Identity Metasystem 기술 및 동향

Technologies for Identity Metasystem

김수형 (S.H. Kim) 디지털ID보안연구팀 선임연구원
진승헌 (S.H. Jin) 디지털ID보안연구팀 팀장

목 차

인터넷이 실생활과 밀접하게 연관됨에 따라, 사람들은 누구나 의지와는 크게 상관없이 자신의 아이덴티티를 인터넷으로 연결된 수많은 장소들에 노출시켜야 하는 상황에 놓이게 되었고, 이렇게 노출된 아이덴티티들을 이용하여 좀 더 많은 가치를 생산하고자 하는 시도들을 경험하게 되었다. 또한 인터넷을 좀 더 안전하고 신뢰성 있는 공간으로 만들기 위한 노력으로 이용자들의 아이덴티티에 기반한 서비스 사이트들이 증가하는 추세에 있다. 이에 따라 아이덴티티 정보들을 안전하게 관리하고 유통할 수 있는 기술들이 연구되기 시작하였으며, 본 고에서 설명하는 Identity Metasystem은 그러한 기술들 중 가장 최근에 등장한 기술에 속한다. Identity Metasystem은 표준화된 기술들을 사용하여 다양한 ID 관리 시스템들과의 연동을 쉽게 하면서, 사용자에게 일관성있고 통제할 수 있는 ID 서비스를 제공하고자 하는 기술로, 본 고에서는 이러한 Identity Metasystem 기술과 개발 현황에 대하여 살펴본다.

Ⅰ. 서론

인터넷 기술이 발전하고 언제 어디서나 접속 가능한 통신수단이 제공되면서 인터넷 참여자들은 인터넷을 통해 좀 더 많은 정보를 소비하게 되었으며, 더 나아가 주어진 정보를 수동적으로 소비하는 입장에서 자신의 아이덴티티(이하 'ID'라 하며, 사람 또는 사물을 특징지을 수 있거나 연관시킬 수 있는 모든 속성들을 의미함)에 기반하여 직접 정보를 생산하거나 정보의 가치를 평가하는 등의 능동적으로 참여하는 주체가 되어가는 추세에 있다. 또한 초창기 인터넷 사이트들이 익명성을 보장하는 것으로 사용자들의 참여를 유도하였다면, 현재의 인터넷 내에 구축된 가상사회 혹은 서비스 제공 사이트들은 좀 더 높은 신뢰성과 서비스 품질을 보장하고 불특정 다수로부터 커뮤니티 구성원들을 안전하게 보호하기 위해, 참여자들에게 자신임을 증명할 수 있는 고유 신상정보들을 요구하게 되었다.

이러한 추세와 요구 변화는 인터넷을 통해 경제·사회 활동을 하는 개인들과 서비스 제공자 모두에게 ID 관리에 대한 부담을 가중시켰고, 이러한 증가된 부담으로 인해 ID 관리 시스템에 대한 요구가 구체화되어 SAML[1], Liberty Alliance[2], Shibboleth[3] 등 다양한 기술들과 시스템들이 이러한 요구사항을 만족시키기 위해서 등장하였다. 그러나 현재까지 이러한 기술들 중 어느 것도 인터넷 참여자들 대부분이 인정할 수 있는 대표적인 ID 관리 기술과 시스템으로 자리잡지 못하였으며, 또한 기존 기술들만으로는 이용자들의 개인정보에 대한 자기통제권 결여, 피싱(phising) 사이트에 유출된 개인정보의 불법 사용으로 인한 피해 증가, 특정 사이트에서의 개인정보 오남용 등 ID와 관련된 인터넷 위험요소들을 제거할 수 없었다.

초기의 ID 관리기술은 분산 저장된 ID 정보를 시스템들간 연계하여 공유함으로써 사용자에게는 SSO라는 기술적 혜택을 제공하고 서비스 제공자들에게 새로운 비즈니스를 창출할 수 있는 계기를 마련하는데 좀 더 중심을 두었다. 그러나 이러한 기술들은 조직간의 비즈니스 협약이 선행되어 상호 신뢰 도메인을 구축해야 한다는 어려움이 존재하였으며, 프로토콜 상에서 사용자의 승인단계가 포함될 수 있기는 하지만 본질적으로 사용자가 직접 자신의 정보를 제어할 수 있는 장치가 부족하다는 문제가 노출되었다. 또한 실세계에서의 개인들이 지갑 속에 자신의 다양한 신분증명 카드를 소지하고 있다가 주어진 컨텍스트에 따라 적절한 카드를 제시하는 것과 같이 인터넷에서의 다양한 사용자 활동을 일관성 있게 지원할 수 있는 ID 관리 시스템은 제공되지 못하였다.

