2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

XML 기반 차세대 PKI(Public Key Infrastructure) 표준 기술 분석

김세영° , 송준홍, 원덕재, 이형석, 신동규, 신동일
세종대학교 컴퓨터공학과
e-mail : seykim@gce.sejong.ac.kr

Technology Analysis of Next Generation PKI(Public Key Infrastructure) based on XML

Seyoung Kim, Junhong Song, Duckjae Won,
Hyoungseok Yi, Dongkyoo Shin, Dongil Shin
Department of Computer Engineering, Sejong University

요 약

최근 주목할만한 인터넷 보안기술 중 공개키 암호화 시스템을 이용해 향상된 보안수준을 제공하기 위한 기반 기술인 PKI(Public Key Infrastructure)는 각종 전자상거래 제반기술로 작용한다는 점에서 중요성이 부각되고 있다. 이와 더불어 최근 차세대 웹 표준문서 포맷으로 부상되고 있는 XML(eXtensible Markup Language)은 B2B 문서교환과 데이터 전송 및 검색 부문에서 광범위하게 활용됨으로써, XML문서에 대한 보안 및 XML을 활용한 PKI 기술적용을 위한 표준화 작업 또한 활발히 연구되고 있다. 그 결과 Microsoft, Verisign 그리고 Webmethods가 주축이 되어 XML기반 차세대 PKI기술인 XKMS(Xml Key Management Specification)를 개발하였으며, XKMS 표준화 작업에 그 외 다수의 주력업체들이 참여하고 있다. 이에 본 논문에서는 XKMS의 표준화를 진행중인 표준화 단체의 동향을 파악하고, PKI의 전반적인 기술 및 XKMS 기술의 내부적인 구조를 분석한다.

1. 서론

최근 주목할만한 인터넷 보안기술 중 공개키 암호화 시스템을 이용해 향상된 보안 수준을 제공하기 위한 기반 기술인 PKI는 각종 응용 시스템 및 전자상거래 기반기술로 작용한다는 점에서 그에 따른 중요성이 부각되고 있으며, PKI의 보급 또한 지속적으로 증가하고 있는 추세이다[1]. 이와 더불어 최근 차세대 웹 표준문서 포맷으로 부상되고 있는 XML은 B2B 문서교환과 데이터 전송 및 검색 부문에서 광범위하게 활용됨으로써[2], 이에 따른 XML 문서에 대한 보안 및 XML문서 형식에 따라 XML을 활용한 PKI 기술을 적용하기 위한 표준화 작업 또한 활발히 연구되고 있다. XML을 이용한 각종 데이터 및 문서는 웹 상에 존재하게 되며, 가상공간에서 문서의 처리는 제 3자에 의해 위조나 변경이 가능하다. 이에 XML 데이터 및 문서를 보호하는 일은 현재 필수적인 사안으로 대두되고 있다. 또한, 기업 간 전자상거래(B2B)의 경우 메시지를 웹 상에서 상호간에 주고받으며, 제 3자에 의한 변조나 삭제를 막기 위한 무결성, 신분에 대한 인증 및 부인방지에 대한 검증이 필요하다. 이에 대한 대안으로 전자서명 기법을 사용하게 된다.

XML 전자서명 관련 표준화는 W3C(World Wide Web Consortium)와 IETF(Internet Engineering Task Force)에서 주도적인 표준화 작업을 담당하고 있으며[5], 현재 W3C에서 수행하고 있는 거의 모든

업무가 XML에 기반 한 기술개발, XML 기술 이용, XML 어플리케이션의 개발과 연관되어 있다. 각 XML 기술 워킹그룹의 활동 중 보안 및 전자서명에 관련된 표준화는 XML-Signature 워킹그룹에서 진행되고, 최근 새롭게 조직된 XML-Encryption 워킹그룹에서 한층 더 강화된 보안 서비스를 제공하기 위해 상위단계의 보안구조에 대한 표준화 작업이 진행되고 있다.

이러한 추세에 따라, 최근 Microsoft와 Verisign, Webmethods등 3개사는 XML기반 차세대 PKI기술인 XKMS를 개발하였으며, XKMS 표준화 작업에 휴렛패커드(HP), 볼티모어, IBM, 퓨어에지솔루션스, 로이터 등이 참여하고 있다. 이에 본 논문에서는 XKMS의 표준화를 진행중인 표준화단체의 XML 보안동향을 파악하고, XKMS의 내부 구조 및 전반적인 기술을 분석한다.

