인터넷 신원 관리 2.0에 대한 분석과 3.0에 대한 전망

박승철*

Analysis of Internet Identity Management 2.0 and Perspective of 3.0

Seung-chul Park*

이 논문은 2011년도 한국기술교육대학교 교육연구진흥비를 지원받았음

요 약

재 인터넷의 서비스 제공자 중심적(service provider-centric)이고 고립형(isolated)의 신원 관리 1.0 모델(identity management 1.0 model)은 사용자 편의성 부족, 고비용 구조, 프라이버시 보호 어려움, 그리고 신뢰 인프라 부재 등의 여러 가지 문제를 안고 있다. 이러한 문제를 개선하기 위해 Passport/Live ID, Liberty Alliance/SAML(Security Assertion Markup Language), CardSpace, OpenID 등 SSO(Single Sign On) 서비스에 기초한 다양한 신원 관리 2.0 모델들이 개발되어 왔으나 실제 인터넷 환경에서 아직까지 신원 관리 1.0 모델을 대체할 수 있을 정도로 광범위하게 수용되지 못하고 있다. 본 논문은 현재 개발되고 있는 대표적인 신원 관리 2.0 모델들을 비교분석하고, 분석 결과를 바탕으로 미래 인터넷을 위한 신원 관리 3.0 모델의 개발 방향을 제시하고자 한다.

ABSTRACT

Current identity management 1.0 model, which is service provider-centric and isolated, has several problems such as low usability, high cost structure, difficulty in privacy protection, and lack of trust infrastructure. Though various SSO-based identity management 2.0 models including Passport/Live ID, Liberty Alliance/SAML, CardSpace, and OpenID have been recently developed in order to overcome those problems, they are not widely accepted in real Internet environment so as to replace the existing identity management 1.0 model. This paper firstly analyzes the widely-known identity 2.0 models in a comparative way, and then presents a perspective on the development direction of identity management 3.0 model for future Internet.

키워드

신원 관리, 인증, 단일 사인온, 프라이버시

Key word

Identity Management, Authentication, Single Sign-On, Privacy

* 정회원 : 한국기술교육대학교 (scpark@kut.ac.kr)

접수일자 : 2011. 05. 16
심사완료일자 : 2011. 06. 07

Ⅰ. 서 론

인터넷상의 신원 관리(identity management)는 인터넷 서비스 참여자를 표현하는 신원 정보(identity information)의 등록(registration), 증명 정보 발급(credential issuance), 신원 확인(verification), 신원 정보 유지 및 공유(maintenance and sharing), 신원 정보 폐지(revocation) 등 신원 생명 주기(identity life-cycle) 동안의 신원 관련 모든 동작을 담당한다[1].

현재 인터넷에서 사용되고 있는 신원 관리 1.0 (identity management 1.0) 모델은 각 서비스 제공자(service provider)가 자신의 요구사항에 맞는 신원 관리 환경을 독자적으로 구축하고 운영하며, 사용자는 각 서비스 제공자가 요구하는 신원 정보를 반복적으로 제공하고, 각 서비스 제공자로부터 서로 다른 신원 증명 정보를 발급받고 유지하고 사용하는 서비스 제공자 중심적(service provider-centric)인 사일로(silo) 형태의 고립형 모델이다[2]. 현재의 신원 관리 1.0 모델 환경에서 사용자는 자신이 접근하는 서비스 제공자들에게 반복적으로 신원 정보를 등록해야 하고, 서비스 제공자에 의해 발급된 많은 수의 신원 증명 정보(credentials)를 관리해야 하며, 서비스 제공자를 접근할 때마다 반복적으로 로그인(login)을 해야 하는 등 사용상 많은 불편함에 직면해 있다.

서비스 개발자 또한 별도의 신원 서버(identity server)와 인증 장치(authentication device)를 포함하는 별도의 신원 관리 시스템을 개발해야 하고, 유지하고 보수하고 운영해야 하므로 시간적 측면과 비용적 측면에서 고비용 비효율 상황에 직면하고 있다. 뿐만 아니라 신원 관리 1.0 모델 환경에서 사용자는 자신이 접근하고자 하는 서비스 제공자의 신원 관리에 대해 스스로의 판단에 근거하여 신뢰 여부를 결정해야 하므로, 사용자가 잘못 판단하여 피싱 공격(phishing attack)에 노출될 수 있고, 악의적이거나 부주의한 서비스 제공자에 의해 신원 정보가 노출될 수 있는 위험이 높은 실정이다[1,2].

몇 년 전부터 현재 사용되고 있는 신원 관리 1.0 모델의 문제점들을 개선하기 위해 Passport/Live ID 모델[3,4], Liberty Alliance/SAML 모델[5,6], CardSpace 모델[7], OpenID 모델[8] 등 다양한 형태의 새로운 신원 관리 모델들이 개발되어 왔다.

