인터넷 ID 관리 서비스 기술 동향

김승현* 진승헌** 정교일***

비 대면으로 거래를 해야 하는 인터넷 환경에서 자신의 존재를 증명할 수 있는 방법은, 신뢰할 수 있는 Identity를 보여주는 것이다. 하지만 인터넷 환경에서 사용자가 이용하는 서비스의 수가 증가하면 할수록 개인이 보유하는 Identity의 수는 늘어나고, 이들을 관리하는 것뿐만 아니라 기억하는 것마저 힘들어지는 실정이다. 인터넷 ID(IDentity) 관리 서비스는 이러한 Identity 관리 문제를 해결하기 위해 제안되었다. 인터넷의 모든 Identity를 연결하여 쉽고 편안하게 인터넷을 이용할 뿐만 아니라, 개인정보를 비롯한 Identity 정보를 쉽게 관리하는 것이 인터넷 ID관리 서비스의 목적이다. 현재 인터넷 ID 관리 서비스는 SAML, 리버티 얼라이언스, WS-* 와 같은 표준들과 패스포트, 3-D Secure, 시볼레, PingID 네트워크와 같은 서비스들이 제공되고 있다. 본 고는 인터넷 ID 관리 서비스와 관련된 표준 및 서비스들의 동향을 살펴보았다.

목 차

* ETRI 인증기반연구팀/연구원
** ETRI 인증기반연구팀/팀장
*** ETRI 정보보호기반연구그룹/그룹장

I. 서 론

1969년 인터넷은 미국 국방부가 구축한 ARPANET에서 시작하여 지금은 전세계 사람들이 시간과 공간을 초월하여 만나고 정보를 공유할 수 있는 공간이 되었다. 하지만 보안을 고려하지 않았던 인터넷의 초기 개념 때문에, 현재의 인터넷 환경은 유해 정보가 범람하고 남의 정보와 사생활을 엿보며 악용하는 위험한 상황에 처해지게 되었다.

이러한 인터넷 환경에서 신뢰성을 확보하기 위해서는, 신빙성 있는 자신의 Identity를 유지해야 한다. 인터넷을 사용하는 사람은 누구나 수많은 로그인을 하게 되는데, 로그인을 한다는 것은 나의 신원을 해당 사이트에 증명하는 과정이라고 볼 수 있다. 이렇게 인터넷에서 사용하는 신원을 네트워크 Identity라고 한다.

수많은 사이트에 산재된 네트워크 Identity를 안전하게 관리해야 하지만, 네트워크 Identity가 늘어날수록 관리 부담이 가중된다. 이 문제를 해결하기 위하여 'Identity 관리'라는 개념이 등장하게 되었다. Identity 관리는 현재 기업이나 계열사 단위로 이루어지고 있으며, 개인이 관리해야 하는 Identity의 수를 줄여주는 기능을 하고 있다. 하지만 현재의 대응으로는 인터넷 레벨에서 Identity를 효율적으로 관리하기 어렵다. 따라서 '인터넷 ID 관리'가 필요한 것이다.

II. 인터넷 ID 관리

1. 네트워크 Identity

네트워크 Identity란, 여러 서비스 제공자가 보유한 개인의 식별자(Identifier)를 포함한 모든 속성 정보를 말한다. 여기서의 속성 정보로는 이름, 전화번호, 사회보장번호, 주소, 신용카드, 지불 정보 등이 포함된다. 네트워크 Identity를 개인과 기업의 입장에서 구분해 볼 수 있는데, 우선 개인의 입장에서 네트워크 Identity는 금융, 의료 기록과 같은 프라이버시 정보들을 모두 포함하는 것으로 반드시 주의 깊게 보호할 필요성이 있다. 이와는 달리 기업의 입장에서 네트워크 Identity는 고객과 구성원들에 관한 정보를 의미하며, 이를 이용하여 좀 더 나은 서비스를 제공해 줄 수 있게 된다[1].

Identity가 독자적으로 흩어져서 관리되고 있는 현재 상황에서, 개인이 네트워크 Identity를 관리하기에는 많은 어려움이 있다. 각각의 Identity를 증명하기 위해서는 해당 사이트에 설정해둔 식별자와 패스워드의 조합을 기억해야 하고, 계정마다 관리되고 있는 개인 정보를 최신의 정보로 유지해야 한다. 보통의 경우, 개인은 동일한 식별자와 패스워드를 사용하거나, 혹은 여러 개의 식별자, 패스워드를 사용하고 어딘가에 이 정보를 기록하는 식으로 문제를 해결하려고 한다. 하지만 이 방법들은 사용자를 번거롭게 할 뿐만 아니라, 악의적인 사용자에게 노출되기도 쉽다는 문제가 있다. 노출된 식별자와 패스워드는 해당 사이트뿐만 아니라 사용자가 가진 모든 계정에도 악영향을 미칠 수 있다.

