情 報 保 護 學 會 誌
第 13 券 第 3 號, 2003. 6

# 안전한 전자거래를 위한 XML 키 관리 기술

박 남 제*, 문 기 영*, 손 승 원*, 송 유 진**, 원 동 호***

요 약

XML(eXtensible Markup Language)은 인터넷 기반 정보시스템의 정보 교환 양식으로 그 활용도가 증가하고 있으며, 여러 형태의 문서를 통합하고 전달하는 전자거래의 표준으로 인식되고 있다. 이러한 환경에서 전자거래 시 교환되는 XML 문서의 보다 안전한 보안 서비스를 하기 위한 방안으로 새로운 기술과 기존의 기술들을 융합할 수 있는 모듈화 되고 확장된 보안 기술이 필요하다. XML 정보보호기술 중 XML 키 관리 명세(XKMS)는 다양하고 복잡한 기능의 전자거래 어플리케이션에서 XML 문서의 서명을 검증하거나 암호화하는 공개키의 관리를 위한 프로토콜을 정의한다. 본 고에서는 XML 기반 보안서비스 특성에 착안하여 안전한 전자거래를 위한 XML 키 관리 기술과 표준화 과정에서 논의되고 있는 기술적 이슈에 대해 살펴보고 국내외 동향을 알아보고자 한다.

## Ⅰ. 서 론

최근 XML이 인터넷 전자거래와 데이터 전송 및 검색 부문 등에서 광범위하게 이용됨에 따라 XML 문서에 대한 보안 문제가 대두되고 있다. 전자문서 및 데이터를 보호하는 일은 전자거래에서 필수적인 사항이며, XML 보안에 대한 연구개발 또한 활발히 진행되고 있다.

XML 보안은 보안 메커니즘을 최소 단위로 정의함으로써, 어플리케이션의 필요에 따라 부분 암호화가 가능하다. XML 환경에서 보안을 위한 핵심요소 중 하나는 암호키의 안전한 관리이다. 암호에 의해 보호되는 XML 문서 보안은 직접적으로 키에 대한 보호에 달려있다. 암호키의 적절한 관리는 보안을 위한 암호의 효과적인 사용에 필수적인 요소이다. 따라서, 신뢰성 있게 수행되어야 하는 전자거래에서 XML 키 관리의 연구 개발이 중요하다.

W3C(World Wide Web Consortium)에서 최근 PKI(Public Key Infrastructure) 및 공개키 인증서와 XML 어플리케이션의 통합이 용이하도록 Verisign, Microsoft 및 WebMethods가 개방형 XML 키 관리 명세(XKMS)를 작성하였다[1,5].

XKMS(XML Key Management Specification)는 차세대 인터넷 언어인 XML에 기반을 두고 있으며, XML 전자서명 표준과 조합하여 사용에 적합성을 위한 공개키 등록과 배포를 위한 프로토콜들을 정하고 있다. 공개키 암호기술은 XML 전자서명과 XML 암호화 및 기타 여러 보안 응용에 필수적으로 사용되며, 전자서명을 위해 송신측에서 개인키로 서명하고, 수신측은 상대방의 공개키로 서명을 검증한다. 또, 암호화에서는 공개키로 암호화하고 개인키로 복호화한다. XML 키 관리는 서명을 검증하거나 암호화하는 공개키의 공유를 효율적으로 도와주는 기능을 규정하는 것이다.

본 고에서는 안전한 전자거래를 위한 XML 정보보호기술 중 하나인 XML 키 관리 기술에 대해 소개한다. XML 키 관리에 대해 기술하며, W3C에서 진행 중인 표준안에 근거하여 XML 키 관리의 구조와 처리절차를 중심으로 설명한 다음, 표준화 진행 중의 기술적 논의사항에 대해 살펴보고, 국내외 제품 개발 동향을 서술한다.

* 한국전자통신연구원 네트워크보안연구부 ({namjepark,kymoon,swsohn}@etri.re.kr)
** 동국대학교 정보산업학과 (song@mail.dongguk.ac.kr)
*** 성균관대학교 정보통신공학부 (dhwon@dosan.skku.ac.kr)

## Ⅱ. XML 키 관리 기술

암호키 관리는 일반적으로 키 분배, 키 위탁 및 키 복구를 말한다. 키 관리 시스템은 암호키를 관리하며, 공격 이외의 장해 등의 경우에, 암호화되어 데이터를 복호화 가능하도록 하기 위한 기반이다. XML 키 관리 명세인 XKMS는 다양하고 복잡한 기능의 전자거래 어플리케이션에서 전자문서의 서명을 검증하거나 암호화하는 공개키를 관리하는 프로토콜로 정의된다[1].

