상거래를 위한 보안 플랫폼", 전자통신동향분석, 제17권 제6호, 2002년 12월.

[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, Sept. 2001

[3] The XML Security Suite: Increasing the security of e-business.http://www.106.ibm.com/developerworks/library/xmlsecuritysuite/index.html#1/

[4] XML Encryption, Requirements and design considerations, http://lists.w3.org/Archives/Public/xml-encryption/2000Apr/att-0005/01-xmlenc.html/

[5] Proposed approach to XML encryption, http://lists.w3.org/Archives/Public/xml-encryption/2000Oct/att-

0006/01XML_Encryption Paper.doc/

[6] Donald E. Eastlake, Kitty Niles, Secure XML, Pearson addison wesley, 2003.

[7] XML Key Management Specification (XKMS), http://www.w3.org/TR/xkms/ http://www.w3.org/TR/2001/NOTE-xkms-20010330/

[8] XML-Signature Syntax and Processing, http://www.w3.org/TR/2000/CR-xmldsig-core-20001031/

[9] Microsoft XML Security Developer's Guide, http://msdn.microsoft.com/xml/xmlguide/ security.asp/

[10] Simple Object Access Protocol (SOAP) 1.1, W3C Note 08 May 2000, 11W3C XML-Signature Syntax and Processing, W3C Candidate Recommendation 20 August 2001.

[11] Web Services Description Language (WSDL) 1.1, W3C Note 15 March 2001.

[12] XML Key Management Specification (XKMS) Version 1.1, W3C Note 30 March 2001.

[13] XML Schema Part 1: Structures, W3C Recommendation, 2 May 2001.

[14] XML Schema Part 2 : Datatypes, W3C Recommendation, 2 May 2001.

[15] XML Trust Center, http://www.xmltrustcenter.org

[16] Balimore, XML Key Management Specification Bulk Operation (X-BULK), http://baltimore.com/

[17] PKCS#1, Kaliski, B., "PKCS #1: RSA Encryption, Version 1.5.", RFC 2313, March 1998

[18] PKCS#10, Kaliski, B., Nystrom, M., "PKCS #10: Certification Request, Syntax Specification Version 1.7" RFC 2986, November 2000.

[19] WSDL, E. Christensen, F. Curbera, G. Meredith, S. Weerawarana, Web Services Description Language(WSDL) 1.0 September 25, 2000, http://www.w3.org.org/TR/wsdl/

[20] XMLDSIG, D. Eastlake, J. R., D. Solo, M. Bartel, J. Boyer , B. Fox , E. Simon. XML-Signature Syntax and Processing, World Wide Web Consortium. http://www.w3.org/TR/xmldsig-core/

[21] Phaos Solution, http://www.phaos.com/

[22] Versign Solution, http://www.verisign.com/developer/xml/index.html/

[23] Hunter, David, Begining XML, Birmingham UK : Wrox Press Ltd, 2000.

[24] Ray, Erik T. Learning XML. Sebastopol, CA : O Reilly and Associates, 2001.

[25] Blake Dournaee, XML Security, RSA Press, 2002.

[26] 박남제, "XKMS 표준화 이슈", TTA IT Standard Weeky, 2003-24호, 2003

[27] 박남제, 원동호 외 3명, "안전한 전자거래를 위한 XML 키 관리 기술", 정보보호학회지, 13(3), 2003.

[28] 박남제, 문기영, "EXSO/XKMS 서비스 플랫폼 구조", CISC 2003, 2003.

[29] 박남제 외 2명, "XML 키 관리기술", 주간기술동향(통권 1104호), 2003.

저 자 소 개

박남제 (E-mail : namjepark@etri.re.kr)
2000. 동국대학교 정보산업학과(학사)
2003. 성균관대학교 정보보호학과(석사)
2003~현재 한국전자통신연구원 정보보호연구본부 능동보안기술연구팀
관심 분야 : XML 정보보호, 전자상거래 보안, 무선인터넷 보안, 전자지불시스템, 컨텐츠 보호 등

문기영 (E-mail : kymoon@etri.re.kr)
1986. 경북대학교 전자공학과(학사)
1989. 경북대학교 전자공학과(석사)
1992~1994. (주) 대우정보시스템 기술연구소
1994~현재 한국전자통신연구원 정보보호연구본부 능동보안기술연구팀 과제책임/선임연구원
관심 분야 : XML 정보보호, 응용보안, 분산시스템, 트랜잭션 등

송유진 (E-mail : song@mail.dongguk.ac.kr)
1982. 한국항공대학교 전자공학과(학사)
1987. 경북대학교 정보 시스템 전공(석사)
1995. 일본 Tokyo Institute of Technology(박사)
1988~1996. 한국전자통신연구원 선임 연구원
1996~현재 동국대학교 전자상거래대학원 교수
1998~현재 한국정보보호학회 이사
1998~현재 ISO/IEC JTC1/SC27-Korea 전문위원
관심 분야 : 암호 및 인증이론, 전자상거래보안 응용, 전자거래 화폐/전자지불, 스마트 카드보안, 컨텐츠 보호 등