따라서 이를 보완하는 새로운 ID 관리 기술이 요구되었는데, 이러한 요구사항을 만족시킬 수 있는 것으로 최근 부각되는 것 중 하나는 본 고에서 다루는 Identity Metasystem(이하 'ID 메타시스템'이라 함)이다. ID 메타시스템은 'Laws of Identity[4]'라는 ID 관리 시스템이 가져야 할 법칙 혹은 요구사항들에서부터 출발하여 구체화되고 공론화된 개념적 시스템이며, 마이크로소프트가 주축이 되어 진행하고 있는 ID 관리 프로젝트들의 핵심 아키텍처이기도 하다[5]. ID 메타시스템은 다양한 컨텍스트마다 존재하는 다수의 ID들을 통제하고 관리하는 시스템으로 기본적으로는 기존의 ID 관리 시스템을 포괄·연동시킬 수 있는 메타 시스템으로 자리잡고자 한다. 이러한 ID 관리 메타 시스템은 인터넷 세상에서 표준으로 통용되는 기술들을 통해 설명되며, 사용자의 인터넷 접속 수단이나 서비스 제공 환경 또는 통신 프로토콜 등에 구애 받지 않는다는 것을 전제로 하고, 또한 사용자에게 자기정보 통제권을 부여하는 ID 서비스 제공을 목표로 한다.

본 고의 Ⅱ장에서는 이러한 ID 메타시스템의 근간이 되는 기반 기술들에 대해 소개하고 Ⅲ장에서는 ID 메타시스템의 아키텍처와 프로토콜, 현재까지 진행된 개발현황에 대해서 설명한다. 그리고 마지막으로 Ⅳ장에서는 본 고에서 살펴본 바를 간략히 정리한다.

Ⅱ. ID 메타시스템 기반 기술

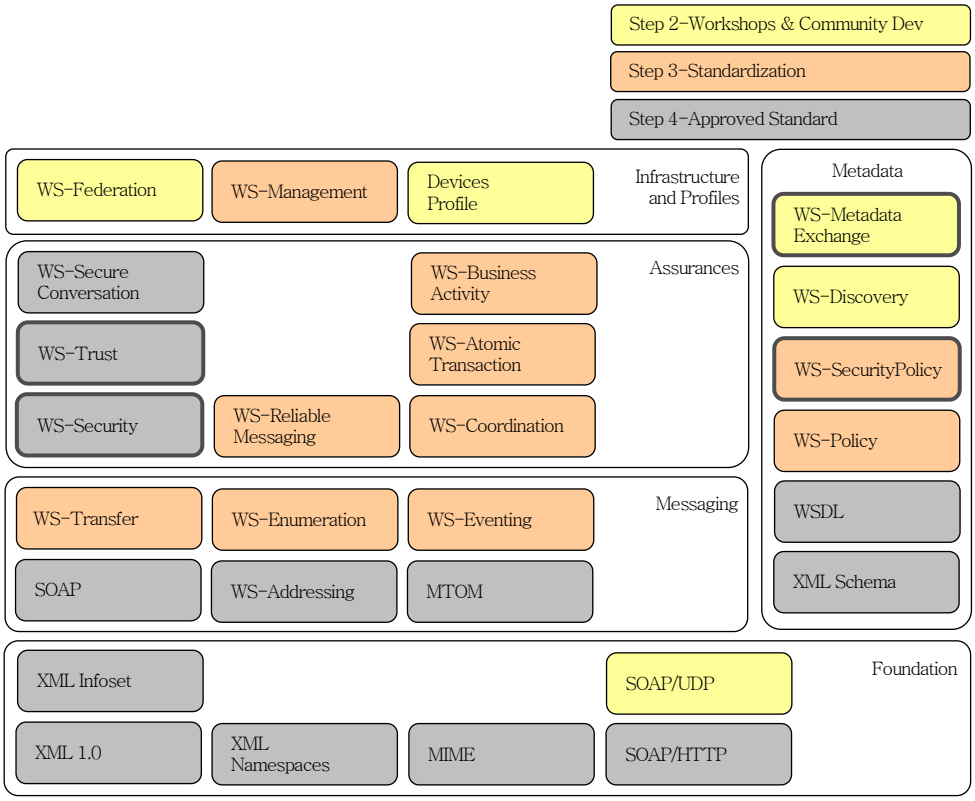
앞서 서론에서 언급한 바와 같이, ID 메타시스템

은 기존 ID 관리 시스템 또는 가까운 미래에 등장할 새로운 시스템들간 상호연동이 가능하기 위해서 표준화된 기술들을 사용한다. (그림 1)의 웹서비스 명세(WS-*)들이 이러한 표준 기술에 해당되며, 굵은 윤곽선으로 표기된 부분은 ID 메타시스템을 이해하는 데 핵심이 되는 기술들이다. WS-* 명세는 대부분 벤더 업체들에 의해서 처음 개발되어, 본 고에서 설명하는 ID 관리 기술분야에서 뿐만 아니라 SOA [6], 그리드[7] 등의 차세대 웹 기술을 위한 배경 기술로 넓게 인용되고 일부는 이미 특정 응용분야에서 이용되고 있다. 따라서 OASIS, W3C 등의 표준 기구에서는 중요성이 인정된 WS-* 명세들을 국제 표준으로 개발 완료하였거나 개발중에 있다.

