4

ID 관리 기술 및 표준화 동향

한국전자통신연구원 ▌조영섭 · 진승헌 · 정교일
순천향대학교 ▌염흥열

1. 서 론

인터넷의 확산과 발전에 따라 인터넷 전자상거래, 전자정부, 전자의료 등과 같은 다양한 전자거래가 활성화되고 있다. 그러나 현재 사용자가 인터넷 서비스를 이용하기 위해서는 일반적으로 서비스마다 자신의 Id(Identifier)와 개인 정보를 사전에 등록하고, 서비스를 이용하기 전에 등록된 Id로 인증을 받아야 한다. 이와 같이 사용자 Id와 개인정보로 이루어진 사용자 ID (Identity)를 등록하는 과정은 사용자가 새로운 인터넷 서비스를 받기 위해서 매번 반복해야 한다. 이에 따라 인터넷 사용이 증가할수록 사용자가 직접 관리해야 하는 ID가 증가하여 사용자의 불편을 초래하고 동일한 패스워드의 중복 사용으로 인한 보안성 문제를 발생시키며 사용자의 패스워드 분실로 인한 기업의 서비스 비용 증가 등의 문제가 발생한다. 또한 인터넷 서비스들간에 사용자 인증 정보가 공유되지 않고 있어 사용자가 여러 서비스를 이용하는 경우 각각의 서비스마다 매번 새롭게 인증을 받아야하는 불편이 발생한다. 또한 일반적인 인터넷 서비스 제공자들이 서비스 제공에 필요한 이상의 개인정보 등록을 요구하고, 서비스 제공 업체에 따라 사용자 개인정보 관리의 정도에 차이가 있어, 사용자 개인정보의 유출 및 노출의 위험이 증가되는 문제가 발생한다[1].

특히 Ubiquitous 환경과 Web 2.0의 출현과 진전에 따라, 기존 서비스들의 융합, 사용자의 참여, 정보의 공유가 매우 중요해지는 향후 인터넷 환경에서는 사용자 ID 정보의 수가 기하급수적으로 증가하며, 정보 공유에 따른 ID 유출 및 노출의 위협이 더욱 높아질 것이다. 이에 따라, 사용자의 ID를 안전하게 관리하는 기술은 인터넷 환경의 핵심 인프라로 인식되고 있다. 본 고에서는 이와 같은 ID 문제를 해결하기 위해 현재 진행되고 있는 ID 관리 기술의 연구와 표준화 동향에 대하여 살펴본다.

2. ID 관리 기술 연구 동향

현재 ID 관리 시장은 Liberty Alliance로 대표되는 기업들과 Microsoft가 양분하고 있다. 그러나 DIDW(Digital ID World)는 2006년에 ID 관리 시장이 확대되어 블로그, 일반 기업, RSS 리더, 위키(wiki), 사교 네트워크뿐만 아니라 검색 분야에도 ID 프로파일을 이용한 제품이 출시될 것으로 내다보았고 위험 관리(Risk Management) 분야에서 ID 관리가 중요하게 고려될 것으로 예상하였다. 특히 사용자 중심의 ID 관리 기술이 출현하고 그 중에서도 상용화에 한 발 앞선 URL 기반의 ID 관리가 주목 받을 것으로 예상하였다. NetMesh의 CEO이자 YADIS(Yet Another Decentralized Identity Interoperability System) 프로젝트를 운영하고 있는 Johannes Ernest는 앞으로 ID 관리 시장에서 사용자 중심(User-controlled)의 ID 관리가 주목을 받을 것이라고 예상했다[2].

그림 1은 2006년 현재 ID 관리 시스템들의 현황을 도식화 한 것이다.

Company-controlled Identity는 기업이 개인에게 ID를 부여한 뒤 개인이 어떤 ID를 관리하고 공유할 것인가를 결정한다. Liberty Alliance 표준에 기반한 ID 관리 시스템이 대표적이며, 2007년 현재 Libety Alliance 표준에 기반한 ID와 장치들이 정부, 교육, 의료 등의 다양한 분야에 10억 개가 넘게 적용되고 있다.