2. 관련연구

2.1 PKI

XML 전자서명과 더불어, 전자서명을 구현하는데 필요한 핵심기술은 PKI라 할 수 있다. 전자상거래 시스템은 공개키 암호시스템에 바탕을 두고 실현되어야 사용자 공개키의 신뢰성과 안전성을 보장받을 수 있다. 공개키 기반구조(PKI)는 공개키 암호방식을 사용하는 암호시스템에서 사용자의 공개키를 안전하고 신뢰성 있게 공표 하는 수단을 제공한다[6]. 따라서 안전하고 신뢰성 있게 사용자의 공개키를 공표하기 위한 공개키 기반 구조는 인터넷 전자상거래 시스템에서 매우 중요한 역할을 수행할 것이다. 그러나, PKI 자체보다는 응용 프로그램에서 요구하는 보안 요구사항을 분석하고, 사용자의 편의성과 보안성을 동시에 만족시키면서 이를 기반으로 응용 시스템을 이용한다는 데 의미가 있다. PKI 시스템은 인증기관(CA), 등록대행기관(RA), 디렉터리서버(DS) 등으로 구성되며, 응용분야는 보안메일, 전자상거래, 싱글사인온, 가상사설망, 전자상거래, CALS/EDI, PC보안, m커머스, 인터넷뱅킹, 사이버트레이딩, 그룹웨어등 다양하다.

3. XML 기반 차세대 PKI 기술(XKMS) 분석

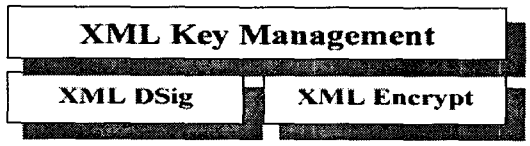
3.1 XKMS의 개요

최근 미국의 Microsoft와 보안전문업체인 Verisign, WebMethods가 공동 개발하고, 다수의 주류기업들이 연계하여 W3C의 웹 표준화 단계의 진행을 위하여 XKMS명세서를 제출했다.

XKMS는 차세대 인터넷언어인 XML에 기반을 두고 있으며, 기업이나 개발자들이 XML 웹 서비스에 PKI 전자 서명과 암호화의 사용효율성을 극대화할 수 있도록 지원하고 있다. 즉, XKMS는 개발자에게 전자상거래 응용 시스템에 적용할 전자서명과 데이터 암호화를 보다 용이하게 할 목적으로 개발된 것이다. 전자서명을 위한 보안 소프트웨어, 온라인 인증, 데이터 암호화 등의 기능들은 전자상거래 사이트 상에서 협정되는 안전한 거래와 계약을 지원하며, XKMS 기술은 개발자들이 전자 인증과 다른 온라인 보안기능을 전자상거래 응용시스템에 쉽게 접목할 수 있게 한다. XKMS는 응용 시스템을 공개키 내부구조에 결부시킴으로써 소프트웨어 개발자들이 PKI를 좀더 저렴하고 쉽게 사용할 수 있도록 하기 위한 새로운 방식이며, PKI를 보편화시키기 위한 것이다[4].

3.2 W3C의 XKMS 명세서

이 문서는 XML 암호화를 위해서 W3C와 IETF에 의해 개발된 XML 전자서명 표준 명세서와 연계된 효율적인 활용을 목적으로 개발되었으며, 공개키의 등록과 배포를 위한 프로토콜을 명시한다. XKMS의 전체적인 구조에 대한 설계 목적은 W3C의 XML Digital Signature 워킹그룹과 XML Encryption 워킹그룹의 활동 결과[3]를 보완하기 위한 것이다. 다음의 [그림1]은 XKMS와 XML-DSig와 XML-Encrypt사이의 관계를 도식화한 것이다.



[그림 1] XKMS 및 XML DSig, Encrypt 사이의 관계

XKMS는 크게 X-KISS(XML Key Information Service Specification)와 X-KRSS(XML Key Registration Service Specification)의 두 영역으로 구성되어 있다. X-KISS는 XML전자서명 요소 내에 포함된 공개키 정보를 해석하는 Trust Service에 대한 프로토콜을 정의하고, <ds:KeyInfo> 내에 포함된 데이터 처리를 위한 요구사항에 대한 서비스 등을 클라이언트에게 제공한다. 이 프로토콜 설계의

핵심적인 목표는 기본적인 PKI에서의 XML구문의 확립과 복잡성의 제거로 인해, 응용 시스템에 대한 실현을 최대한 단순화하는 것이다. XKMS에서의 기본적인 PKI는 X.509/PKIX, SPKI (Simple Public Key Infrastructure) 및 PGP (Pretty Good Privacy)와 같은 다른 명세서에 기초를 두고 있다.