공개키 암호 시스템을 이용해 향상된 보안 수준을 제공할 수 있는 기반 기술인 PKI가 응용 프로그램에서 요구하는 보안 요구사항을 분석해 사용자의 편의성과 보안성을 동시에 만족시키면서 이를 기반으로 응용 시스템을 이용하는데 점차 활용되어가고 있다. 일반적인 PKI 구현의 복잡성에 비해 XML의 단순성은 비즈니스 시스템간 데이터의 간편한 응용성을 제공한다. 그러므로, XKMS와 XML 신뢰 서비스(Trust Services)의 주요 목적은 XML 어플리케이션을 일반적인 PKI 구현의 복잡성으로부터 분리하는 것이다[그림 1]. XKMS는 PKI 기능이 필요한 XML 클라이언트에게 XML 기술을 이용한 공개키 인증 관리 기능을 제공해 기존 PKI 인증 체계와 쉽게 연동이 가능하도록 한다. XKMS를 이용한 PKI 서비스 상에서는 클라이언트에서 공개키 관리를 위한 ASN.1 인코딩/디코딩 불필요하며, 공개키 검증에 필요한 모든 인증서 처리 기능을 XKMS 서버에서 수행하게 되어 PKI 기반의 XML 전자서명 및 암호 응용 개발이 보다 용이해진다. PKI와 비교한 XKMS의 장점은 다음과 같다[5].

• 구현의 용이성

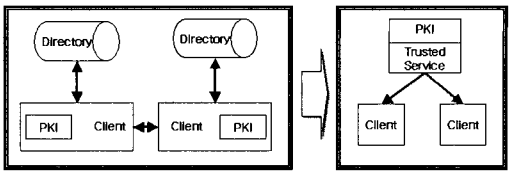
XKMS는 PKI의 복잡성과 신뢰 처리를 서버측 컴포넌트에게 이동시킨다. 클라이언트의 요청에 따라 인증서 검증, 정보 추출 등의 기능을 서버에서 수행한다.

• 개방형 표준성

XKMS 플랫폼은 개방형이며, 산업적 표준이다.

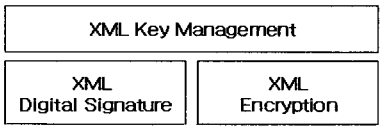
• 모바일 장치의 접근 가능성

초 경량화된 최소 기능의 클라이언트 인터페이스를 통해 무선 환경에서 적용이 용이하다.




[그림 1] 일반 PKI구조와 XKMS 적용 후의 구조

XKMS는 암호 기능이 있는 XML 어플리케이션을 인증하기 위한 포괄적이고 개방적 및 표준적인 접근방식을 취한다. 구조는 XML 전자서명과 XML 암호화 워킹그룹의 W3C 표준화 활동과 호환성이 있도록 설계된다[1,5]. 다음 [그림 2]는 XKMS의 전체 구조에서 XML 전자서명과 XML 암,복호화 사이의 관계를 나타낸 것이다[1].



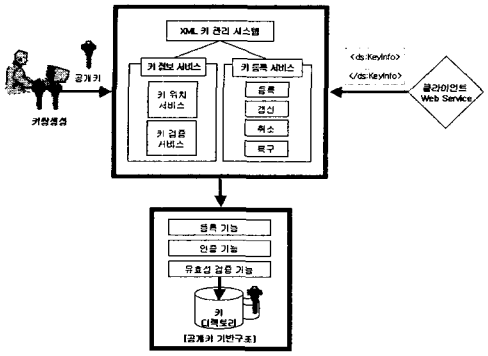

[그림 2] XML 전자서명, 암호화와 XKMS간 관계

XKMS의 주요 목적은 전자서명을 검증하거나 데이터를 암호화하기 위해 사용되는 공개키 사용자에게 필요한 키의 위치를 명시하고, 이름이나 속성정보를 해당 비밀키 소유자와 연결시키는 것이다[1]. XKMS는 크게 XKISS(XML Key Information Service Specification)와 XKRSS(XML Key Registration Service Specification)의 두 영역으로 구성되어 있다[표 1].

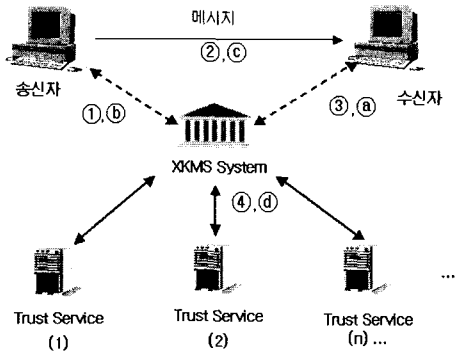
두 프로토콜은 XML Schema Language, WSDL (Web Services Definition Language)에 의해 정의된 메시지 사이의 관계와 SOAP(Simple

[표 1] XKMS 구성요소

| 구분 | 내 용 |
|---|---|
| 키 정보 서비스 (XKISS) | · XML 전자서명, XML 암호화된 데이터와 관련 키 정보 처리를 지원하기 위한 프로토콜<br>· 식별 정보가 주어졌을 때, 필요로 하는 공개키 위치와 식별자 정보, 공개키 연결 기능 지원 |
| 키 등록 서비스 (XKRSS) | · 키 쌍 소유자에 의한 키 쌍의 등록을 지원하는 프로토콜<br>· 'Trust Services'로서 요청과 응답의 메시지 교환으로 구성 |




〔그림 3〕 XKMS 서비스 구조




〔그림 4〕 XKISS의 암호화 및 전자서명 절차

Object Access Protocol)을 채택하는 프로토콜 내에서 표현된 구조로 정의된다〔그림 3〕. 여러 응용 형태의 객체 구조에서 XKMS의 적용도 가능하다[1,7]

이러한 각 프로토콜들은 간단한 요청 및 응답으로 구성되는 프로토콜 교환을 설명한다. XML 인증 기반의 XML 인터페이스 프로토콜은 특정 PKI(예를 들면, X.509)를 필요로 하지 않지만 X.509v3, SPKI (Simple PKI) 및 PGP (Pretty Good Privacy)와 같은 전통적인 표준을 포함한 기반과 상호 호환성이 있도록 설계된다.