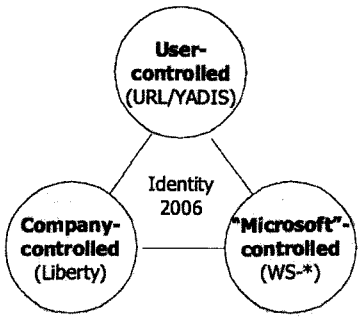

그림 1 The Identity Landscape 2006
출처 http://netmesh.info/jernst/

Microsoft-controlled Identity는 WS-* 표준에 기반한 ID 관리 시스템으로, Kim Cameron이 Law of Identity를 통해 주장한 ID 메타시스템이 CardSpace로 구현된 것이다. CardSpace는 OASIS 표준인 WS-Security를 기반으로 하여 X.509, Kerberos, SAML(Security Assertion Markup Language)과 같은 보안 토큰 포맷을 모두 사용할 수 있으며 Windows Vista를 통해 광범위하게 적용될 것으로 예상된다.

User-controlled Identity는 ID 제공자(IdP, Identity Provider), 개인정보, ID 사용 정책을 개인이 통제하는 시스템으로서, 기업에 속한 ID가 아니라 사용자 스스로 ID를 생성하고 관리하는 것을 특징으로 가진다. 대표적인 User-controlled Identity로는 URL을 ID로 사용하는 OpenID[3], LID[4], YADIS[5]를 들 수 있다.

이와 같은 분류는 2006년도에 ID 분야에 대한 연구가 광범위하게 진행되고 이에 따라 서로간의 융합이 진행됨에 따라, 2006년도 12월에 다음 그림 2와 같이 갱신되었다[6].

URL-based는 기존의 다양한 URL-based 기술들이 OpenID로 통합되는 경향을 보이며 주로 일반 대중(grassroots) 영역과 웹 2.0 응용 영역에서 활용된다. Invisible은 Company-controlled를 대체하며 주로 기업 내부 또는 기업간 ID 영역에서 활용된다. Card-based는 Microsoft-controlled를 대체하며 사용자가 Card 형태로 자신의 ID 정보 제공을 선택할 수 있으며 CardSpace는 window vista와 함께 제공된다.

현재 각각의 ID 분야는 상호간에 통합 및 융합 작업을 진행하고 있다. URL-based와 Invisible의 경우 OpenID와 SAML의 융합 작업이 진행되고 있으며, Microsoft는 CardSpace에서 OpenID를 지원할 계획을 밝히기도 했다.

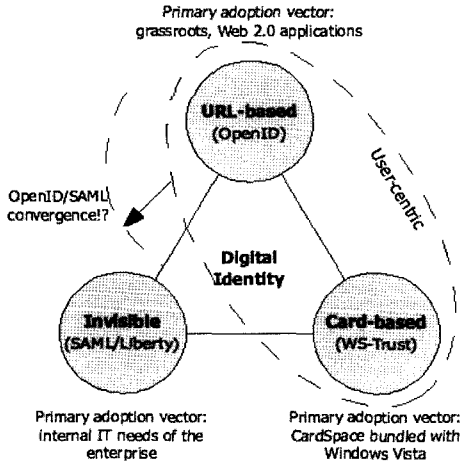

그림 2 The Identity Landscape 2006 updated
출처 http://netmesh.info/jernst/

3. ID 관리 기술

본 장에서는 ID 기술 분야의 대표적인 기술인 Liberty Alliance, Microsoft CardSpace와 OpenID에 대하여 기술한다.

3.1 Liberty Alliance

Liberty Alliance[7]는 연방화된 네트워크 ID 관리와 ID 기반의 서비스를 위한 공개 표준을 개발할 목적으로 2001년 9월에 결성되었고, 2007년 현재 150여 개의 멤버를 가진 조직으로 성장하였다. 국내에서는 ETRI가 Liberty Alliance의 Affiliation member로 활동하고 있다. 그림 3은 Liberty Alliance 구조를 나타낸다.

그림에서 ID-FF(Federation Framework)는 Federated Identity 관리와 인터넷 SSO에 대한 표준을 제정하고 있으며 현재 SAML v2.0으로 통합되었다. ID-WSF(Web Service Framework)는 사용자가 자신의 Identity 정보를 다른 시스템에 공유할 수 있도록 해 주는 웹 서비스 프레임워크를 정의한다. ID-SIS(Service Interface Specification)는 ID-WSF를 이용하여 공유되는 사용자 Identity의 표준 규격을 정의하며, 사용자 개인 프로파일 정보와 조직 내의 프로파일 정보를 나타내는 Personal Profile와 Employ Profile이 규정되어 있으며, Presence, Contact Book, Geo-Location 등이 지속적으로 제정되고 있다.

