해외의 대규모 OpenID 도입 사례

김승현* 진승현**

OpenID 는 인터넷 사용자들이 여러 다른 웹사이트들을 하나의 ID 로 로그인하게 만들어 주는 분산 Identity 서비스다. 기술 측면에서 OpenID 는 핵심 스펙의 개발 및 검증이 완료된 상태이며, 최근 들어 활발하게 도입되고 있다. 특히 대규모 사이트에서의 적용이 본격화되는 추세로 Yahoo!, Microsoft, Google 등의 사이트가 대표적인 OpenID 제공자로 동작하고 있다. 본 고에서는 OpenID 적용 사례 중, 규모나 기술적인 측면에서 주목할만한 가치가 있는 사례를 중심으로 OpenID 의 적용 방향 및 개선 사항을 살펴보기로 한다. ▨

목 차

Ⅰ. 서 론

Ⅱ. 대규모 OpenID 적용 사례

Ⅲ. 결 론

* ETRI 디지털 ID 보안연구팀/연구원
** ETRI 디지털 ID 보안연구팀/팀장

Ⅰ. 서 론

OpenID 는 인터넷 사용자들이 여러 다른 웹 사이트들을 하나의 ID 로 로그인하게 만들어주는 분산 identity 서비스다. OpenID 는 누구나 시스템을 만들어서 사용할 수 있으며, 무료로 이용할 수 있고 공개 표준을 따른다. OpenID 는 하나의 ID 체계를 제공하기 때문에 각 사이트마다 서로 다른 ID/패스워드를 사용할 필요가 없어지며, 사이트에 제공할 개인정보를 사용자가 직접 제어할 수 있다.

기술 측면에서 OpenID 는 핵심 스펙의 개발 및 검증이 완료된 상태이며, 최근 들어 활발하게 도입되고 있다. 특히 대규모 사이트에서의 적용이 본격화되는 추세로 AOL, BBC, Google, IBM, Microsoft, MySpace, France Telecom(Orange), VeriSign, Yahoo! 등의 사이트가 OpenID 제공자로 동작하고

<표 1> Yahoo!, Microsoft, Google 의 OpenID 지원 현황

대상	Yahoo!	Microsoft	Google
사용자 수(억 명)*	3.68	2.56	0.91
기존 인증방법	id/pw	live id	id/pw
도입시기**	OP: 2008/1/17	RP: 2008/6/23 OP: 2008/10/28	RP: 2008/1/18 OP: 2008/10/29
역할	OP	OP RP(healthvault.com)	OP RP(blogger.com)
지원버전	2.0	2.0	1.1, 2.0

* 사용자 수: 2008 년 2 월 조사 [1]
* * RP(Relying Party): OpenID 지원 사이트, OP(OpenID Provider): OpenID 제공자

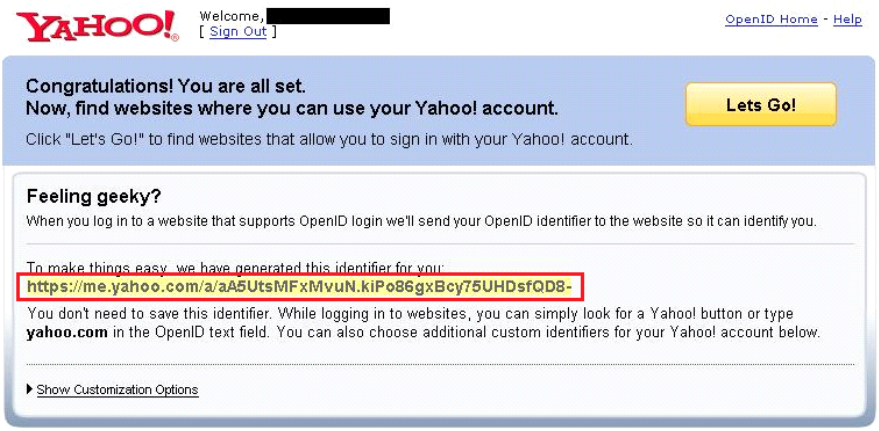
있다. 본 고에서는 이들 적용 사례 중, 규모나 기술적인 측면에서 주목할만한 가치가 있는 사례를 중심으로 살펴보기로 한다. 선택된 사례는 Yahoo!, Microsoft, Google 이며, 각 업체의 OpenID 지원 현황은 <표 1>과 같다.

II. 대규모 OpenID 적용 사례

1. Yahoo!

가. Yahoo! Email

2008 년 1 월, Yahoo!는 공식적으로 OpenID 제공자가 되었음을 발표하였다[2]. Yahoo! 계정을 가진 사용자는 OpenID 지원 사이트에서 사용할 OpenID URL 로 'me.yahoo.com', 'www.yahoo.com', 'www.flickr.com'을 사용할 수 있다. 기존의 OpenID 인증 스펙 v1.1 에서는 사용



(그림 1) Yahoo!의 OpenID 로그인 화면

자가 고유하게 할당된 OpenID URL 를 입력하고, 해당 OpenID 제공자로 이동한 뒤에 인증 절차를 수행해야만 하였다. 하지만 그 방식은 사용자의 OpenID 가 매번 노출되기 때문에 프라이버시가 우려된다는 의견이 있었다. 따라서 Yahoo!측은 OpenID 인증 스펙 v2.0 이 권고하는 것처럼 OpenID URL 입력 창에 OpenID 제공자 주소를 입력하는 것만으로 동작 가능하도록 구성하였다(가령, http://me.yahoo.com/userid 에서 http://me.yahoo.com 으로 사용 가능).