### 2.1 키 정보 서비스 (XKISS)

XML 신뢰 기반의 중심인 XML 키 정보 서비스는 XML 기반 어플리케이션에서 신뢰할만한 제 3자에 의해 XML 전자서명, XML 암호화 데이터 또는 기타 공개키 사용과 관련된 키 정보의 처리를 지원하는 프로토콜을 정의한다[1]. 주요 기능은 주어진 식별자 정보에 필요한 공개키의 위치를 부여하고 공개키를 연결하는 것이다〔그림 4〕.

XKISS의 전자서명 절차는 다음과 같다[3,8].

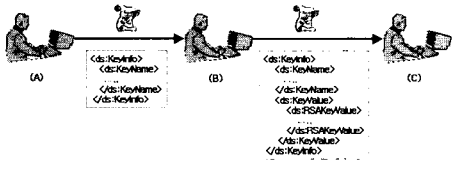
① 송신자는 자신의 공개키를 서버에 등록한다.
② 서명된 메시지가 수신자에게 전송된다.
③ 수신자는 공개키를 불러와서 서명을 검증한다.
④ 키의 정보가 없거나 위의 경우가 아니면, XKMS 서버가 다른 XKMS 혹은 다른 형태의 서비스로부터 서명된 키 정보를 가져온다.

XKISS의 메시지 암호화 절차는 다음과 같다[4,8].

ⓐ 수신자가 자신의 공개키를 서버에 등록한다.
ⓑ 송신자는 수신자의 공개키를 불러와 메시지를 암호화한다.
ⓒ 수신자가 메시지를 받아서 복호화한다.
ⓓ 키의 정보가 없거나 위의 경우가 아니면, XKMS 서버가 다른 XKMS 혹은 다른 형태의 서비스로부터 암호화 키 정보를 가져온다.

XML 전자서명 내에서 서명자의 공개키에 대한 정보를 〈ds:KeyInfo〉에서 선택적으로 포함할 수 있다. 이 키의 정보는 서명자에게 선택된 공개키에 대한 인증을 허용하며, 서명 자체에 대한 암호와의 연계가 가능하다[1]. 예를 들면 (A)가 서명한 키 데이터를 포함하는 〈ds:KeyInfo〉 요소만으로 (B)에게 서명된 문서를 보냈다면, 메시지를 받은 후 (B)는 서명의 유효성을 위해 요구되는 부가적인 정보를 검색한다. 그리고, (C)에게 문서 전송 시에는 〈ds : KeyInfo〉내에 이 정보를 추가한다〔그림 5〕.

키 정보 서비스 프로토콜 설계의 핵심적인 목표는 기본적인 PKI에서의 구문과 복잡성을 극복하고, 응용 구현의 복잡함을 최소로 하기 위한 것이다. 기본적인 PKI는 X.509/PKIX, SPKI 및 PGP와 같은 다른 명세에 기초를 두고 있다. XKMS의 적용 범위는 각 구현 어플리케이션마다 다르기 때문에 특정 응용 어플리케이션에서의 강화된 PKI 서비스를 지원하기 위해 계층적 서비스 모델로 세분화시킴으로




〔그림 5〕 〈ds:KeyInfo〉 전송 메시지에 대한 예시

〔표 2〕 Tiered Service Model

| 구분 | 서비스명 | 내용 | 비고 |
|---|---|---|---|
| Tier 0 | - | 어플리케이션에 의한 〈ds:KeyInfo /RetrievalMethod〉 요소 처리 | M |
| Tier 1 | Location | 어플리케이션에 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 | O |
| Tier 4 | Assertion Status | 신뢰 확인상태의 관리 | O |

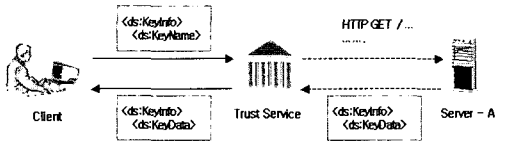
(M:Mandatory, O:Optional)

업무에 따른 정확한 처리 계층을 선택할 수 있도록 정의하고 있다[1].

각각의 계층적인 구조 내부에서 신뢰 서비스는 복잡한 구문과 의미의 효율적인 조작, 디렉토리와 데이터 저장 하부 구조로부터의 정보검색, 상태확인 및 취소, 인증 관계의 생성과 처리와 같은 기능을 클라이언트에게 제공한다.

### 2.1.1 키 위치정보 서비스 (Locate Service)

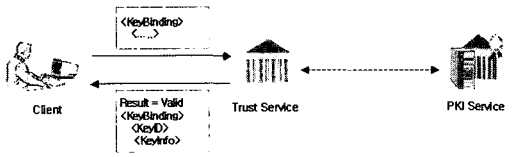
프로토콜 Tier 0은 〈ds:RetrievalMethod〉의 처리로서 XML 전자서명 명세서에 따라 응용 프로그램에 의해 처리되며, Trust Service가 없이 처리된다[1,8]. 프로토콜 Tier 1은 키 위치정보 서비스로서, XML 서명을 포함하는 XML 문서를 검증해야 하는 어플리케이션이 있으면, 이 어플리케이션은 〈ds : Signature〉 요소를 포함하는 XML 문서를 참조하는 파일이나 스트림(Stream), URI(Uniform Resource Identifier) 값을 받아들인다. 서명의 유효성을 검증하기 위해 클라이언트에 의해 인증 경로를 통해서 유효성을 확인한다〔그림 6〕.