또 다른 문제는 번거로운 Identity 등록 과정이다. 사용자가 개인 정보를 손으로 일일이 입력하는 불편함이 있기 때문에, 대부분의 사용자들은 이런 입력 과정에 지쳐 있다. 그리고, 자신이 가입한 계정의 Identity 정보를 관리하고 최신 정보로 항상 유지시키는 과정은 불편하고 현실적으로 불가능하다는 문제가 있다.

2. 인터넷 ID 관리

인터넷 ID 관리는 기존의 Identity관리 문제점들을 해결하기 위하여 등장하였다. 네트워크 Identity를 인터넷 레벨에서 관리해주기 때문에, 개인이 관리하는 부담을 없애고 현재와는 차원이 틀린 인터넷 환경을 제공해줄 수 있게 된다.

Identity 관리는 사용자, 서비스, 정보통신기기 등 네트워크에 연결되는 개체의 Identity 속성, 신원 증명서(Credential), 정보 이용 자격(Entitlement) 등을 포함한 네트워크 Identity의 생명주기를 전체적으로 관리해주는 플랫폼 기반 구조이다. Identity 관리를 통하여 조직의 내부 통신망이나 외부 통신망으로부터 접속해오는 사용자 또는 단말기를 인증하고 해당하는 권한을 확인하며 정보 자원에 대한 적절한 접근 권한을 인가해주는 과정을 처리할 수 있게 된다. 즉, 기존의 AAA(Authentication, Authorization, Audit/Account) 기술, P3P 기술, 패스워드 재설정 기술, 패스워드 동기화 기술, 계정관리 셀프 서비스, 관리 권한 위임, SSO,[1] 메타 디렉토리, LDAP(Lightweight Directory Access Protocol) 등 여러 기술을 망라하여 구현된 복잡한 시스템이 바로 Identity 관리 시스템이다[2].

Identity 관리는 기업 내부와 계열사 전체를 관리하는 단계를 넘어서, 인터넷 레벨에서 Identity 관리를 제공하려는 시도가 외국에서 진행되고 있다. 이러한 움직임은 Identity를 관리하는 방식에 따라서 크게 중앙화된 방식과 연방화된 방식으로 나누어 볼 수 있다.

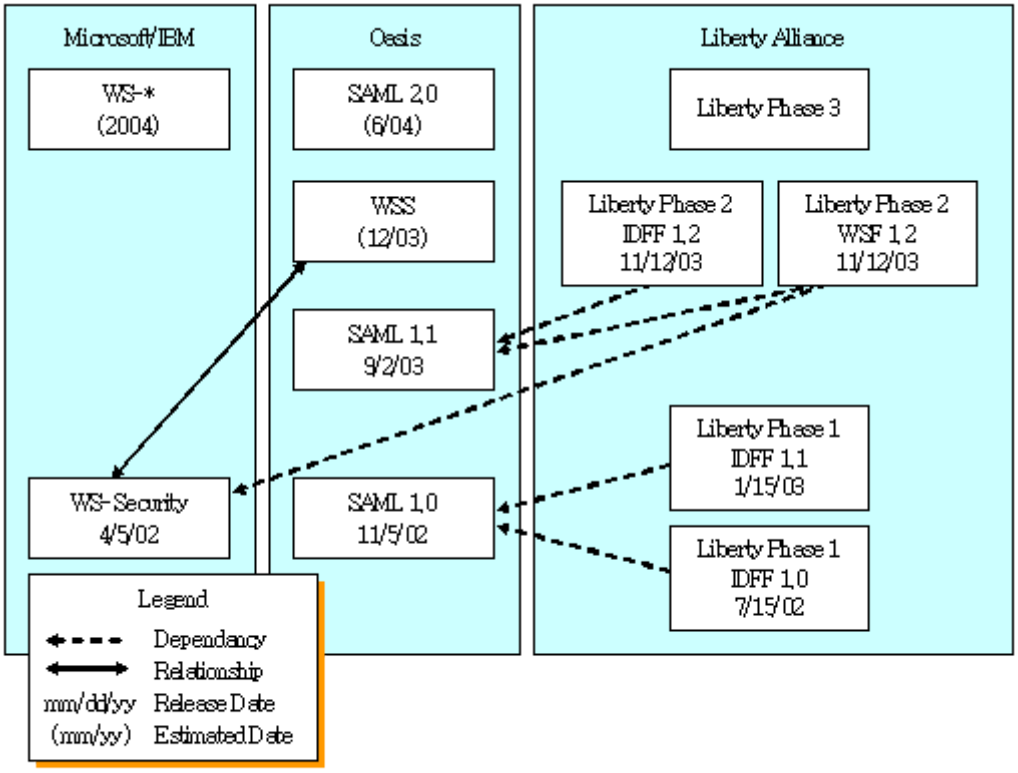
중앙화된 Identity 관리는 모든 기관들이 각자 보유하고 있던 Identity 관련 정보를 하나의 데이터 저장소에 집중화하는 방식이다. 모든 정보가 한곳에 있기 때문에 엄격한 모니터링 및 추적이 가능하며, 데이터의 접근, 이용, 저장, 가공, 처리 방법을 통제할 수 있다. 하지만 이 방식은 프라이버시 문제, 중앙 서버에 문제가 발생하면 모든 작업이 중단되는 문제 등의 단점을 가지고 있다.