또한 Yahoo!는 사용자의 프라이버시가 노출되지 않게 하기 위해 별도로 일회용(One-Time) OpenID 를 만드는 기능 또한 제공한다. (그림 1)은 Yahoo! 사용자를 위해 생성된 일회용 OpenID 를 보여준다.

나. Yahoo! Flickr

Flickr[3] 는 Yahoo!의 사진 및 동영상 호스팅 서비스로, 대표적인 Web 2.0 사이트 중 하나다. 사용자들은 Flickr 에서 개인의 사진을 공유할 수 있으며, 사진에 태그를 설정하여 검색할 수 있다. 2008 년 11 월 현재, Flickr 는 30 억 개 이상의 사진을 보유하고 있다.

Yahoo!는 Flickr 주소를 OpenID URL 로 사용하는 서비스를 2008 년 1 월에 소개하였다. 이 서비스는 OpenID 스펙에서 지정한 Delegation 기능을 이용한 것이다[4]. Flickr 의 사용자 페이지를 살펴보면 아래와 같이 Yahoo!의 OpenID 제공자를 가리키는 <link> 태그를 확인할 수 있다. 사용자가 자신의 Flickr 페이지를 OpenID URL 로 제시하면, OpenID 지원 사이트는 <link> 태그 내용을 바탕으로 Yahoo!의 OpenID 제공자에게 해당 사용자의 인증정보를 요청하게 된다[5].

```
<link rel="openid2.provider" href="https://open.login.yahooapis.com/openid/op/auth" />
```

Flickr 의 사례는 기존의 OpenID 제공자와는 다른 접근 방법을 가진다. 기존의 OpenID 제공자는 사용자로부터 신뢰를 받고 있으며 사용자의 계정 정보를 바탕으로 OpenID 를 제공하였다. 하지만 OpenID 를 제공하는 것만으로는 부가 서비스나 수익모델을 창출하기 어렵기 때문에 여러 OpenID 제공자들은 단순한 인증을 넘어서 신원을 증명하거나 확인된 신원정보를 활용하는 서비스를 제공하려는 움직임을 보인다. 그와 반대로 Flickr 는 사진을 공유하는 소셜 네트워크로 시작하여 지금은 OpenID 제공자로 변화하였다. Flickr 주소를 OpenID 로 사용하는 사람은 자신의 신원을 '사진'과 '친구'들로 증명할 수 있기 때문에 더욱 신뢰 있는 사용자로 인식될 수 있다.

다. 사용성 테스트

OpenID 는 비즈니스 측면에서 사용자들의 가입 부담을 덜어주는 효과가 있다고 소개된다. 하지만 실제로 사이트에 적용한 결과를 보면 OpenID 의 개념이 사용자들을 오히려 혼란스럽게

만드는 경우가 빈번하다. 이 때문에 2008 년 7 월, Yahoo!는 32~39 세의 인터넷 중・고급 수준인 여성 사용자를 대상으로 OpenID 의 사용성에 대한 테스트를 수행하였다.[6]

Yahoo!의 테스트 결과에서 OpenID 의 사용성과 관련된 여러 문제점을 도출할 수 있었다. 우선 웹 페이지는 기존의 로그인 방식과 OpenID 로그인 창을 한 화면에 제시하여 사용자를 혼란스럽게 만들었으며, OpenID 자체를 사용하는 방식도 OpenID URL 을 직접 입력하는 방법, ID Selector 를 사용하는 방법, OpenID 제공자의 주소를 입력하는 방법 등 다양하여 혼란을 유발하였다. 로그인 과정에서도 불필요한 페이지가 존재하며, 로그인 흐름을 이탈시키는 링크가 존재하는 경우도 있다. OpenID 로 로그인한 뒤, 사용자는 다음 번에는 웹사이트의 ID/패스워드로 로그인할 수 있다고 생각하기도 한다.

Yahoo!는 이 결과를 바탕으로 자사의 OpenID 서비스를 개선하였다. OpenID 제공자와 OpenID 지원 사이트 간의 강한 파트너십을 구축하였으며, 이를 통해 간단하면서도 명확한 로그인 페이지와 프로세스를 정립하였다. 그리고 사용자에게 일관된 사용 흐름을 제시하였다.