Liberty Alliance의 ID 관리 기술을 활용하기 위해서, 인터넷 서비스 제공자인 SP(Service Provider)는 사전에 IdP(Identity Provider)와 다양한 정책에 대한 협의를 통해 CoT(Circle of Trust)를 구성해야 한다. 일반적으로 CoT는 단일 또는 소수의 IdP와 다수의 SP로 구성된다.

다음 그림 4는 Liberty Alliance에서 사용자에게 제공하는 SSO 기능의 수행 과정을 도식화 한 것이다.

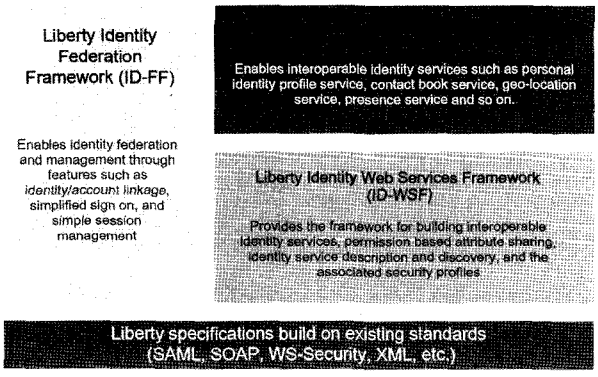

그림 3 Liberty Alliance Architecture
출처: Liberty Technology Tutorials, Liberty Alliance

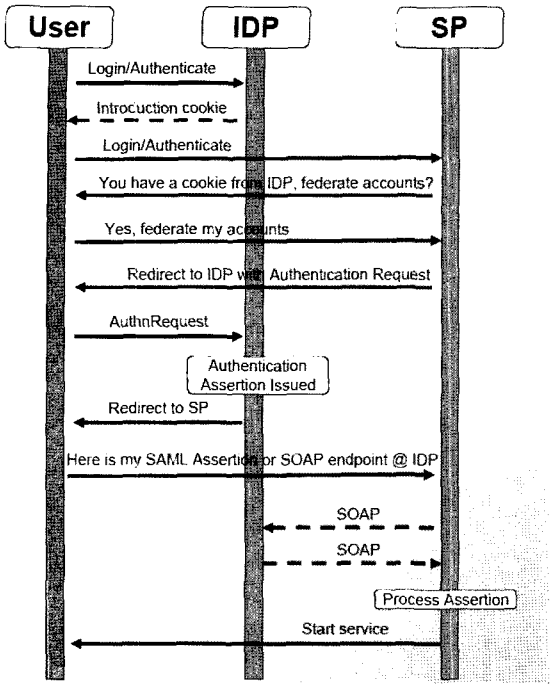

그림 4 Liberty Alliance SSO & Federation 흐름도
출처: Liberty Alliance Developer Tutorial, Liberty Alliance

그림에서 사용자는 IdP에 먼저 로그인 과정을 통해 사용자 인증을 수행한다. 사용자는 인증 과정을 통해 IdP 도메인에 대한 Introduction 쿠키를 전달받게 된다. 사용자가 인터넷 서비스를 이용하기 위해 SP에게 서비스를 요청하면, SP는 사용자가 자신에게 이미 인증된 사용자인지 확인한다. 만약 인증되지 않은 사용자라면, IdP에게 사용자를 인증해 줄 것을 요청한다. 이 과정에서 SP와 IdP는 사용자를 식별하는데 있어, Pseudonym을 이용한다. Pseudonym은 사용자 식별 자용으로 random하게 생성된 난수로 구성되며 SP와 IdP에서 사용자에 대하여 각각 생성한다. IdP와 SP는 SSO를 위해 자신이 사용자를 식별하는 Pseudonym을 서로 교환하여 Federation Record를 구성한다. SP의 요청에 따라, IdP는 사용자가 만약 인증되지 않았다면 사용자를 인증한 후, 사용자의 인증 사실을 SAML assertion으로 생성한 후, 이에 대한 reference 값인 artifact를 SP에게 전달한다. SP는 artifact를 SOAP 통신을 이용하여 IdP에게 전달한 후, 사용자 인증 상태 정보를 가져오게 된다. 이 정보가 사용자를 적절히 인증하였으면, 이 후부터 사용자에게 자신의 서비스를 제공하게 된다.

