EXSO/XKMS 서비스 플랫폼 구조

박남제*, 문기영*

*한국전자통신연구원, 능동보안기술연구팀

EXSO/XKMS Service Platform Infrastructure

Nam-Je Park*, Ki-Young Moon*

*Active Security Technology Research Team, ETRI.

요 약

최근 XML(eXtensible Markup Language)이 인터넷 전자거래와 데이터 전송 및 검색 부문에서 광범위하게 이용됨에 따라 중요한 거래들의 온라인 인증을 위한 암호키 관리가 요구되므로 XML 기반의 키 관리에 대한 연구 개발이 필요하다. 그러나 현재 여러 나라에서 이러한 XML 키 관리 기술에 대한 연구와 함께 XML 키 관리 시스템들이 시범 모델로 개발되고 있는 것에 반해 국내에서는 연구 및 개발이 미흡한 실정이다. 본 논문에서는 XML 키 관리의 개념에 대하여 살펴보고, 이를 바탕으로 설계한 EXSO/XKMS 서비스 플랫폼에 대해 설명하고자 한다. EXSO/XKMS에 대해서는 기반 플랫폼 구조 및 구현한 EXSO /XKMS 서비스 컴포넌트에 대해 기술하고, 개발 중인 서비스 시스템의 기능 및 특징에 관하여 기술한다.

I. 서론

XML은 인터넷과 e-비즈니스를 위한 글로벌 표준으로서 전자상거래의 보급 속도와 비례하여 XML의 활용도 증가하고 있다. 이러한 환경에서 데이터 및 문서를 보호하는 일은 전자거래에서 필수적인 사안이며, XML 문서 보안에 대한 연구 개발이 필요하다.

최근 세계 각 국에서는 이러한 XML 환경의 중요 거래에 대한 온라인 인증을 제공하기 위한 방안으로 PKI 및 공개키 인증서와 XML 어플리케이션의 통합이 용이하도록 XML 키 관리에 관한 연구가 활발히 진행되고 있으며, 이를 구현한 시범 시스템들도 개발되고 있다. 그러나 국내에서는 아직까지 XML 기반의 신뢰성을 제공하기 위한 XML 키 관리 시스템을 구축할 수 있는 실제 시스템들에 대한 연구 및 개발이 미흡한 실정이다.

따라서 본 논문에서는 XML 키 관리 시스템에 필요한 요구사항 및 요소 기술들을 분석한다. 이를 기반으로 하여 기 개발된 EXSO/XKMS(ETRI XML Security Orchestra/XML Key Management System) 서비스 컴포넌트를 소개하고, 개발 진행중인 EXSO /XKMS 서비스 플랫폼의 구조 및 각 구성 요소의 기능을 살펴보고, 시스템의 특징을 설명하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 연구의 배경이 되는 XML 키 관리 기술에 대해 분석한다. 3장에서 EXSO/XKMS 서비스 플랫폼의 구조 및 기능, 특징에 대해 살펴본 다음 4장에서 결론을 맺는다.

II. XKMS 개요

PKI(Public Key Infrastructure) 및 공개키 인증서와 XML 어플리케이션의 통합이 용이하도록 Verisign, Microsoft 및 WebMethods는 개방형 XKMS(XML Key Management Specification) 명세안을 작성하였다[1]. XKMS는 전자서명, 암호화된 XML 문서를 지원할 경우 PKI 기능을 XML 기반 어플리케이션에게 용이하게 지원할 수 있는 공개키의 관리를 위한 프로토콜을 정의한다. 공개키 기술은 XML 전자서명과 XML 암호화, 기타

여러 보안 응용에 필수적으로 사용된다. 전자서명을 위해 개인키로 서명하고, 수식측은 상대방의 공개키로 서명을 검증한다. 또, 암호화에서는 공개키로 암호화하고 개인키로 복호화한다. XML 키 관리는 서명을 검증하거나 암호화하는 공개키의 공유를 효율적으로 도와주는 기능을 정의하는 것이다.

XKMS의 2가지 주요 부분은 다음과 같다[1].

