인터넷 ID 관리 시스템 개요 및 비교

Overview and Comparison of Internet Identity Management System

조영섭 (Y.S. Cho) 디지털ID보안연구팀 선임연구원
진승헌 (S.H. Jin) 디지털ID보안연구팀 팀장

목 차

인터넷의 확산과 웹 2.0 환경의 도래에 따라, 사용자가 관리해야 하는 디지털 형태의 ID 정보가 기하 급수적으로 증가하고 있다. 이것은 사용자의 ID 관리 부담, 동일한 패스워드의 반복적인 사용으로 인한 보안성 저하, ID 정보의 유출에 의한 사용자 프라이버시 침해 문제 등을 발생시키고 있다. 따라서 사용자를 인증하고, 사용자의 ID 정보를 관리해주는 ID 관리 시스템이 매우 중요해지고 있다. 본 고에서는 인터넷 규모의 온라인 서비스를 대상으로 사용자를 인증하고 사용자의 ID 정보를 관리하는 대표적인 ID 관리 시스템인 SAML, CardSpace, OpenID를 살펴 보고, 이들 시스템의 특징을 비교 분석한다.

Ⅰ. 서론

인터넷의 확산과 발전에 따라 인터넷을 이용한 전자상거래가 활성화되고 있다. 다양한 전자상거래, 웹 포털, 게임 등에 대한 참여를 통해 사용자는 기존 오프라인 생활뿐만 아니라 다양한 온라인 생활을 영위할 수 있게 되었다. 일반적으로 온라인 응용 서비스 제공자들은 사용자에게 서비스를 제공하기 위해 사전에 사용자들이 개인정보를 등록하고, 사용자 식별자인 Id(Identifier)와 패스워드를 등록하도록 하고 있다.

그러나 사용자들이 온라인에서 사용하는 서비스가 증가함에 따라, 사용자들에게 발급된 Id와 패스워드는 그 수가 기하급수적으로 증가하고 있다. 사용자들은 이들 정보를 관리하기 위해 자신의 계정 정보를 문서로 관리하거나 또는 동일한 Id와 패스워드를 반복 사용하고 있는 실정이다. 이것은 하나의 Id와 패스워드만 유출되더라도 모든 서비스에서 사용자의 계정이 유출되는 문제를 발생시킨다.

또한 사용자가 온라인 서비스 제공자에 등록한 개인정보는 서비스 제공자의 관리 부실 또는 해킹 등에 의해 유출이 되는 경우가 발생하고 있다. 이와 같은 사용자 Id와 패스워드의 분실 및 관리 문제, 개인정보 유출의 위협은 인터넷 서비스 발전에 저해 요인으로 작용하고 있다. 이와 같은 문제는 사용자의 참여와 정보 공유가 더욱 많아질 웹 2.0 환경과 수많은 정보기기에서 정보를 유기적으로 공유하며 서비스를 제공할 유비쿼터스 환경에서 더욱 커질 것으로 예상된다[1].

본 고에서는 사용자의 Id, 패스워드, 개인정보로 구성된 ID (Identity)를 안전하게 관리하는 ID 관리 시스템(IDMS) 중에서 최근에 특히 많이 연구되고 활용되고 있는 인터넷 규모의 ID 관리 시스템에 대하여 고찰한다. 본 고에서는 대표적인 인터넷 ID 관리 시스템인 SAML, CardSpace, OpenID의 개요를 기술하고 이들 시스템에 대한 특징을 비교 분석한다.

● 용 어 해 설 ●

Identity: Identity는 사전상으로 "개인의 구별되는 특징이나 개성"을 의미하며, 개인의 특징, 신상정보, 선호도 같은 것들을 모두 포함하는 정보로 일반적으로 사용자의 Id, 신상정보, 비신상정보, credential로 구성된다.

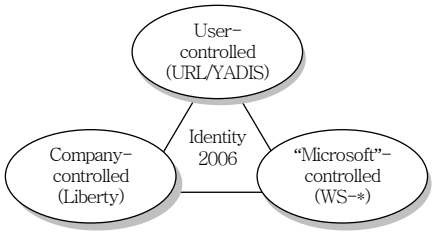
Ⅱ. ID 관리 기술 연구 동향

NetMesh의 CEO이자 YADIS 프로젝트를 운영하고 있는 Johannes Ernest는 2006년 현재 ID 관리 시스템들의 현황을 세 가지 유형으로 분류하였다[2]. (그림 1)은 ID 관리 시스템의 유형을 도식화한 것이다.