〔그림 6〕 Tier 1의 키 위치정보 서비스 구조

### 2.1.2 키 유효성 검사 서비스 (Validate Service)

프로토콜 Tier 2인 키 유효성 검사 서비스는 이름과 공개키 간의 연결에 대한 신뢰를 확인하는 일을 한다. 이 서비스는 이전 단계인 키 위치검색 서비스를 포함하고 있으므로 이름과 키 간의 관계를 알아보는 것뿐만 아니라 키의 위치도 알아낸다[1]. 클라이언트는 공개키와 다른 데이터들 사이의 여러 값을 전달받아 공개키와 연계하여 응답받은 데이터의 유효성을 검증한다.



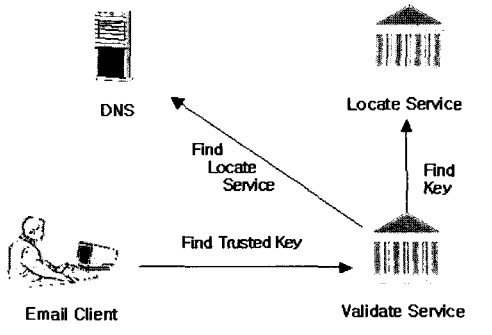

〔그림 7〕 Tier 2의 키 유효성 검사 서비스 구조

### 2.1.3 기타 서비스

Tier 3,4의 Assertion Service는 장기 신뢰성 관계들이나 신뢰성 확인 상태 등의 서비스를 정의한다. AssertionStatus는 키 결합과 같은 가정문의 상태를 나타내기 위해 사용되며, 정의된 데이터 요소에 의해 진행된다. 이 서비스들은 XKMS 2.0에서 Tier 1,2에 포함되어 정의되고 있다[1].

키 위치정보와 유효성 검사 서비스는 XKMS 서비스에서 공개키의 정보를 포함하고 있는 것으로서 함께 연동하여 사용될 수도 있다. 〔그림 8〕은 DNS 서비스를 이용한 XKMS 서비스 예시를 나타내고 있다[1].

서비스 서버는 클라이언트에게서 암호화된 메일을 받아 키 검색 서비스에서 키를 찾거나 DNS 구조를



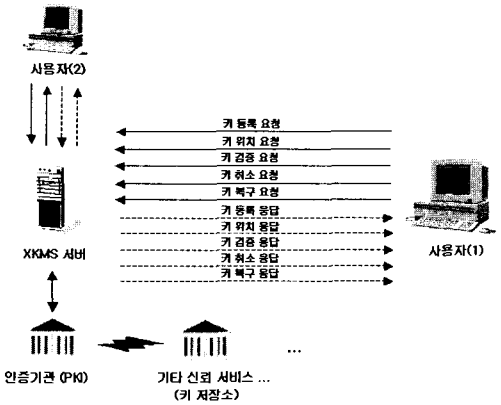

〔그림 8〕 DNS 서비스를 이용한 XKMS 서비스 구조

이용해 키를 찾아 그 유효성을 검증하는 서비스를 진행한다.

### 2.2 키 등록 서비스 (XKRSS)

키 등록 서비스는 키 쌍이 XKMS와 관련되어 계속 사용될 수 있도록 키 쌍 소유자에 의한 키 쌍의 등록을 지원하는 프로토콜을 정의한다[1]. 공개키는 등록된 즉시 키 등록 서비스를 포함하는 다른 웹 서비스와의 결합으로 사용되어질 수 있다[그림 9].

PKIX에 의해 정의된 기존의 인증서 관리 프로토콜은 인증서 라이프사이클의 일부만을 지원하거나 복잡하여 XML 어플리케이션에는 적당하지 않다. X- KRSS는 이러한 문제를 극복하기 위한 클라이언트 중심의 키 라이프사이클 관리 프로토콜이다. 서비스는 전체 인증서 라이프사이클을 키의 등록(Registration), 갱신(Reissue), 폐기(Revocation) 및 키 복구(Key Recovery)와 같은 단순한 단일 명세로 정의한다. 여기서 각각의 동작을 살펴보면 다음과 같다[1].




[그림 9] 키 등록 서비스의 구조

#### 2.2.1 등록 (Registration)

키 쌍 소유자는 등록 단계에서 자신의 공개키를 XKMS 서버에 등록한다. 공개키는 키 등록 서비스에 명시된 전자서명을 수행한 요청서에 포함되어 전송된다. 이때 요청에는 이름과 속성정보, 인증정보, 개인키 소유증명(Proof-of-Possession) 등의 정보가 포함될 수 있다[1].

① 이름과 속성정보 : 소유자는 이름과 속성정보를 저장하기 위해 서버에 요청하고 계속해서 공개키를 사용하여 전자정보를 전달한다. 등록서버는 이러한 정보를 요청된 것으로서 등록하거나 적용 가능한 정책에 따라 수정 또는 대체할 수 있다.

② 인증정보 : 등록서버가 키 소유자를 인증하기 위해 필요로 하는 정보이다. 그러나, 이 정보는 일반적으로 공개키 사용자에게 제공되지 않는다.