이러한 새로운 신원 관리 모델들은 기본적으로 특정 신원 관리 서버의 사용자 인증 결과를 포함하는 신원 정보를 다른 서비스 제공자들이 공유할 수 있게 함으로써, 고립형의 신원 관리 1.0 모델들과 차별화되어 신원 관리 2.0 모델로 불리어 진다[9]. 신원 관리 2.0 모델들은 기본적으로 신원 서버에 로그인하면 그 결과를 공유하는 다른 서비스 제공자를 로그인없이 접근할 수 있게 하는 단일 사인온(single sign-on) 기반의 서비스 편의성을 제공한다.

그리고 서비스 제공자에게는 신원 서버의 신원 관리 서비스를 활용할 수 있게 함으로써 신원 관리에 대한 부담을 들어주는 장점이 있다[1,10]. 이러한 신원 관리 2.0 모델들은 실제 시스템으로 구현되어 일부 적용되고 있으나, 아직 기존 신원 관리 1.0 모델을 대체할 수 있을 정도로 실제 인터넷 환경에서 광범위하게 수용되지 못하고 있다.

본 논문은 대표적인 신원 관리 2.0 모델들의 비교분석을 통해 신원 관리 1.0에 비해 많은 장점을 가지고 있는 신원 관리 2.0 모델들이 실제 인터넷 환경에서 적용되지 못하는 이유를 분석하고자 한다. 그리고 분석 결과를 바탕으로 미래 인터넷 환경에서 실질적으로 수용될 수 있는 신원 관리 3.0 모델의 개발 방향을 전망하고자 한다.

Ⅱ. 신원 관리 2.0 모델 관련 연구

최근의 신원 관리 2.0 모델들의 개발은 하나의 신원 서버를 통해 모든 서비스 제공자들에게 신원 관리 서비스를 제공하는 중앙집중형 모델, 상호 협약을 통해 신원 서버와 서비스 제공자들이 신원 관리 서비스를 공유하는 연방형 신원(federated identity) 관리 모델, 서비스 제공자 중심(service provider centric)의 기존 신원 관리 모델에서 사용자 중심(user centric)의 신원 관리 모델로의 전환, 폐쇄형 ID 기반의 신원 관리 모델에서 개방형 ID 기반의 신원 관리 모델로의 전환 등 다양한 방향으로 진행되어 왔다.

2.1. 중앙 집중형 신원 관리 모델 : Passport/LiveID

Passport와 그 후속 모델인 LiveID는 마이크로소프트에서 서비스 제공자 중심의 고립형 인증 시스템 환경에서 발생하는 편의성 부족과 고비용 구조 문제를 해결하고, 사용자의 신원 정보를 안전하게 관리하기 위하여 개발한 웹 기반의 중앙 집중형 통합 신원 관리 모델이다[3,4]. Passport/LiveID 모델에서는 사용자의 모든 신원 정보가 마이크로소프트에 의해 관리되는 Passport 서버에 등록되고, 유지되고, 관리된다.

그리고 사용자가 서비스 제공자에 로그온하고자 하는 경우 해당 사용자에 대한 인증 요구는 사용자의 웹 브라우저를 경유하여 Passport 서버에게 전달되고, 모든 인증 서비스는 Passport 서버에 의해 통합적으로 제공된다. 사용자에 대한 인증이 성공적으로 완료되면 Passport 서버는 해당 서비스 제공자와 미리 정의된 열쇠로 암호화한 인증 정보를 담은 Redirect 메시지를 사용자 웹 브라우저에게 전달한다. 이 때 Passport 서버는 암호화된 쿠키(GLOBALAUTH-cookie)를 웹 브라우저에게 제공한다. 이 쿠키 정보는 해당 사용자가 다시 Passport 서버를 방문할 때 로그인 절차를 생략하기 위해 사용된다. 해당 사용자에 대한 인증 결과가 성공적이면 서비스 제공자는 해당 사용자 웹 브라우저에게 암호화된 쿠키(LOCAL-cookie)를 제공한다. 이 쿠키 정보는 해당 사용자가 동일한 서비스 제공자를 다시 방문할 때 인증 절차를 생략하기 위해 사용된다.

2.2. 연방형 신원 관리 모델 : Liberty Alliance/SAML

Liberty Alliance는 IT 관련 다양한 분야의 기관들이 신원 정보의 프라이버시 보호와 보안을 유지하면서 다수의 서비스 제공자로부터 비집중형 인증에 기초한 개방형의 단일 사인온 표준을 제정하고 진흥시키기 위하여 결성되었다. Liberty Alliance의 신원 관리 모델은 신뢰 동아리(CoT-Circle of Trust) 기반의 신원 연방화(identity federation) 개념에 기초하고 있다. CoT는 상호 사업적인 협약을 통해 신뢰 관계를 형성한 Liberty 아키텍처를 따르는 서비스 제공자(SP-Service Provider)들과 신원 제공자(IdP-Identity Provider)들의 연방(federation)이다[5,11].