3.2 Microsoft CardSpace

Microsoft가 SSO 서비스와 단일 ID로 여러 정보시스템에 접근할 수 있도록 2000년에 발표된 .NET Passport[8]는 2억 명이 넘는 사용자를 확보했음에도 불구하고 단일 회사가 개인 ID를 중앙집중 방식으로 관리하는 단일 ID 체계의 보안성과 프라이버시 보호에 대한 우려로 인해 성공하지 못하였다. 이에 따라 Microsoft는 .NET Passport의 문제점을 보완하기 위해 WS-* 프로토콜과 XML 기반의 SOAP, SAML 등을 이용한 ID 메타시스템인 CardSpace를 개발하였다. CardSpace[9]는 .NET Passport와는 달리 단일 IdP 대신 여러 IdP를 관리할 수 있으며 CardSpace 소유자가 접속하는 사이트에 적합한 ID를 Card 형태로 제공하여 사용자가 선택할 수 있도록 하였다. CardSpace는 실질적인 사용자 ID 정보를 포함하지는 않고 있으며 ID 정보 제공자 정보를 가지도록 함으로써 ID 메타시스템의 역할을 수행하며, 사용자가 반드시 ID Card를 선택하도록 함으로써 사용자가 서비스 이용시 명시적으로 참여를 하도록 하였다.

그림 5는 CardSpace가 동작하는 예를 보이고 있다.

먼저 사용자가 서비스 제공자(RP, Relying Party)에서 서비스를 요청하면, RP는 CardSpace를 구동시킬 수 있는 특별한 태그를 가지고 있는 로그인 페이지를 사용자 브라우저(IE 7.0)에 응답한다. 사용자 브라우저는 응답에 포함된 태그 정보를 확인하여 RP에서 요청하는 사용자 ID 정보를 확인하고 이 정보를 제공하는 ID Card들이 포함된 화면을 사용자에게 출력한다. 사용자는 화면에서 적절한 ID Card를 선택하게 되며 선택된 Card 정보에 따라, 해당 ID 제공자인 IdP에게 사용자 정보가 요청된다. IdP는 사용자 정보를 CardSpace에게 사용자 정보를 전달하면, CardSpace는 이 정보를 RP에게 전달하게 된다.

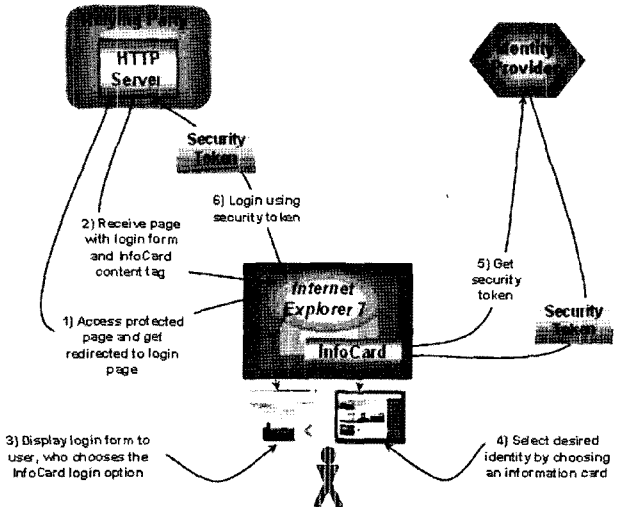

그림 5 CardSpace 동작 흐름도
출처: Introducing Windows CardSpace, Microsoft MSDN

Microsoft의 CardSpace는 Window 환경뿐만 아니라 Open Source 환경에서도 활발히 개발되고 있다. OSIS (Open Source Identity Selector) 프로젝트의 경우 CardSpace를 오픈 소스로 구현하려하고 있으며, Ping Identity는 Apache 서버에서 사용할 수 있는 CardSpace 모듈을 공개하였다.

3.3 OpenID

OpenID는 Six Apart사에 의해 개발 중인 URL 기반 Identity 시스템이다. 2006년에 제안된 많은 URL 기반 Identity 시스템이 현재는 OpenID로 수렴되어 가고 있다.

현재 OpenID 시스템에서 제공하는 주요 기능은 사용자가 자신이 이용하려는 각 사이트마다 계정을 갖지 않더라도 서비스를 사용할 수 있도록 하는데 있다. 이를 위해 OpenID는 사용자가 자신의 계정이 개설되어 있지 않은 서비스 제공 사이트(Consumer)에 접속할 때 자신을 인증할 수 있는 사이트(Server)에서 인증과정을 수행하고 그 결과를 서비스 제공 사이트에게 전달하는 기능을 제공한다.

