e-비즈니스를 위한 전자거래 정보보호기술

서 창 호* 윤 보 현** 이 태 훈***

◈ 목 차 ◈

1. 서 론
2. XML 정보보호 기술
3. 웹서비스 보안 프레임워크 기술
4. 표준화 동향
5. 활용 예
6. 결 론

1. 서 론

인터넷과 네트워크 환경의 발달로 분산 처리 환경이 발전하면서 여러 가지 어플리케이션들은 네트워크에 연결된 여러 호스트에서 실행 가능하다. 현재 사용되고 있는 웹 환경의 특성상 어플리케이션에 대한 공격이 쉽기 때문에 보안의 중요성은 점점 커지고 있다. 현재 어플리케이션 계층에서 동작하는 웹 서비스가 차세대 e-비즈니스를 주도할 것으로 많은 주목을 받으면서 웹 서비스를 기술하는 WSDL (Web Service Description Language)[2]과 웹 서비스의 검색을 위한 UDDI(Universal Description, Discovery and Integration)[3], 그리고 웹 서비스의 서비스 호출을 책임지는 SOAP(Simple Object Access Protocol)[4,5]등의 XML 형식의 표준기술 사용이 폭 넓게 성장해 가고 있다. 그러나 안전한 서비스 제공 측면에서 웹 서비스는 폐쇄 환경에서 존재하지 않았던 새로운 보안 고려 사항들을 부각시키고 있다. 그 중 개발자들의 입장에서 우려하는 부분은 비 인가된 권한의 사용, 서비스 거부, 데이터 노출 또는 변경, 송수신 부인 등에 관한 보안 사항들이다[6].

본 논문에서는 안전한 e-비즈니스를 주도할 웹 서비스에 대해 알아보며, XML 정보보호기술, 웹 서비스 보안 프레임워크 기술 및 웹 서비스의 표준화 동향 그리고 웹 서비스 기술을 이용한 활용 예를 보여주고, 차세대 e-비즈니스에 대한 전망을 제시한다.

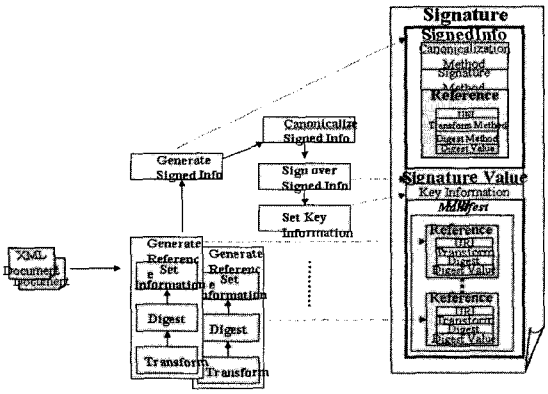
2. XML 정보보호 기술

XML은 문서의 데이터 표현 형식을 향상시키는데 중점을 두고 만들어진 것으로 문서의 위·변조, 데이터 삭제 등 보안에는 취약하다. XML이 웹 서비스의 표준으로 정해짐에 따라 XML 보안은 과거 웹 보안의 일부분에서 독립하여 새로운 분야로 분류되었다. 현재 XML 보안에 대한 명세는 W3C에서 제정하고 있으며, 그 중 대표적인 XML-Signature[7], XML-Encryption[6], XKMS(XML Key Management Specification)[8], SAML(Security Assertion Markup Language)[9], XACML(eXtensible Access Control Markup Language)[10]에 대해 간단하게 소개한다.

2.1 XML - Signature

W3C는 IETF(Internet Engineering Task Force)와 공동으로 XML 트랜잭션에 이용할 수 있도록

* 공주대학교 응용수학과
** 목원대학교 컴퓨터교육과
*** 광주대학교 컴퓨터전자통신공학부

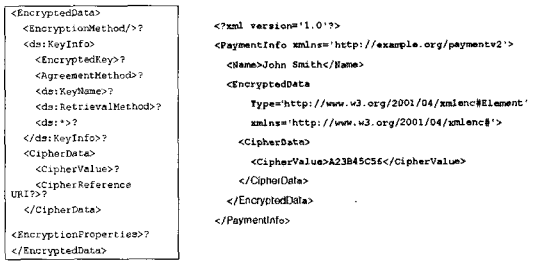


(그림 1) XML-Signature

설계된 디지털 서명을 정의하여 XML-Signature로 표준화했다. 이 표준에서는 디지털 서명 오퍼레이션의 결과를 가져올 수 있는 스키마를 정의하고 메시지 인증과 무결성, 서명된 데이터에 대한 부인봉쇄 등을 지원하기 위한 내용이 포함되어 있다. XML-Signature의 장점은 특정 문서 전체에 대한 서명 또는 부분적인 서명이 가능하다. XML-Signature가 가지고 있는 이러한 유연성은 서버의 부담을 덜어주고, 사용자의 필요에 따라 서명 할 부분을 선택할 수 있는 융통성을 제공해준다. 또한 Enveloped, Enveloping, Detached등 다양한 형태의 전자서명 형태를 지원하며, 2002년 2월 recommendation 상태로 표준화가 완료된 상태이다.

2.2 XML - Encryption

XML 문서에 기밀성을 제공할 수 있는 XML-Encryption은 W3C에서 2002년 12월 10일자로 recommandation 상태로 표준화가 완료되었으며, XML 기반 데이터의 기밀성을 보장하기 위해 암호화와 복호화 및 결과 표시를 위한 처리를 명시하고 있다. 또한 문서 단위 암호화, 원하는 element 단위의 암호화, element안의 각 단위로의 암호화, 그리고 암호화 된 내용을 복수로 암호화 기능등 다양한 형태의 암·복호 형태 지원이 가능하다. 그림 2는 XML-Encryption의 기본 구조를 나타낸 것이다.