Company-controlled Identity는 기업이 개인에게 ID를 부여한 뒤 개인이 어떤 ID를 관리하고 공유할 것인가를 결정한다. Liberty Alliance[3] 표준에 기반한 ID 관리 시스템이 대표적이며, 2007년 현재 Liberty Alliance 표준에 기반한 ID와 장치들이 정부, 교육, 의료 등의 다양한 분야에 10억 개가 넘게 적용되고 있다.

Microsoft-controlled Identity는 WS-* 표준에 기반한 ID 관리 시스템으로, Kim Cameron이 Law of Identity를 통해 주장한 ID 메타시스템이 CardSpace[4]로 구현된 것이다. CardSpace는 OASIS 표준인 WS-Security를 기반으로 하여 X.509, Kerberos, SAML과 같은 보안 토큰 포맷을 모두 사용할 수 있으며 Windows Vista를 통해 광범위하게 적용될 것으로 예상된다.

User-controlled Identity는 ID 제공자(IdP), 개인정보, ID 사용 정책을 개인이 통제하는 시스템으로 기업에 속한 ID가 아니라 사용자 스스로 ID를 생



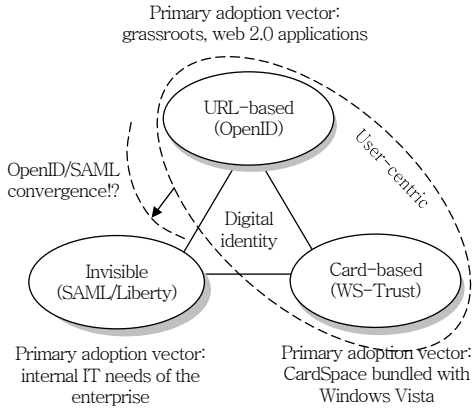
<자료>: http://netmesh.info/jernst

(그림 1) The Identity Landscape 2006

성하고 관리하는 것을 특징으로 가진다. 대표적인 User-controlled Identity로는 URL을 ID로 사용하는 OpenID[5], LID[6], YADIS[7]를 들 수 있다.

이와 같은 분류는 2006년도에 ID 분야에 대한 연구가 광범위하게 진행되고 이에 따라 서로간의 융합이 진행됨에 따라, 2006년도 12월에 (그림 2)와 같이 갱신되었다[8].

URL-based는 기존의 다양한 URL-based 기술들이 OpenID로 통합되는 경향을 보이며 주로 블로그 등과 같은 웹 2.0 응용 영역에서 활용된다. In-visible은 Company-controlled를 대체하며 주로 기업 내부 또는 기업 간의 ID 영역에서 활용된다. Card-based는 Microsoft-controlled를 대체하며 사용자가 card 형태로 자신의 ID 정보 제공을 선택할 수 있으며 CardSpace는 MS의 vista 운영체제와 함께 제공된다.