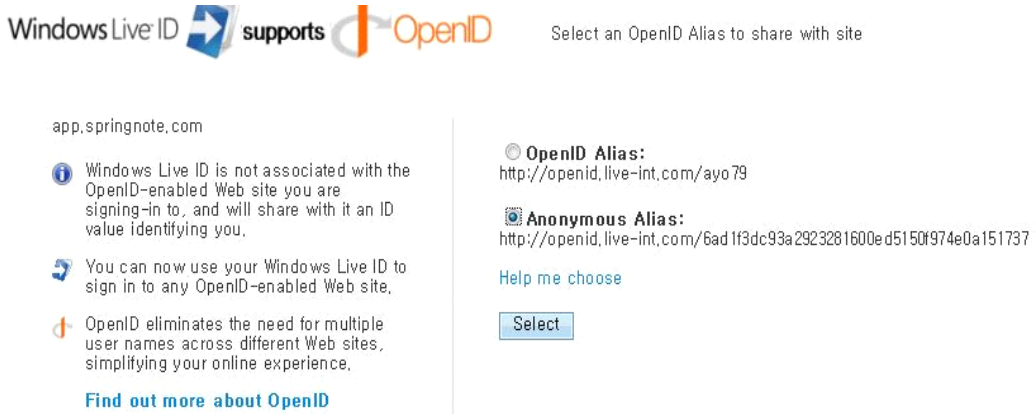
2. Microsoft

가. Live ID

2007 년 2 월에 열린 RSA 컨퍼런스에서, Microsoft 의 빌 게이츠는 OpenID 를 지원하겠다고 발표하였다. 그로부터 20 개월이 지난 2008 년 10 월, Microsoft 는 PDC(Professional Developer Conference) 2008 에서 Windows Live ID 의 OpenID 제공자 지원을 선언하였다. MSN(MicroSoft Network) 계정을 가진 사용자는 OpenID 를 사용할 수 있으며, 현재는 공개 테스트 단계이므로 사용자는 MSN 에 로그인 한 뒤에 OpenID 를 생성해야만 한다. 테스트는 http://login.live-int.com 에서 가능하다.

OpenID 제공자로서 Live ID 는 OpenID 인증 스펙 v2.0 을 지원하기 때문에, 사용자는 자신이 발급받은 OpenID URL 또는 OpenID 제공자의 주소(http://login.live-int.com)를 OpenID 지원 사이트에서 사용할 수 있다. 또한 Yahoo!와 마찬가지로 익명화된 OpenID 를 발급할 수 있기 때문에 사용자가 신뢰하지 않는 OpenID 지원 사이트에서는 익명 OpenID 를 사용할 수도 있다. (그림 2)는 사용자가 OpenID 지원 사이트에 제시할 OpenID 를 선택하는 화면을 보여준다.

Microsoft 는 테스트 페이지를 통해 피드백을 수렴한 뒤, 2009 년에 실제 서비스를 제공할 예정이다[7].



(그림 2) Windows Live ID 의 OpenID 제공 화면

나. Geneva 프레임워크

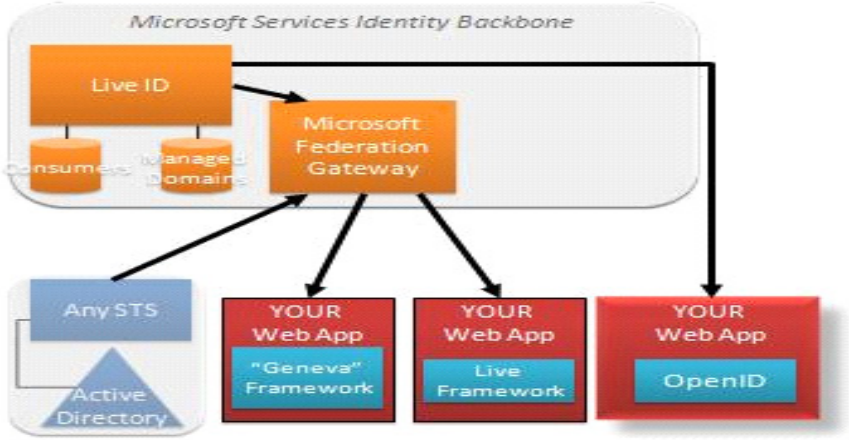
'Geneva'는 Claims 를 이용하여 사용자의 인증 및 인가 작업을 간소화시키는 Microsoft 의 오픈 플랫폼이다. Claims 는 Identity 속성을 포함하는 집합 단위로, Identity 메타시스템[8]이라는 Microsoft 의 비전을 구현한 오픈 아키텍처에서 다른 시스템의 동작을 제어하는데 사용된다. 'Geneva'는 오픈 Identity 시스템 간의 상호운용성을 지원하며, 간소화된 단일 사용자 접근 모델로 다른 애플리케이션과 시스템들에게 향상된 보안 협업 기능을 제공한다.

<표 2>와 같이 'Geneva'는 Claims 기반의 시스템 접근을 제공하는 3 가지 플랫폼 컴포넌트로 이루어진다.

<표 2> Geneva 플랫폼의 컴포넌트

컴포넌트	기능
Geneva 프레임워크	- Claims 를 인식하는 .NET 어플리케이션 작성 지원 - 사용자 인증 작업을 애플리케이션 외부(ex. STS(Security Token Services))에서 수행함
Geneva 서버	- Claims 와 다른 종류의 토큰의 발급 및 변형(transform) - 사용자 접근 관리 - 간단한 Federation 지원
Windows CardSpace	- 사용자가 접근 결정을 쉽게 하도록 지원

Geneva 플랫폼은 OpenID 를 지원한다고 알려져 있다. 이는 Geneva 플랫폼의 Identity Backbone 이 Live ID 를 지원하는데, 앞 절에서 언급한 것처럼 Live ID 가 OpenID 를 지원하기 때문이다. OpenID 처럼 매우 가벼운 공개 표준을 지원함으로써, Geneva 플랫폼은 ID 관리 솔루션을 가볍게 통합하려는 사용자에게도 효과적인 대안이 된다. (그림 3)은 Geneva 플랫폼과 OpenID 의 연동 흐름을 나타낸다[24].