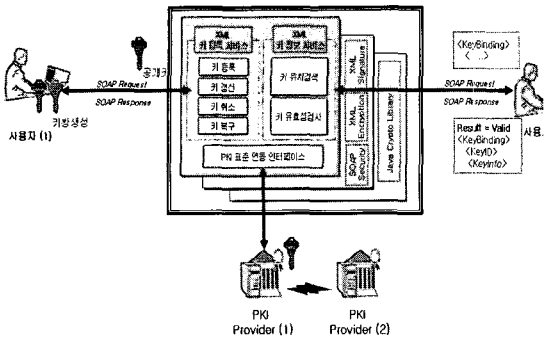
(그림 2) XML-Encryption

2.3 XKMS

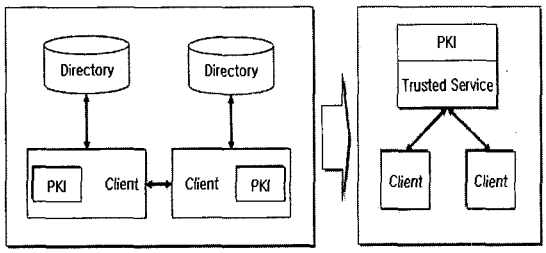
XKMS(XML Key Management Specification)은 전자서명, 암호화된 XML 문서를 지원할 경우 PKI기능을 XML 기반 어플리케이션에게 용이하게 지원할 수 있는 공개키 관리를 위한 프로토콜로써, 포괄적이고 표준적인 접근 방식을 취하는 구조를 가진다.

XML 기반 트랜잭션의 신뢰성 있는 지원을 위한 온라인 인증에 대해 암호 키 관리 문제 해결을 위해 필요하며, 최초 설계 목적은 XML 전자서명과의 연동 시, 기존 PKI 시스템에 대한 복잡성을 클라이언트에게 숨겨 키 관리 부담을 신뢰 서비스(Trust Serivce)[13]에 위임해 그 구현을 용이하게 하기 위함이다. 주요 목적은 전자서명을 검증하거나 데이터를 암호화하기 위해 사용되는 공개키 사용자에게 필요한 키의 위치를 명시하고, 이름이나 속성 정보를 해당 개인키 소유자와 관련지어 주는 것을 말한다. XKMS는 인증서 정보를 제공하는 X-KISS(XML Key Information Service Specification)과 X-KRSS(XML key Registration Service Specification)의 두 부분으로 구성된다.

XKMS는 전통적인 PKI 구현의 복잡성에 비해 XML의 단순성으로 비즈니스 시스템 간 데이터의 간편한 응용성을 제공한다. XKMS와 XML 신뢰 서비스의 주요목적은 XML 어플리케이션을 전통적인 PKI 구현의 복잡성으로부터 분리하자는 것이다. XKMS는 XML처리가 수행되는 클라이언트 플랫폼 상에서 복잡하거나 전문화된 PKI 어플리케이션 도움 없이 XML 기반 시스템이 신뢰적 관계를



(그림 3) XKMS 전체 흐름도



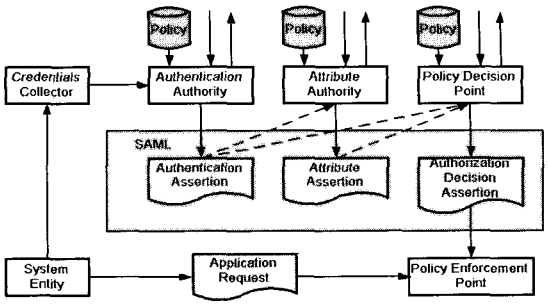
(그림 4) 일반 PKI 구조와 XKMS 적용후의 구조

구축한다. 또한 XKMS는 어플리케이션을 공개키 기반 구조에 결부시킴으로써 소프트웨어 개발자들이 그림 4와 같이 PKI를 좀더 저렴하고 쉽게 사용할 수 있도록 하기 위한 방식이며, 사용자 측면에서 PKI를 단순화 시키는 것이다.

2.4 SAML

SMAL은 OASIS의 STTC(Security Services Technical Committee)가 제안한 것으로 이질적인 웹 접근 관리와 보안 제품간에 인증과 인가 정보를 교환하기 위해 제안된 XML 기반 프레임워크이다.

그림 5를 보면 SAML을 이용하여 시스템 엔터티가 접근 제한된 자원에 접근하는 유즈케이스(use-case)의 흐름을 나타낸 것이다. 우선, 보증 정보(credential information)를 모아 credential assertion을 구성한다. 다음으로는 수집된 보증 정보를 이용해 사용자를 인증하게 된다. 인증 시 authentication assertion을 전달하기 위해서 PKI 서비스를 이용할 수도 있다. 추가적인 요구에 따라 session

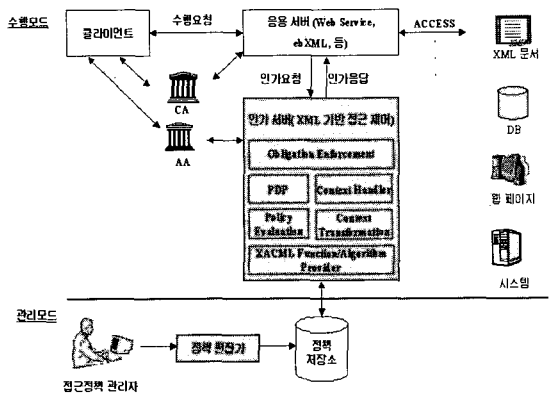


(그림 5) SAML 아키텍처

assertion 또는 authorization decision assertion 단계로 진행된다.

2.5 XACML

OASIS의 XML정보보호 표준중의 하나인 XACML은 자원 및 시스템에 대한 사용자의 접근 권한을 명시하는 접근제어 정책에 대한 표준화 된 언어의 제공을 목적으로 하는 XML기반의 접근 제어 언어이다. XACML의 정의에 따라 각각의 사용자별 XML 데이터 접근 정책을 수립하고 적용 할 수 있다. 접근에 대한 허가 또는 거부와 같은 단순한 접근 제어를 하는 것이 아니라 보다 미세한 접근 제어 모델을 제공한다[10,11].