<자료>: http://netmesh.info/jernst/

(그림 2) The Identity Landscape 2006 Updated

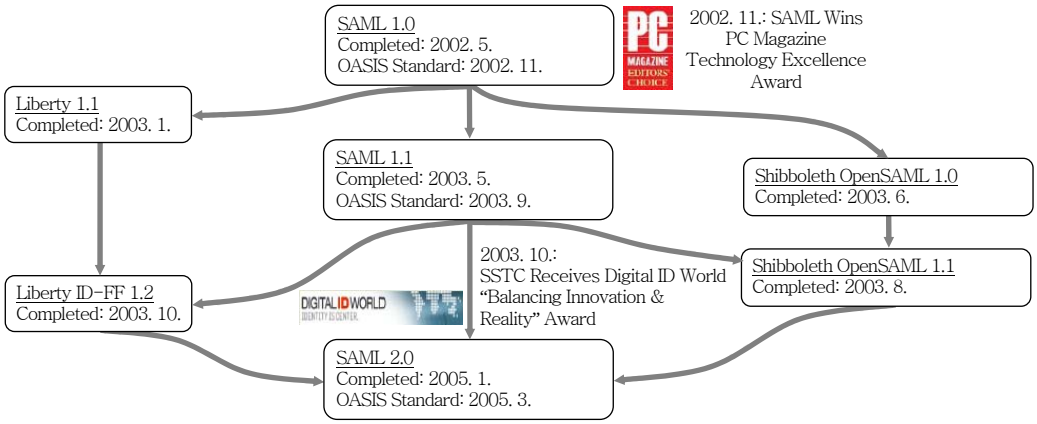
Ⅲ. 인터넷 ID 관리 시스템

본 장에서는 대표적인 인터넷 ID 관리 시스템인 SAML, CardSpace, OpenID에 대하여 기술한다. 기존 ID 관리 시스템이 기업 내부 또는 기업과 파트너 사와의 ID 통합 및 관리에 초점을 둔 반면, 인터넷 ID 관리 시스템은 인터넷 상에서 일반적인 온라인 서비스에 쉽게 적용할 수 있다는 특징을 가지고 있다.

1. SAML

SAML[9]은 보안관련 ID 정보의 통신을 위한 XML 기반 프레임워크로서 OASIS SSTC에서 표준화가 진행되고 있다. SAML 표준은 ID assertion의 구조와 프로토콜, assertion을 HTTP 등과 같은 하부 프로토콜로 매핑하는 바인딩과 브라우저 SSO, 웹 서비스 보안 등과 같은 일반적으로 사용하는 경우에 상호운용성을 확보하기 위한 프로파일 등으로 구성된다.

(그림 3)은 OASIS SAML 표준화 진행 상황을 도



<자료>: Liberty Technology Tutorials, Liberty Alliance

(그림 3) SAML 표준화 진행

식화한 것이다.

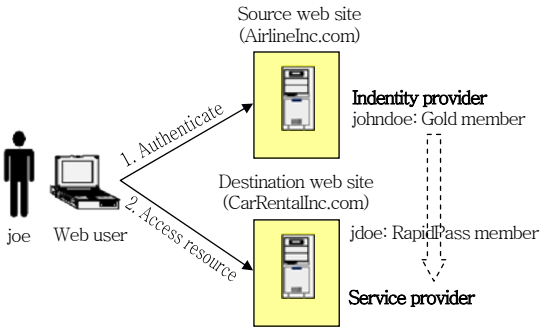
(그림 3)에서와 같이 SAML은 초기 version 1.0에서 1.1 그리고 현재 2.0이 제정된 상태이다. SAML은 Liberty Alliance와 Shibboleth와 같은 ID 관련 표준안들의 내용을 수용하면서 진화해 왔다. 2006년 SAML 2.0은 ITU-T에 제출되어 X.1141로 표준화 되었다.

(그림 4)는 SAML의 동작 흐름 예를 보인다.

(그림 4)에서 사용자는 IdP에 Johndoe라는 이름으로 계정을 가지고 있으며, SP에는 jdoe라는 이름의 계정을 가지고 있는 상태이다. 사용자가 SP에 접근하여 서비스를 요청하게 되면, SP는 IdP에게 사용자의 인증을 요청한다. 사용자는 IdP에게 인증을 받고 IdP는 사용자의 인증 결과를 SP에게 전달한다. SP는 IdP의 인증 결과를 바탕으로 사용자에게 서비스 제공 여부를 결정하게 된다. 이 경우에 IdP와 SP는 서로 신뢰 관계를 사전에 설정하고 있으며, 동일한 사용자에 대하여 각기 서로 상대방에서 어떠한 이름으로 식별하는지에 대한 연계 record를 가지고 있게 된다.

SAML은 현재 enterprise 수준의 ID 관리 기술에서 핵심적으로 사용되는 표준으로 상대적으로 높은 보안성, 상호운용성 및 유연성을 제공하고 있다. 그러나 블로그에서 댓글을 작성할 때와 같이 단순히 사용자 인증만을 제공하는 환경에 활용하기에는 복잡한 측면이 있다. 이것은 SAML이 상대적으로 프로토콜이 무겁고 시스템 부하를 많이 요구하는 전자서명, XML 문서 처리 등을 필수적으로 요구하기 때문이다.