WS-* 명세들은 상호의존적이어서 어느 하나로 완결되지 않으며, 통신 프로토콜 스택과 같이 여러 표준들이 서로 보완적인 역할을 수행하도록 구성되어 있다. 예를 들어, WS-Security[8]가 웹서비스 프레임워크를 사용하여 통신하는 두 참여자 간의 메시지 전송을 보호하는 방법을 설명하고 있기는 하지만 서로 다른 도메인에 속해 있는 메시지 송·수신자 간에 크리덴셜(credential)을 어떻게 발급하여 전송하고 입증할지에 대해서는 다루지 못하고 있는데, 이를 보완하기 위해 WS-Trust[9]가 사용된다.

ID 메타시스템은 이러한 WS-Trust 기술표준에서 설명하는 방법을 이용하여 사용자 ID 정보를 신뢰성 있고 안전하게 송수신하는 문제를 해결하고자 하며, 서로 다른 도메인에 속한 참여 주체들 간에 보안과 관련된 정책을 표현하고 전달하기 위해서 WS-SecurityPolicy[9]와 WS-MetadataExchange (이하 WS-MEX)[10] 기술을 함께 적용한다.

WS-Security는 1.1 버전이 2006년 2월에 OASIS 표준으로 채택되었으며, WS-Trust는 2007년 3월에 보안세션 구축 방법 등을 설명하는 WS-Secure Conversation[9]과 함께 OASIS 표준으로 채택되



(그림 1) WS-* 명세 스택

었다. 그리고 IBM과 MS 등에 의해 처음 개발된 WS-SecurityPolicy는 OASIS WS-SX TC에서 1.2 버전으로 개발중에 있으며, WS-MEX는 IBM과 MS 등에 의해서 2006년 8월경에 1.1 버전이 공개되었다. 본 장에서는 위의 기술들에 대해 ID 메타시스템을 중심으로 간략하게 소개하고자 한다.

1. Security Token

웹서비스 보안을 설명하기 위해 가장 많이 인용되는 기술은 WS-Security이다. WS-Security는 XML 전자서명과 XML 암호화 기술을 통하여 메시지의 안전한 전송을 가능하게 하며, 또한 인증 및 권한제어 등을 위해 메시지 헤더에 다양한 보안토큰을 삽입하는 방법을 정의한다.

ID 메타시스템에서도 마찬가지로 사용자 개인정보를 전달하기 위해 보안토큰을 사용하는데, 기본적으로 WS-Security에서 정의하는 보안토큰과 동일한 형태와 메커니즘으로 설명될 수 있다. 다만 보안토큰 내 데이터의 이용범위 측면에서는 메타시스템에서의 보안토큰이 좀 더 확장된 개념으로 볼 수 있다. 즉, ID 메타시스템의 보안토큰은 인증 및 권한제어를 위한 용도를 넘어 개인이 특정 서비스 사이트에 가입 신청하기 위해 필요한 개인정보를 전달할 때, 특정 물품을 구매하기 위해 신용카드정보를 전달할 때 등의 다양한 컨텍스트에서 사용되며, 웹서비스가 아닌 브라우저 기반 웹 환경에서도 사용될 수 있다.

ID 메타시스템에서 설명하는 보안토큰 포맷은 WS-Security의 부가표준들에서 설명하는 SAML [11], X.509, Kerberos 등으로 설명될 수도 있지만, 포맷에 대한 제한을 두지는 않고 있다. 보안토큰 내 데이터는 '클레임(claim)'이라는 누군가가 특정 주체에 대해 설명하는 주장들로 구성되며, 주장을 입증할 수 있는 정보와 보안토큰에 대한 소유증명정보 등이 함께 포함될 수 있다. 앞서의 '누군가'는 인터넷에서 활동하는 사람과 사물들 모두 대상이 되며 특정 주체인 나 자신이 포함될 수 있다. 그리고 이후 설명될 WS-Trust에서의 보안토큰서비스(STS)를 구축하고 특정 주체의 요구에 의해서 보안토큰을 발급하는 책임을 갖는다.

2. WS-SecurityPolicy & WS-MEX

웹서비스 제공자는 WS-Policy를 통해 정책을 정의하고 웹서비스 애플리케이션이 수행되는 환경을 구축한다. 정책은 하나 또는 그 이상의 정책 선언을 통해 표현되는데, 예를 들어, 정책 선언을 통해 웹서비스에 대한 요청이 암호화된 메시지로 전달되어야 한다거나 또는 수용할 수 있는 최대 메시지 크기를 지정할 수도 있다. WS-SecurityPolicy는 이러한 WS-Policy 프레임워크에 보안 정책 정의 셋을 추가한 것으로, 버전 1.2 명세에서는 WS-Security, WS-Trust, WS-SecureConversation에 대한 보안 정책들을 주로 다루고 있다. ID 메타시스템에서 언급되고 있는 보안 정책들도 이러한 범위를 넘어서지는 않으며, 주로 ID 메타시스템 참여자들간 협상이 어떻게 이루어질 수 있는지를 설명하기 위해 이용된다. 이에 대한 내용은 III장에서 다시 다루기로 한다.