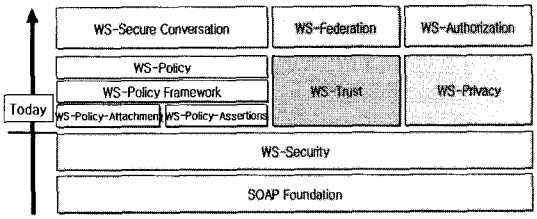
(그림 6)XACML 아키텍처

XACML은 XML로 기술된 정책 언어와 접근제어 결정 요구/응답 언어로 구성되어 있다. 정책 언

어는 규칙, 정책 및 정책 셋 등에 관한 통상적인 접근제어 요구사항들에 대해 기술하고 있으며 함수들, 데이터 타입들 및 조합 논리 등에 대해서도 정의하고 있다. XACML은 2003년 7월에 XACML v1.1 표준이 완성됐고, 현재 XACML v2.0 개발이 진행 중이다[5].

3. 웹서비스 보안 프레임워크 기술

2002년 4월, IBM, MS, Verisign은, 웹 서비스 개발자들이 안전한 SOAP 메시지 교환을 할 수 있도록 하는 메커니즘인 Web Services Security (WS-Security) 스팩을 합동으로 발표했으며, 이 개념 스택에서 세가지 부분(정책(Policy)레이어의 두 요소와 연합 레이어의 한 요소)이다[그림 7].



(그림 7) WS-Security RoadMap

3.1 웹서비스 보안 프레임워크 기술

웹 서비스의 보안 기능과 컴포넌트를 가진 포괄적 모델을 제공하려면 현재 사용 가능한 프로세스들과 기술들을 향후 애플리케이션의 변화하는 보안 요구사항과 통합해야 한다. 그것은 통일된 개념을 필요로 하며, 기술적인 문제 (안전한 메시징)와 비즈니스 프로세스 문제(정책, 리스크, 신임) 양쪽에 대한 솔루션을 필요로 한다. 마지막으로 플랫폼 업체, 애플리케이션 개발자, 네트워크와 인프라 제공자 및 고객에 의한 조화로운 노력을 요구한다. 여기에서 설명하는 보안 전략은 아래에서 소개되는 WS-Security 사양 보안 모델의 전략적 목표와 초석을 제공한다.

또한 웹 서비스 엔드포인트 정책(WS-Policy), 신임 모델(WS-Trust), 프라이버시 모델(WS-Privacy)과 함께 메시지 보안 모델(WS-Security)을 포함한다. 이러한 기초 사양들은 신임 도메인들간에 상호작용 가능한 안전한 웹 서비스를 구축할 수 있도록 하는 기초를 제공하며, 이러한 기초 사양들을 기반으로 안전한 통신(WS-SecureConversation), 연합된 신임(WS-Federation) 및 인증 (WS-Authorization)을 위한 후속 사양들을 제공한다.

이 보안 사양들을 결합하여 현재의 보다 기본적인 보안 메커니즘으로는 구현하기 어려운 많은 시나리오들을 가능하게 한다.

3.1.1 WS-Security

WS-Security는 메시지 무결성과 기밀성을 통해 보안 품질을 제공하기 위하여 SOAP 메시징의 개선 사항을 기술하며, 또한 이 사양은 SOAP 메시지 내에 보안 토큰을 어떻게 첨부하고 포함시킬 것인지를 기술한다. 마지막으로, 이진수로 암호화된 보안 토큰(예 : X.509 인증서)을 지정하기 위한 하나의 메커니즘이 제공하며, 광범위한 보안 모델과 암호화 기술들을 수용하기 위해 독립적으로 혹은 결합되어 사용될 수 있다.

WS-Security는 보안 토큰을 메시지와 결합시키기 위한 범용 메커니즘을 제공하며, 특정 유형의 보안 토큰을 요구하지 않고 확장 가능하도록 설계되었다. 예를 들어, 요청자는 신원 증명과 그들이 특정 비즈니스 인증서를 가지고 있다는 증명을 제공할 수 있다.

또한 메시지가 변경 없이 전달되었음을 보장하기 위해 보안 토큰과 함께 XML 서명을 활용함으로써 메시지 무결성이 제공된다. 무결성 메커니즘은 잠재적으로 다수의 actor에 의한 여러 서명을 지원하고 추가적인 서명 포맷을 지원하도록 확장될 수 있도록 설계되었으며, 서명은 보안 토큰을 참조할 수 있다.

이와 유사하게, 메시지 기밀성은 SOAP 메시지의 일부분을 비밀로 유지하기 위해 보안 토큰과 결합된 XML 암호화를 활용함으로써 제공된다. 암호화 메커니즘은 추가적인 암호화 기술, 프로세스, 다

수의 actor에 의한 작업등을 지원하도록 설계되었고, 암호화는 또한 보안 토큰를 참조할 수 있다.

마지막으로 WS-Security는 이진수 보안 토큰을 암호화하는 메커니즘을 기술한다. 구체적으로, 이 사양은 애매하게 암호 처리된 키들을 어떻게 포함시킬지 뿐 아니라 X.509 인증서와 Kerberos 티켓을 어떻게 인코딩하는지를 기술하며, 또한 메시지에 포함된 보안 토큰의 특성을 더 자세히 기술하기 위해 사용될 수 있는 확장성 메커니즘을 포함한다.

3.1.2 WS-Policy

WS-Policy는 발신자와 수신자가 각자의 요건과 기능을 어떻게 지정하는지를 설명한다.

WS-Policy는 완전히 확장 가능하며, 설명된 요건과 기능의 유형에 제한을 두지 않는다. 그러나 사양은 프라이버시 속성, 인코딩 포맷, 보안 토큰 요건 및 지원되는 알고리즘과 같은 몇 가지 기본 서비스 속성을 규정한다. 이 사양은 일반적인 SOAP 정책 포맷을 정의하며, 이는 단순한 보안 정책 이상을 지원할 수 있으며, SOAP 메시지에 서비스 정책을 첨부하는 메거니즘도 정의한다.

3.1.3 WS-Trust

WS-Trust는 직접적인, 그리고 중개된 신임 관계(third-party와 중개자 포함)를 구축하기 위한 모델을 설명한다.

이 사양은 기존의 직접적인 신임 관계가 어떻게 보안 토큰 발행 서비스의 생성을 통해 중개된 trust를 위한 기초로 사용되는지를 설명하며, 이 보안 토큰 발행 서비스는 무결성과 기밀성을 보증하면서 필수적인 보안 토큰을 전달하기 위해 WS-Security를 기반으로 구축된다. 그리고 이 사양은 어떻게 몇 개의 기존 신임 메커니즘이 이 신임 모델과 연동하여 사용될 수 있을지를 나타낸다.