CoT에서 서비스 제공자(SP)는 사용자에게 서비스를 제공하는 실체이다. SP는 효과적인 서비스 제공 등을 위해 일반적으로 자체적인 인증(authentication) 및 인가(authorization) 메카니즘 포함하는 자체적인 신원 관리 기능을 가지고 있지만, 단일 사인온 서비스와 신원 정보의 안전한 관리 등을 위해 CoT내의 신원 제공자(IdP)에게 신원 관리 서비스를 의존할 수 있다. CoT 내에서 사용자에 의해 선택되는 IdP는 CoT내의 SP들에 대해 해당 사용자에 대한 신원 관리 서비스를 대신 제공하는 실체이다. IdP는 신원 서비스 제공 과정에서 필명 또는 가명(pseudonym) 지원과 신원 정보 제공에 대한 사용자 동의 및 제어(consent and control)를 통해 사용자의 프라이버시가 보호될 수 있게 하고, 보안 메카니즘을 통해 신원 정보가 SP에게 안전하게 전달되도록 보장한다.

Liberty Alliance 신원 관리 모델은 단일 사인온 서비스 제공을 위해 CoT내의 IdP를 포함하는 다수의 SP들이 특정 사용자를 참조하기 위해 사용하는 식별자와 신원 속성들을 해당 사용자의 동의에 의해 연방화한다. 한 사용자의 신원은 연방화 과정에서 SAML(Security Assertion Markup Language)[6] 어써션(assertion)으로 상호 공유되고, 연방화 과정에서 생성된 필명 형태의 공유 식별자를 통해 연방 도메인 내의 IdP의 인증 결과를 SAML 어써션으로 상호 공유한다.

2.3. 사용자 중심의 신원 관리 모델 : CardSpace

CardSpace 신원 관리 모델[7,12,13]은 사용자로 하여금 신원 정보를 단순하면서도 안전하고 신뢰적인 방법으로 제공할 수 있게 하는 클라이언트 소프트웨어인 신원 선택장치(identity selector), 사용자에게 InfoCard라 불리는 XML 파일 형태의 가상의 신원 카드를 발급하고 신원 서비스를 제공하는 신원 서비스 제공자(IdP), 그리고 CardSpace 신원 서비스를 사용하는 서비스 제공자(SP)로 구성된다.

CardSpace 사용자는 다수의 IdP로부터 자신이 원하는 InfoCard를 발급받고 필요하면 자신이 InfoCard를 직접 만들 수도 있다. InfoCard는 사용자에 대한 기본적인 신원 정보와 함께 InfoCard를 발급한 IdP 정보와 해당 IdP가 발행하는 신원 증명에 관한 정보(예, 신원 증명 유형 등)를 포함하고, InfoCard 사용자 사이트와 InfoCard를 발급한 IdP간에 할당된 유일한 열쇠에 의해 자동 인증됨으로써 패스워드 사용 없이 InfoCard의 도용 위험을 방지한다.

CardSpace 사용자 클라이언트가 접근하는 SP는 인

증 서버가 전자서명한 비트맵 인증서와 CardSpace를 지원하는 SP임을 표시하는 정보와 함께 신원 요구사항(identity requirements)을 클라이언트에게 전송한다. 신원 요구사항은 해당 SP가 수용할 수 있는 보안 토큰(신원 증명 정보)의 유형 리스트(예, SAML 2.0 토큰), 신뢰하는 IdP 리스트, 필요한 신원 정보 리스트 등이 포함된다. SP의 신원 요구사항을 수신한 클라이언트의 신원 선택장치는 SP의 신원 요구사항에 부합하는 InfoCard들을 선정하여 사용자에게 알려주고, 사용자는 자신이 SP에게 제공하고자 하는 InfoCard를 선택한 후 카드를 발급한 IdP에게 카드 정보를 제공하고 SP에게 제공할 보안 토큰(security token)을 요청한다. IdP는 클라이언트와 InfoCard에 대한 인증 작업을 수행하고 인증이 성공적이면 클라이언트가 요청한 보안 토큰을 제공한다. 사용자 클라이언트는 IdP가 발급한 보안 토큰을 SP에게 전달하고, SP는 수신한 보안 토큰을 확인하여 자신의 요구사항을 충족시키면 클라이언트에게 서비스를 제공한다.

CardSpace는 오프라인 상에서 신용카드, 명함, 신분증 등 다양한 신원 카드를 필요에 맞게 사용자가 선택하여 사용하는 것처럼 클라이언트의 신원 선택장치를 사용하여 SP의 요구사항에 맞는 신원 카드를 선택하여 사용할 수 있고, 신원 정보의 제공을 제어할 수 있다는 점에서 사용자 중심의 신원 관리 모델이라 할 수 있다.