③ 비밀키 소유의 증명 : 전자서명 키 쌍을 등록할 경우, 등록 요청을 전자서명하기 위한 해당 비밀키의 사용은 비밀키 소유의 증명으로서 동작 한다. 그러나, 다른 형태의 키 쌍에 따라 별개의 소유증명 필드가 필요할 수 있다.

등록 서버는 요청을 수신한 뒤, XML 형식의 응답을 전송한다. 이 응답 문서에는 요청에 대한 처리 결과(승인, 거절, 대기 등)와 공개키와 함께 등록되어 있는 이름 및 속성 정보를 전송한다. 요청 거절의 경우를 제외하고는 추후 참조될 키 쌍 식별자를 전송한다.

#### 2.2.2 갱신 (Reissue)

이 서비스는 키 등록 후 키를 재발행하는 것으로 재발행 요청은 키의 최초 등록 과정과 동일하다[1]. 서비스 기능은 클라이언트가 이전에 요청했던 키 등록 정보를 갱신할 수 있게 한다. 서비스 정책은 이러한 요청에 요구되는 인증을 확인받아 진행된다.

#### 2.2.3 폐기 (Revocation)

키 폐기 기능은 클라이언트가 이전에 요청했던 키 등록 정보를 취소할 수 있게 한다. 이 서비스는 상태가 키 폐기 요청을 전송함으로써 이루어진다[1]. 서비스 정책은 이러한 요청에 요구되는 인증을 지시한다. 폐기 요청을 하였으나 키 등록 서비스에 요청에 대한 기록이 없으면 결과 코드 값은 키 정보가 없다고 전달되는 것을 제외한 키 폐기 작업은 최초 키 등록 작업과 동일하다.

#### 2.2.4 키 복구 (Key Recovery)

키 복구 작업은 다음 부분을 제외하고는 최초 키 등록 작업과 동일하다[1]. 키 복구 요청은 요청에 대한 응답 시간이 필요할 수 있으며, 결과 값이 보류될 수도 있다. 만약 키 등록 서비스에 요청에 대한 정보가 없으면 결과 값은 키 정보가 없다고 전달된다.

키 복구 요청 순서는 기 등록된 공개키에 대응되는 개인키를 분실한 경우에 오프라인 방법으로 키 관리자에게 복구 신청하면 관리자는 오프라인으로 키 복구 인증코드를 신청하여 서버에게 전달하는 과정으로 진행된다.

위와 같이 키 등록 서비스는 X.509v3와 같은 PKI의 경량화 인터페이스로서 사용될 수 있으며, 완전한 기능의 PKI가 필요하지 않는 어플리케이션에서 인증서 없는 키의 등록을 지원하기 위해 사용될 수 있다.

## 2.3 XKMS 데이터 요소

### 2.3.1 XKISS 메시지 형식

XKISS 메시지 형식은 W3C XML Schema에 정의되어 있고, 모든 값들은 데이터 요소로서 코드화 되어 있다[1]. 특히, XKMS는 타입의 적용이 엄격하고, SOAP 내의 개체와 상호 호환성을 가진다. XKISS 메시지 형식은 크게 Command Data, Locate Service, Validate Service 요소들로 나눌 수 있다〔표 3〕. 이것이 정의하는 추가적인 구조의 경우 모든 값들은 요소 데이터로써 전송된다[1].

### 2.3.2 XKRSS 메시지 형식

프로토콜 연산은 클라이언트에서 서버로 보내어지는 하나의 요청 메시지에 따라 등록서비스에서 클라이언트로 보내어지는 하나의 응답 메시지로 이뤄진 절차로 구성된다. XKRSS 메시지 형식 중 Command Data와 Registration Service 요소들을 살펴보면 다음의 〔표 4〕와 같다[1].

## 2.4 XKMS 암호화 알고리즘

XKMS에서 사용되는 XML 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[1,10].

〔표 3〕 XKISS 메시지 형식

| 구분 | | 상태 | 내용 |
|---|---|---|---|
| Command Data 요소 | Result Code | Success | 연산 성공 |
| | | NoMatch | 주어진 상황이 제공한 검색 결과와 일치하는 것이 없음 |
| | | Incomplete | 요청된 정보의 일부만 제공됨 |
| | | Failure | 알 수 없는 원인으로 연산 실패 |
| | | Refused | 연산의 거부 |
| | | Pending | 연산은 차후 처리를 위해 대기되었음 |
| | Assertion Status | Valid | 연결이 정당함 |
| | | Invalid | 연결이 정당하지 않음 |
| | | Indeterminate | 가정의 상태값이 결정되지 않음 |
| | Reson | Issuer Trust | 신뢰 서비스에 의해 신뢰할 수 있다고 간주함 |
| | | Status | 신뢰 서비스는 믿을 만한 상태를 증명 |
| | | Validity Interval | 요청이 유효한 값을 가질 수 있음 |
| | | Signature | 서명이 확인되었음 |
| Location Service 요소 | Request 메시지 | Query | 추가 데이터가 요구되는 공개키를 지정하는 〈ds:KeyInfo〉 요소를 포함하는 하나의 복잡한 구조 |
| | | Response | 클라이언트가 요청하는 데이터 요소를 지정하는 식별자의 순서를 응답으로 돌려줌 |
| | Response 메시지 | Answer | 응답 속성으로 나타낼 수 있는 정보를 제공하는 〈ds:KeyInfo〉 요소들을 포함하는 문자열의 순서 |
| Validate Service 요소 | Validate Interval | NotBefore | 유효성 간격의 시작점 |
| | | NotAfter | 유효성 간격의 끝점 |
| | KeyID | 키의 URI 식별자를 지정함 | |
| | Key Usage | Encryption | 키 쌍은 암호화와 해독을 위해 사용 |
| | | Signature | 키 쌍은 서명과 확인을 위해 사용 |
| | | Exchange | 키 쌍은 키 교환을 위해 사용 |
| | Key Binding | KeyName, KeyID, KeyValue와 X509Data를 포함하는 공개키 관련 데이터 요소 사이의 연결 가정함. | |
| | Validate | Query | 완전하고 유효한 하나의 키 연결 구조 |
| | | Respond | 클라이언트가 요청한 데이터 요소들을 나타내는 식별자의 순서는 반환됨 |
| | Validate Result | Answer | 유효한 결과를 포함하는 키 연결 구조의 순서 |