최근 SAML은 이와 같이 문제를 해결하기 위해 XML 전자서명을 무시하거나 또는 단순한 서명 메커니즘으로 대체하는 SAML SimpleSign 바인딩과 같이 경량화된 표준을 제정하고 있다.



<자료>: SAML V2.0 Technical Overview, OASIS

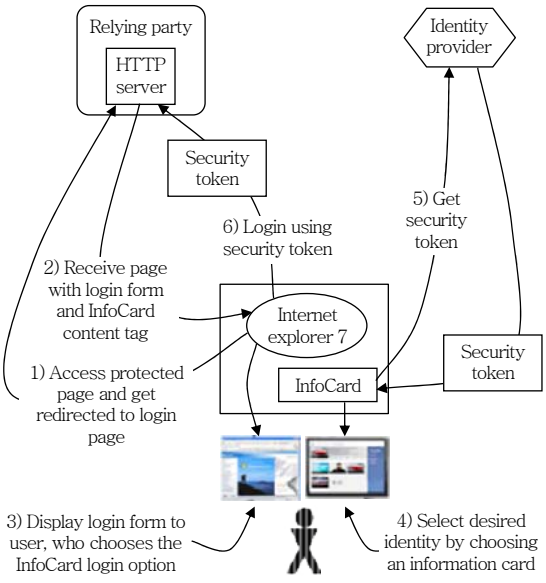
(그림 4) SAML 동작 흐름도

2. CardSpace

CardSpace[8]는 Window Vista 운영체제와 함께 탑재된 응용 프로그램이다. CardSpace는 사용자의 ID 정보를 InfoCard라 불리는 카드 형태로 관리한다. InfoCard는 사용자에게 ID 정보를 제공하는 IdP의 위치와 해당 IdP에서 발급하는 실제 사용자 ID 정보가 무엇인지를 시각화하여 사용자에게 제공한다. 즉 CardSpace는 실제 사용자의 ID 정보를 발급하는 IdP 역할을 수행하지 않고, IdP들에 대한 정보를 제공하는 ID 메타시스템의 역할을 수행한다.

(그림 5)는 CardSpace의 동작 흐름을 보인다.

먼저 사용자가 서비스 제공자(RP)에서 서비스를 요청하면, RP는 CardSpace를 구동시킬 수 있는 특



<자료>: Introducing Windows CardSpace, Microsoft MSDN

(그림 5) CardSpace 동작 흐름도

별한 태그를 가지고 있는 로그인 페이지를 사용자 브라우저(IE 7.0)에 전달한다. 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 선택하며, 선택된 card 정보에 따라, 해당 ID 제공자인 IdP에게 사용자 정보가 요청된다. IdP가 사용자 정보를 CardSpace에게 전달하면, CardSpace는 이 정보를 다시 RP에게 전달하게 된다.

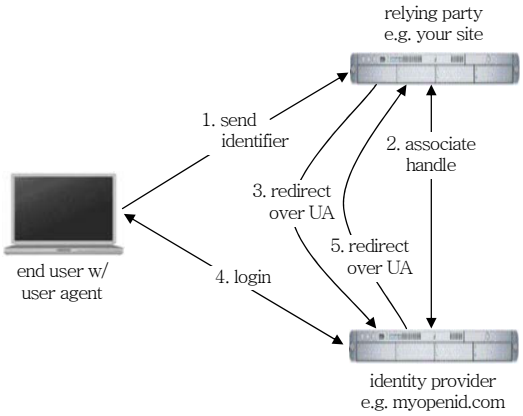
CardSpace는 일반적인 사용자 환경이 아닌, 시스템 환경에서 동작하기 때문에 높은 보안성을 제공하며, RP가 정보를 처음 요청할 때 사용자에게 RP에 대한 시각정보를 제공하여 RP의 수용 여부를 판단할 수 있도록 지원함으로써 피싱 공격 등을 완화시키는 장점이 있다.