(그림 3) Geneva 플랫폼과 OpenID 의 연동 흐름

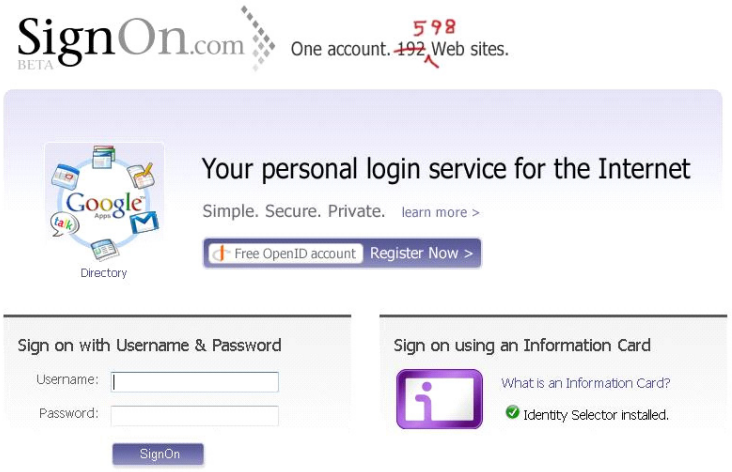
최근 발표된 Microsoft 의 클라우드(Cloud) 컴퓨팅 환경인 Azure 에서도 OpenID 를 사용할 수 있다. Geneva 플랫폼을 통해 서드파티 STS 의 Claims 를 이용하거나 직접 OpenID 제공자로부터 Claims 를 발급받아 사용하는 애플리케이션을 개발할 수 있다[9].

다. CardSpace

Windows CardSpace 는 Microsoft 가 추구하는 Identity 메타시스템에서 클라이언트 역할을 수행하는 소프트웨어이다. 사용자가 웹사이트의 서비스나 애플리케이션을 이용하는 과정에서 CardSpace 는 사이트에 제공할 Identity 정보를 선택하고 제시하는 기능을 지원한다. CardSpace 와 같은 기능을 하는 Identity 클라이언트 소프트웨어를 Identity Selector 라고 부른다. 일반적인 Identity Selector 처럼, CardSpace 는 사용자의 디지털 Identity 에 대한 정보를 보관하며 실생활에서 사용하는 카드와 같은 형태로 사용자에게 보여준다. CardSpace 의 일관된 UI 덕분에 사용자는 여러 웹사이트와 애플리케이션에서 자신의 Identity 를 쉽게 사용할 수 있다[10].

OpenID 는 주로 보안상의 문제를 해결하기 위한 방안으로 CardSpace 를 사용한다. OpenID 의 가장 큰 문제로 피싱(phishing) 공격에 취약하다는 단점이 있는데, 이를 해결하는 안전한 로그인 방식으로 CardSpace 가 사용될 수 있다. 이 경우 CardSpace 는 OpenID 프로토콜에는 전혀 영향을 미치지 않으며, 단지 OpenID 제공자에 로그인하는 방법 중 하나로 사용된다. 대표적인 적용 사례로는 Windows Live ID, PingID 의 SignOn.com 을 들 수 있다. (그림 4)는 SignOn.com 의 CardSpace 로그인 화면을 보여준다.

PingID 는 2007 년 6 월, OpenID 제공자인 SignOn.com 에 세계 최초로 Microsoft 의 CardSpace



(그림 4) SignOn.com 의 CardSpace 로그인 화면

를 지원하였다[11]. 구동 절차는 다음과 같다. 우선 사용자가 SignOn.com 사이트에 기존 ID/패스워드 방식으로 가입한 후, 부가 인증 방식으로 CardSpace 를 사용하는 방법을 추가한다. 가입 및 CardSpace 설정 이후, SignOn.com 의 메인 페이지에서 사용자가 CardSpace 를 이용한 인증 방식을 선택하고 SignOn.com 에 등록한 인증 카드를 제시하면 로그인이 처리된다.

OpenID 에 CardSpace 를 적용한 또 다른 사례로 Sxip 의 방안이 있다. 2007 년 8 월, Sxip 은 OpenID 와 CardSpace 의 호환 방안을 다룬 스펙을 공개하였다. 이 스펙에 따르면 OpenID 토큰 내용을 포함하는 인증 카드 스키마를 정의하고, 기존에 CardSpace 가 SAML 토큰을 얻는 것처럼 OpenID 토큰을 획득해야 한다. 즉, CardSpace 가 OpenID 를 하나의 인증 토큰으로 받아들이는 방안이며, 기존의 OpenID 프로토콜 또한 대폭 수정되어야 한다.

Sxip 은 스펙을 제안하는 동시에 데모 사이트[12]를 구축하여 실제 동작 과정을 체험할 수 있게 하였다. 이 방식은 OpenID 지원 사이트에 OpenID 를 직접 입력할 필요가 없다는 특징이 있다. OpenID 지원 사이트에서 CardSpace 가 구동되며, 사용자가 선택한 OpenID 제공자로부터 OpenID 토큰을 받아오기 때문에 피싱 사이트가 개입할 수 없다. 사용자는 CardSpace 의 카드 선택 화면에서 본인이 사용하고 싶은 OpenID 제공자의 InfoCard 를 선택하면 된다[13].