연방화된 Identity 관리는 기존의 Identity 관리가 한 영역에서 이루어지는 점을 해결하기 위하여 나온 개념으로, 모든 기관들이 하나의 보안 정책으로 통합된다는 것은 현실적으로 불가능하다는 관점을 가지고 있다. 연방화된 Identity 관리 방식은 기관에게 독자적인 보안 정책들을 지원하면서, 다른 기관과는 표준화된 절차로 Identity 정보를 주고 받도록 도와준다. 네트워크에 한번 로그인하여, 여러 영역에서 관리되는 Identity를 사용한다는 생각이 들지 않도록 자연스럽게(Seamless) 네트워크 간을 이동하는 것이 연방화된 Identity 관리의 특징이다.

Ⅲ. 인터넷 ID 관리 표준

인터넷 레벨의 Identity 관리 서비스를 제공하기 위하여 여러 단체에서 스펙을 제안하고 솔루션을 만들었다. 그러한 시도는 인터넷 레벨의 Identity 관리를 위한 표준화의 필요성을 공감하도록 하였고, (그림 1)과 같은 표준안들이 나왔다.

- SAML(Security Assertion Markup Language) 1.0: SAML은 도메인 간에 사용자 정보를 안전하게 교환하기 위해 만들어진 확장 언어로, SOAP 프로토콜을 통하여 제공된다. SAML은 보안 토큰의 형식을 정의하고, 프로파일에서는 이들 assertion을 [2] 사용하여 웹 SSO를 제공할 수 있는 방법을 정의하였다. SAML은 3가지 종류의 assertion을 정의하였는데, 바로 인증, 속성 정보, 인가 정보에 관한 것이다.



(그림 1) 인터넷 ID 관련 표준

- SAML 1.1: SAML 1.0 스펙의 피드백과 수정 사항을 주로 반영하였다. 1.0과 마찬가지로 도메인 간의 표준화된 양방향 SSO를 정의하였다. 또한 디지털 인증서를 이용한 SAML assertion 서명 방법에 대한 가이드라인, 기업간의 상호 호환성 문제, assertion과 서버측의 기능 요소들, 구현 프로파일, 요청/응답 메시지 프로토콜 등이 정의되어 있다. SAML 1.0과 달라진 점은 기본 assertion 레벨이 호환되지 않는다는 것이다. XML 스키마 식별자를 사용하는 SAML 1.1 스키마는 SAML 1.0 assertion의 유효성을 검증할 수 없게 되었다.
- SAML 2.0: SAML 2.0 은 지난 2003년 9월부터 정식으로 개발 중이며, 위원회는 2004년 2,3분기 중에 완전한 드래프트가 나와서 업계의 리뷰가 이루어지리라고 예상하고 있다. SAML 2.0은 주로 개발자들의 요구 사항을 반영하고, 리버티 ID-FF 1.2에서 나온 SAML의 기능상 미미한 점들을 보완하는 측면으로 작성될 것이다. 그리고 SAML 2.0은 이전 버전에서 연기된 몇 가지 기능들을 포함할 것이다. 이 스펙은 아직 초기 단계지만 리버티 2단계와 ID-FF 1.2의 상당 부분에 관여되리라 예상된다.
- 리버티(Liberty) 1단계(ID-FF 1.0: IDentity-Federation Framework): 리버티는 연방화된 네트워크 Identity 관리와 Identity기반의 서비스를 위한 공개 표준을 개발할 목적으로 2001년 9월에 결성되었고, 2004년 현재 170여 개의 멤버를 가진 조직으로 성장하였다. ID-FF라고 불리우는 리버티 표준 스펙의 1 단계는, 연방화된 네트워크 Identity 관리를 시작하기 위한 작업을 담당한다. 여러 기능 중에서, 신뢰 관계를 맺은 CoT(Circle of Trust) 내의 서비스 제공자들이 보유하고 있는 Identity들을 연결해주고 SSO를 지원한다. 추가로 Identity 연동, Identity 제공자 알림 서비스, 익명 Identity 매핑과 글로벌 로그 아웃 서비스도 지원한다. 리버티 1단계는 SAML 1.0을 확장한 SAML assertion을 사용하며, 연방 조직 내부의 멤버들을 Identity 제공자와 서비스 제공자라는 역할로 구분하여 정의하였다.
- 리버티 1 단계(ID-FF 1.1): ID-FF 1.0 스펙에서 나온 피드백과 문제점을 보완하였다.
- 리버티 2 단계 (ID-FF 1.2): 리버티 1 단계에서 ID-FF가 지원하는 옵트-인[3] 방식의 계정 연결과 SSO 서비스에 추가하여 익명성 서비스와 가맹 관계 설정 기능 등을 추가하였다. 익명성 서비스는 사용자의 Identity를 보여주지 않고 일부 상태 정보만을 요구할 때 사용하는 기능으로, 리버티 2 단계에서는 일회용 Identity assertion을 이용하여 익명성을 제공한다. 가맹 관계 설정 기능은 사용자가 직접 가맹 사이트들을 선택하여 Identity를 연동하는 프로토콜이다. 리버티 2단계는 SAML assertion을 이용하여 직원과 고객에 관한 정보를 사이트 간에 주고받을 수 있는 메커니즘을 제공한다.
- 리버티2 단계(ID-WSF 1.0: IDentity-Web Services Framework): 기존의 리버티 프레임워크에 웹 서비스를 통한 디스커버리 기능과 Identity와 관련된 서비스를 제공해 주도록 확장하였다. 사용자가 공유하기로 결정한 정보만을 선택적으로 제공해주는 허가-기반의 속성 정보 공유 서비스(Permissions-Based Attribute Sharing), 사용자의 Identity 서비스 위치를 자동으로 찾아주는 Identity 디스커버리 서비스, 사용자가 제공해야 하는 개인 정보를 대신 제공해주는 서비스, 프라이버시와 보안에 관련된 요구 사항을 명시하는 보안 프로파일 서비스, 사용자가 모바일 환경에서 웹 서비스를 쉽게 이용할 수 있는 확장 클라이언트 지원 서비스 등을 ID-WSF가 지원하게 된다. 리버티 2단계는 SAML 1.1에서 정의한 메시지와 프로토콜 바인딩을 채용하고, WS-Security의 안전한 SOAP 메시지를 통하여 보안을 제공한다.