2.4. 개방형 ID 기반의 신원 관리 모델 : OpenID

OpenID는 사용자가 선택한 누구나 알 수 있는 URL(또는 XRI) 형태로 표시되는 하나의 신원 ID를 모든 웹 사이트에 사용할 수 있게 하는 간단하고 개방적이며 분산형의 신원 관리 모델이다[8,14]. OpenID 사용자는 자신의 브라우저를 통하여 접근하고자 하는 임의의 OpenID 지원 웹 사이트(RP-Relying Party)에 자신의 OpenID를 입력하기만 하면 되므로 웹 사이트별로 별도의 신원 정보를 등록하고 로그인 필요가 없어지고, 따라서 웹 사이트도 사용자 신원 정보를 관리하고 인증 작업을 수행할 필요가 없어진다.

OpenID는 OpenID 제공자(OP-OpenID Provider)에 의해 발급되고, OP에 대한 자격 제한은 없기 때문에 누구나 OP가 될 수 있다. 사용자는 OP를 선택하여 특정 URL의 OpenID를 생성할 수 있고, 자신의 신원 정보를 직접 관리하고자 하면 자기 서버가 자신의 OpenID에 대한 OP가 될 수도 있다. OP는 웹 사이트(RP)를 대신하여 자신이 발급한 OpenID에 대한 인증 서비스를 제공하고, 웹 사이트의 요청에 따라 사용자의 동의를 획득하여 사용자의 신원 정보를 제공할 수 있다.

목표 웹 사이트(RP)는 사용자가 입력한 OpenID URL을 기초로 Yadis 프로토콜 또는 HTML 기반의 발견 메카니즘을 사용하여 OP의 URL을 발견한다. RP는 사용자의 접근 요청을 발견된 OP에게 redirect함으로써 해당 OpenID에 대한 인증을 의뢰한다. 신원 서버인 OP는 해당 사용자에 대해 자신의 인증 메카니즘을 사용하여 인증을 실시한다. OP가 어떤 인증 메카니즘을 사용할 것인지는 전적으로 OP에 달려있는 문제이다. 만약 해당 사용자가 OP에 이미 로그인 상태에 있으면 이 과정은 생략될 수 있다.

OP는 OpenID에 대한 인증 결과를 담은 어써션을 서명된 redirect 메시지로 해당 RP에게 전달한다. RP는 OP로부터 수신한 redirect 메시지의 서명을 확인하고 인증 결과를 확인한다. 인증 결과가 성공이면 RP는 해당 사용자에게 인가(authorization) 작업을 수행한다. 이 과정에서 RP는 OP에게 해당 사용자에 대한 추가적인 신원 정보를 요청할 수 있다. OpenID 신원 관리 모델에서 RP에 대한 신뢰 여부는 기본적으로 사용자가 판단하게 한다.

OpenID 2.0은 사용자가 사용자 ID 대신 자신의 신원을 관리하고 있는 OP의 URL을 접근하고자 하는 웹 사이트에 제시하고, OP는 해당 사용자에 대해 필명(pseudonym) 형태의 ID를 발급하여 해당 웹 사이트에 사용하게 하는 것을 가능하게 한다. 이는 웹 사이트 간에 해당 사용자의 접근 사실 공유를 어렵게 만들어 프라이버시 보호를 가능하게 하기 위한 것이다.

III. 신원 관리 2.0 모델 비교분석

여기서는 [1,15,16]등의 관련 연구를 참고하여 미래 인터넷 신원 관리의 가장 중요한 요구사항으로 판단되는 사용자 편의성(usability), 프라이버시(privacy), 신뢰성(trustworthiness), 그리고 확장성(scalability) 관점에서 앞에서 기술한 신원 관리 2.0 모델들을 비교분석한다.

3.1. 사용자 편의성 비교 분석

중앙 집중형의 Passport 신원 관리 모델은 기본적으로 하나의 신원 서버만을 사용하여 모든 서비스 제공자에 대해 별도의 사용 절차 수행 없이 단일 사인온 서비스를 제공하므로 높은 사용자 편의성을 제공한다. CoT 기반의 연방형 신원 관리 서비스를 제공하는 Liberty Alliance 신원 관리 모델은 서비스 제공자별 독립적인 신원 정보 관리를 가능하도록 해야 하므로 사용자는 많은 수의 신원 증명 정보를 관리할 수밖에 없다. 또한 Liberty Alliance 신원 관리 모델은 CoT내에서만 단일 사인온 서비스를 제공하므로 다수의 CoT를 접근하는 경우 반복적인 로그인을 피할 수 없다. 무엇보다 Liberty Alliance 신원 관리 모델에서 사용자는 자신이 선택한 신원 서버와 CoT내의 다른 서비스 제공자들에 대한 복잡한 신원 연방화 절차를 수행해야 한다.