하지만 이 방안은 CardSpace 가 OpenID 표준을 지원해야 하고 OpenID 제공자와 지원 사이트 모두 CardSpace 를 지원해야 한다는 부담이 존재한다. OpenID 측은 CardSpace 하나를 지원하기 위해서 너무 많은 절차를 변경해야 하지만, 현재 CardSpace 의 사용빈도가 매우 낮기 때문에 효용성이 떨어진다[14]. 또한 OpenID 지원 사이트는 사용자에게 여러 가지 로그인 옵

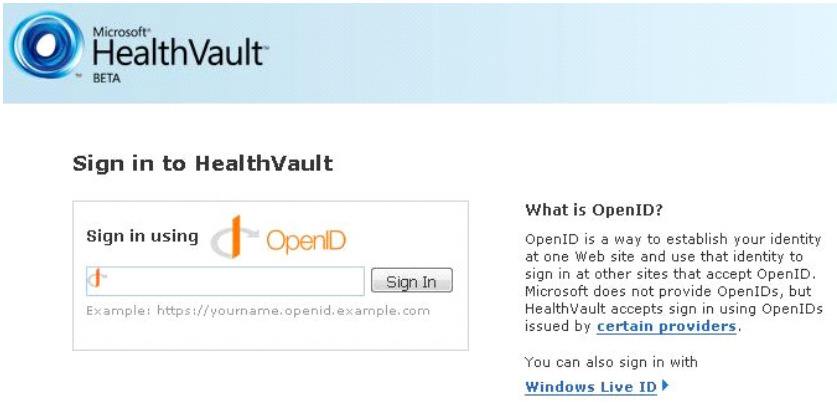
션(ID/패스워드, OpenID, CardSpace 등)을 보여주어야 하는데, 이 또한 사용자에게는 혼란스러운 경험이 될 수 있다[15].

라. HealthVault

Microsoft 의 HealthVault[16]는 개인의 건강 정보를 중앙에 수집, 저장, 공유하는 시스템이다. HealthVault 는 의료 장비, 각종 의료 기관 및 보험 회사에서 생성된 의료 정보를 개인이 일괄 조회하거나, 이를 개인이 지정한 의료 시설과 공유하는 동시에 보건 관련 검색 서비스도 제공한다. 온라인 의료기록 서비스와 함께 의료 전문 검색 엔진의 보안을 강화한 버전인 헬스볼트 서치(HealthVault Search) 기능 또한 포함된다[17]. 향후 온라인 의료 서비스는 급증할 것으로 예상되며, Google 또한 의료 서비스인 GoogleHealth 를 제공하고 있다[18].

HealthVault 가 취급하는 건강 정보는 ID 정보 중에서도 매우 민감한 수준에 해당하기 때문에 인증을 비롯한 보안 기술이 중요하게 고려되어야 한다. 초기 HealthVault 사이트는 Windows Live ID 의 인증체계만 지원하였다. 그러나 2008 년 6 월, HealthVault 는 Live ID 뿐만 아니라 OpenID 를 지원한다는 계획을 공개하였으며, 2008 년 11 월 현재 OpenID 를 지원하고 있다. (그림 5)는 HealthVault 의 OpenID 로그인 화면을 보인다.

OpenID 의 보안 문제를 고려하여 HealthVault 는 VeriSign[19], TrustBearer[20], My OpenID[21]의 OpenID 만 허가한다. VeriSign 은 Seatbelt 솔루션을 통한 피싱 대응 기술과 기타 보안 수준이 높으며, TrustBearer 는 하드웨어 토큰을 로그인 과정에 사용한다[22]. 그리고 MyOpenID 는 가장 많은 가입자를 보유한 OpenID 제공자이며, 클라이언트용 SSL 인증서를 로그인 과정에서 사용할 수 있다. HealthVault 측은 추가로 two-factor 인증이나 하드웨어 토큰,



(그림 5) HealthVault 의 OpenID 로그인 화면

SSL 같은 부가 항목을 만족시키기 위해 OpenID 의 PAPE 스펙[23] 활용을 고려 중이다.

HealthVault 의 사례는 Geneva 플랫폼과도 관련되어 있다. HealthVault 가 받아들이는 Open ID 는 몇 개의 신뢰하는 OpenID 제공자에서 나오는데, 이들은 모두 Microsoft 의 서비스 수준을 만족하는 안전한 Claims 제공자들이다. Microsoft 서비스의 Identity Backbone 은 HealthVault 모듈을 하나의 파일럿 프로젝트로 진행하고 있으며, Microsoft Federation Gateway 레벨에서 다른 Identity 제공자와 동일하게 구성한다[24].

3. Google

가. Bloggers

2007 년 11 월, Google 은 자사의 블로그 서비스인 Bloggers 에 시범적으로 OpenID 를 이용한 덧글달기 기능을 제공하였다[25]. Bloggers 서비스의 덧글 시스템은 각 사용자가 덧글 정책을 설정할 수 있는데, 기존에는 '익명 사용자', 'Google 계정이 있는 사용자', '해당 블로그의 구성원만' 덧글을 달도록 정할 수 있었으나 시범 서비스에서는 OpenID 를 보유한 사용자도 덧글을 쓰도록 설정할 수 있다.

(그림 6)은 Bloggers 서비스에서 덧글을 쓸 때, 사용할 ID 를 선택하는 화면이다. OpenID 를 지원하는 AOL/AIM, 라이브저널, TypeKey, Wordpress 뿐만 아니라, 기타 모든 OpenID 도 사용할 수 있다.