첫째, X-KISS(XML Key Information Service Specification)는 XML 기반 어플리케이션에서 신뢰할 만한 제3자에 의해 XML 전자서명, XML 암호화 데이터 또는 기타 공개키 사용과 관련된 키 정보의 처리를 지원하는 프로토콜을 정의한다. X-KISS의 기능은 주어진 식별자 정보에 필요한 공개키의 위치를 부여하고 공개키를 연결하는 것이다. 프로토콜 설계의 핵심적인 목표는 기본적인 PKI에서의 구문과 복잡성을 극복하고, 응용 구현의 복잡함을 최소로 하기 위한 것이다. 기본적인 PKI는 X509/PKIX, SPKI(Simple PKI) 및 PGP (Pretty Good Privacy)와 같은 다른 명세에 기초를 두고 있다.

둘째, X-KRSS(XML Key Registration Service Specification)은 키 쌍이 XKMS와 관련되어 계속 사용될 수 있도록 키 쌍 소유자에 의한 키 쌍의 등록을 지원하는 프로토콜을 정의한다. 공개키는 등록된 즉시 X-KISS를 포함하는 다른 웹 서비스와의 결합으로 사용되어질 수 있다.

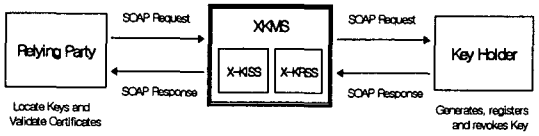

그림 1 : XKMS 기본 프로토콜

두 프로토콜은 XML Schema Language, WSDL (Web Services Definition Language v1.0)에 의해 정의된 메시지 사이의 관계와 SOAP(Simple Object Access Protocol v1.1)을 채택하는 프로토콜 내에서 표현된 구조로 정의된다[7]. 다른 부합되는 객체 인코딩 구조에서의 XKMS의 표현 또한 가능하다. 이러한 각 프로토콜들은 간단한 요청 및 응답으로 구성되는 프로토콜 교환을 설명한다. XML 신뢰 기반의 XML 인터페이스 프로토콜은 특정 PKI(ex. X.509)를 필요로 하지 않지만 X.509v3, SPKI 및 PGP와 같은 전통적인 표준을 포함한 기반과 상호 호환성이 있도록 설계 되어야 한다.

Ⅲ. EXSO/XKMS 서비스 플랫폼

1. EXSO/XKMS 구조 및 기능정의

EXSO/XKMS는 XKISS와 XKRSS 서비스 컴포넌트 모듈 및 클라이언트로 구성되어 있으며, 그 각각의 기능은 다음과 같이 정의된다.

1) EXSO/XKISS
- 키 위치 검색(Locate)
- 키 유효성 검사 (Validate)
- 장기 신뢰성 관계 및 신뢰성 상태확인

2) EXSO/XKRSS
- PKI 서버 기능 연동
- 키 등록 (Registration)
- 키 갱신 (Reissue)
- 키 폐기 (Revovation)
- 키 복구 (Recovery)

3) EXSO/XKMS 클라이언트
- EXSO/XKMS 서버에게 L. S. 요청
- EXSO/XKMS 서버에게 V. S. 요청
- EXSO/XKMS 서버에게 키 등록 요청
- EXSO/XKMS 서버에게 키 갱신 및 폐기 요청
- EXSO/XKMS 서버에게 키 복구 요청

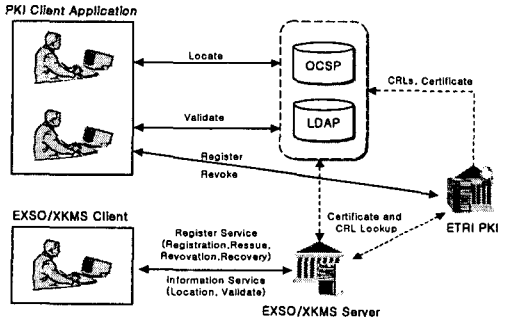

그림 2 : PKI 서비스 연동의 EXSO/XKMS 서비스 구조

2. 서비스 컴포넌트 구조

자바를 기반으로 하는 도구들은 이 기종간의 포팅 과정 필요없이 다중 플랫폼 환경의 프로그램을 개발하는 경우에 시간적/경제적으로 많은 이득

을 가져올 수 있는 장점이 있다. 특히 클라이언트/서버 프로그램을 개발하는 경우, 개발 환경이 다를 수 있음에도 불구하고 같은 모듈을 그대로 사용할 수 있다.