CardSpace 신원 관리 모델의 경우 서비스 제공자들의 신원 서비스 요구사항을 충족시킬 수 있는 수의 InfoCard를 유지하고 관리해야 된다. 그리고 서비스 제공자에 대한 신원 증명 정보 제공시에 InfoCard 발급시에 설정된 유일한 열쇠에 의해 자동 인증을 수행하므로 패스워드 등에 의한 별도의 사인온 절차를 필요로 하지 않는다. OpenID의 경우 하나의 개방형 신원 ID와 해당 신원 ID를 할당한 신원 서버(OP)의 신원 관리 서비스를 통해 OpenID를 지원하는 모든 서비스 제공자를 접근할 수 있고, 신원 관리 서비스를 위한 별도의 사용 절차를 요구하지 않는다. 신원 관리 2.0 모델들에 대한 사용자 편의성 관점에서의 비교 분석 결과는 표 1과 같다.

표 1. 사용자 편의성 비교 분석
(H: High, M: Middle, L: Low)
Table. 1 comparative analysis of usability

	Passport	Liberty Alliance	CardSpace	OpenID
Usability	H	L	M	H

3.2. 프라이버시 비교 분석

중앙 집중형 Passport 신원 관리 모델의 가장 큰 단점은 프라이버시 문제에 있다. 사용자에 의한 신원 정보 제어, 사용자 ID에 대한 익명성 제공을 통한 신원 결합 행위 차단, 그리고 신원 서버에 의한 사용자의 신원 정보사용 행위 관찰 배제 등 모든 프라이버시 요구사항에 대해 Passport 모델은 문제점을 안고 있다. 프라이버시 보장 부재 문제는 Passport 신원 관리 모델이 인터넷상에서 확장될 수 없게 만든 가장 큰 요소가 되고 있다.

Liberty Alliance의 연방형 신원 관리 모델의 경우 사용자가 CoT내에서 신원 서버를 선택할 수 있고 신원 서버의 신원 정보에 대한 사용자 제어를 허용한다. 그리고 Liberty Alliance는 연방화된 사용자 신원에 대한 서비스 제공자별 필명(pseudonym) 발급을 통해 신원 결합을 방지할 수 있게 한다. 반면 사용자의 서비스 제공자 접근 정보는 비록 사용자에 의해 연방화 과정에서 동의가 되었다할 지라도 동일한 CoT내의 신원 서버에 의해 관찰될 수 있다는 측면에서 프라이버시 문제 발생의 소지를 안고 있다.

CardSpace 신원 관리 모델은 사용자가 InfoCard를 발급할 신원 서버를 선택하고, 서비스 제공자의 신원 요구 사항을 충족시키는 신원 서버를 선택할 수 있으며, 신원 서버의 신원 정보에 대한 사용자 제어를 허용한다. 그리고 CardSpace 모델에서 사용자의 서비스 제공자 접근 정보를 사용자의 신원 선택장치를 통해 신원 서버로부터 차단할 수 있기 때문에 신원 서버의 사용자 서비스 제공자 접근 행위 관찰로부터 자유로울 수 있다.

OpenID 신원 관리 모델의 경우 사용자가 신원 서버를 선택할 수 있고, 신원 서버의 신원 정보에 대한 사용자 제어를 허용하고, OpenID 2.0을 통해 필명(pseudonym)을 지원한다. 그러나 사용자의 모든 서비스 제공자 접근 기록이 신원 서버에 의해 관찰될 수 있다는 측면에서 프라이버시 문제를 안고 있다. 신원 관리 2.0 모델들에 대한 프라이버시 관점에서의 비교 분석 결과는 표 2와 같다.

표 2. 프라이버시 비교 분석
Table. 2 comparative analysis of privacy

	Passport	Liberty Alliance	CardSpace	OpenID
Privacy	L	M	H	M

3.3. 신뢰성 비교 분석

Passport와 같은 중앙 집중형 신원 관리 모델의 가장 큰 장점은 마이크로소프트와 같은 대형 기관에 의해 관리되는 신원 서버를 신뢰할 수 있다는 점이다. 사용자는 Passport 서버에 의한 자신의 신원 정보의 안전한 관리를 신뢰할 수 있고, 서비스 제공자는 사용자 신원 정보 관리와 신원 보증 수준을 신뢰할 수 있다. 그러나 Passport 중앙 집중형 신원 관리 모델의 경우 서비스 제공자에 대한 신뢰 여부는 전적으로 사용자의 판단에 달려 있기 때문에 서비스 제공자에 대한 신뢰 수준은 낮다. Liberty Alliance 연방형 신원 관리 모델은 기본적으로 신뢰 동아리인 CoT에 속한 서비스 제공자들에 의해 신뢰성이 검증된 신원 서버를 사용하므로 신원 서버에 대한 높은 신뢰성을 확보한다. 마찬가지로 신원 서버에 의해 신뢰성이 검증된 서비스 제공자에 대해서도 높은 신뢰성을 확보할 수 있다. 즉, Liberty Alliance 신원 관리 모델은 CoT라는 신뢰 인프라가 높은 신뢰성을 제공한다.