3. OpenID

OpenID는 URI 기반 ID 개념을 근간으로 설계된 경량화된 ID 시스템이다. OpenID는 초기부터 매우 단순한 사용 환경을 목적으로 설계되었다. 즉, 블로그가 신원이 확인되지 않은 사용자들의 댓글로 인해 공격 받는 등의 문제를 해결하는 것이 초기 목적이었다. 따라서 OpenID는 초기부터 다른 ID 기술에 비해 복잡성이 제거되었고, 이는 최근 사용자들의 참여가 확대되는 웹 2.0 환경에 쉽게 적용될 수 있는 장점으로 작용한다.

(그림 6)은 OpenID가 동작하는 예를 보이고 있다.

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



<자료>: OpenID Open Distributed Identity Management, http://openid.net/

(그림 6) OpenID 동작 흐름도

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. 최근에는 조직 변경 등으로 인해 URL의 링크가 깨지는 문제를 해결하기 위해 제안된 XRI를 사용자의 식별자로 활용할 수 있도록 확장되고 있다. 또한 OpenID는 공개된 프로토콜을 이용하며 별도의 비용을 요구하지 않는 무료 기술이기 때문에 진입 장벽이 낮으며 추가적인 비용이 많이 발생하지 않는 장점을 가지고 있다.

그러나 OpenID는 사용자들이 하나의 ID를 가지고 여러 서비스를 이용하기 때문에 RP간의 공모를 통해 사용자의 행동 패턴이 인지될 수 있다는 문제와 ID 정보공유 등에서 제약을 가지고 있다. 또한 적용서비스와 개인정보 제공 범위에 따라 IdP에 대한 신뢰성 미흡으로 인한 프라이버시 문제가 발생할 수 있다. 최근 OpenID 2.0에서는 이와 같은 문제를 보완하기 위한 작업이 진행되고 있다.

Ⅳ. 인터넷 ID 관리 시스템 비교

본 장에서는 ID 시스템을 구분하는 중요한 요소인 식별자, 속성정보 제공, 인증, ID 정보흐름, IdP 발견 방식을 기준으로 앞장에서 설명한 SAML, CardSpace, OpenID의 특징을 분석한다.

1. 식별자

RP 또는 SP에서 사용자를 식별하기 위해 사용하는 Id는 ID 시스템을 구별하는 중요 인자이다. 특히, 서로 다른 RP에서 사용하는 사용자 식별자(Identifier)가 동일할 경우, RP들의 공모에 의해 사용자의 행동 패턴이 확인될 수 있다는 점에서 ID 관리 기술이 채택하는 식별자는 사용자 프라이버시에 중요한 영향을 미친다.

일반적으로 ID 시스템에서 사용하는 사용자 식별자는 다음과 같이 분류할 수 있다.

• Global 식별자

사용자가 모든 RP에서 하나의 식별자만을 사용한다. 이 방식은 매우 단순하여 구현이 쉽지만, RP들의 공모로 인해 사용자의 행동 패턴을 알 수 있다는 점에서 사용자 프라이버시가 침해될 수 있다는 문제를 가지고 있다. 또한, 사용자 Id와 패스워드가 유출되는 경우, 모든 RP 서비스에서 사용자 계정이 유출되는 문제가 발생한다는 단점을 가지고 있다.

• Pair-wise Pseudonyms

이 방식에서는 사용자에 대하여 IdP와 RP 사이에만 유일하게 존재하는 쌍방향 pseudonym을 식별자로 사용한다. RP들이 사용자를 식별하는 식별자가 서로 다르기 때문에 RP들의 공모에 의해 사용자의 프라이버시가 침해될 우려는 없다.

• 일회성 식별자

이 방식은 사용자가 RP에 접근할 때마다 일회성(one-time) 식별자를 제공한다. 이 방식에서는 RP조차도 접근하는 사용자를 식별할 수 없기 때문에 사용자의 프라이버시 침해 문제가 발생하지 않는다. RP는 식별자를 통해 사용자를 식별하기 보다는 사용자의 권한 등과 같은 다른 정보를 이용하여 사용자를 식별하게 된다.

SAML은 위에서 기술한 모든 타입의 식별자를 지원하며, 특히 pseudonym을 잘 지원할 수 있도록 여러 가지 메커니즘을 정의하고 있다.

CardSpace는 self-issued 또는 제 3의 기관에서 RP들이 사용자를 식별할 수 있도록 해주는 PPID를 발급하는 것을 허용한다. PPID는 IdP와 RP 사이에서 사용자를 식별할 수 있도록 해주는 쌍방향 pseudonym이다.