웹서비스에서 말하는 메타데이터는 XML schema, WSDL, policy 등이다. 웹서비스 이용을 위해서 웹서비스 소비자는 웹서비스 생산자와 이러한 메타데이터(이용 가능한 서비스, 서비스 이용을 위한 접근주소, 이용방법, 이용정책 등)를 미리 상호 교환해야 하는데, 이 때 WS-MEX 기술이 사용된다. ID 메타시스템에서는 참여주체들간 보안 정책과 관련된 메타데이터를 전송하기 위해서 WS-MEX 명세를 인용하고 있다.

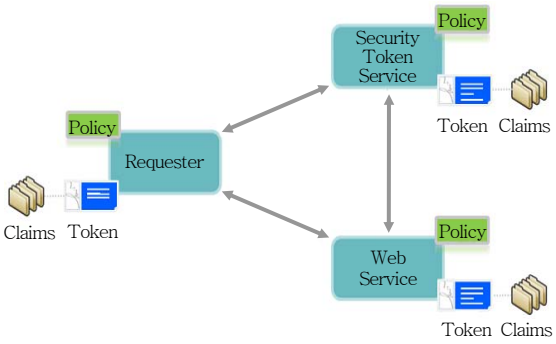
3. WS-Trust

인터넷을 통해 서비스 요청자와 서비스 제공자 두 주체간에 상호 신뢰성 있는 통신을 하기 위해서는 요청자가 제시하는 클레임들을 제공자가 확인할 수 있어야 하는데, 통상적으로 이것은 요청자와 제공자간에 클레임 항목과 보안토큰 형태, 클레임 증명정보 등을 사전 합의 하에 공유하고 있다는 것을

전제로 한다. 즉 서비스 제공자와 서비스 요청자간에는 신뢰관계가 구축되어 있고, 구축된 신뢰를 바탕으로 상호 소통할 수 있는 것이다. 그러나 ID 메타시스템의 참여자들은 이러한 신뢰관계가 구축되지 않은 상황에서도 협상을 통한 방법으로 앞서의 전제조건을 만족시킨다. ID 메타시스템에서 참여자들간 협상은 WS-SecurityPolicy와 WS-MEX를 통해 타 주체의 능력범위와 요구사항 등을 파악하고 Ⅲ장에서 설명될 Identity Selector가 중간에서 작용하고 소비자가 직접 참여하도록 함으로써 완료된다. 그리고 협상으로 결정된 합의사항, 즉 클레임 항목과 보안토큰 형태 및 증명방법 등을 제공하기 위해서 WS-Trust 기술이 사용된다.

WS-Trust는 서로 다른 신뢰 도메인 내의 참여 주체들을 위한 보안토큰의 발행, 교환, 검증, 폐기 등의 기술을 제공하여 웹 서비스 보안 모델을 확장하기 위한 것이나, ID 메타시스템은 이러한 WS-Trust가 제공하는 서비스를 이용하면서도 웹서비스가 아닌 환경에서 보안토큰의 발급, 교환, 검증 등을 가능하게 하고 있다.

(그림 2)는 WS-Trust 명세에서 설명되는 기본 모델이다. 웹서비스 제공자와 웹서비스 요청자, 보안토큰서비스는 모두 자신의 정책들을 가지며, 자신 혹은 신뢰관계가 구축된 타 주체에 대한 클레임들을 생성할 수 있다고 가정된다. 또한 보안토큰서비스는 웹서비스 제공자 신뢰 도메인에 추가되어 타 도메인에서 발행한 보안토큰을 웹서비스 시스템에서 쉽게 검증할 수 있는 형태로 교환하는 것이 가능하며, 발급된 보안토큰이 제 3자에 의해 불법 이용·변경되는 것을 방지할 수 있는 메커니즘을 포함한다.



(그림 2) WS-Trust 기본 모델

Ⅲ. ID 메타시스템

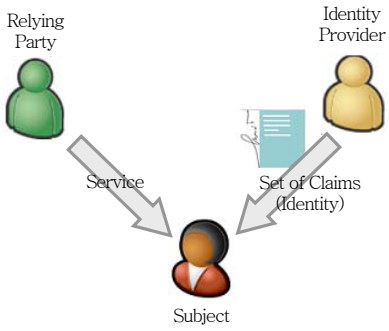
본 장에서는 ID 메타시스템의 아키텍처와 기본 프로토콜에 대해서 설명하고, 현재 진행되고 있는 개발 프로젝트들의 현황에 대해 소개한다.