OpenID 시스템은 사용자 ID가 등록, 관리되고 있는 OpenID 서버를 이용해서 인증을 제공한다. 인증과정에서 OpenID 서버는 ID로 사용되는 URL 정보만을 이용하여 사용자를 인증하며 또한 누구든지 추가로 소요되는 비용 없이 OpenID 관리 시스템이 될 수 있으며 OpenID 식별자를 기반으로 인증을 제공하는 사이트들을 운용할 수 있다. 또한 이 시스템들은 인터넷 웹 표준을 준수하기 때문에 모든 웹 브라우저를 지원한다.

그림 6은 OpenID가 동작하는 예를 보이고 있다.

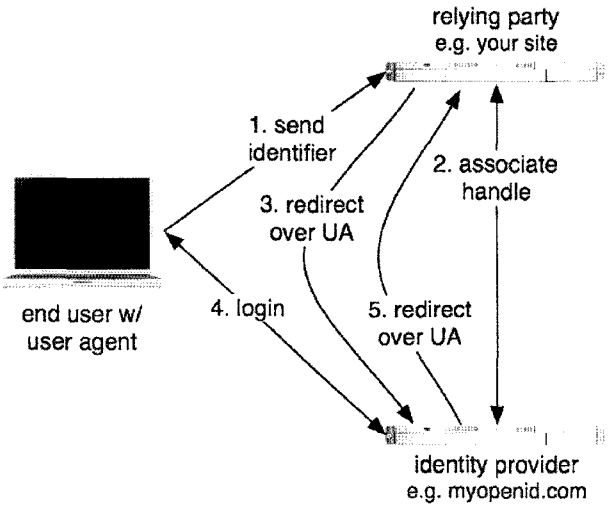

그림 6 OpenID 동작 흐름도

출처: OpenID Open Deistributed Identity Management, http://openid.net/

먼저 사용자가 RP(Consumer)에서 서비스를 요청하고 만약 RP에 사용자가 인증되지 않은 상태이면, RP는 사용자 식별자를 요청한다. 사용자는 자신의 사용자 식별자를 RP에게 전달한다. RP는 사용자 식별자를 통해 IdP(Server)를 확인하고 IdP와 associate 과정을 거쳐 자신과 IdP 간의 세션, 암호 키 등과 같은 공유 암호를 설정한다. 이 과정이 종료되면, RP는 사용자 브라우저를 경유하여 IdP에게 인증을 요청한다. IdP는 사용자가 인증되지 않았다면 사용자를 인증하고 사용자의 인증 사실을 사용자 브라우저를 경유하여 RP에게 전달한다. RP는 사용자 인증정보를 확인하고 사용자에게 서비스 제공 유무를 결정한다.

OpenID는 다른 ID 시스템과 비교하여 여러 가지 장점을 가진다. 사용자의 식별자로 URL을 사용한다는 장점을 가진다. URL은 일반 인터넷 사용자들에게도 친숙한 개념으로 다른 ID 관리 시스템에 비해 사용자들의 접근성을 높이는 장점이 있다. 또한 OpenID는 공개된 프로토콜을 이용하며 별도의 비용을 요구하지 않는 무료 기술이기 때문에 진입 장벽이 낮으며 추가적인 비용이 많이 발생하지 않는 장점을 가지고 있다. 또한 Liberty Alliance 등에서는 SSO 기능이 CoT 내로 한정되는 반면에 OpenID는 인터넷 규모를 대상으로 하기 때문에 영역의 범위가 제한되지 않는 장점을 가진다. 마지막으로 OpenID는 OpenID의 서버의 이외에 응용의 설치와 부가적인 개인정보 요청 없이 온라인상에서 기존의 웹 브라우저만을 이용해 개인에 대한 인증기능을 수행한다는 장점을 가진다.

그러나 2007년 초부터, 스팸, 피싱, MITM(Man In The Middle) 공격 등에 OpenID가 취약할 수 있다는 문제가 제기되고 있으며, 이에 따라 피싱 대처 방안들이 다수 제시되고 있다. 또한 최신 버전에서는 Attribute 정보를 상호 연동할 수 있는 스펙들을 작성하고 있다.

4. ID 기술 표준화 동향

4.1 OASIS SAML

OASIS는 XML 관련 표준을 제정하는 기관이다. SAML [10]은 OASIS의 Security Services TC에서 제정하고 있는 표준으로 객체에 대한 인증, 인가, 속성 정보를 안전하게 교환하기 위한 프로토콜로, 현재 2.0 버전까지 발표되어 있다.