마지막으로, 신임 모델은 원칙적으로 위임과 구체화를 명확하게 허용하지만, 이를 지시하지는 않고, 위임은 구체화와 일관성을 가지지만, 추가적인 레벨의 추적성은 제공하지 않는다.

3.1.4 WS Privacy

웹 서비스를 개발, 관리, 사용하는 조직들은 종종 자신들의 프라이버시 정책을 명확하게 표명하고, 들어오는 요청들이 발신자에게 이러한 정책을 따르도록 요구하도록 할 필요가 있다.

WS-Policy, WS-Security 및 WS-Trust를 결합하여 사용함으로써 조직들은 프라이버시 정책을 명시하고 이를 따르도록 지시할 수 있으며, 프라이버시 용어가 WS-Policy 설명에 어떻게 포함될 수 있는지, 그리고 프라이버시 클레임을 메시지와 연결시키는데 WS-Secrutity을 어떻게 사용할 수 있는지를 나타낸다. 마지막으로, 이 사양은 사용자 선호와 조직적인 실행 요구에 대해 이들 프라이버시 클레임을 평가하는데 WS-Trust 메커니즘이 어떻게 사용될 수 있는지를 설명이 가능하다.

3.1.5 WS-SecureConversation

WS-SecureConversation은 웹 서비스가 요청자 메시지의 신원을 어떻게 확인하고 요청자가 서비스의 신원을 어떻게 확인하며 상호 신원 확인된 보안 문맥을 어떻게 구축하는지를 나타낸다.

WS-SecureConversation은 세션 키, 파생 키(derived key), 및 메시지당 키를 구축하는 방법을 설명한다. 마지막으로, WS-SecureConversation은 서비스가 문맥 (보안 속성과 관련 데이터에 관한 클레임 집합)을 어떻게 안전하게 교환할 수 있는지를 나타내며, 이를 위해 WS-Security와 WS-Trust에 정의된 보안 토큰 발행 개념과 교환 메커니즘을 설명하고 이를 기반으로 구축된다. 예를 들어, 한 서비스는 이들 메커니즘을 이용하여 비공유(비대칭) 키를 사용하는 보다 강력한 보안 토큰을 발행할 뿐 아니라 약한 대칭 키 기술을 사용하는 보안 토큰을 지원할 수 있다.

WS-SecureConversation은 메시지가 다양한 전송 및 중개층을 이동할 수 있도록 SOAP 메시지 계층에서 작동하도록 설계될 수 있다. 이것은 다른 메시징 프레임워크에서의 사용을 배제하는 것은 아니며, 시스템의 보안을 더욱 향상시키기 위해 선택된 링크상에서 전송 레벨 보안을 WS-Security와 WS-

SecureConversation과 함께 사용할 수 있다.

3.1.6 WS-Federation

WS-Federation은 WS-Security, WS-Policy, WS-Trust 및 WS-SecureConversation를 이용하여 연합된 신임 시나리오를 구축하는 방법을 정의한 것으로, 중개되고 있는 신임의 유형을 가리키고 제한하고 확인하기 위한 신임 정책을 설명한다.

이 WS-Federation은 또한 신임 관계를 관리하기 위한 메커니즘을 정의한다.

3.1.7 WS-Authorization

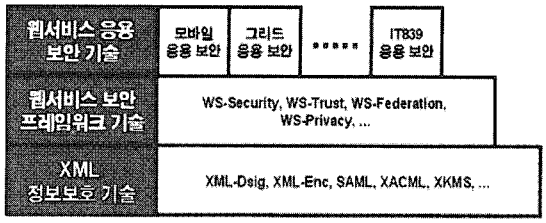
WS-Authorization은 웹 서비스에 대한 접근 정책이 어떻게 지정되고 관리되는지를 설명하는 것으로 특히, 보안 토큰 내에서 클레임이 어떻게 지정되고 이 클레임들이 엔드포인트에서 어떻게 해석될지를 나타낸다.

이 WS-Authorization은 인증 포맷과 인증 언어 모두에 대해 유연하고 확장성 있도록 설계되며 광범위한 시나리오가 가능해져, 보안 프레임워크의 장기적인 생존력이 보증된다.

3.2 기본적인 웹 보안 기술 구성요소

웹서비스 보안기술은 기술 특성에 따라 XML 정보보호 기술, 웹서비스 보안 프레임워크 기술, 웹서비스 응용보안 기술로 구분된다.

첫번째 XML 정보보호 기술은 XML 기반 서비스나 시스템을 위한 보안 기반 기술로 인증, 인가, 기밀성, 무결성, 부인봉쇄 등의 보안서비스 및 보안정보 관리 기능을 제공하며, 세부기술로는 XML 전자서명 및 암호화 기술, XML 기반 보안정보 교환기술, XML 기반 접근제어기술, XML 기반 공개키 관리기술 등이 있으며, 두번째로 웹서비스 보안 프레임워크 기술은 XML 정보보호 기술을 기반으로 웹서비스에서 안전하게 정보를 교환하고 자동화된 방법으로 상호의 보안 정책을 처리하여, 안전하고 통합된 비즈니스를 가능하게 하며, 세부기술로는 통신보안 기술, 보안정책 기술, 프라이버시 보호



(그림 8) 웹서비스 보안기술

기술, 보안세션 관리 기술, 신뢰관리 기술 등이 있다.

마지막으로 웹서비스 응용 보안 기술은 상기 2가지 보안기술을 이용하여 IT839로 대변되는 차세대 인프라 및 서비스, 모바일/그리드/시맨틱 웹서비스와 같은 환경에서 공통적인 보안 위험 요소를 해결할 수 있는 메커니즘과 다양한 디바이스와 비즈니스 환경을 고려하여 각 응용별로 특화된 보안 프로파일들을 제공하며, 세부기술 분류로는 웹서비스 응용보안 프로파일 기술과 웹서비스 보안 상호 운영성 지원 기술이 있다.