1. 아키텍처

ID 메타시스템의 참여자들은 (그림 3)과 같이 메타시스템을 준용하는 서비스 제공자(relying party), 서비스 이용자(subject) 그리고 보안토큰을 발급하는 ID 제공자(Identity Provider: 이하 'IDP'라 함)들로 구성되며, 사용자가 IDP와 서비스 제공자 중심에 서서 자기 정보를 통제할 수 있도록 한다.

ID 메타시스템에서의 참여자들 역할은 다음과 같이 간략히 정의할 수 있다.

- ID 제공자: 보안토큰 발급자. 사용자에 대한 ID 정보를 생성·관리하면서 사용자의 요구에 의해 관리되는 ID 정보를 사용하여 보안토큰을 발급한다.
- 서비스 제공자: 보안토큰 소비자. 보안토큰을 통해 서비스 이용접근 주체를 식별하고 식별된 사용자에게 자신이 소유하거나 관리하는 서비스를 제공한다.
- 사용자: 서비스 이용자. 서비스 제공자와의 특정



(그림 3) ID 메타시스템 참여주체

컨텍스트 하에서 자신의 ID를 ID 제공자를 통해 전달하고 서비스를 이용한다.

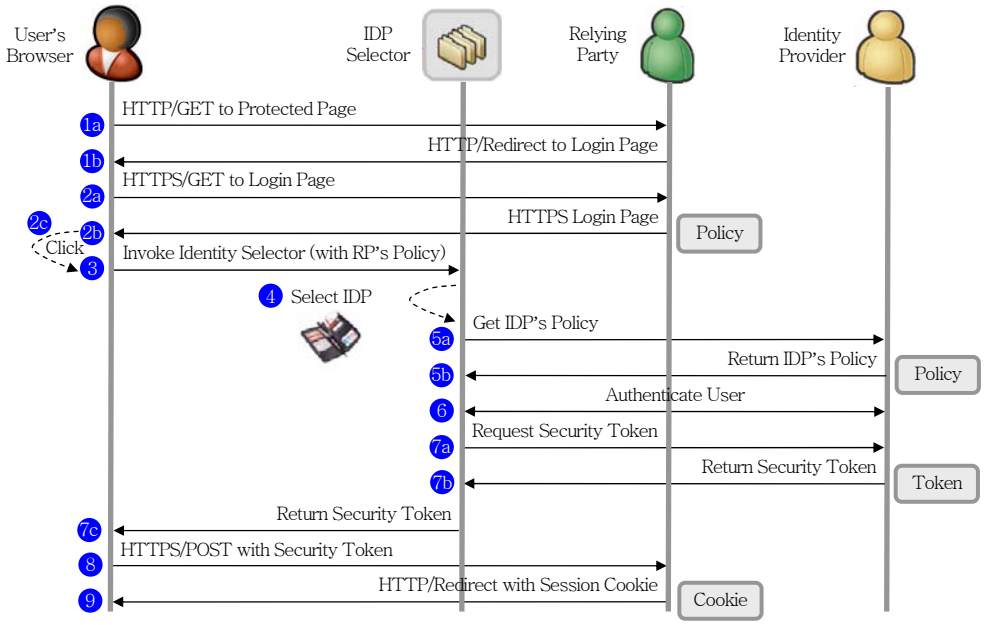
지금까지 ID 메타시스템의 기반 기술과 참여자들에 대해 알아보았는데, 이외에 ID 메타시스템의 아키텍처를 이해하는 데 중요한 구성요소 중 하나는 사용자 측에 존재하는 ID 선택기(Identity Selector: ID는 IDP에서 제공하는 것이기 때문에 IDP Selector라고도 할 수 있음)이다. ID 선택기는 서비스 제공자와 사용자 사이의 협상을 중재하고, 협상의 결과로서 요청된 보안토큰을 사용자의 선택과 승인을 통해 지정된 IDP로부터 전달받고, 전달받은 보안토큰을 서비스 제공자에게 최종 전달하는 역할을 수행한다. 또한 사용자에 대해 보안토큰을 발급해 줄 수 있는 IDP 목록과 IDP가 제공해 줄 수 있는 클레임 항목들 및 IDP에 접속할 수 있는 주소, 서비스 이용 히스토리 정보 등을 관리하는 역할을 수행한다. ID 메타시스템을 통해 사용자가 자기정보를 통제할 수 있다는 것은 사용자 ID의 흐름이 서비스 제공자와 IDP간 직접 연결되는 것이 아닌 사용자를 통해서만 가능한 것이므로 사용자가 수행해야 하는 작업은 이전의 웹 환경과는 크게 다르다. 따라서 ID 선택기는 이러한 작업들을 사용자 대신 자동 수행해주며, 또한 사용자가 좀 더 쉽고, 직관적이고, 일관성 있는 방법으로 인터넷을 이용할 수 있도록 돕는다.