(그림 6) Bloggers 의 덧글 로그인 화면

2008 년 1 월, Google 은 Bloggers 서비스에 OpenID 를 정식으로 지원하였다. 시범 서비스에서 수행했던 것처럼 Bloggers 는 OpenID 지원 사이트의 역할을 수행하여 사용자는 OpenID 로 덧글을 달 수 있다[26]. 또한 Bloggers 계정을 이용하여 OpenID 제공자의 역할도 수행한다. Bloggers 서비스는 각 사용자 블로그에 아래와 같이 OpenID 제공자를 알려주는 Delegation 기능을 제공하는데, OpenID 제공자의 주소가 'http://www.blogger.com/openid-server.g'임을 확

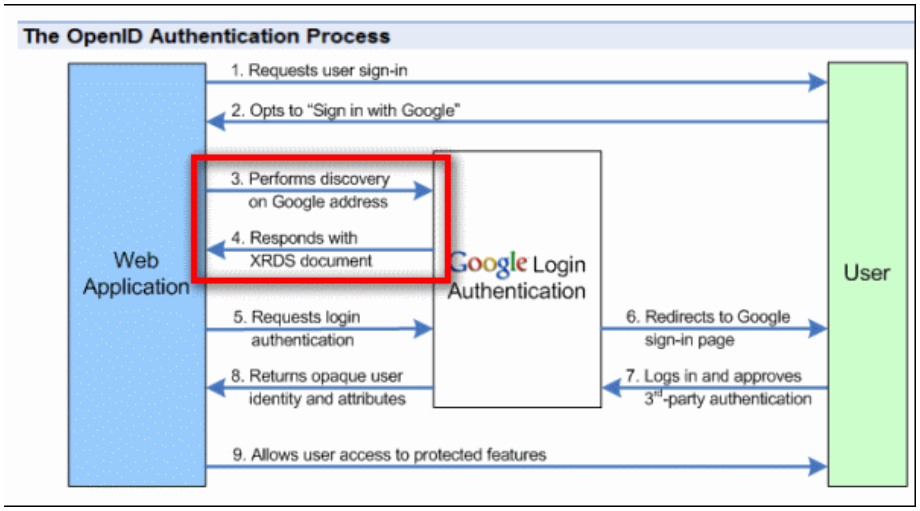
인할 수 있다. 이 OpenID 제공자는 Google 의 사용자 계정이 아니라, Bloggers 서비스의 사용자 계정 정보를 이용한다.

```
<link rel="openid.server" href="http://www.blogger.com/openid-server.g"/>
```

OpenID 제공자로서 Bloggers 는 OpenID 인증 스펙 v2.0 을 지원한다. 그리고 OpenID 지원 사이트로서, Bloggers 는 OpenID 인증 스펙 v1.1 과 v2.0 을 지원한다.

나. Gmail

2008 년 10 월, Google 은 OpenID 제공자가 되었음을 발표하였다. Google 의 OpenID 는 타 OpenID 지원 사례와 구분되는 2 가지 특징이 있다. 첫번째는 OAuth 의 지원이다. OpenID 지원 사이트가 사용자의 정보를 추가로 요청할 경우, 가령 Google 의 Data API 혹은 Portable Contact 와 OpenSocial API 등으로 데이터를 요구할 때, Google 은 OAuth 를 통해 사용자의 허락을 받게 된다. 두 번째는 기존의 OpenID 대신 Gmail 주소를 OpenID URL 에 사용하는 방안이다. (그림 7)에서 3 단계는 기존 URL 방식의 OpenID 가 아니라, 제시된 Gmail 을 이용하여 XRDS 를 가져오는 절차를 보인다[27].

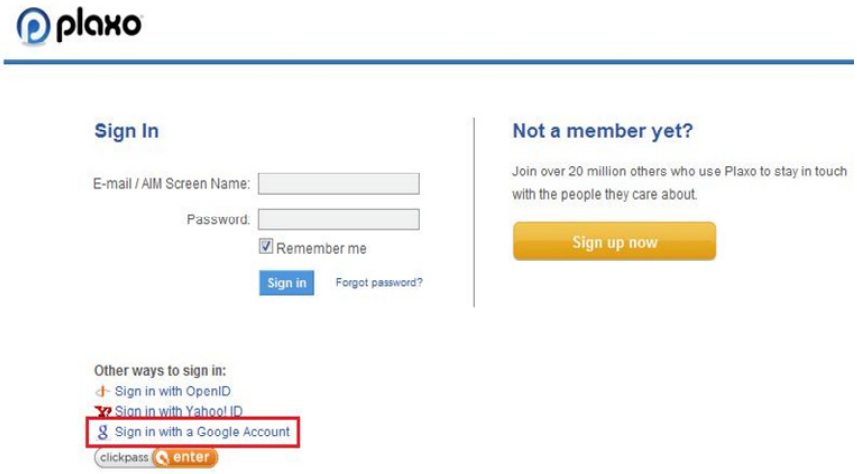


(그림 7) Google 의 OpenID 인증 흐름

OpenID 커뮤니티에서도 Email 주소를 OpenID 로 사용하는 방안을 고려한 적이 있었지만, 프라이버시와 스팸 문제를 우려하여 채택하지 않았다. 하지만 Google 은 사용자 편의성을 고려할 때 URL 방식의 OpenID 는 좋지 않다고 평가하였다. Email 을 사용하는 방식은 현재의 OpenID

표준이 허용하지 않으므로 기존의 OpenID 지원 사이트들은 사용할 수 없으며, 별도로 URL 이 아닌 Email 형식의 OpenID 를 해석하는 모듈이 필요하다.