그림 7은 OASIS SAML 표준화 진행 현황을 도식화한 것이다. 현재 SAML 2.0이 표준으로 제정된 상태이다.

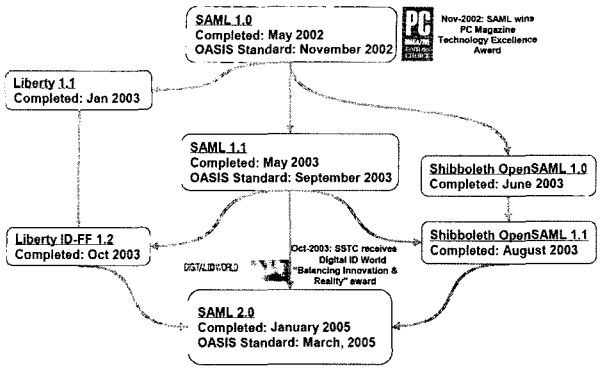

그림 7 SAML 표준화 진행
출처: Liberty Technology Tutorials, Liberty Alliance

SAML V2.0을 구성하는 주요 스펙을 다음과 같다.

▪ Core

이 스펙에서는 assertion의 구조와 SAML assertion과 관련된 요청 및 응답 프로토콜에 대하여 기술한다.

▪ 바인딩

SAML 요청/응답 메시지를 기존에 존재하는 하부 프로토콜로 매핑하는 방식을 기술한다. 메시지를 바인딩하는 하부 프로토콜로는 HTTP, SOAP, Reverse SOAP(PAOS)와 URI 방식이 있다.

▪ 프로파일

프로파일은 SAML assertion을 프레임워크나 프로토콜에 어떻게 삽입시키고, 이렇게 삽입된 메시지에서 어떻게 추출하는지에 대한 방법을 규정하는 규칙이다. 이 스펙은 SSO 프로파일, Artifact Resolution 프로파일, Assertion 질의/응답 프로파일, 이름 식별자 매핑 프로파일, SAML 속성 프로파일 등을 규정하고 있다.

▪ 메타데이터 프로파일

SAML을 기반으로 IdP와 SP(Service Provider)가 정보를 교환하기위해서는 서로가 지원하는 프로토콜, 프로파일, 서비스 엔드포인트(endpoint), 공개키 인증서, provider ID 등과 같은 정보가 필요하다. SAML은 이와 같은 부가적인 정보를 메타데이터로 부른다. 이 스펙은 메타데이터의 구조를 규정하고 IdP와 SP의 메타데이터를 인터넷 상에서 공개하는 방법과 공개된 메타데이터를 검색하는 방법을 규정한다.

▪ 인증 문맥(Authentication Context)

SP는 사용자에게 제공하는 서비스의 특성에 따라 IdP가 어떠한 방식으로 사용자를 인증했는지를 확인해야 할 필요가 있다. 즉, SP가 사용자에게 자금 이체와 같은 금융 서비스를 제공하는 경우, 사용자의 인증 방식이 최소한 인증서를 이용하거나 또는 인증서와 생체 정보를 이용할 것을 요구할 수 있다. 이와 같은 경우, 사용자에게 서비스를 제공할 것인지에 대한 SP의 판단은 단순히 IdP가 사용자를 인증하였는지에 대한 정보뿐만 아니라 사용자를 어떠한 방식으로 인증하였는지에 대한 부가적인 정보가 필요하다. 이 스펙은 IdP가 사용자를 어떠한 방식으로 인증하였는지를 SP에게 알려주기 위해, 사용자를 인증하는 각각의 방식에 대하여 하나씩 인증 클래스를 정하고 이것이 어떠한 의미를 지니는지를 규정한다.

4.2 WS-*

WS-* 스펙은 웹 서비스의 보안을 위해 생성되는 표준 스펙들을 포괄한다. WS-* 스펙은 Microsoft와 IBM이 주축이 되고, Verisign 등 여러 업체가 참여하여 제정되고 있다.

그림 8은 IBM과 Microsoft가 공통으로 작성한 Web Service Security의 Roadmap이다.