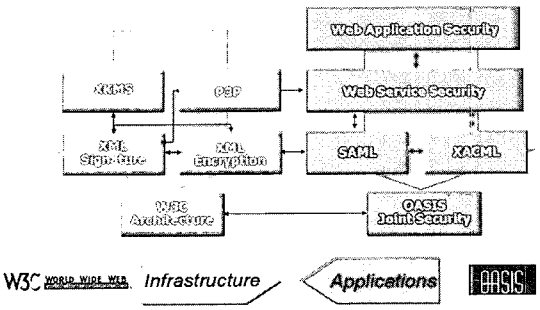
그림 8에는 웹서비스 보안 기술을 구성하는 요소 기술들의 계층구조가 나타나 있다. XML 정보보호 기술은 웹서비스 보안 프레임워크 기술의 근간이 되며, 웹서비스 보안 프레임워크 기술은 안전한 웹서비스를 위한 기반 인프라 구축에 필수적으로 요구되는 기술이며, 웹서비스 응용보안 기술은 이 웹서비스 보안 프레임워크를 기반으로 특정 응용별 보안 프로파일을 해결하기 위한 기술이다.

4. 표준화 동향

4.1 국외 표준화 현황

웹서비스 보안 분야의 표준화를 위한 대표적인 기구는 W3C 및 OASIS가 있으며, XML 정보보호 서비스 기술 분야와 웹서비스 보안 프레임워크 기술 분야에서의 WS-Security에 대한 표준화를 일부 완료하였거나 진행 중에 있다.

웹서비스 플랫폼 개발을 주도 하고 있는 IBM과 MS와 같은 기업체들은 그들의 기술 로드맵에 따라 웹서비스 보안프레임워크 기술 분야에서의 새로



(그림 9) 웹서비스 보안 기술 관련 표준화 현황

운 웹서비스 보안 표준들을 제시하고 있으며, 일부는 W3C와 OASIS에 제출되어 표준에 반영되었다.

WS-I는 웹서비스의 상호운영성을 보장하기 위해 필요한 응용 시나리오와 프로파일들을 정의하는 조직으로 보안과 관련된 웹서비스 보안 프로파일을 준비 중에 있다.

Mobile 서비스를 웹서비스와 융합하거나 Grid Computing 분야에서 웹서비스를 활용하고자 하는 OMA 혹은 Global Grid Forum (GGF)과 같은 단체들은 각각의 응용 기술에서 필요한 별도의 보안 표준들을 준비하고 있다[그림 9].

4.1.1 W3C(World Wide Web Consortium)

W3C는 웹서비스의 기반 기술인 SOAP과 WSDL에 대한 표준을 승인하였고, XML 서명, XML 암호화, XML 기반 키 관리, 등과 같은 XML 정보보호 기술에 대한 표준을 승인하였거나 해당 표준을 개정 작업 중에 있다.

XML 전자서명 기술은 W3C와 IETF의 공동 작업으로 표준화를 완료하였다. 핵심이 되는 문서는 XML Signature Syntax and Processing으로 XML 전자서명의 구문 및 처리 방법을 규정하였으며, Canonical XML및 Exclusive Canonical XML은 XML 전자서명을 적용하기 위해 XML 문서를 정규화된 형태로 변환하는 방법을 정의하였고, XPath Filter는 XML 문서의 일부분을 서명하기 위한 변환을 정의하였다.

XML 암호화 기술은 W3C에서 표준화를 완료하였다. XML 암복호 기술에 대한 표준 문서로는 XML Encryption Syntax and Processing을 비롯해 Decryption Transform for XML Signature, XML Encryption Requirements 이 있다.

W3C는 Microsoft와 Verisign, Web Methods가 공동 개발하고, Baltimore, Entrust Technologies, Citigroup, IBM, IONA Tech- nologies, PureEdge Solution, Hewlett Packard, Reuters Limited, Science RSA Security, Application International 등이 웹 표준으로 제출한 XML 키 관리 명세서에 대해 워킹그룹을 구성하여 표준화를 진행하고 있다. W3C의 XKMS 워킹그룹은 클라이언트가 웹서비스로부터 키 정보 (키 값, 인증서, 관리 혹은 신뢰 데이터)를 얻도록 XML 응용과 프로토콜 명세를 개발하는 작업을 수행한다.

W3C에 참여하여 활동 중인 국내 단체는 한국전자통신연구원 (ETRI), 한국전산원 (NCA), 전자상거래 표준화 통합포럼 (ECIF), 한국정보통신산업협회 (KAIT) 등이 있다.

4.1.2 OASIS

OASIS는 웹서비스를 설명하고 검색할 수 있는 UDDI V.2에 대한 표준을 승인하였고, 보안정보교환을 위한 XML 프레임워크 기술, XML 기반의 접근제어 기술, 웹서비스 메시지를 안전하게 전송할 수 있는 기술 등, XML 정보보호 기술과 웹서비스 보안 프레임워크 기술에 대한 표준을 승인하였거나 해당 표준을 개정 작업 중에 있다.

SAML은 OASIS SSTC(Security Services Technical Committee)에 참여한 많은 업체들의 상호 협력적인 노력에 의해 작성되었으며 SAML v1.1이 2003년 OASIS의 표준으로 승인되었다. 최근에는 Liberty Alliance에서 제정된 표준들을 일부 수용하고 웹서비스에서 요구되는 기능들을 포함하여 SAML v2.0에 대한 개정 작업을 진행 중에 있다. SAML의 초기 버전은 브라우저 기반의 단일사용승인 (Single Sign-On: SSO)를 제공하는데 목적이 있었으나 점차 통합 Identity 관리와 웹서비스의 보안 토큰으로서의 역할이 가능하도록 범위가 확장되어 대부분의 웹서비스 보안 프레임워크에 수용될

것으로 보인다.

XACML은 2003년에 XACML v1.0이 OASIS 표준으로 채택된 상태이다. 현재는 v2.0에 대한 개정 작업을 수행하고 있는데, XACML에 기반을 둔 다양한 응용 프로파일들에 대한 표준화도 함께 진행하고 있다.