CardSpace 신원 관리 모델의 경우 사용자는 자신의 신원 서버를 선택하여 InfoCard를 발급받을 수 있고, 서비스 제공자는 자신이 요구하는 사용자 신원 요구사항을 신원 서버에게 제시하고, 적절한 신원 보증 수준을 제공하는 신원 서버의 신원 관리 서비스를 제공받을 수 있다. 또한 CardSpace는 서비스 제공자에 대한 인증서를 사용자에게 제시한다. 그러나 CardSpace 신원 관리 모델에서 신원 서버와 서비스 제공자의 신뢰성에 대한 최종 판단은 사용자에 의해 이루어진다. 따라서 사용자의 관련 지식, 서비스 사용 습관 등에 따라 전체적인 신뢰성이 의존하는 문제점이 있다. OpenID 신원 관리 모델은 신원 서버에 대한 신뢰성 판단을 전적으로 사용자에게 의존하고, 서비스 제공자는 사용자가 제시한 신원 서버를 사용하기 때문에 신원 서버에 대한 신뢰성이 낮은 문제점이 있다. 또한 OpenID는 서비스 제공자에 대한 신뢰성을 높일 수 있는 어떤 서비스도 제공하지 않는다. 신뢰할 수 없는 서비스 제공자에 의한 위조된 서비스 제공자로의 사용자 redirect는 심각한 피싱 공격(phishing attack) 문제를 야기할 수도 있다. 신원 관리 2.0 모델들에 대한 신뢰성 관점에서의 비교 분석 결과는 표 3과 같다.

표 3. 신뢰성 비교 분석
Table. 3 comparative analysis of trustworthiness

	Passport	Liberty Alliance	CardSpace	OpenID
Trustworthiness	M	H	M	L

3.4. 확장성 비교 분석

Passport와 같은 중앙 집중형 신원 관리 모델의 가장 큰 단점 중의 하나는 확장성(scalability) 부족이다. 중앙 집중형의 Passport 서버를 통한 모든 사용자에 대한 신원 서비스 제공은 한계가 있을 수밖에 없다. 그리고 단일 신원 서버를 통해 다양한 서비스 제공자의 신원 서비스 요구 사항을 충족시키는 것도 매우 어려운 일이다. 뿐만 아니라 사용자와 서비스 제공자가 선택할 수 있는 다양한 신원 증명 기술의 개발과 적용을 위해 신원 서버간의 서비스 경쟁이 반드시 필요하다. Passport와 같은 중앙 집중형 신원 관리 모델을 결국 다양한 신원 증명 기술의 개발과 적용을 방해하는 중요한 요인이 된다.

분산 신원 관리 모델인 Liberty Alliance는 사용자 지원 측면에서 확장성의 문제는 없지만 CoT를 형성하는 신원 서버와 서비스 제공자간에 사업적인 협약을 통해 신뢰 관계를 형성하여야 하고, 사용자에 의한 신원 연방화 절차 수행이 필요하기 때문에 많은 수의 서비스 제공자를 수용하기 어려운 모델이다. 그렇지만 CoT 구성 시에 서비스 제공자들이 요구하는 신원 증명 기술을 지원하는 신원 서버를 포함시킬 수 있으므로 다양한 신원 증명 기술 지원에 어려움을 야기하지 않는다.

CardSpace와 OpenID 신원 관리 모델은 기본적으로 특정 신원 서버에 의존하지 않는 분산형의 신원 관리 서비스를 제공하고, 신뢰 관계 구축을 위한 사용자 구성(configuration) 절차 등을 별도로 요구하지 않으므로 확장성 측면의 문제점이 발생하지는 않는다. 신원 관리 2.0 모델들에 대한 확장성 관점에서의 비교 분석 결과는 표 4와 같다

표 4. 확장성 비교 분석
Table. 4 comparative analysis of scalability

	Passport	Liberty Alliance	CardSpace	OpenID
Scalability	L	M	H	H

Ⅳ. 신원 관리 3.0 전망

3장의 분석 결과를 토대로 최근 개발된 신원 관리 2.0 모델들의 장점, 단점, 그리고 개선점을 정리하면 표 5와 같다.

표 5를 통해 우리는 사용자 편의성(usability) 관점에서 Passport와 OpenID와 같이 사용자는 가능하면 적은 수의 신원 서버의 신원 관리 서비스를 통해 모든 서비스 제공자를 접근하는 것이 바람직함을 알 수 있다. 그러나 프라이버시(privacy)와 확장성(scalability) 관점에서 신원 관리 모델은 중앙집중형 대신 사용자와 서비스 제공자의 선택권이 보장되는 분산형(distributed)이 되어야 함을 알 수 있다.

그리고 표 5를 통해 우리는 Liberty Alliance와 같이 신뢰 인프라(trust infrastructure)를 통한 신원 서버와 서비스 제공자에 대한 신뢰성(trustworthiness) 제공이 요구됨을 알 수 있다. 그리고 신뢰 인프라의 구축이 Liberty Alliance와 같이 참여자의 상호 협약 기반의 폐쇄형으로 이루어지는 것은 확장성 측면에서 제약이 있을 수밖에 없다는 것도 알 수 있다. 따라서 보다 개방적인 신뢰 인프라(open trust infra) 기반의 신원 관리 모델 구축이 필요함을 알 수 있다.