OpenID는 사용자 식별자로 URL과 XRI를 사용한다. 즉 global 식별자를 지원한다.

2. 속성 정보

ID 관리 시스템의 주요 역할 중의 하나는 RP들이 사용자에게 서비스를 제공하기 위해 필요한 사용자 정보를 제공하는 것이다. 이때 IdP가 제공하는 정보를 일반적으로 사용자 ID 정보 또는 속성 정보라 부른다.

SAML은 속성 정보를 제공하기 위해 속성 assertion을 제공한다. 속성 assertion은 확장 가능한 XML 스키마로 정의되어 있어, 현재 가능한 모든 정보와 향후 필요한 정보까지도 수용할 수 있다.

CardSpace는 자신이 설치된 PC에서 사용자의 이름, 주소, 이메일 등과 같은 개인 정보 프로파일을 제공하는 IdP를 제공한다. 이것은 매우 특수한 IdP로 self-issued IdP가 된다. 따라서 CardSpace 자체에서는 사용자의 개인정보 프로파일에 초점을 맞춘 속성 정보만을 제공한다. 또한, CardSpace는 제3의 IdP들이 자체적으로 사용자의 ID 속성 정보를 제공하는 것을 허용한다. 이때 제공되는 속성 정보는 IdP가 결정하며, CardSpace는 단지 IdP에서 발급된 정보를 사용자가 확인할 수 있도록 하는 메커니즘과 RP로 재전송(relay)하는 기능만을 제공한다.

OpenID는 별도의 속성 정보를 제공하는 메커니

즘을 지원하지 않았다. 그러나 최근 OpenID V2.0에서는 속성 정보를 제공하는 메커니즘을 지원한다.

3. 인증

ID 시스템은 사용자가 IdP에게 한 번만 인증을 받으면 모든 RP 서비스를 이용할 수 있도록 해주는 SSO 서비스를 제공한다.

SAML은 RP가 IdP에게 사용자 인증을 요청할 때, IdP가 어떠한 강도의 인증 방식으로 사용자를 인증해야 할지를 나타내는 인증 문맥(authentication context)을 함께 전달할 수 있다. 이 경우, IdP는 요청된 인증 문맥에 해당하는 방식으로 사용자를 인증해야 한다. 인증 문맥은 PKI, Kerberos, 생체인식, 패스워드 등과 같은 다양한 인증 방식을 지칭할 수 있다.

CardSpace에서 사용자는 RP들에게 자신이 적절한 보안 키를 가지고 있다는 것을 증명함으로써 인증을 받는다.

OpenID는 SAML의 인증 문맥과 같이 RP가 인증 강도를 설정하는 기능은 없으며, 사용자를 인증하는 것은 IdP가 판단하여 수행한다.

4. ID 정보 흐름

IdP가 RP에 사용자 ID 정보를 제공하는 방식은 다음과 같이 분류할 수 있다.

• Front Channel

ID 정보가 IdP에서 RP로 전달될 때 사용자 에이전트를 경유하는 방식을 나타낸다. 일반적으로 사용자 에이전트는 웹 브라우저가 된다.

• Back Channel

ID 정보가 IdP에서 RP로 직접 전달된다.

Front channel은 사용자가 ID 정보 흐름의 중간에 위치하고 있기 때문에 정보 흐름에 대한 실시간 사용자 동의 등과 같은 방식을 이용하여 사용자에게 개선된 프라이버시를 제공할 수 있다.

Back channel은 사용자 에이전트의 보안이 허술하거나, 사용자 ID 정보를 캐시(cache)함으로써 생기는 보안상의 문제 등을 해결할 수 있다. 또한 사용자가 오프라인 상태인 경우에도 ID 정보를 RP에 제공할 수 있다는 장점을 가진다.

SAML은 다양한 브라우저 바인딩을 통해 front channel을 지원한다. 또한 SOAP 바인딩을 통해 IdP에서 RP로 ID 정보를 직접 전달하는 back channel도 지원한다.

CardSpace의 경우에는 모든 정보가 사용자 브라우저를 경유하도록 하는 front channel만 지원한다.