2. 프로토콜

ID 메타시스템을 통해 수행되는 기본 프로토콜은 사용자가 브라우저를 사용하느냐 또는 웹서비스 클라이언트(rich client)를 사용하느냐에 따라 약간 차이가 있다. 본 고에서는 현 인터넷 환경에 비추어 가장 많이 사용되리라 예상되는 브라우저 기반의 프로토콜을 (그림 4)와 같은 단계별로 설명한다.

(1) 사용자 서비스 접근

인터넷 웹 사이트(즉, 서비스 제공자)는 인터넷 접속이 가능한 모든 사람들에게 노출되어 있기 때문에 특정 보호되어야 할 페이지에 접근하는 사용자에 대해 신원 확인과정을 먼저 수행한다. 따라서 신원이 확인되지 않은 사용자의 보호페이지 요청은 사용자 확인을 수행하는 페이지(e.g. 로그인 페이지)로 리다이렉트 된다.



(그림 4) ID 메타시스템에서의 기본 프로토콜

(2) 사용자 Identity 요구

사용자의 신원 확인 방법은 웹 페이지에 구축된 사용자 신원 확인 장치에 따라 다양하다. 통상 식별 ID 및 비밀번호를 요청하는 것이 일반적이지만 더 높은 보안수준을 요구하는 사이트에서는 인증서 혹은 바이오 정보를 사용할 것을 요청하기도 한다. ID 메타시스템에 기반한 웹 사이트는 사용자에게 요청할 클레임 항목들과 보안토큰 타입 및 IDP 정보(서비스 제공자는 지정된 IDP로부터 보안토큰을 발급받도록 요구할 수도 있음) 등을 정책으로 정의하고 정책정보를 사용자 신원 확인 페이지에 기술하여 브라우저로 전달하는 방법을 사용한다.

(3) ID 선택기 실행

(2)번째 단계에서 설명한 바와 같이, 웹 사이트는 사용자 확인 페이지 내에 웹 사이트의 정책과 요구하는 클레임 항목 등을 기술한다. 또한 이러한 정보를 전달받아 처리할 수 있는 ID 선택기를 사용자 확인 페이지 내 object 태그를 통해 지정한다. 사용자 브라우저는, 예를 들어 PDF 문서 뷰어를 호출하는 것과 같이 ID 선택기를 호출한다.

(4) 사용자의 IDP 선택

ID 선택기는 (2)번째 단계에서 전달받은 요구 클레임 항목들과 보안토큰 타입을 지원할 수 있는 IDP 목록들을 자동적으로 분류하고 분류된 목록을 카드 형태(ID 메타시스템에서 각 IDP 항목들은 지갑 속의 신용카드와 같은 모습으로 설명됨)로 디스플레이하여 사용자가 IDP 목록들 중 하나를 선택할 수 있도록 하는데, 이것은 사용자에게 직관적이고 일관성 있는 인터페이스를 제공하는 ID 선택기의 능력 중 하나이다.

(5) IDP 정책 수령

사용자가 디스플레이 된 목록들 중에서 특정 IDP를 선택하면 ID 선택기는 기 저장된 IDP 정보를 바탕으로 IDP 보안정책을 수령한다(WS-MEX). 이렇게 수령된 정보에는 사용자 인증 정책, 암호화 알고리듬, 키 정보 등을 포함하고 있다. 또한 ID 선택기와 IDP 간 통신 채널을 보호하기 위한 방법들이 포함될 수 있다.

(6) IDP에 대한 사용자 인증

사용자는 (5)번째 단계에서 수령한 IDP의 인증 정책에 따라 인증에 필요한 정보를 IDP에 제공해야 한다. IDP는 제공된 사용자 인증정보를 확인하고 보안토큰 발급을 허용한다. ID 메타시스템에서 사용자에 대한 인증 방법과 강도에 대해 따로 기술하고 있지는 않으나, 통상 IDP가 제공하는 ID의 중요성 또는 ID가 사용되는 컨텍스트에 의해 인증 강도가 결정된다. 참고로, Liberty 프로젝트[2]와 같은 federated 모델에서는 IDP의 인증방법을 서비스 제공자가 결정할 수 있는 방법을 제공하나, ID 메타시스템과 같은 user-centric 모델에서는 기본적으로 서비스 제공자가 IDP에게 이러한 인증 방법을 직접 요청하지는 않는다.

(7) 보안토큰 요청

ID 선택기는 사용자 인증이 완료되면, (2)번째 단계에서 서비스 제공자가 제공한 클레임 항목들에 대한 보안토큰을 발급하도록 IDP의 STS에 요구한다(WS-Trust). STS는 요구된 클레임들을 포함한 보안토큰을 생성하고 생성된 토큰을 자신의 비밀키로 서명하여 보안토큰의 무결성을 보장한다. STS에 의해 서명된 보안토큰은 ID 선택기에 전달되며, ID 선택기와 사용자는 보안토큰의 클레임 항목과 내용을 확인한다.