WS-Security는 SOAP 메시지의 무결성, 신뢰성, 인증을 포함하는 메시지 수준의 보안성을 제공하기 위한 스펙으로 OASIS에 제안되어 WSS(Web Services Security)[11] TC에서 표준화가 완료되었다. WS-Security는 바이너리 보안토큰을 인코딩하는 방식과 X.509 인증서 또는 Kerberos 티켓 등을 사용하는 방식 등을 정의하고 있다. WS-Security는 다른 WS-* 표준이 운용되는 기반 환경이 된다.

WS-Trust는 신뢰 관계를 형성하는 방법으로, 당사자간에 직접 신뢰관계를 형성하는 방법과 신뢰할 수 있는 중간 계층을 통해 신뢰관계를 형성하는 방법을 규정한다. WS-Policy는 시스템의 정책을 설정하는 방식에 대해 규정한다. WS-SecurityPolicy는 보안에 특화된 시스템 정책을 설정하는 것으로, 수신자와 송신자가 보안에 대한 요구사항과 자신이 지원 가능한 보안 정도를 명시하는 방법을 제공한다. WS-Federation은 사이트 또는 조직간 ID 연동을 위한 스펙이다. 또

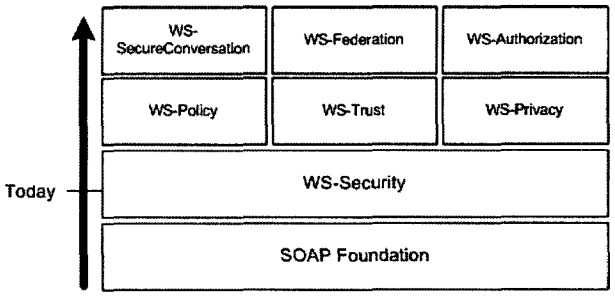

그림 8 Web Service Security Roadmap
출처: Security in a Web Services World: A Proposed Architecture and Roadmap, Microsoft MSDN

한 프라이버시, 인가, 보안 통신을 위한 스펙들로 WS-Privacy, WS-Authorization, WS-SecureConversation이 제정되고 있다. 현재 WS-Trust, WS-SecureConversation, WS-SecurityPolicy가 OASIS의 WS-SX(Web Services Secure Exchange)[12] TC에 제안되어 표준화가 수행되고 있다.

4.3 기타 표준화 동향

ID 관리 기술이 보편화되고 연구가 활발히 진행됨에 따라, ITU-T는 2006년에 SAML 2.0을 X.1141 Security Assertion Markup Language(SAML 2.0) 표준으로 제정하였으며 ITU-T SG 17 그룹에서 ID 관리 기술 분야의 표준화를 진행하고 있다. 국제 표준화기구인 ISO/IEC JTC1/SC27은 ID 관리시스템 연구를 위한 WG5(Privacy, Identity and Biometric Security)를 새로 구성하였고 [13], 경제협력개발기구(OECD: Organization for Economic Co-operation and Development)에서도 정보보호작업반(WPISP: Working Party on Information and Security)을 구성, 전자정부서비스 및 전자상거래 활성화를 위해 ID 관리 프레임워크에 대한 연구를 진행하고 있다.

국내에서는 TTA PG 101을 중심으로 ID 관리 기술 분야에 대한 표준화가 진행되고 있다. TTA에서는 2006년 SAML 2.0의 Core, 바인딩, 프로파일 부분에 대한 국내 표준화 작업을 완료하였다.

5. 결 론

인터넷을 통해 일상적인 업무의 처리는 기존 오프라인에서 수행하던 업무 처리 작업에 비해 시공간적인 제약을 해결함으로써 사용자에게 편의성과 경제성을 제공하였다. 그러나 현재의 인터넷 환경에서는 인터넷 서비스를 이용하기 위해서 사용자의 Id와 패스워드 및 사용자의 이름, 주민번호, 주소, 연락처, 전자메일 등의 개인정보를 등록해야만 하고 이들 정보를 사용자가 직접 관리해야 하는 것이 일반적이다. 또한 서비스 제공 업체들 사이에 인증 정보가 공유되지 않기 때문에 사용자에게 SSO를 제공하지 못하고 있으며, 이는 서비스 활용을 위해 사용자가 매번 인증을 해야 하는 불편을 초래하고 있다. 이와 같이 서비스 제공자에게 등록된 사용자 ID 정보들은 사용자의 동의 없이 다른 업체에 제공되거나 또는 노출 및 유출의 위협이 직면하고 있는 실정이다. 특히 Web 2.0과 유비쿼터스 환경의 도래에 따라 이와 같은 문제를 더욱 심화시킬 것으로 예상된다.