- 리버티3단계(ID-SIS: IDentity Services Interface Specifications): 리버티 3단계는 기업들에게 표준화된 방법을 제공하여, Identity를 기반으로 하는 서비스를 구축할 수 있도록 도와준다. 이들 서비스는 리버티 2단계에서 나온 ID-WSF 위에서 제공된다. 초기에 나온 서비스는 기본 프로파일 정보를 제공해주는 ID-Personal/Employee 프로파일 서비스로, 사용자의 등록 과정에 사용된다. 이름, 주소, 회사 주소, E-Mail 같은 정보를 보유하고 있으면서 필요할 때 해당 정보를 알려주고, 다른 서비스와 상호 동작할 수 있다. 이 표준안들은 1.0 버전의 스펙이 나온 상태이며, ID-WSF를 이용하여 속성 정보를 교환하는 서비스를 추가할 예정이다. 예를 들어, 전자 지갑이나 일정/주소록 서비스 같은 기능들이 이전에 완성된 프레임워크 위에서 동작하게 될 것이다.
- WS-Security: WS-Security 스펙[4]은 보안 토큰을 이용한 무결성과 신뢰성을 웹 서비스 메시지(SOAP)에 반영하기 위한 메커니즘을 정의한다. 메시지의 무결성, 신뢰성, 인증을 포함하는 메시지 보호 수준(Quality of Protection)을 제공하기 위한 SOAP 메시지의 활용 방안이 기술되어 있다. 바이너리 보안 토큰들을 인코딩하는 방법을 설명하는 부분에서, X.509 인증서나 커버로스(Kerberos) 티켓 등을 사용하는 방식과 인증서의 특성들을 설명하는 확장 메커니즘이 추가되어 있다. WS-Security는 보안 토큰에 사용할 수 있는 여러 범용 기술을 제공하기 때문에, 다양한 종류의 보안 모델과 암호화 기술에 적용될 수 있다는 특징을 가진다. WS-Security는 정해진 보안 토큰뿐만 아니라, 여러 형식을 사용하여 확장할 수 있도록 설계되어 있다.
- WS-Security Extensions(WS-Trust, WS-Policy, WS-Federation): 웹 서비스 중심의 메커니즘을 기반으로 보안 도메인에서 사용할 인증, 인가, 정책에 대한 스펙을 제공한다. WS-Trust는 신뢰 관계를 맺는 방법을 정의하는데, 직접 맺는 방법과 신뢰할 수 있는 중간 계층을 통해서 맺는 방법을 소개하고 있다. 신뢰 관계를 맺은 기관들은 WS-Security를 사용하여, 보안 토큰을 안전하게 전달하기 위한 발급 서비스를 제공하게 된다. 추가적으로 WS-Trust는 기존의 신뢰 메커니즘을 활용하는 방안과 권한 위임, 대행에 대한 서비스를 명시할 계획이다.
  WS-Policy는 수신자와 송신자가 자신들의 요구 사항과 지원 가능한 정도를 명시하는 방법을 제공한다. 요구 사항과 지원 정도를 명시하는 방식에는 제한이 없지만, 이 스펙에서는 프라이버시 정보, 인코딩 형식, 보안 토큰 요구 사항, 지원되는 알고리즘 같은 몇 가지 기본 서비스를 위주로 설명하고 있다. WS-Policy는 단순한 보안 정책 이상을 지원하는 SOAP 형식을 정의하고, SOAP 메시지에 정책을 포함시키는 메커니즘을 정의할 예정이다.
  WS-Federation은 연방화된 신뢰 시나리오를 구축하는 방법을 정의하고, 커버러스와 PKI 기반 구조를 연동하는 방법 같은 것들을 표현한다. WS-Security, WS-Policy, WS-Trust, WS-SecureConversation 스펙에 기반하고, 신뢰 정책을 사용해 자신이 요구하는 신뢰 형식을 전달・제한・확인하는 절차를 정한다. WS-Federation은 신뢰 관계를 관리하는 메커니즘에 대한 정의도 추가할 것이다.
- OASIS WSS(Web Services Security): OASIS(Organization for the Advancement of Structured Information Standards) 기술위원회는 WS-Security와 여러 보안 토큰 타입들에 대한 표준화 단계를 완성하는 작업에 주력하고 있다. 그 중의 하나인 WSS 기술위원회[5]의 주요 목적은 IBM과 Microsoft에서 제안한 웹 서비스 보안의 기초 작업을 보완하여 표준화하는 것이다. OASIS WSS 기술위원회는 다른 표준에서 더 높은 레벨의 보안 서비스를 제공하기 위하여 2002년 4월에 공표된 웹 서비스 보안 로드맵에서 WS-Security 스펙을 작성하였다. 2004년 4월에 나온 1.0 표준안은 SOAP 메시지 보안, 사용자 이름 토큰 프로파일, X.509 토큰 프로파일이 포함되어 있으며, 현재는 SAML 토큰, XrML 토큰, 커버로스 토큰에 관한 프로파일을 작성 중이다.