실제 적용을 위하여, Google 은 협력 사이트에서 Google 계정으로 OpenID 를 사용하는 방법 및 절차를 제공하였다[28]. Google 은 Plaxo 나 Zoho 처럼 협력 관계를 맺고 있는 OpenID 지원 사이트에 대하여 "Sign in with Google" 버튼을 추가하였다. 이 버튼은 'https://www.google.com/accounts/o8/id'라는 OpenID 제공자를 지정하고 있기 때문에, 사용자가 버튼을 누르면 해당 OpenID URL 로 이동하여 XRDS 를 가져온 뒤 로그인을 할 수 있다. 또한 OpenID URL 입력 창에 Gmail 주소를 입력하여 Google 의 계정으로 매핑하는 방법도 제공한다. (그림 8)은 Plaxo 의 로그인 화면을 보인다. 로그인 버튼 아래에 있는 링크를 클릭하면 Google 계정으로 로그인할 수 있다.



(그림 8) Google 로그인 버튼이 추가된 Plaxo 의 로그인 화면

Google 은 자사의 여러 Data API 와 함께 인증 API 를 제공한다. Google 은 Federated 로그인 단계에 OpenID 인증 스펙 v2.0 을 지원하며, 개발자는 인증 API 를 통해 사용자의 Google 계정 정보를 이용한 로그인을 처리할 수 있다[29].

Google 에 가맹된 사이트가 아니더라도 OpenID 를 사용할 수 있다. 사용자가 OpenID URL 로 'https: //www.google.com/accounts/o8/id'를 직접 입력할 경우, OpenID 인증 스펙 v2.0 기반의 OpenID 지원 사이트에 로그인 할 수 있다[30].

(그림 9)는 국내 OpenID 지원사이트인 Springnote 에 Google 의 OpenID 로 로그인하는 화면을 보인다. 사용자가 Springnote 에서 OpenID URL 로 'https://www.google.com/accounts/o8/id'

(그림 9) Google 의 OpenID 로그인 확인 화면

를 입력한 뒤 Google 로 이동하여 로그인을 완료하면, (그림 9)와 같이 Springnote 에 로그인 정보를 제공할 지 물어보는 화면이 출력된다. '계속해서 로그인 진행' 버튼을 누르면 Springnote 에 로그인되는 화면을 확인할 수 있다.

Google 은 OpenID 제공자가 되었지만, Bloggers 를 제외한 OpenID 지원 사이트가 될 계획은 현재 없다. Google 의 담당자에 따르면, Google 이 OpenID 를 완전히 지원하기 어려운 이유는 Google Apps 와 같은 리치(rich) 클라이언트에 로그인 절차가 하드코딩 되었기 때문이다. 코드를 수정하는 작업은 간단하지만 Google 의 다른 파트 전체의 동의를 얻어야 하기 때문에 OpenID 지원사이트가 되기는 쉽지 않다.

다. 로그인 테스트

2008 년 9 월, Google 은 Federated 로그인의 사용성과 관련된 연구 결과를 발표하였다. 이 연구의 목표는 사용자들이 이미 알고 있는 기존의 로그인 개념을 최대한 이용하는 동시에 사용성을 고려한 새로운 로그인 개념을 설계하는 것이다. 또한 대규모 적용을 고려하여, 확장성과 점진적인 개선을 지원할 수 있는 로그인 개념을 지향한다[31].

대규모 적용을 고려하여 Google 은 OpenID 를 염두에 두고 있다. 사용자 인터페이스는 RP(Relying Party, 지원 사이트)가 여러 IDP(ID Provider, ID 제공자)를 신뢰할 수 있도록 설계되어야 하며, 다양한 Federation 프로토콜(OpenID, SAML, 또는 AOL, Yahoo, Microsoft, Google 이 사용하는 전용 프로토콜)을 지원할 수 있어야 한다. 일반적인 RP 는 소수의 큰 IDP 가 제공하는 프로토콜을 사용하지만, OpenID 는 RP 가 다수의 IDP 를 지원할 수 있기 때문에 대규모 적용에 적합하다는 평가를 받았다[32].

Google 은 OpenID 스펙과는 달리 Email 주소를 OpenID 로 사용하는 방안을 추진 중이다. OpenID 커뮤니티 일각에서는 Google 이 OpenID 스펙을 따르지 않았다며 불쾌한 반응을 보이지만, Google 은 OpenID 표준이 개선될 것으로 믿고 있다. Google 은 RP 가 IDP 와 상호동작하

기 위해 필요한 자동 OpenID 디스커버리 메커니즘, 특정 IDP 가 지원하는 인증 방법을 확인하는 방법 등을 OpenID 스펙에 추가한 상태이다.

그러나 보안과 관련해서는 마땅한 해결책을 제시하지 못하고 있다. 현재 OpenID 커뮤니티에서는 툴바를 이용하거나 Yahoo!의 Sign In Seal 같이 쿠키를 이용한 피싱사이트 판별 기술 등이 활용되고 있다. Google 의 연구 보고서에는 피싱(phishing)을 고려해야 할 이슈라고 언급하지만, 적절한 대응책은 제시하지 않고 있다.