〔표 4〕 XKRSS 메시지 형식

| 구분 | | 상태 | 내용 |
|---|---|---|---|
| Command Data 요소 | Reson | Private | 암호화된 비밀키를 응답에서 반환하라는 요청 |
| Registration Service 요소 | Authentication | 인증요소는 요청의 인증 데이터를 포함하며, 인증 데이터의 형식에 의해 결정됨 | |
| | Request 메시지 | Template | 클라이언트에서 요청하는 요소가 등록된다고 규정하는 하나의 키 연결 구조 |
| | | Authentication | 정보의 신뢰를 제공하는 XML 문서 요청의 인증 |
| | | Response | 클라이언트가 요청하는 데이터 요소를 응답에서 반환한다고 규정하는 식별자의 순서 |
| | Response 메시지 | Key binding | 서비스에 의해 등록되는 키 연결을 기술 |
| | | Private | 등록 서비스가 생성하는 개인키 매개변수의 값처럼 서버가 제공하는 추가적인 정보를 제공 |

## Ⅲ. XKMS 보안 요구사항

### 3.1 기본 보안 고려사항

XKMS 서비스를 제공하기 위해서는 상호 운영성(interoperability), 범용성(scalability), 효율성(efficiency), 신뢰성(reliability) 및 보안성(security) 등을 고려하여야 한다[1,2]. XML 정보보호는 기본 보안 요구사항을 고려하면서 전송계층 및 응용계층에서 안전성이 제공되어야 하고, XKMS 서비스로서 안전하게 제공하기 위한 보안 대책도 필수적으로 요구된다. 여기서 XML 기반 응용 서비스에서의 기본 보안 요구사항을 기반으로 XKMS의 보안 요구사항을 살펴보면 다음 표 6과 같다.

이러한 기본 보안 요구사항 외에 부가적으로 요구되는 보안 요구사항은 다음과 같다. XKMS 서비스는 기존의 PKI와 상호 연동되면서 구축된 PKI 시스템 변경을 최소로 하는 등 실용적이어야 하며, 활용성을 높이기 위해 키 백업 기능 외에 키 로밍 서비스 등과 같은 부가 서비스를 제공할 수 있어야 하고, 사용자의 프라이버시를 최대한 보장함으로써, 사

〔표 5〕 XKMS 지원 알고리즘

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

〔REQUIRED(○),RECOMMENDED(△),OPTIONAL(◈)〕

〔표 6〕 기본 보안 요구사항

| 내용 | 요구사항 |
|---|---|
| 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. |

용자의 자발적 키 위탁을 유도할 수 있어야 한다[2].

### 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[8].

### 3.3 전송 계층상의 보안 요구사항

XKMS 메시지와 데이터 요소는 전송에 따른 보안요소를 가지고 있지 않아 전송 시에 보안 문제인 요청과 응답 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, 서비스 메시지를 보호하기 위해서는 소켓 레벨 보안이나 패킷 레벨의 보안이 사용되는데, SOAP 혹은 TLS(Transport Layer Security)를 사용하여 소켓 레벨 보안을 유지할 수 있으며, 패킷 레벨 보안은 IPSEC(IP Security)을 주로 사용한다[1,8].

XKMS 클라이언트는 PKI에 대한 의존없이 신뢰 서비스를 사용할 수 있다. 하지만, 서비스 자체에 대한 신뢰성을 확인하기 위한 방법은 클라이언트가 가지고 있어야 한다.

## Ⅳ. 국내외 동향 및 주요 이슈사항

### 4.1 국내외 기술 및 표준화 동향

XKMS는 W3C에 의하여 주도적으로 개발되고 있다. W3C는 최근 Microsoft와 Verisign, Web Methods가 공동 개발하고, Baltimore, Entrust Technologies, Citigroup, IBM, IONA Technologies, PureEdge Solution, Hewlett Packard, Reuters Limited, Science RSA Security, Application International 등이 웹 표준으로 제출한 XML 키 관리 명세서를 승인하고 워킹그룹을 구성하여 표준화를 진행하고 있다. W3C의 XKMS 워킹그룹은 클라이언트가 웹 서비스로부터 키 정보(키 값, 인증서, 관리 혹은 신뢰 데이터)를 얻도록 XML 어플리케이션과 프로토콜 명세를 개발하는 일을 한다. 최초 설계 목적은 XML 전자서명과 연동 시 기존 PKI 시스템에 대한 복잡성을 클라이언트에게 숨겨 키 관리 부담을 서비스 서버에 위임해 그 구현을 용이하게 하기 위함이었다. 2001년 XKMS 명세서가 발표된 이후 관련 툴킷들이 명세 주도 기업을 중심으로 참조 구현 제공되고 있다. 이와 같이 XML 키 관리 기술은 모두 표준화 진행으로, 이를 완전히 구현한 제품도 세계적으로 드문 실정이다.