Ⅳ. 인터넷 ID 관리 기술

1. 패스포트

패스포트[6]는 Microsoft사에서 개발한 단일 로그인 시스템으로, 웹상에서 가장 큰 인증 서비스라고 말할 수 있을 만큼 수백만의 Hotmail과 MSN 메신저 사용자들이 참여하고 있다. 패스포트의 가장 큰 특징은 중앙에서 관리되는 사용자 계정이다. 사용자는 Microsoft가 관리하는 중앙의 패스포트 서버를 통하여 서비스에 가입하고, 자신의 신원을 제시하여 인증받게 된다.

패스포트는 SSO 서비스를 통해서 사용자가 한번 로그인만으로 가맹 사이트를 추가 인증 없이 자유롭게 이동할 수 있도록 하였다. 가맹 사이트는 패스포트의 강력한 인증 시스템을 통해서 사용자를 인증하기 때문에 독자적인 인증 시스템을 구축할 필요가 없어진다. 더욱이 패스포트 시스템은 사용자의 프라이버시에 관련된 정보를 저장하고 사용자를 인증하는 역할을 담당하기 때문에, 높은 레벨의 보안 기술로 유지되고 있다. 수차례 지적된 문제였던 사생활 보호 정책을 강화하여, 사용자가 동의하지 않은 정보 수집과 이용을 배제하고 사용자 중심의 관리 정책을 지원하였다. 또한 사용자가 로그인 할 때 같은 정보를 중복해서 입력해야 하는 번거로움을 피하기 위하여 패스포트가 가지고 있는 정보로 채워주는 템플릿 기능 등을 제공하고 있다.

패스포트는 복잡한 구조를 가지고 있는 COM 기반의 API로 구현되어 있다. 패스포트를 이용해서 인증하려는 사이트들은 이 API를 사용해서 패스포트 서버에 요청하고, 인증 여부를 판단하는 결과를 받아서 서비스 제공 여부를 결정한다. 패스포트는 현재 2.5 버전이 나와있는 상태로 기존의 여러 보안 문제점들을 해결하였으며, SSL(Secure Socket Layer)을 지원하여 사용자의 Identity정보를 안전하게 전달할 수 있도록 하였다.

패스포트는 더욱 분산되고 연방적인 모델에 목표를 두고 있다. 게다가 Microsoft는 다음 버전의 패스포트에서 커버로스(Kerberos)[7]를 지원하겠다고 공표하였다. 커버로스의 지원은 두 가지 중요한 의의를 가진다. 첫 번째는 커버로스가 표준이라는 점이고, 두 번째는 커버로스가 다중 인증 도메인에서 동작할 수 있기 때문이다. 연방화된 버전의 패스포트는 커버로스를 이용하여 영역간의 연동을 가능하게 할 것이다.