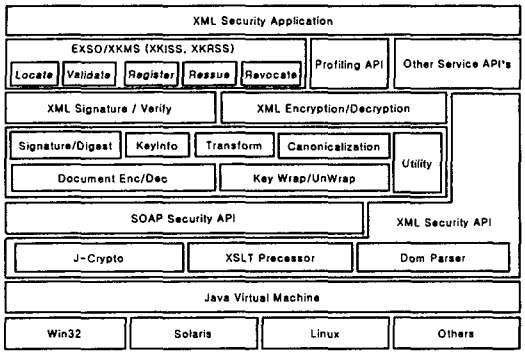

그림 3 : EXSO/XKMS 서비스 플랫폼 기반구조

EXSO/XKMS 서비스 플랫폼은 자바 플랫폼에서 XML 키 관리 기능에 대한 접근과 개발을 위한 프레임워크이다. XML Security API는 암호화와 관련된 XML 보안 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 지원 하며, 이를 기반으로 EXSO/XKMS 서비스 컴포넌트들이 구성 되어진다. 이렇게 각 기능별로 이뤄진 EXSO/XKMS 컴포넌트들을 중심으로 XML 키 관리 서비스 어플리케이션 프로그램들이 이뤄지게 되는 것이다.

EXSO/XKMS 서비스 어플리케이션 이외에도 XML Security API 및 기반 암호 API에서 제공되어지는 라이브러리를 응용하여 여러 XML 관련 어플리케이션의 보안을 제공할 수 있다. 위의 그림 3은 EXSO/XKMS 서비스 플랫폼의 기반구조를 나타내고 있다.

XKMS 라이브러리의 기반이 되는 자바 암호 라이브러 리는 암호화 알고리즘과 그에 관련한 매개 변수들을 CAPI (Cryptographic Application Programming Interface) 기반으로 구성되어 있다. 그림 4는 시스템 개발자들이 EXSO/XKMS를 구축시 CAPI를 통해서 구현 서비스 컴포넌트들을 사용하는 구조를 나타낸 것이다.

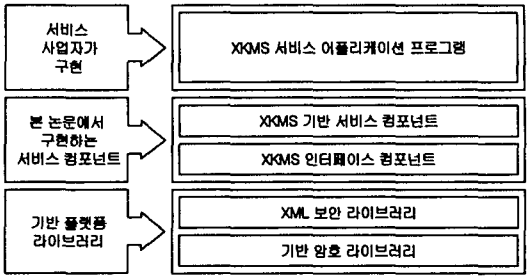

그림 4 : CAPI 기반의 EXSO/XKMS 시스템 구축

앞서 살펴본 EXSO/XKMS 서비스 플랫폼 기반 구조를 중심으로 각 모듈별 주요 구성요소를 살펴보면 다음과 같다.

1) EXSO/XKMS 서비스 클래스 계층 : XKISS의 Validate의 요청과 결과를 위해 사용되는 Key Binding 요소, XKISS의 Locate 요청 및 결과처리, 반환된 'Pending' 결과값의 유효성 검사를 요청처리, XKISS의 Validate 요청 및 결과 처리,

EXSO/XKMS 라이브러리의 초기화와 구성을 위한 클래스 유틸리티, 메시지 클래스의 객체, 요청 메시지의 객체, 결과 메시지의 객체 등을 포함하고 있다.

2) EXSO/XKMS 인터페이스 클래스 계층 : XKISS KeyUsage 요소 값, 요청 메시지의 PendingNotification Mechanism 속성 값, StatusCode 와 함께 사용되어지는 XKISS Reason 요소 값, 요청 메시지의 RespondWith 속성 값, XKMS 결과 메시지의 ResultMajor 와 ResultMinor 속성 값, XKISS Status 요소 값, 알고리즘, NameSpace, 객체를 위한 URI String 변수 정의 등을 포함하고 있다.

3. 서비스 컴포넌트 기능

EXSO/XKMS는 PKI 기능이 필요한 XML 서명 및 암호 클라이어트에게 XML 기술을 이용한 공개키 인증 관리기능을 제공해 기존 PKI 인증 체계와 쉽게 연동이 가능하도록 한다. EXSO/XKMS 서비스 컴포넌트를 이용해 PKI 서비스 상에서는 클라이언트에게 공개키 관리를 위한 ASN.1 인코딩

/디코딩 불필요하며, 공개키 검증에 필요한 모든 인증서 처리 기능을 서버에서 수행하게 되어 PKI 기반의 XML 서명 및 암호 기반의 보안 응용개발이 보다 용이해진다.