(8) 보안토큰 전달

확인된 보안토큰은 ID 선택기에 의해 브라우저를 통해 서비스 제공자에 전달된다(ID 메타시스템이 구현된 실제 모습에 따라 다르겠지만, 이 때 ID 선택기의 다양한 장치들이 작용하여 보안토큰과 함께 다른 부가정보들이 포함될 수 있다). 보안토큰을 전달하는 단계는 기존 웹 프로토콜의 변경 없이 수행되

어야 하기 때문에 통상 POST 메시지 내에 포함되어 전달하는 방법이 이용된다. 본 고에서는 설명되지는 않지만 만약 서비스 제공자가 웹서비스를 제공하고 있다면, WS-Security의 헤더에 보안토큰을 포함하여 전달하는 방식이 이용되며, 브라우저 기반 환경과는 달리 SSL을 이용한 보호세션이 구축되어 있지 않기 때문에 보안토큰 소유권 증명(proof of possession) 정보가 추가적으로 포함될 수 있다.

전달된 보안토큰을 통해 서비스 제공자는 자신이 요구한 클레임 항목들을 추출・검증하고, 만약 사용자 인증용도로 ID를 요구하였다면 사용자 식별 ID를 통한 사용자 멤버십 확인과정을 수행한다.

(9) 인증세션 생성 및 서비스 이용

일반적인 웹 사이트에서는 사용자 인증세션을 유지하기 위해 cookie를 브라우저에 전달하는 방식을 이용하는데, ID 메타시스템은 사용자가 인증된 이후의 행위들에 대해서는 따로 언급하지 않는다. 따라서 메타시스템을 적용한 서비스 제공자는 기존 시스템에 적용된 기술(e.g. cookie)을 그대로 사용할 수 있다.

3. 개발 현황

ID 메타시스템은 최종 구현 시스템의 세부 설계서가 아닌 기본 요구 기능과 개념적 아키텍처를 설명하고 있는 것으로, 앞서 설명된 기반 기술들을 사용하고 표준 아키텍처를 준수한다면 누구나 자신이 목적하는 형태로 개발에 참여할 수 있다. 현재 메타시스템을 구현하는 작업은 두 단체를 통해 수행되고 있는데, 하나는 ID 메타시스템에 대한 개념과 아키텍처를 주도적으로 개발한 마이크로소프트이며, 다른 하나는 마이크로소프트와 협력하지만 OS와 브라우저 등을 마이크로소프트 플랫폼을 사용하지 않고 구현하려는 Higgins가 있다.

가. CardSpace

마이크로소프트는 차세대 OS인 윈도비스타에 'CardSpace[12]'라는 ID 선택기를 기본적으로 탑재하고 있으며, IE 7.0에 ID 선택기를 호출할 수 있는 모듈을 플러그인 시켰다. 윈도비스타는 .NET 3.0 프레임워크[13]에 기반한 서비스들을 제공하는데, .NET 3.0이 CardSpace 기술을 포함하고 있는 것이다. 따라서 .NET 3.0을 따로 다운로드 받아 설치한 윈도 XP에서도 CardSpace를 이용할 수 있다. 또한 .NET 3.0에 새롭게 추가된 기술인 WCF을 통해 WS-* 기술을 제공하며, 이를 통해 CardSpace가 IDP와 통신하기 위한 기능을 제공받는다. 그리고 CardSpace는 앞서 설명된 ID 선택기의 역할뿐만 아니라 personal STS를 포함하고 있어, 사용자가 직접 IDP가 되어 서비스 제공자에 자신의 신상정보를 제공해 줄 수도 있도록 하였다. 그러나 personal STS가 생성할 수 있는 클레임 항목은 12개의 신원정보들로 고정되어 있다.

마이크로소프트는 ID 메타시스템의 이용을 활성화하고 다양한 플랫폼에서 동작 가능한 제품 개발을 장려하기 위해 마이크로소프트가 공개한 웹서비스 기술규격에 대해 라이선스 없이 무상 이용할 수 있도록 하였다(OSP).

나. Higgins

이클립스(Eclipse) 재단에서 운영되는 오픈 소스 프로젝트인 Higgins[14]는 윈도 CardSpace와 같은 ID 메타시스템을 목표로 개발을 진행중에 있으며, 2006년 2월경부터 IBM과 노벨 등의 업체들로부터 후원을 받고 있다.

Higgins는 마이크로소프트 플랫폼(윈도 OS, IE 브라우저, .NET 프레임워크 등)에 국한되지 않는 시스템을 제공하면서, CardSpace와 같은 다른 ID 관리 시스템들과의 상호연동 문제를 컨텍스트 제공자라는 개념을 통해 해결하고자 한다. 그리고 Higgins가 CardSpace와 다른 점은 플랫폼 이외에도, Higgins가 URI로 IDP 정보를 관리할 수 있는 방법(URI I-Card)을 제공하며, 사용자가 인터넷을 통해 접할 수 있는 다양한 컨텍스트별로 개인정보속성(attribute: 클레임과 유사한 개념임) 항목을 분리 관

리할 수 있도록 온톨로지 기술을 적용하고 있다는 것 등이다.