X-KRSS는 공개 키 정보의 등록을 처리하는 웹 서비스에 대한 프로토콜을 정의한다. 공개키는 등록된 즉시 X-KISS를 포함하는 다른 웹 서비스와의 결합으로 사용되어질 수 있다.

두 프로토콜은 XML Schema Language, WSDL(Web Services Definition Language v1.0)에 의해 정의된 메시지 사이의 관계를 정의하고, SOAP(Simple Object Access Protocol v1.1)을 채택하는 프로토콜 내부에서 표현되는 구조를 정의한다. 또한, 다른 응용에 부합되는 객체 인코딩 구조에서 내부적인 XKMS의 표현 역시 가능하다.

3.3 XKMS의 내부 구조

① X-KISS

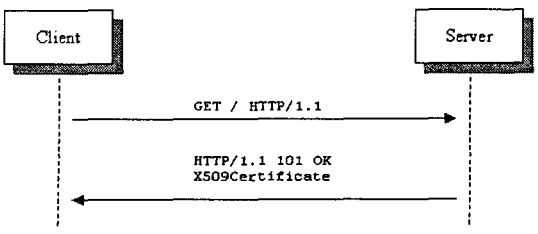
공개키, XML-DSig 및 XML-Encrypt와 결합하여 키 정보처리 서비스를 지원하기 위한 프로토콜이다. XML 전자서명 내에서 서명자의 공개키에 대한 정보를 <ds:KeyInfo>내에서 선택적으로 포함할 수 있다. 이 키의 정보는 서명자에게 선택된 공개키에 대한 인증을 허용하며, 서명자체에 대한 암호와의 연계가 가능하다.

② Key Information Service Protocol

특정 응용에서는 한층 더 심화된 PKI서비스를 요구한다. 이러한 요구를 지원하기 위해 XKMS에서는 계층적 서비스 모델로 세분화시킴으로써, 업무에 따른 정확한 처리 계층을 선택할 수 있도록 정의하고 있다.

- Tier 0 : <ds:RetrievalMethod>의 처리

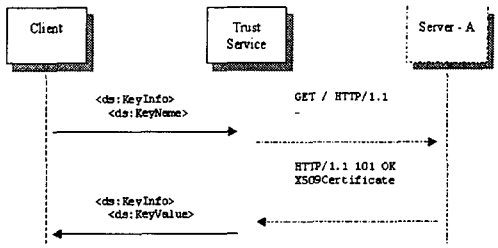
XML 전자서명 명세서에 따라 응용 프로그램에 의해 처리되며, Trust Service가 없이 처리된다.



[그림 2] Tier 0 Protocol의 구조

- Tier 1 : Locate Service

<ds:KeyInfo>가 포함하는 데이터의 처리는 Trust Service에 위임되며, 공개키를 가진 <ds:KeyInfo>를 반환하고, <ds:KeyInfo>의 유효성은 클라이언트에 의해 수행된다.



[그림 3] Tier1 Protocol의 구조

다음의 그림은 클라이언트에서 <KeyName>과 <KeyValue> 요소의 데이터에 대한 요청을 보내고, 응답을 받는 예제를 나타낸다.

```
<Locate>
  <Query>
    <ds:KeyInfo>
      <ds:RetrievalMethod
URI="http://www.PKeyDir.test/Certificates/01293122"
Type="http://www.w3.org/2000/09/xmldsig#X509Data"/>
    </ds:KeyInfo>
  </Query>
  <Respond>
    <string>KeyName</string>
    <string>KeyValue</string>
  </Respond>
</Locate>
```

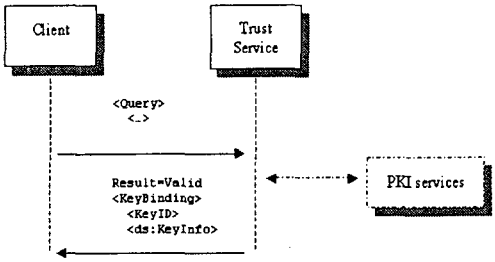
[그림 4] 문서 서명 데이터 요청(Request) 예제

```
<LocateResult>
  <Result>Success</Result>
  <Answer>
    <ds:KeyInfo>
      <ds:KeyName>O=XMLTrustCernter.org
                  OU="Crypto"
                  CN="Alice"</ds:KeyName>
      <ds:KeyValue>...</ds:KeyValue>
    </ds:KeyInfo>
  </Answer>
</LocateResult>
```