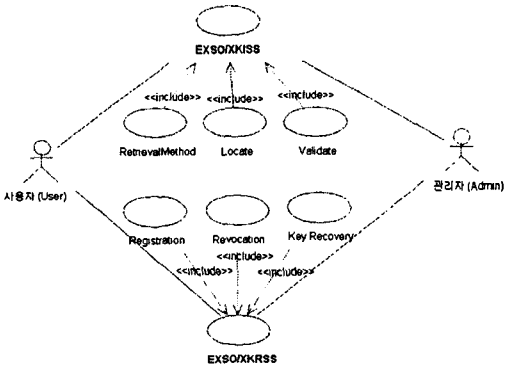

그림 5 : 메인 컴포넌트 유스케이스

EXSO/XKMS 서비스 컴포넌트들은 크게 키 관리(등록) 요청과 키 정보 요청의 두 가지로 구분된다. 이것은 각각 XKISS와 XKRSS의 역할을 수행한다. 이 메인 유스케이스를 처리하기 위한 메시지 처리는 별도의 메시지 처리 클래스에서 수행하며, 클라이언트에서 XKMS 서버로의 요청 메시지는 SOAP 메시지 보안 형태로 설계한다. 그림 6은 EXSO/XKMS 서비스 플랫폼 기반의 서비스 운영도를 나타내고 있다.

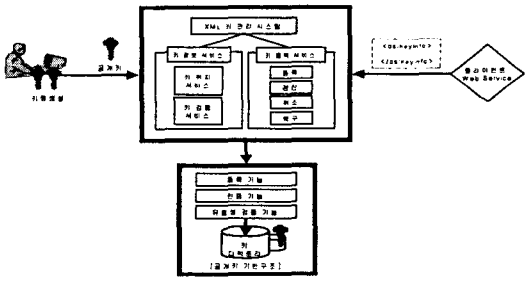

그림 6 : EXSO/XKMS 서비스 운영도

EXSO/XKMS 서비스 컴포넌트들은 XML 정보보호 기술들을 요소 기술로 관계하고 있으며, 그 기술들과의 상관 관계를 살펴보면 그림 7과 같다.

알파벳의 흐름은 EXSO/XKMS가 웹 시큐리티 서비스를 이루는 XML-Dsig와 XML-Enc를 기반으로 PKI과의 연동되는 것을 뜻하고, 숫자의 흐름은 전자서명 서비스 기반기술 연계의 흐름을 뜻한다.

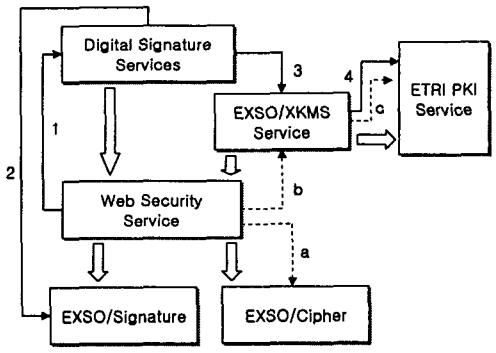

그림 7 : EXSO/XKMS와 기반기술의 상관관계도

4. EXSO/XKMS의 특징

EXSO/XKMS 서비스 컴포넌트는 운영 서비스 개발자들이 실제 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 제공해주는 모듈을 별도로 제공하고 있다. 그리고, CAPI에 기반한 플랫폼 제공으로 시스템 개발자 편의성을 제공하고 있다. EXSO/XKMS 서비스 컴포넌트를 기반한 EXSO/XKMS 시스템는 다음과 같은 특징을 지닌다.

1) 다양한 보안 운영 정책 지원

EXSO 플랫폼 환경의 다양한 보안 운영 정책을 지원할 수 있도록 수동 및 자동의 운영 정책 설정 기능을 제공한다.

2) 안전한 키 관리 서비스 제공

키의 안전한 복구를 위한 블라인드 기법을 적용하며, 키 갱신/폐기/복구의 사용자에 대한 관리 및 편리한 GUI 인터페이스를 통한 효율적 서비스를 제공한다.