XML 정보보호 기술 중 XML 전자서명, XML 암호 기술은 한국전자통신연구원(ETRI)에서 기 개발하여 보유하고 있는 상태이며〔10〕, XML 기반 통신 메시지 보안기술, XML 기반 키 관리 서비스 기술, XML 기반 접근제어 기술, XML 기반 보안 정보교환 기술, 무선 환경을 위한 XML 정보보호 기술 등은 국내에서 연구개발이 진행되고 있다[11].

Verisign에서는 TSIK(Trust Services Integration Kit)라는 툴킷에 XML 키 관리의 라이브러리를 지원하는 시제품을 개발하였으며[8], 이 제품은 XML

전자서명 및 XML 암호화, XML 키 관리 표준의 참조 구현(Reference Implementation)으로 개발되었다. Sun Microsystems는 별도의 보안 기술을 제안하고 있지는 않으며, 자사의 플랫폼에 XML 보안 기술을 적용하기 위해 JCP(Java Community Process)를 통해 자바 API 표준화를 추진중이다. 'JSP104'는 XML Trust Service APIs로써 XKMS의 자바 API 구현을 목표로 하고 있다. Baltimore는 많은 양의 키 정보를 효과적으로 등록하기 위해 'X-BULK(XKMS Bulk Operation)'를 발표하여 XKMS 능력을 확장시키고 있으며[6], Entrust는 참조 구현을 통해 자사의 상품을 검증하고 있다[8]. IBM에서도 WSDK(Web Service Tool Kit)을 기반으로 개발 중에 있으며, Microsoft에서는 자사의 .NET Framework에 XKMS 기능을 통합해 넣어 시제품으로 개발하였다. RSA Security, Phaos 등의 회사들도 연구개발을 진행 중이거나 시제품을 개발하고 있다.

국내의 경우 ETRI 정보보호연구본부에서 ESES (ETRI Secure E-Commerce Services) XML 보안 플랫폼을 기반으로 최근 표준화 작업이 진행중인 W3C 기준안에 따라 기술 개발을 진행하고 있다[10,11].

### 4.2 XKMS 주요 논의사항

2001년 3월 XKMS 1.0이 발표된 이후 2003년 6월 현재 XKMS 2.0 버전의 Draft 상태로 계속 표준화가 이루어지고 있다. XKMS 2.0에서는 기존 내용을 XKMS WG에서 논의하여 메시지 정의 및 프로토콜상의 보안 요구사항 등을 추가로 정의하고 있다[1,2]. 현재 W3C의 XKMS WG에서 논의되고 있는 주요 사항들을 보면 다음과 같다[1].

- 서비스 위치 정보(Service location Information)

다른 도메인의 서비스 연결 시 XKMS 서비스의 위치 정보에 대한 획득 지침이 명확하지 않다.

- 모호한 연결성(Ambiguous binding)

Key Naming의 경우 Key Name이 다른 도메인에서 같을 수 있어, 규격에서는 DNS Name, RFC822 Name, IP 주소, e-mail 주소를 권고하고 있지만 명확한 key Naming 규정이 있어야 한다. 그리고, 여러가지 예외상황에 대한 정책이 미흡하다.

- 유효성 정책(Validation Policy)

규격에서는 유효성 검증 정책에 대한 설정을 지원하지 않고 있다. PKI에서는 인증서가 대기 및 정지 상태에 대한 자세한 내역을 나타낼 수 있으나 XKMS에서는 '유효, 폐기, 미결'의 3가지 상태만 제공한다.

- 키 복구 서비스(Recovery Service)

XKMS에서는 개인키의 저장, 권한설정, 전송방법 등이 설정되어 있지 않다. 그리고, 키 로밍 서비스를 위한 키 복구 정책이 검토되어야 한다.

- 인증 정책(Certification Policy)

인증서 확장 영역의 인증서 정책필드는 정책 검증 시 중요하지만, 규격에서는 명확히 규정하고 있지 않다. PKI에서는 인증서에 대한 검증을 실시할 때, 인증서 정책 연결 및 인증서 정책 검증에 대해 중요하게 인식되고 있으나 XKMS에서는 규정하고 있지 않다.

- 대칭키 서비스(Symmetric Key Management)

효율적인 상황에 적합한 대칭키 서비스 지원에 대한 논의가 진행되고 있다.

위의 주요 내용과 함께 속성 인증서, 익명의 요청자에 대한 처리, Privacy 정책 및 XAdES(XML Advanced Electronic Signature)에 대한 지원 여부가 제안 및 검토되고 있다.

## V. 결 론

본 고에서는 안전한 전자거래를 위해 XML 문서에 대한 정보보호로서 XML 기반 PKI 기술인 W3C의 XML 키 관리 기술 및 관련 기술 동향을 살펴보았다. XKMS를 통해서 응용시스템을 공개키 내부구조에 연결함으로써 개발자들이 PKI를 좀더 쉽게 사용할 수 있게 될 것이며, PKI가 보편화될 것으로 기대된다.