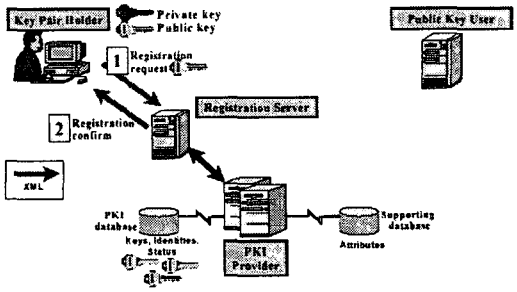
[그림 5] 문서 서명 응답(Respond) 예제

- Tier2 : Validate Service

Tier2에서는 <ds:KeyInfo>내에 포함된 데이터들이 한층 더 많은 정보를 전달해준다. 클라이언트는 공개키와 다른 데이터들 사이의 조합상태에 대한 정보들을 획득할 수 있다. 또한, 공개키와 연계하여 응답 받은 데이터의 유효성을 제공한다.



[그림 6] Tier 2의 키 검증 서비스 구조



[그림 7] X-KRSS내에서의 키 등록

각각의 계층적인 구조 내부에서 Trust Service는 다음과 같은 기능을 클라이언트에게 제공한다.

- 복잡한 구문과 의미의 효율적인 조작
- 디렉토리와 데이터 저장 하부 구조로부터의 정보 검색
- 상태확인 및 철회
- 신뢰관계의 생성과 처리

③ X-KRSS

기존의 PKIX와 같은 인증관리 프로토콜은 인증 처리과정의 일부만을 지원하거나 지나치게 복잡해 소규모 XML 어플리케이션에는 적당하지 않았다. X-KRSS는 이러한 문제를 극복하기 위한 클라이언트 측에 초점을 맞춘 완전한 키 관리 프로토콜이다. 또한, X-KRSS는 X.509 v3과 같은 하부 PKI시스템의 경량 인터페이스 역할을 수행할 수 있다.

X-KRSS는 키 등록, 키 폐기 및 키 복구의 전체 인증 처리과정을 단순한 단일 명세서에서 지원한다.

X-KRSS의 키 등록은 키 쌍의 소유자가 등록 단계에서 자신의 공개키를 등록 서버(Registration Server) 내부에 등록한다. 공개키는 이때 KRSS에 명시된 전자 서명을 수행한 요청서에 포함되어 전송된다. 이때 요청에는 이름과 속성 정보, 인증 정보, 개인 키 소유 증명(Proof-of-possession)와 같은 정보가 포함 될 수 있다.

등록 서버는 요청을 수신 한 뒤, XML형식의 응답을 전송한다. 이 응답 문서에는 요청에 대한 허용, 거부, 대기 등의 처리결과 및 공개키와 함께 등록되어 있는 이름, 속성 정보 등을 전송한다. 이 때, 요청 거절의 경우를 제외하고는 추후 참조될 키 쌍 식별자를 전송한다.

일반적인 요청 및 응답은 아래의 그림과 같은 순서를 가진다.

4. 결론 및 향후 연구방향

본 논문에서는 XKMS의 표준화를 진행중인 표준화 단체의 동향을 파악하고, PKI의 전반적인 기술 및 XKMS 기술의 내부적인 구조를 분석하였다. XML이 전자상거래를 위한 표준 기술로 부상하고 있는 현실을 반영해 볼 때, XML 보안에 대한 표준화된 방식의 도입으로 XML을 사용하는 전자상거래에서의 효율적인 PKI 적용 방안을 연구해 나가야 할 것이다. 또한, XML 문서 교환시의 보안이 강화된 시스템의 개발이 절실히 요구되므로, XML 보안 시스템의 구축에 대한 연구가 활발히 진행되기를 기대한다.

5. 참고 문헌

[1] Prasad, V.; Potakamuri, S.; Ahern, M.; Lerner, M.; Balabine, I.; Dutta, P., "Scalable policy driven and general purpose public key infrastructure (PKI)", Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference , Page(s): 138 -147

[2] Extensible Markup Language (XML), http://www.w3c.org/XML

[3] XML Encryption Syntax and Processing http://www.w3.org/TR/2001/WD-xmlenc-core-20010626

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

[5] XML-Signature Syntax and Processing, http://www.w3.org/TR/2001/PR-xmldsig-core-20010820

[6] Younglove, R.W., "Public key infrastructure. How it works", Computing & Control Engineering Journal, Volume: 12 Issue: 2 , April 2001, Page(s): 99 -102