OpenID는 CardSpace와 같이 front channel만 지원한다. 그러나 최신 버전인 OpenID 2.0에서는 IdP와 RP 간에 직접 ID 정보를 전달하는 back channel을 지원한다.

5. IdP 발견

RP는 사용자에게 온라인 서비스를 제공하기 위해 사용자 인증을 IdP에게 요청하며, 또한 서비스 제공에 필요한 사용자 ID 정보를 IdP에게 요청할 수 있다. 이 경우, RP는 어떤 IdP에게 사용자 인증과 ID 정보 제공을 요청할 것인지를 결정해야 한다. 이와 같이 RP가 IdP를 결정하는 과정을 IdP 발견(discovery)이라고 한다. IdP 발견을 위해 ID 시스템은 IdP 정보를 ID 시스템에 선 등록하는 과정을 요구하기도 한다.

SAML은 별도의 IdP 등록 과정을 요구하지 않는다. IdP 발견을 위해서는 쿠키(cookie) 메커니즘을 제공한다. 이것은 IdP 도메인과 RP 도메인을 동일하게 설정하고, IdP 정보를 사용자 브라우저에 도메인 쿠키로 설정하는 것이다. 이와 같은 방식을 이용하면, 사용자가 RP에 접근할 때, IdP 정보를 포함하는 쿠키가 함께 전달되어 RP에서 IdP의 위치를 확인할 수 있게 된다.

CardSpace는 사용자가 IdP 정보를 CardSpace에 설치하는 과정을 통해 IdP를 등록한다. 사용자 ID 정보를 제공하는 IdP는 CardSpace가 정의한

card 형태의 파일로 자신의 정보를 생성하여 사용자에게 제공하고, 사용자는 이 정보를 CardSpace에 설치하여 IdP를 등록하게 된다. RP가 IdP를 발견하는 방식은 CardSpace가 대행한다. RP는 자신이 필요한 ID 정보나 인증을 요청할 때, 해당 요청 정보를 일단 사용자 에이전트에게 전달한다. 사용자 에이전트에 의해 구동된 CardSpace는 RP에서 요청하는 정보와 현재 CardSpace에 설치된 IdP 정보를 비교하여 적절한 card를 사용자에게 제시하여 사용자가 직접 원하는 IdP를 선택할 수 있도록 해준다.

OpenID는 별도의 IdP 등록 과정을 제공하지 않는다. 사용자는 RP에게 서비스를 요청할 때, 자신의 식별자로 global URI를 제공한다. 이 URI는 IdP의 host 정보와 사용자 식별자로 구성된다. 따라서 RP는 식별자의 host 정보를 이용하여 IdP를 결정할 수 있게 된다.

V. 결론

본 고에서는 현재 인터넷 규모로 ID 기능을 제공하는 시스템인 SAML, CardSpace, OpenID의 개요와 기술적인 특성을 ID 시스템의 중요 요소인 식별자, 속성정보 제공, 인증, ID 정보 흐름 및 IdP 발견을 통하여 비교 분석하였다. SAML은 많은 보안성과 확장성을 제공하지만 상대적인 복잡성을 가지고 있으며, CardSpace는 직접적인 IdP 기능을 제공하지 않는 ID 메타시스템이며, OpenID는 블로그와 같은 웹 2.0 환경에서 가벼운 ID 시스템으로 활용되고 있다.

● 용 어 해 설 ●

인터넷 IDMS (Identity Management System): 애플리케이션과 웹 사이트에서 사용자 속성 정보가 공유될 수 있도록 하는 표준화된 메커니즘을 정의한 아키텍처

인터넷 ID 시스템은 각기 고유한 특징과 서로 중복되는 기능을 보유하고 있다. 향후, 인터넷 ID 시스템은 이와 같이 중복되는 기능의 제거를 위해 상호간에 통합과 융합이 발생할 것으로 예상된다.

약 어 정 리

Id	Identifier
ID	Identity
IDMS	IDentity Management System
IdP	Identity Provider
PPID	Private Personal Identifier
RP	Relying Party
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign-On
URI	Uniform Resource Identifier
XRI	eXtensible Resource Identifier
YADIS	Yet Another Decentralized Identity Interoperability System

참 고 문 헌

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

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

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

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

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

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

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