주력인 패스포트 서비스에 추가하여, Microsoft는 새로운 인증 기술을 개발하겠다는 계획을 발표하였다. TrustBridge라고 불리우는 이 기술은 고객이 구매하여 자신만의 서비스를 제공할 수 있으며, Microsoft의 웹 서비스 보안 로드맵[8]에 기반한 XML 메시지를 통하여 다른 TrustBridge 서버와 통신할 수 있다. 2004년 5월 말에 열린 TechEd 컨퍼런스[9]에서는 TrustBridge 기술을 ADFS(Active Directory Federation Service)라고 부르기로 하고, 2005년에 공개되는 윈도 서버 2003의 업데이트로 포함할 계획을 공표했다. ADFS는 기관 간에 연방화된 Identity관리를 가능하게 해주며, 현재 Microsoft의 Identity 플랫폼에서 부족했던 웹 환경에서의 SSO 기능을 제공하게 될 것이다. 또한 OASIS의 표준인 WS-Security를 지원하고, 현재 개발 중인 WS-Trust, WS-Policy, WS-SecureConversation, WS-Federation, WS-Authorization, WS-Privacy도 포함할 계획이다.

2. 3-D Secure

3-D Secure는 'Verified by Visa'[10] 서비스에서 사용하는 프로토콜이다. 3-D Secure 프로토콜은 카드를 발급한 은행들을 통하여, 현재 계정 정보를 제시한 사람이 실제로 카드의 소유주임을 증명해 주는 역할을 한다. 카드 정보를 확인해야 할 때, 카드 소유주임을 인증받지 못하면 해당 카드는 사용할 수 없게 된다.

3-D Secure는 범용의 인증 프로토콜이라기보다는 지불쪽과 관련된 인증 프로토콜로서 설계되었다. 디렉토리 서버와 비슷한 기능으로, 중앙에 디렉토리가 있어서 모든 구현자들이 참고하기로 동의한 것이다. 3-D Secure 프로토콜은 신용카드 번호를 특정 발급 은행으로 연결시켜 두어서, 인증 요청을 해당하는 발급 은행에게 전달한다.

은행은 3-D Secure 프로토콜을 통해 상인에게 assertion을 발급한다. 이 assertion은 카드를 제시한 사용자가 실제로 그 카드를 발급받았고 트랜잭션을 수행할 수 있도록 허가 받았다는 것을 나타낸다. 카드 발급자는 카드 소유자들의 암호나 기타 수단을 이용해서 이를 증명하고, 해당 결과를 소매상들에게 실시간으로 알려준다. 3-D Secure는 인터넷상에서 불법으로 카드를 사용하려는 시도를 막을 수 있으며, 소비자가 온라인을 통해서 물건을 사는 과정을 더욱 신뢰하도록 도와준다.

3. 시볼레

시볼레(Shibboleth)[11]는 Internet2/MACE 프로젝트의 하부 프로젝트로 IBM의 재정적 지원을 받고 있다. 시볼레 아키텍처는 접근 제어로 관리되는 리소스를 기관 간에 공유할 수 있는 실제 기술과 프레임워크를 개발하며, 접근 제어를 결정할 때 필요한 권한 정보를 안전하게 교환할 수 있는 방법에 초점을 맞추고 있다. 초기에 시볼레는 대학 기관 간 자원을 공유하기 위하여 제안되었기 때문에, 한 대학의 학생이나 교수가 다른 대학이 소유한 자원을 접근할 수 있도록 하였다.

기관 사이트는 외부 사용자가 접근할 때, 사용자의 기관에게 정보를 요청한다. 개인 정보가 요청되고 전달될 때, 시볼레는 SAML assertion을 사용하여 속성 정보를 안전하게 제공한다. 기관 사이트가 속성 assertion을 받으면 이를 확인하고, 적당한 권한을 부여하게 된다. 시볼레 아키텍처는 퍼미션을 기반으로 속성 정보를 제공하므로, 얻을 수 있는 정보가 일반적이고 특정 사용자를 지칭하지 않는다는 것이 특징이다. 이러한 인가 결정은 사용자의 역할, 기관 같은 정보에 기반하게 된다.

시볼레에서는 'Club'을 통하여 정책 도메인 개념을 표현한다. Club이란 기관들의 집합으로, SAML/시볼레 프로토콜을 사용해서 속성 정보를 교환한다. 시볼레는 기관이 독자적으로 정책/레벨을 결정할 수 있다. 그리고 최종 사용자의 프라이버시 정보를 보호하는 것에 최우선의 목표를 두고 있어서 사용자 자신이 정보 공유 정도를 명시할 수 있다.

시볼레는 2003년 7월에 버전 1.00이 나왔고, 8월 중순에 버전 1.1, 2004년 5월 중순에 버전 1.2가 소스 코드로 공개되었다. SAML의 공개 소스[12]를 사용하였고, 아파치, IIS같은 웹 서버에서 동작할 수 있도록 구현했으며 연방화된 PKI 기반으로 동작이 가능하도록 하였다. 현재 시볼레는 대학 간이나 다른 국제적인 교류에 활용되고 있으며, 대표적으로 InCommon[13], InQueue[14], SWITCH[15] 프로젝트에 도입되어 있다.