Higgins 프로젝트를 통해 수행된 결과는 2007년 여름 경에 Higgins Trust Framework 1.0으로 발표될 예정에 있다.

Ⅳ. 결론

지금까지 ID 메타시스템의 등장배경과 기반기술, 아키텍처, 기본적인 ID 관리 흐름에 대해서 설명하였다. 설명한 바와 같이 ID 메타시스템은 ID 관리 시스템의 메타시스템을 표방하면서 탄생한 개념이며 사용자 중심으로 ID 흐름을 관리하는 모델을 지향한다. 그러나 아직 사용자, 서비스 제공자, IDP 모두를 지원하는 제품들이 제공되지는 않고 있으며, 이러한 제품들이 인터넷에 배포되고 사용자가 직접 다양한 경험을 수행하는 단계에 이르기까지에는 약간의 시간이 필요한 것으로 보이기 때문에 ID 메타시스템에 대한 실질적인 평가는 훨씬 뒤로 미뤄야 할 듯하다. 하지만 현재 ID 메타시스템은 많은 ID 전문가들로부터 큰 관심의 대상이 되고 있으며, 윈도즈라는 거대한 지원동력을 등에 기대고 있는 기술이기 때문에 ID 관리 기술 분야에서 향후 충분히 영향력을 행사할 것이라는 것을 의심할 수는 없을 것이다.

그리고 본 고에서 설명되지는 않았지만, 토큰을 기반으로 동작하는 ID 메타시스템과 URL/URI를 기반으로 동작하는 ID 관리 시스템 등의 상호연동 문제를 해결하기 위해 마이크로소프트, IBM, 노벨, 구글, Verisign 등의 업체들이 참여한 프로젝트인 OSIS[15]가 2006년 중순에 출범한 바 있다. 이는 ID 시스템들 간의 연동 문제가 하나의 특정 기술에 의해서가 아니라 기술개발 업체들 서로간의 협력에 의해서 가까운 미래에 해결될 것이라는 것을 기대해 볼 수 있다. 또한 이러한 활발한 움직임들로 인해 사용자들이 새로운 ID 관리 체계에 적응해야 하는 시기가 빠르게 도래할 것이라는 것을 짐작하게 한다.

● 용 어 해 설 ●

신뢰(Trust): 본 고에서 설명되는 두 주체간 신뢰는 하나의 행위주체에서 주장하는 내용과 요청하는 서비스를, 선약에 의해서, 다른 행위주체가 받아들이거나 수행할 것이라는 의미를 내포한다. 이러한 신뢰관계는 직접적으로 혹은 중재자를 통해 간접적으로 구축되기도 하며, 신뢰 기간도 모델에 따라 다양하다.

약 어 정 리

ID	IDentity
IDP	IDentity Provider
OASIS	Organization for the Advancement of Structured Information Standards
OSIS	Open-Source Identity System
OSP	Open Specifications Premise
SAML	Security Assertion Markup Language
SOA	Service Oriented Architecture
SP	Service Provider
SSL	Secure Socket Layer
SSO	Single Sign-On
STS	Security Token Service
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
WCF	Windows Communication Foundation
WSS	Web Service Security

참 고 문 헌

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

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

[3] Shibboleth, http://shibboleth.internet2.edu/

[4] Kim Cameron and Michael B. Jones, “Design Rationale behind the Identity Metasystem Architecture,” USENIX Security, Jan. 2006.

[5] 마이크로소프트, “Microsoft’s Vision for an Identity Metasystem,” 마이크로소프트 기술백서, 2005. 5.

[6] 오라클, “웹서비스 보안: SOA 보안을 위해 필요한 요소,” 오라클 기술백서, http://www.oracle.com/technology/global/kr/tech/standards/pdf/security_kor.pdf, 2006. 10.

[7] 이성현, 이재승, 문기영, “웹서비스 기반 그리드 보안 기술 동향,” 전자통신동향분석, 제22권 제1호, 2007. 2., pp.24-36.
[8] OASIS Web Services Security TC, http://www.oasis-open.org
[9] OASIS Web Services Secure Exchange TC, http://www.oasis-open.org
[10] IBM, Microsoft et., “Web Services Metadata Exchange,” http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-mex/metadataexchange.pdf, 2006. 8.
[11] OASIS Security Services TC, http://www.oasis-open.org
[12] Microsoft CardSpace, http://msdn2.microsoft.com/en-us/netframework/aa663320.aspx
[13] Microsoft .NET Framework 3.0, http://msdn2.microsoft.com/en-us/netframework/aa663309.aspx
[14] Higgins Trust Framework Project, http://www.eclipse.org/higgins/
[15] Open Source Identity System, http://osis.netmesh.org/wiki/Main_Page