WS-Security는 OASIS WSS TC에서 표준화를 진행하고 있다. WS-Security 표준 문서 중 가장 핵심이 되는 것은 WS-Security 2004 (Web Services Security v1.0)로, 2004년 OASIS 표준으로 채택되었다. 이 문서에서는 SOAP 메시지에 대한 보안을 제공하기 위해 SOAP extension들의 집합을 정의하고 이들에 대한 구문 및 처리 방법을 규정하였다. X.509 Certificate Token Profile은 X.509 인증 프레임워크를 WS-Security에 적용하기 위한 구문과 처리 규칙을 규정하며, Username Token Profile은 웹 서비스 사용자가 사용자 ID (username)로 웹 서비스 제공자에게 인증 받기 위한 처리 방법을 규정하였다. 이밖에 보안 토큰과 관련된 다수의 프로파일들이 표준화 진행 중으로 아직 드래프트 상태이다.

OASIS에 참여하여 활동 중인 국내 기관과 업체는 한국전자통신연구원, 전자상거래 표준화 통합포럼, 한국전자거래협회 (Korea CALS/EC), 한국전자거래진흥원 (KIEC), 한국전산원, 한국무역정보통신, 티맥스소프트 등이 있다.

4.1.3 국외 업체의 표준화 활동 현황

IBM과 Microsoft는 웹서비스 보안 표준을 선도하는 업체들로서 2002년에 이들 업체 공동으로 웹서비스 보안에 대한 아키텍처와 표준화 로드맵을 발표하였고, 이후 보안 관련 문서들에 대한 작업을 IBM과 Microsoft 뿐만 아니라 다수의 기업체와 연합하여 진행해 왔다. 특히 IBM, Microsoft, Verisign이 작성한 WS-Security는 OASIS에 제출되어 표준으로 승인되었다. 또한 WS-Security 기반 하에서 보안 기능을 확장할 수 있는 WS-Trust, WS-Federation, WS-SecureConversation 명세서를 작성하였으며, 현재 이들 명세서들 간 혹은 다른 표준 명세서들과의 상호 운영 문제점들을 검토하는 중이다. 그리고 사용자 프라이버시 보호를 위한 WS-Privacy와, 접근제어 정책과 데이터를 정의하는 WS-Authorization에 관한 명세를 2004년 연말에 발표할 계획인 것으로 알려져 있다.

WS-Federation는 상이한 보안 체계(security domain)에 속한 웹서비스 응용들 간 사용자의 신원, 속성, 인증에 대한 중재를 가능하게 하는 메커니즘을 설명하는 명세로, IBM과 Microsoft 등의 산업체 공동 작업을 통해 2003년 WS-Federation v1.0이 발표되었다. WS-Federation은 Liberty Alliance의 표준 문서들 일부와 목적과 기능에서의 중복이 있어 앞으로 조정 과정이 있을 것으로 예상된다.

WS-Trust와 WS-SecureConversaion는 각각 IBM과 Microsoft 등의 산업체 공동 작업을 통해 2004년 WS-Trust v1.1과 WS-SecureConversation v1.1이 발표되었다.

4.2 국내 표준화 현황 및 전망

웹서비스 보안을 위한 국내 표준화 활동은 XML 정보보호기술 분야에서만 부분적으로 진행되고 있으며 주로 전자상거래 표준화 통합 포럼 (ECIF), 한국정보통신 기술 협회 (TTA), 인터넷보안기술 포럼 (ISTF), 웹 코리아 포럼을 중심으로 이루어지고 있다.

전자상거래 표준화 통합 포럼 산하 전자거래기반 기술위원회에서는 한국전산원, 한국전자통신연구원, 이노디지털, 쌍용정보통신, 다산기술 등의 국내 기관과 업체들이 참여한 보안인증 워킹그룹을 구성하여 XML 기반 보안 기술의 표준화 현황 파악과 기술개발, 산업 분야 적용을 논의하고 있다. 보안인증 워킹그룹은 2002년에 XML 전자서명 표준안 등을 포함한 총 5개의 XML 기반 보안 표준안을 상정하여 2004년 하반기에 표준으로 채택될 예정이고, 2003년에는 XML 암호 구문 관련 표준 및 XACML, SAML, XKMS의 적합성, 상호운용성 평가 표준을 정의하였다. 현재는 웹서비스와 ebXML 저장소 (repository) 등에서 활용할 통합접근관리 (EAM) 시스

템 구축을 위한 XML 기반 보안기술 적용지침 표준제정을 위해 초안을 작성 중에 있다.

한국정보통신 기술협회 산하의 IT 응용기술 위원회에서는 고려대학교, 한국전자통신연구원, 한국전산원, KTF, 넷피아닷컴, 한국정보통신기술협회, 서경대학교 등의 국내 산학연들이 함께 참여한 웹 프로젝트 그룹을 구성하여, 웹 기반기술 관련 표준 개발 및 차세대 웹 기술 표준 개발을 수행할 예정이다.

인터넷보안기술 포럼은 안철수 연구소, 이니텍, 장미디어 인터렉티브, 케이사인 등 인터넷 보안기술 분야의 민간 업체들이 중심이 되어 구성된 민간 포럼으로 인터넷 보안기술 관련 국제 표준화 활동에 공동대응하고 시장 수요를 반영한 사실표준의 개발을 위해 창립되었다. 현재 네트워크 분과, PKI 분과, 무선 분과, 보안관리 분과로 구성되어 전자서명 인증서 프로파일 표준, 암호메시지 규격 표준, 무선 전자서명 인증서 프로파일 표준, 보안시스템의 통합관리를 위한 API 표준 등을 포함한 23개의 표준을 제정하였다. 또한 IETF (Internet Engineering Task Force), ISO/IEC, JTC, ITU-T 등의 국제 표준화 회의 및 포럼에 참여하는 등 다양하고 꾸준한 활동을 통해 인터넷 보안기술 관련 최신 기술 정보의 수집, 분석, 보급 및 활용을 촉진하고 있다.

웹코리아 포럼은 정부와 산·학·연에 걸친 통합적인 정보 교환을 통해 국제적인 웹 기술과 표준을 국내 보급하고 국제적 표준화 동향에 공동 대응하는 것을 목표로 하며, 현재 웹서비스 WG, 웹 보안 WG, 웹 기반기술 WG 등을 구성하고 운영 중에 있다. 웹코리아 포럼은 웹 관련 국내외 기술정보를 수집 및 분석, 보급하는 활동을 하고 있으며 각 분과별로 국내 현실에 맞는 표준화 연구 및 표준안을 개발 중에 있다. 또한 웹 기술/표준/응용/정책 관련 세미나와 워크숍 등의 행사 개최를 통해 정보 교환 및 전문가 양성 등에 기여하고 있다.