3) 국제 표준단체의 표준 준용

W3C, IETF의 XML-DSig, XML-Enc, XKMS 표준을 준용한 XML 기반의 PKI 서비스 기능을 제공한다. 현재 EXSO/XKMS는 XKMS 1.0 기반으로 표준화가 진행중인 XKMS 2.0 명세안을 수용하고 있다.

4) 기존 PKI와의 연동성

현재 국내에서 인증서를 발급하는 공인인증기관의

PKI 시스템들과 상호 연동성을 최대한 보장하기 위해 PKI 연동 표준 API를 이용해 적합한 연동 인터페이스 모듈을 제공하며, 기능 추가로 인한 시스템 변경을 최소화할 수 있다.

5) 다양한 응용서비스 지원 인터페이스

PKI/KMI/PMI 등 외부 응용 서비스 지원을 위한 게이트웨이 형태의 독립적인 서버 운용을 할 수 있는 인터페이스를 제공한다. 공인 및 사설 인증기관에서 등록기관으로 운영이 가능하며, 응용서비스의 통합 적용도 가능하다.

6) 모바일 환경 적용 지원

인증서 발급에 대한 처리 및 검증 처리 기능을 EXSO/XKMS 서버에서 수행하기 때문에 휴대폰 단말기 환경에서 EXSO/XKMS 서비스를 제공할 수 있다.

7) 서비스 이용자의 프라이버시 보장

서비스 이용자의 프라이버시를 최대한 보장하며, 서버가 Perfect forward secrecy를 제공하도록 설계함으로써, 키가 외부에 노출되어도 안전성을 보장한다.

8) 하드웨어 모듈에 의한 키 관리 지원

스마트 카드 지원 모듈에 의한 X-Bulk 프로토콜 인터페이스 제공 및 관리자 서버의 안전한 관리를 위한 USB 보안 토큰 및 IC카드 등의 휴대용 보안 저장장치로 접근 통제를 지원해 안전성과 효율성을 지원한다.

Ⅳ. 결론

최근 XML 기술의 유연성이 인식되기 시작하면서 XML 정보보호 기술에 대한 연구가 활발히 진행되고 있으며, XML 기반의 중요 전자거래 정보에 대한 인증을 위한 암호키 관리가 필수적인 요소가 되었다. 따라서 본 논문에서는 시스템 개발자들에게 EXSO/XKMS 시스템 구축 시 사용이 용이한 인터페이스와 플랫폼을 제공할 수 있는 EXSO/XKMS 서비스 컴포넌트 개발 사례를 설명하며 EXSO/XKMS 서비스 플랫폼의 구조 및 특징에 대해 기술하였다. 향후 안전한 전자거래를 위한 보안 플랫폼에 대한 연구를 기반으로 보다 안전한 서비스를 제공할 수 있는 환경을 구축할 수 있는 연구가 진행되어야 할 것이며, 기존 여러 시스템들과 XKMS의 연동을 위한 솔루션의 모델 연구가 지속되어야 할 것이다.

참고문헌

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

[2] XML Key Management Requirements, W3C Working Draft 9 Janyary 2003.

[3] Mark Bartel, John Boyer, Bard Fox, Brian LaMacchia and Ed Simon, "*XML Signature Syntax and Processing*", http://www.w3.org TR/xmldsig-core/

[4] Takeshi Imamura, Blair Dillaway and Ed Simon, "*XML Encryption Syntax and processing*", http://www.w3.rg/TR/xmlenccore/, 2002

[5] Phillip Hallam-Baker, "W3C XKMS workshop position paper," *Proceedings of XKMS Workshop*, July 19, 2001, Redwood City, CA

[6] Balimore, XKMS Bulk Operation (X-BULK), http://www.baltimore.com

[7] Blake Dournaee, *XML Security*, RSA Press, 2002.

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

[9] OASIS, "Web Service Security", http://www-106.ibm.com/, Apr. 2002.

[10] JooYoung Lee, JuHan Kim, JaeSeung Lee, KiYoung Moon, and Hyun-Sook Cho, "ESES: XML Security for Secure Electronic Commerce," *Proceedings of WISA 2001*, Sep. 2001.

[11] 문기영, 손승원, "XML 정보보호 개요", *정보처리학회지*, 10(2), PP.108-116, 2003.

[12] 박남제 외, "안전한 전자거래를 위한 XML 키 관리 기술", *정보보호학회지*, 13(3), 06. 2003.