III. 결 론

본 고에서는 Yahoo!, Microsoft, Google 의 OpenID 제공 및 지원 사례에 대해 살펴보았다. 국내외의 대형 포털을 비롯한 여러 사이트에서 OpenID 를 제공하고 있지만 일반 대중이 쉽게 OpenID 를 사용하며 모든 사이트가 OpenID 를 지원하기 위해서는 많은 시간과 노력이 필요하다.

ETRI 디지털 ID 보안연구팀은 OpenID 의 보안성과 사용자 편의성을 강화한 기능을 전자 ID 지갑 솔루션에 추가하였다. 전자 ID 지갑의 로그인 서비스는 사용자가 기존에 발급받은 카드 형식의 로그인 정보를 선택하면 해당 사이트와 상호인증 절차를 거쳐 서로의 신원을 확인한다. OpenID 제공자에 전자 ID 지갑 솔루션을 구축하면 해당 사이트를 직접 방문하여 ID/PW 를 입력하지 않아도 안전하게 서비스를 제공받을 수 있다. 또한 OpenID 지원 사이트에서 전자 ID 지갑을 자동으로 구동할 수 있으며, OpenID 제공자 카드를 선택하는 것으로 OpenID URL 를 자동으로 입력 및 제출할 수 있다. 이 과정에서 OpenID 지원 사이트는 별도의 작업 없이도 전자 ID 지갑을 사용하게 된다.

또한 OpenID 커뮤니티는 보안이나 사용자 경험(UX)의 개선을 통해 안정성을 높이고 있으며, 여러 워킹 그룹에서 다양한 확장 기능에 대한 기술 및 스펙 작업을 진행 중이다. 이러한 추세에 발맞추어, OpenID 는 더욱 다양한 분야에 적용될 전망이다.

<참 고 문 헌>

[1] Mark Brownlow, “Email and webmail statistics”, EMAIL MARKETING REPORT, Apr. 2008.
[2] http://www.businesswire.com/news/google/20080117005332/en
[3] http://www.flickr.com
[4] Marshall Kirkpatrick, Flickr to Authenticate OpenID –Is This The Yahoo! CES Announcement?, http://www.readwriteweb.com/, Jan. 2008.
[5] Simon Willison, “Yahoo! Flickr, OpenID and Identity Projection”, http://simonwillison.net/, Jan. 2008.

[6] Beverly Freeman, "Yahoo! OpenID: One Key, Many Doors", OpenID User Experience Research, Jul. 2008.
[7] Mike Walker, "Windows Live ID now supports OpenID Identity Framework", MSDN, Oct. 2008.
[8] Microsoft Corporation, "Microsoft's Vision for an Identity Metasystem", MSDN, Jul. 2005.
[9] Kim Cameron, "Project Geneva – Part 4", http://identityblog.com, Nov. 2008.
[10] http://en.wikipedia.org/wiki/cardspace
[11] Phil Windley, "Linking OpenID and CardSpace: SignOn.com", http://www.windley.com/, Jun. 2007.
[12] https://openidcards.sxip.com/
[13] Mike Jones, "Information Cards for OpenID", http://self-issued.info/, Aug. 2007.
[14] Gerald Beuchelt, "OpenID InfoCards: Painful or Promising?", http://beuchelt.blogdns.net/, Aug. 2007.
[15] Eric Norman, "Law 7 and OpenID Information Cards", http://ejnorman.blogspot.com/, Aug. 2007.
[16] http://healthvault.com
[17] Ina Fried, "Microsoft plans medical-record service", CNET News, Oct. 2007.
[18] https://www.google.com/health/
[19] http://pip.verisignlabs.com
[20] http://openid.trustbearer.com
[21] http://www.myopenid.com
[22] Jason Kincaid, "Microsoft's First Step In Accepting OpenID SignOns –HealthVault", http://www.techcrunch.com/, Jun. 2008.
[23] D. Recordon, J. Bufu, J. Hoyt, "OpenID Provider Authentication Policy Extension 1.0-Draft 2", OpenID Community, Oct. 2007.
[24] Kim Cameron, "Project Geneva – Part 5", http://www.identityblog.com/, Nov. 2008.
[25] "New feature: OpenID commenting", http://bloggerindraft.blogspot.com/, Nov. 2007.
[26] Duncan Riley, "Google Offers OpenID Logins Via Blogger", http://www.techcrunch.com/, Jan. 2008.
[27] Frederic Lardinois, "Google Clarifies Its OpenID Implementation", http://www.readwriteweb.com/, Oct. 2008.
[28] "Federated Login for Google Account Users", http://code.google.com/
[29] Frederic Lardinois, "Google is Now an OpenID Provider", http://www.readwriteweb.com/, Oct. 2008.
[30] Frederic Lardinois, "Google Clarifies Its OpenID Implementation", http://www.readwriteweb.com/, Oct. 2008
[31] Eric Sachs, "Usability Research on Federated Login", http://sites.google.com/site/oauthgoog/UXFedLogin, Sep. 2008.
[32] Eric Sachs, Yariv Adan, Dirk Balfanz, Breno de Medeiros, Brian Eaton, "Google OAuth & Federated Login Research", http://sites.google.com/site/oauthgoog/Home, Sep. 2008.

* 본 내용은 필자의 주관적인 의견이며 IITA 의 공식적인 입장이 아님을 밝힙니다.