표 5에서 신원 정보에 대한 프라이버시 보호는 CardSpace와 같이 사용자가 자신의 신원 정보를 제어하고, 사용자가 자신의 제어 영역 내에 있는 장치를 통해 신원 서버와 서비스 제공자간의 통신을 중계함으로써 불필요한 신원 정보 공유를 차단할 수 있는 사용자 중심(user-centric)의 신원 관리를 통해 이루어지는 것이 바람직함을 알 수 있다.

표 5. 신원 관리 2.0 모델 특징 요약
Table. 5 summary of characteristics of identity management 2.0 models

	장점	단점	개선점
Passport	usability	privacy, scalability	trustworthiness
Liberty Alliance	trustworthiness	usability	privacy, scalability
Cardspace	privacy, scalability	-	usability, trustworthiness
OpenID	usability, scalability	trustworthiness	privacy

따라서 우리는 미래 인터넷을 위한 신원 관리 3.0 모델은 그림 1과 같은 방향으로 발전되어야 할 것으로 판단한다.

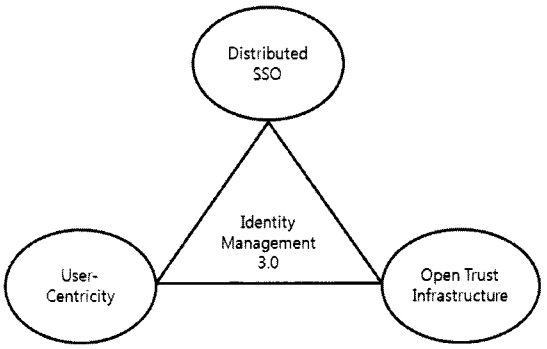

그림 1. 신원 관리 3.0 모델 발전 방향
Fig. 1 development direction of identity management 3.0 model

본 논문이 전망하는 신원 관리 3.0 모델은 2.0 모델이 가지고 있는 단일 사인온(SSO-Single Sign-On)의 장점을 분산 신원 관리 모델을 통해 제공하되 가능하면 작은 수의 신원 서버의 신원 관리 서비스를 통해 모든 서비스 제공자를 접근할 수 있게 한다. 사용자가 사용할 최대 신원 서버의 수는 표준화된 신원 보증 수준(level of identity assurance)의 수가 될 것이다. 예를 들어 [17]의 표준을 적용할 경우 사용자는 수준별 1개의 공인된 신원 서버를 포함하는 최대 4개의 공인 신원 서버를 사용함으로써 서비스 제공자가 요구하는 모든 신원 서비스를 제공받을 수 있다.

그리고 신원 관리 3.0 모델은 Liberty Alliance의 폐쇄형 신뢰 인프라의 확장성 문제를 극복할 수 있도록 개방형 신뢰 인프라(open trust infrastructure)에 기초하여야 될 것으로 판단한다. 신원 관리 3.0 모델은 충분한 확장성을 제공하는 개방형 신뢰 인프라(open trust infrastructure)가 신원 서버의 신원 보증 수준을 공인하고(certificate), 서비스 제공자의 신원 정보 보호 수준(level of identity protection)을 공인함으로써 사용자에게 신뢰성을 제공하게 될 것이다. 사용자는 개방형 신뢰 인프라를 통해 공인된 신원 서버와 서비스 제공자를 화이트 리스트(white list)등을 통해 확인할 수 있다. 동일한 신원 보증 수준을 제공하는 모든 신원 서버는 상호동작(interoperability)을 보장함으로써 하나의 신원 서버를 통해 해당 수준의 신원 관리 서비스를 요구하는 모든 서비스 제공자를 접근할 수 있게 한다.

인터넷을 통한 민감한 데이터 공유가 더욱 활성화될 미래 인터넷 환경에서 프라이버시 보호는 신원관리에서 매우 중요한 요구사항이 된다. 신원 관리 3.0 모델은 CardSpace와 같이 사용자가 자신의 신원 정보를 제어하고, 사용자가 자신의 제어 영역 내에 있는 신원 중계 장치(identity relay device)를 통해 신원 서버와 서비스 제공자간의 통신을 중계함으로써 불필요한 신원 정보 공유를 차단할 수 있는, 사용자 중심(user-centric)의 신원 관리서비스를 제공함으로써 프라이버시 보호를 강화하게 될 것이다. 사용자 중심의 신원 관리 모델은 신원 중계 장치가 OCSP[18]등과 같은 검증 프로토콜(validation protocol)을 통해 신원 서버와 서비스 제공자의 인증 상태를 자동으로 확인할 수 있게 함으로써, 사용자의 판단에 의존하는 개방형 신뢰 인프라 기반의 신뢰성 제공의 문제점을 보완하는 장점도 기대할 수 있다.