본 고에서는 현재 국내외에서 연구, 개발되고 있는 ID 관리 기술과 표준화 동향에 대하여 기술하였다. Web 2.0은 ID 관리 기술에도 많은 영향을 주어, 현재 ID 관리 기술은 URL-based, Invisible, Card-based로 구분할 수 있다. 현재 각각의 기술은 고유한 사용자 ID 관리 기술의 특성을 가지고 있으며 서로 간의 융합이 진행되고 있지만, 향후에는 이와 같은 융합이 더욱 더 가속화될 것으로 예상된다.

참고문헌

[1] 인터넷 ID 관리 서비스 2006년도 기술 백서, 한국전자통신연구원 디지털ID보안연구팀, 2006.

[2] Johannes Ernst, The Identity Landscape of 2006, http://netmesh.info/jernst/Digital_Identity/three-standards.html.

[3] OpenID, http://openid.net/

[4] LID, http://lid.netmesh.org/

[5] SXIP, http://www.sxip.com/

[6] Johannes Ernst, Updating The Identity Landscape of 2006, http://netmesh.info/jernst/Digital_Identity/updating-three-standards.html

[7] Liberty Alliance Project, http://www.projectliberty.org/

[8] Microsoft, .NET Passport overview, http://msdn.microsoft.com/

[9] Microsoft, Introducing Windows CardSpace, http://msdn.microsoft.com/

[10] SAML, http://www.oasis-open.org/committees/security/

[11] Web Services Security, http://www.oasis-open.org/committees/wss/

[12] Web Services Secure Exchange, http://www.oasis-open.org/committees/ws-sx/

[13] ISO/IEC JTC1/SC27 WG5 N4721, Information Technology - Security Techniques - A Framework for Identity Management, Oct., 2005.

조 영 섭

1993 인하대학교 전자계산공학과 학사
1995 인하대학교 대학원 전자계산공학과 석사
1999 인하대학교 대학원 전자계산공학과 박사
1998～현재 한국전자통신연구원 디지털ID보안 연구팀 선임연구원
관심분야 : Digital Identity Management, 인증인가, 정보보호
E-mail : yscho@etri.re.kr

진 승 헌

1993 숭실대학교 전자계산학과 학사
1995 숭실대학교 대학원 전자계산학과 석사
2004 충남대학교 대학원 컴퓨터과학과 박사
1994～1996 (주)대우통신 종합연구소 연구원
1996～1999 (주)삼성전자 통신연구소 전임연구원
1999～현재 한국전자통신연구원 디지털ID보안 연구팀장/선임연구원
관심분야 : Digital Identity Management, PKI, PMI, 인증인가
E-mail : jinsh@etri.re.kr

정 교 일

1981 한양대학교 전자공학과 학사
1983 한양대학교 산업대학원 전자계산학과 석사
1997 한양대학교 대학원 전자공학과 박사
1980～1981 엠시스템즈 사원
1981～1982 한국전기통신연구소 위촉연구원
1982～현재 한국전자통신연구원 융합보안그룹장/책임연구원
관심분야 : IC Card, Security, Biometrics, 국가기반보호, 신호처리
E-mail : kyoil@etri.re.kr

염 흥 열

1981 한양대학교 전자공학과 학사
1983 한양대학교 대학원 전자공학과 석사
1990 한양대학교 대학원 전자공학과 박사
1982～1990 한국전자통신연구소 선임연구원
1990～현재 순천향대학교 공과대학 정보보호학과 정교수
1997～2000 순천향대학교 산업기술연구소 소장
2000～2006 순천향대학교 산학연컨소시엄센터 소장
1997～현재 한국통신정보보호학회 총무이사, 학술이사, 교육이사, 현 총무이사
2004～현재 OSIA 이사
2003～2004 ITU-T SG17/Q10 Associate Rapporteur
2005～현재 ITU-T SG17/Q9 Rapporteur
2006～현재 정보통신부 정책자문단 정보보호 PM
관심분야 : 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안
E-mail : hyyoum@scho.ac.kr

KCC 2007(한국컴퓨터종합학술대회)

❑ 일　　자 : 2007년 6월 25～27일
❑ 장　　소 : 무주리조트
❑ 내　　용 : 논문발표 등
❑ 주　　최 : 한국정보과학회
❑ 상세안내 : http://www.kiss.or.kr/conference02