시볼레는 2004년 늦여름에 버전 1.30이 나올 예정이다. 이전 버전과 호환되며 복잡한 연방 환경에도 유연성 있게 대처할 수 있도록, 사용자가 자유롭게 정책을 설정할 수 있을 것이다. 현재는 10군데 캠퍼스와 회사에서 시볼레의 정책과 동작을 테스트하고 있는 중이며, 2004년 여름에 상업적으로 활용하고 SAML 2.0 일부를 지원할 계획을 가지고 있다. 또한 시볼레는 Identity관리 서비스와 다른 개념을 통합하려는 시도를 하고 있다. 전세계의 유휴 컴퓨팅 리소스를 모아서 대용량의 컴퓨팅 파워를 제공하는 GRID, 메일링리스트 소프트웨어, 위키, 블로그, 콘텐츠 관리 시스템(ZOPE), P2P(LionShare) 등과 결합하려는 시도가 이루어지고 있다.

4. PingID 네트워크

PingID 네트워크[16]는 최초의 회원제 Identity 네트워크로서, 비즈니스 환경에서 법률적인 요소를 중점으로 하여 개인적인 Identity와 공개적인 Identity간의 상호 동작이 가능하도록 설계되었다. PingID 네트워크는 보안성과 확장성, 그리고 수준 있는

Identity 연동을 보장하는 것을 목적으로 한다. Identity 정보를 공유하기 위해서는 모든 구성원들의 복잡한 요구 사항이 맞아 떨어져야 하는데, PingID 네트워크는 이러한 요구 사항을 만족시키는 방법을 찾고 있었다.

- Identity의 분산화 보강 및 지원
- 기존 기술에 중립을 유지하면서 공개 표준 지원
- 기술과 비즈니스 도입에서의 상호운용성 지원
- 개인의 프라이버시를 상시 보호
- Identity 도용의 위협에서 멤버 보호
- 멤버의 영역 보존 및 강제

PingID 네트워크는 연방화된 Identity 관리를 선택했다. 연방화된 관리에서는 인증 기법마다 다른 정도의 보안을 제공하기 때문에, 자신이 원하는 인증 레벨을 맞추는 작업이 선행되어야 한다. 이를 위하여 PingID는 PICA(PingID Confidence Assertion)라는 개념을 소개한다. PICA는 score라는 숫자를 발급하여 인증 메커니즘의 수준을 보장하는 것으로, score에 따라서 원하는 인증 레벨임을 확인하면 서비스를 제공하고, 아니면 재인증을 요구한다.

연방화된 Identity 서비스를 구축하는 과정은 단순히 기술적인 문제로 국한되지 않는다. 기업들은 서비스 협약을 맺는 과정에서 좀더 많은 이익을 요구하기 때문에 입장 차이를 해소하기가 힘들다. PingID 네트워크는 비용이 많이 들어가는 양방향 협상이나 협약을 맺을 필요 없이, 기관들 간에 Identity 정보를 공유할 수 있도록 해준다. 그러는 도중에도 변함없이 최종 사용자의 프라이버시 정책을 유지하고 있다. PingID 네트워크의 회원제도는 기업들이 독자적으로 협약을 맺지 않아도 되며, 각각의 파트너가 나름대로 연방화된 Identity 전략을 수행하기가 용이하다.

PingID 네트워크를 관리하는 업체는 Ping Identity[17]이다. 연방화된 Identity 관리 소프트웨어와 네트워크 제공 분야의 선두 업계로, SourceID[18]의 초기 스폰서를 하고 있다. SourceID는 Identity 연동 플랫폼을 제공해주기 위한 공개 소스 프로젝트로, SourceID 플랫폼을 통하여 연방화된 Identity 애플리케이션이나 SSO를 구축할 수 있게 한다. 이 플랫폼은 기술 중립적이어서, SAML, 리버티, WS-Federation과 WS-Security를 제공한다. SourceID 플랫폼은 자바와 .NET으로 구현되어 있으며, 리버티의 1단계 스펙을 지원하고, 또한 WS-Federation 버전의 기술도 보유하고 있다.

Ping Identity는 SourceID 로드맵에서도 Identity 연동과 관련된 오픈 소스를 강화하기 위해 리버티 2단계, SAML 1.1, WS-Security, WS-Trust와 WS-Federation 스펙을 지원할 계획을 포함하고 있다. SourceID Identity 플랫폼의 로드맵은, Identity 연동을 지원하는 서로 다른 표준들이 유연성 있고 상호운용성이 보장되기를 바라는 사용자의 요구를 반영하고 있다. 이런 기능을 공개 소스 플랫폼으로 제공함으로써, PingID는 Identity 연동을 원하는 고객들에게 선택의 폭을 넓혀준다.