V. 결론

현재 인터넷 환경의 신원 관리 1.0 모델이 안고 있는 사용자 편의성 부족, 고비용 구조, 프라이버시 보호 어려움, 그리고 신뢰 인프라 부재 등의 문제를 해결하기 위해 Passport/LiveID, Liberty Alliance/SAML, CardSpace, OpenID 등 다양한 형태의 신원 관리 2.0 모델들이 개발되어 왔다. 신원 관리 2.0 모델들은 단일 사인온(single sign-on) 기반의 서비스 편의성 등 여러 가지 장점을 제공함에도 불구하고 아직 기존 신원 관리 1.0 모델을 대체할 수 있을 정도로 실제 인터넷 환경에서 광범위하게 수용되지 못하고 있다. 본 논문은 대표적인 신원 관리 2.0 모델들의 비교분석을 통해 신원 관리 2.0 모델들의 장단점과 개선점을 파악하고, 미래 인터넷을 위한 신원 관리 3.0 모델의 발전 방향을 전망하였다.

미래 인터넷을 위한 신원 관리 3.0 모델은 분산 SSO (Single Sign-On)에 기초하되 표준화된 신원 보증 수준(level of identity assurance)의 개수 정도의 작은 수의 신원 서버를 통해 모든 서비스 제공자를 접근할 수 있게 할 것이다. 또한 신원 관리 3.0 모델은 개방형 신뢰 인프라를 통해 신원 서버의 신원 보증 수준을 인증하고, 서비스 제공자의 신원 정보 보호 수준(level of identity protection)을 인증함으로써 충분한 신뢰성을 제공하게 될 것이다. 그리고 신원 관리 3.0 모델은 사용자 중심(user-centric)의 신원 관리서비스를 통해 완전한 프라이버시 보호를 가능하게 할 것으로 전망된다.

참고문헌

[1] FIDIS, "D3.17:identity Management Systems - recent developments", www.fidis.net, August 2009.

[2] A. Josang and S. Pope, "User Centric Identity Management", AusCERT Conference, 2005.

[3] D. P. Korman and A. D. Rubin, "Risks of the Passport Single Signon Protocol", IEEE Computer Networks, July 2000.

[4] http://en.wikipedia.org/wiki/Windows_Live_ID

[5] Liberty Alliance Project, "Liberty ID-FF Architecture Overview", Liberty Alliance, 2004.

[6] OASIS, "Security Assertion Markup Language(SAML) V2.0 Technical Overview", http://www.oasis-open.org, March 2008.

[7] O. T. Seierstad, "Microsoft Windows CardSpace and the Identity Meta System", Telektronikk 3/4, 2007.

[8] OpenID Foundation, "OpenID Authentication 2.0 - Final", http://openid.net/specs/openid-authentication-2_0.html, Dec. 2007.

[9] T. E. Maliki and J.-M. Seigneur, "A Survey of User-centric Identity Management Technologies", Proc. of Int'l Conference on Emerging Security Information, Systems and Technologies, pp. 12-17, 2007.

[10] E. Maler and D. Reed, "The Venn of Identity - Options and Issues in Federated Identity Management", IEEE Security & Privacy, March/April 2008.

[11] Aries Fajar Dwiputera, "Single Sign-On Architectures in Public Networks(Liberty Alliance)", *INFOTECH Seminar Communication Services,* 2005.

[12] K. Cameron and M. B. Jones, "Design rationale behind the Identity Metasystem Architecture", http://research.microsoft.com/en-us/um/people/mjb/papers/Identity_Meatsystem_Design_Rationale.pdf, 2006.

[13] W. A. Alrodhan and C. J. Mitchell, "Addressing privacy issues in CardSpace", Proc. of 3rd Int'l Symposium on Information Assurance and Security, 2007.

[14] D. Chadwick and S. Shaw, "Review of OpenID", JISC Final Report(http://www.jisc.ac.uk/whatwedo/programmes/einfrastructure/reviewofopenid.aspx), Dec. 2008.

[15] M. Hansen, A. Schwartz, and A. Cooper, "Privacy and Identity Management", IEEE Security and Privacy, March/April 2008.

[16] U. Kylau, I. Thomas, M. Menzel, and C. Meinel, "Trust Requirements in Identity Federation Technologies", Int'l Conf. on Advanced Networking and Applications, 2009.

[17] TTAI.IT-Xeaa, "개체 인증에 대한 보증 프레임워크 (Entity Authentication Assurance Framework)", 한국정보통신기술협회, 2010년 12월 23일

[18] M. Myers, et. al., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999

저자소개

박승철(Seungchul Park)

'85.2 : 서울대 계산통계학과 졸
'87.2 : KAIST 전산학과 석사
'96.8 : 서울대 컴퓨터공학과 박사
ETRI 연구원, 한국IBM, 현대전자 네트워크연구소장, 현대네트웍스(주) 연구소장 역임
현재 한국기술교육대학교 부교수
※관심분야 : 광대역통신망, 멀티미디어통신, P2P 스트리밍, 신원 관리