4.3 기술 개발 현황 및 전망

4.3.1 국내 기술 개발 현황 및 전망

XML 정보보호 기술 분야에서 XML 전자서명과 XML 암호화 기술에 대해서는 기술 개발이 완료된 상태이며, SAML, XACML, XKMS 등이 기술 개발 중에 있거나 응용되고 있는 것으로 파악되며,한국전자통신연구원은 XML 전자서명과 XML 암호화 기능을 포함하는 ESES (Etri Secure E-commerce Services) 패키지를 개발하였으며, STI Security, 비씨큐어, 아이에스시큐리티 등의 업체에서는 이와 관련한 상용 제품을 출시하였다. 그리고 한국전자통신연구원은 SAML, XACML, XKMS에 대한 기술을 개발 중에 있으며, 포스테이터의 e-Business용 XML 보안정보 통합 패키지인 Biz-Safe라는 제품은 XACML 및 SAML을 지원한다고 밝히고 있다. 또한 테오스는 자체 워크플로우 시스템에서 데이터 접근제어를 수행하기 위해 XACML을 응용하고 있다고 한다.

웹서비스 보안 프레임워크 기술 분야에서 현재까지는 WS-Security 부분에서만 기술 개발이 일부 완료된 상태이며 다른 부분에서의 연구 개발 사례는 보고된 바 없으며, 한국전자통신연구원은 자체 개발한 전자서명 및 암호화 기술을 기반으로 하여 WS-Security의 기술 개발을 완료하였다.

WS-Trust, WS-Federation, WS-Policy 등의 기술 분야에서는 아직 까지 기술 개발이 이루어지지 않고 있다.

4.3.2 국외 기술 개발 현황 및 전망

XML 정보보호 기술 분야에서 XML 전자서명과 XML 암호화 기술에 대해서는 기술 개발이 완료된 상태이며, SAML, XACML, XKMS 등은 시제품 수준에 머물러 있으며, IBM, MS, Verisign, Baltimore, RSA, Phaos 등은 XML 전자서명에 대한 상용 제품을 개발 완료되었고, Apache에서는 XML 전자서명의 공개 버전을 선 보였다.

Entegrity의 AssureAccess, HP의 Select Access, Computer Associates의 eTrust SSO, Entrust의 GetAccess 등 다수의 업체가 SAML v1.1을 기반으로 하여 단일사용승인 서비스를 제공하는 솔루션을 개발하고 있으며, Parthenon Computing (Jiffy Software), Sun Microsystems, Lagash Systems 등

에서는 XACML 버전 1.0 혹은 1.1 제품들을 개발하여 호환성 테스트를 진행 중에 있다.

Verisign에서는 TSIK(Trust Services Integration Kit)라는 툴킷에 XML 키 관리의 라이브러리를 지원하는 시제품을 개발하였으며, 이 제품은 XML 전자서명 및 XML 암호화, XML 키 관리 표준의 참조 구현(Reference Implementation)으로 개발되었다. Sun Microsystems는 별도의 보안 제품을 선보이지는 않고 있지만, 자사의 플랫폼에 XML 보안 기술을 적용하기 위해 JCP(Java Community Process)를 통해 자바 API 표준화를 추진 중에 있다. '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, Entrust는 참조 구현을 통해 자사의 상품을 검증하고 있다. IBM에서도 WSDK(Web Service Tool Kit)을 기반으로 개발 중에 있으며, Microsoft에서는 자사의 .NET Framework에 XKMS 기능을 통합한 시제품을 개발하였다. RSA Security, Phaos 등의 회사들도 연구개발을 진행 중이거나 시제품을 개발하고 있다.

DataPower는 XS40 XML Security Gateway라는 제품을 개발하였으며, 이 제품은 XML/SOAP Filtering, Field Level XML 보안, SAML, XACML, WS-Security 기술을 통한 접근제어 기능 등을 제공한다.

기술명	표준화현황	국제기술현황	국내기술현황	관련 기관
XML Signature	W3C Recommendation	상용화 단계	상용화 단계	ETRI, IBM, Entrust, MS 등
XML Encryption	W3C Recommendation	개발 완료 단계	상용화 단계	ETRI, IBM 등
XKMS	W3C Draft 2.0	개발 중(시제품)	개발 중	Verisign, MS 등
XACML	OASIS Committee Spec 1.0	개발 중	개발 중	IBM 등
SAML	OASIS Committee Spec 1.0	개발 중	개발 중	Verisign, SUN 등
WS-Security (Web Service Security)	준비 중 (W3C에 상정 예정)	개발 중	개발 중	MS, IBM, Verisign
SOAP-DSIG	W3C note	개발 중(시제품)	개발 준비	IBM, MS 등
무선XML보안	-	개발 준비	개발 준비	-

(그림 10) 웹서비스 보안 기술 개발 현황

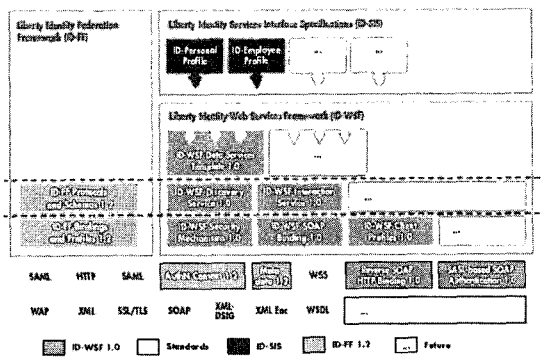
5. 활용 예

The Liberty Alliance Project는 SSO 기술 및 인증, 권한 검색을 위한 개방형 솔루션 표준을 위해 2001년 09월 'SUN'주도로 결성된 협력 기구이다. 현재 스팩 Phase 2.0 발표되었으며, 차후 MS의 Passport기술과 통합 및 보완 관계로 발전 할 예정이다.