V. 결 론

사용자는 많은 사이트에 산재된 네트워크 Identity를 안전하게 관리해야 하지만, 네트워크 Identity가 늘어날수록 관리 부담이 가중된다. 이 문제를 해결하기 위해 'Identity 관리'라는 개념이 나오게 되었고, 인터넷 레벨에서 Identity를 효율적으로 관리하기 위한 방법들이 등장하게 되었다. 이미 인터넷 ID 관리 기술은 활발한 연구와 개발이 진행되어서 표준 및 제품들이 다수 등장하고 있다. WS-Security, WS-*, SAML, 리버티 스펙 같은 표준들과, Microsoft의 .NET 패스포트, 170여 개 기업들이 연합한 리버티 얼라이언스, Verified by Visa의 3-D Secure, 학계에서 주도하는 시볼레, PingID 네트워크 등으로 대표되는 인터넷 ID 관리 시장은 더욱 활성화 되리라 예상한다. 국내에서도 인터넷 ID 관리 시장에 대한 대비를 시작하고 있다. 정보통신부 주관의 선도기반 기술 개발 사업인 'e-Identity 보호용 공통보안서비스 플랫폼 기술 개발'을 통하여, 한국전자통신연구원에서 인터넷 ID 관리 서비스 개발을 착수한 상태이다.

가트너 그룹의 보고서에 따르면 2004년에 가장 유력한 보안 분야는 Identity 관리 분야였다. 다가오는 인터넷 ID 관리 서비스는 연방화된 방식을 중심으로, 이기종이나 모바일 환경을 고려한 플랫폼 독립적인 방식이 대세를 이을 전망이다. 또한 WS-I[19]에서 공개하는 표준이 인터넷 ID 관리 서비스에 중요한 역할을 할 것이기 때문에 이에 대한 준비가 필요하다[20].

전세계 인터넷 환경을 볼 때, Identity 관리 시장은 무궁한 잠재력을 가지고 있는 상태이며 인터넷 레벨의 Identity 관리 서비스를 도입하는 초기 단계라고 볼 수 있다. 현재는 기업 내부나 계열사들 간의 Identity 관리를 위한 시장이 활성화되고 있는 시점이다. 하지만 인터넷 ID 관리 시장은 조만간 성숙될 것이므로, 이에 대한 기술 개발 및 관련 법제도・정책에 관련된 대비가 이루어져야 한다.

<참 고 문 헌>

[1] Liberty Alliance, "Identity Systems and Liberty Specification Version 1.1 Interoperability," A Liberty Alliance Technical Whitepaper, Feb. 2003.

[2] 전길수, 권현조, 정재호, "아이덴티티 위협에 대처하는 아이덴티티 매니지먼트 기술," 정보보호 뉴스, KISA, Mar. 2004.

[3] Federation Standards Overview, Ping Identity, 2003.

[4] WS-Security, http://www-106.ibm.com/developerworks/webservices/library/ws-secure/

[5] OASIS Web Services Security TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
[6] 패스포트, http://passsport.net
[7] Kerberos, http://web.mit.edu/kerberos/www/
[8] 웹 서비스 보안 로드맵, http://msdn.microsoft.com/ws-security/
[9] TechED 2004 Conference, http://www.microsoft.com/technet/community/events/teched04.mspx
[10] Verified by Visa, http://www.verifiedbyvisa.com
[11] Shibboleth Project – Internet2 Middleware, http://shibboleth.internet2.edu
[12] Open SAML, http://www.opensaml.org/
[13] InCommon, http://incommon.internet2.edu/
[14] InQueue, http://inqueue.internet2.edu/
[15] SWITCH, http://www.switch.ch
[16] PingID 네트워크, http://www.pingid.com
[17] Ping Identity, http://www.pingidentity.com
[18] SourceID, http://sourceid.org
[19] WS-I, http://ws-i.org
[20] Ray Wagner, “Act Now to Help Shape Web Services Security Scenarios,” Gartner, Mar. 2004.

---

1) SSO(Single Sign On): 한번의 로그인만으로 다른 모든 사이트를 자유롭게 이용할 수 있는 서비스. 추가적인 인증 절차 없이, 이전에 로그인 한 보안 정보를 사용하여 인증된다.

2) assertion: 신뢰할 수 있는 제3의 기관에 의해 작성된 것으로, 시스템이나 애플리케이션 간에 교환되는 정보를 의미함. 인증 및 승인에 관련된 정보가 XML 인코딩되어 있다.

2) assertion: 신뢰할 수 있는 제 3의 기관에 의해 작성된 것으로, 시스템이나 어플리케이션 간에 교환되는 정보를 의미함. 인증 및 승인에 관련된 정보가 XML 인코딩 되어 있다.

3) 옵트-인(Opt-In): 사용자가 해당 서비스를 사용하기로 명시적인 동의를 한 경우에만 서비스를 제공하는 기능