현재 XKMS 서비스는 국내에서 레퍼런스 사이트 구축 개발이 이루어지고 있으며, 기반되는 요소기술들이 개발되고 있다. 앞으로 XKMS 서비스를 위한 상업용 검토 모델 중 하나로 사용자에게 편리함과 안전성 보장을 위해 보다 효율적인 기본 PKI 및 PMI(Privilege Management Infrastructure), KMI(Key Management Infrastructure) 시스템과 연동하는 방안이 과제로 남아 있다. 응용 서비스 시스템의 게이트웨이 형태가 되어 XKMS가 특정

PKI의 RA로 운용할 수도 있으며, PKI의 CA내에 통합 적용하는 방안도 가능할 것이다. 그리고, 차세대 전자거래 환경인 유비쿼터스 및 웹 서비스를 지원하기 위해 무선 플랫폼에서의 XML 전자서명 및 XML 암, 복호화 기술 개발과 유선상의 XKMS 시스템 연동 및 기타 다른 응용서비스 시스템과의 연동을 위한 지속적인 연구가 필요하다.

XML 기술의 발전과 함께 XKMS 서비스가 공개키 인증관리를 위한 웹 서비스로 발전이 예상되며, 글로벌 환경에서의 PKI서비스 제공을 용이하게 할 수 있도록 국내에서는 XKMS에 대한 구조 및 참조 모델을 정의하고, 여러 보안 취약성을 분석하여 안전성이 지원되는 시스템의 연구개발이 진행되어야 할 것이다. 그리고, 산학연 연계 및 전자상거래 표준화 통합포럼(ECIF), 한국정보통신기술협회(TTA) 등의 표준화관련 기관과의 협력을 통해 필요한 표준을 개발해야 할 것이다.

향후에는 전자거래 환경에서의 안전한 문서 교환을 위한 보안 플랫폼에 대한 연구를 기반으로 웹 서비스가 보다 안전한 서비스를 제공할 수 있는 환경을 구축할 수 있는 연구가 진행되어야 할 것이며, 기존 여러 시스템과 XKMS의 연동을 위한 연구가 선행되어야 하겠다.

## 참 고 문 헌


[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.


## 〈著 者 紹 介〉


**박 남 제 (Nam-je Park)**
**정회원**

2000년 8월 : 동국대학교 정보산업학과 졸업
2003년 8월 : 성균관대학교 정보통신대학원 정보보호학과 석사
2000년 5월~2003년 2월 : (주)뉴레카 정보통신연구소 전임연구원
2003년 2월~2003년 4월 : 행정자치부 자치정보화조합 주임
2003년 4월~현재 : 한국전자통신연구원 능동보안기술연구팀
관심분야 : 전자상거래 보안, XML 보안, 무선인터넷 보안, 전자지불 등

**문 기 영 (Ki-young Moon)**
**정회원**

1986년 2월 : 경북대학교 전자공학과 졸업
1989년 2월 : 경북대학교 전자공학과 석사
1992년 1월~1994년 3월 : (주)대우정보시스템 기술연구소 대리
1994년 3월~현재 : 한국전자통신연구원 능동보안기술연구팀 선임연구원
관심분야 : 전자상거래 보안, 분산시스템, 트랜잭션 등

**손 승 원 (Sung-won Sohn)**
**정회원**

1984년 : 경북대학교 전자공학과 졸업
1994년 : 연세대학교 전자공학과 석사
1999년 : 충북대학교 컴퓨터공학과 박사
1983년~1986년 : 삼성전자(주) 연구원
1986년~1991년 : LG전자(주) 중앙연구소 HI8mm 캠코더 팀장
1991년~현재 : 한국전자통신연구원 정보보호연구본부 네트워크보안연구부장/책임연구원
관심분야 : IC Card, Biometry, Active Network, 생체인식분야 등

**송 유 진 (You-jin Song)**
**정회원**

1982년 : 한국한공대학교 전자공학과 졸업
1987년 : 경북대학교 정보시스템 전공 (석사)
1995년 : 일본 Tokyo Institute of Technology (박사)
1988년~1996년 : 한국전자통신연구원 선임연구원
1996년~현재 : 동국대학교 정보산업학과 교수
1998년~현재 : 한국정보보호학회 이사, ISO/IEC JTC1/SC27-Korea 전문위원
관심분야 : 암호 및 인증이론, 전자상거래보안 응용, 전자화폐/전자지불, 컨텐츠 보호 등

**원 동 호 (Dong-ho Won)**
**종신회원**

1976년 : 성균관대학교 전자공학과 졸업
1978년 : 성균관대학교 대학원 전자공학과 석사
1988년 : 성균관대학교 대학원 전자공학과 박사
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공대 객원연구원
1997년~1998년 : 국무총리실 국가정보화 추진위원회 자문위원
1982년~현재 : 성균관대학교 정보통신공학부 교수
2000년~현재 : 정보통신부 지정 정보보호인증기술연구센터 센터장
2002년~현재 : 대검찰청 컴퓨터범죄수사/감사원 IT 감사 자문위원, 성균관대학교 연구처장
관심분야 : 암호이론, 부호이론, 공개키 기반구조 등