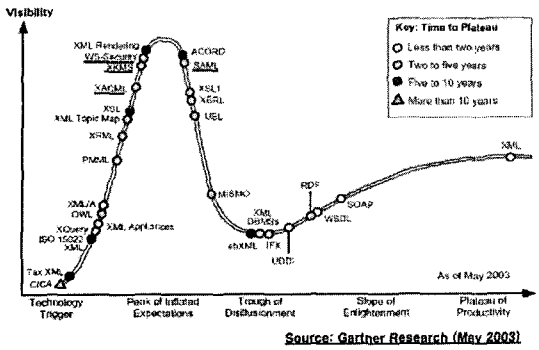
그림 11과 같이 Phase 2.0은 ID-FF를 기반으로 상호 협력적인 ID를 제공하기 위한 프레임워크인 ID-WSF(Identity Web Service Framework)와 간단한 사인 온, 세션관리, ID접근 등의 기능을 통해 ID 연합과 관리를 할 수 있게 하는 규격인 ID-FF (Identity Federation Framework), 그리고 ID-WSF에 의해 제공되어지는 상호 협력적인 ID-based 서비스 형식을 위한 규격 모임인 ID-SIS (Identify Services Interface Specification) 구조로 이루어져있다.

6. 결 론

가트너의 조사 분석결과에 따르면 XML 관련 기술은 현재 상당히 안정된 상태에 도달하였고, 이를 통한 다양한 새로운 응용 기술들이 등장하고 있다는 사실을 알 수 있다. 특히 SAML, XACML, XKMS, WS-Security 등의 XML 보안 관련 기술은 그림 12에 나타난 것처럼 향후 2~5년 내에 기술



(그림 11) The Liberty Alliance-Ver 2.0 구조



(그림 12) XML Hyper Cycle 2003, Gartener

수요가 예상 된다.

웹서비스 보안 프레임워크 기술 분야에서 현재까지는 WS-Security 부분에서만 기술 개발이 완료된 상태이며, 다른 기술에 대해서는 아직 까지 개발이 완료되지 않았으며, 시제품 수준에 머물러 있으며, Sun Microsystems, Verisign, IBM 등에서 WS-Security 제품을 개발 완료하였다. 이들 제품들은 대부분 독립적인 형태의 제품이 아니라 자사의 웹 서비스 플랫폼 혹은 보안 플랫폼에 포함되어 제공되고 있다. 또한 Microsft는 WS-Security, WS-Trust, WS-Policy를 지원하여 안전한 웹서비스 응용을 개발할 수 있도록 하는 WSE (Web Services Enhancements) 2.0을 개발하였다

웹서비스 응용보안 기술 분야에서는 웹서비스를 기존의 응용 분야와 융합하는 시도와 새로운 응용 분야를 웹서비스 기반 하에서 운영하려는 단계에 있기 때문에 아직 보안 기술 개발을 위한 준비가 이루어지지 않고 있다. 따라서 안전한 웹서비스를 구현을 위해 XML Security와 WS-Security적용이 필요하다.

참 고 문 헌

[1] Web Services Architecture WG, "Web Services Architecture, W3C Working Draft", W3C, May 14, 2003.

[2] W3C Web Services Description WG, "Web Services Description Language (WSDL) Version 1.2," W3C, March 3, 2003.

[3] OASIS UDDI Specification TC, "UDDI Version 3.0 Published Specification," OASIS, July 19, 2002.

[4] W3C, "SOAP Version 1.2 Part1: Messaging Framework (W3C Recommendation)", June 2003.

[5] OASIS SS TC, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1", OASIS, September 2003.

[6] OASIS WSS TC, "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)", OASIS, March 2004.

[7] IETF/W3C, "XML-Signature Syntax and Processing (W3C Recommendation)", February 2002.

[8] XML Key Management WG, "XML Key Management Specification (XKMS 2.0) Version 2.0", W3C, April 2004.

[9] Security Assertion Markup Language http://www.oasis-open.org/committees/security

[10] OASIS, eXtensible Access Control Markup Language Version 1.0, 2003.

[11] OASIS XACML TC, "eXtensible Access Control Markup Language (XACML) V1.1", OASIS, August 2003.

[12] Tim Moses, Anne Anderson, Seth Proctor, and Simon Godik, "XACML Profile for Web Service, OASIS TC Working Draft, September 29th, 2003.

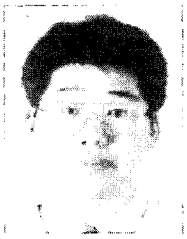
[13] IBM, MS, BEA, RSA, et al., "Web Services Trust Language (WS-Trust) Version 1.1", IBM DeveloperWorks, May 2004.

[14] IBM, MS, BEA, RSA, et al., "Web Services Secure Conversation Language (WS-SecureConversation) Version 1.1", IBM DeveloperWorks, May 2004.

[15] IBM, MS, BEA, RSA, et al., "Web Services Federation Language (WS-Federation)

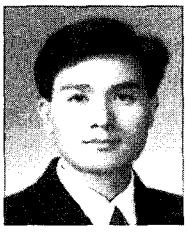
Version 1.0", IBM DeveloperWorks, July 2003.
[16] IBM, MS, BEA, RSA, etc, "Web Services Security Policy (WS-SecurityPolicy) Draft 18", IBM DeveloperWorks, December 2002.
[17] P3P WG, "Platform for Privacy Preferences (P3P) Project".

◐ 저 자 소 개 ◑



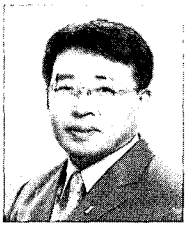
서 창 호

1990년 고려대학교 수학과 학사
1992년 고려대학교 대학원 수학과 석사
1996년 고려대학교 대학원 수학과 박사
2000년~현재 공주대학교 정보보호전공 부교수



윤 보 현

1992년 목포대학교 전산통계학과 학사
1995년 고려대학교 대학원 컴퓨터학과 석사
1999년 고려대학교 대학원 컴퓨터학과 박사
2003년~현재 목원대학교 컴퓨터교육과 조교수



이 태 훈

1982년 한국항공대학교 전자공학과 학사
1984년 아주대학교 대학원 전자공학과 석사
1999년 아주대학교 대학원 전자공학과 박사
1993년~현재 광주대학교 컴퓨터전자통신학부 부교수