韓國IT서비스學會誌
第10卷 第2號
2011年 6月

미래 인터넷 서비스 환경을 위한 인증 시스템 분석*

박 승 철**

Analysis of Authentication Systems for Future Internet Service Environments*

Seungchul Park**

■ Abstract ■

In the current Internet environment, there may exist a number of independently-operating authentication systems even within a single organization, according to the service types and service providing entities. Current silo-style isolated authentication system model has revealed critical problems in the aspects of usability, cost-effectiveness, extensibility and flexibility, and privacy protection. Recently, several next generation authentication systems have been actively developed by leading industrial and standardization institutions, This paper firstly analyzes the problems of current Internet authentication system environments. And then, the underlying idea, operating procedures, and pros and cons of the newly developed next generation authentication systems are analyzed so as to provide the selection guidelines for the new authentication systems and drive further development directions for future Internet authentication systems.

Keyword : Authentication, Identity Management, Privacy

논문투고일 : 2010년 01월 18일 논문수정완료일 : 2011년 03월 06일 논문게재확정일 : 2011년 06월 14일
* 이 논문은 한국기술교육대학교 교육연구진흥비 프로그램의 지원에 의하여 수행되었음.
** 한국기술교육대학교 컴퓨터공학부

1. 서 론

현재 우리가 사용하고 있는 대부분의 인증 시스템은 특정한 그룹의 사용자에게 특정 서비스를 제공하는 서비스 제공자가 자신의 인증 요구사항에 맞게 별도의 인증 시스템 환경을 구축하고 운용하는 서비스 제공자 중심의 모델(service provider centric model)을 따른다[1]. 현재의 서비스 제공자 중심의 인증 시스템 모델은 서비스의 종류에 따라 그리고 서비스 제공 주체에 따라 하나의 조직(organization)내에서도 다수의 서로 독립적인 인증 시스템이 존재하는 사일로(silo) 형태의 고립형 모델(isolated model)이다[2]. 각 서비스 제공자는 자신의 사용자를 위해 별도의 신원 서버와 인증 장치를 구축하고 운용하고, 사용자는 각 서비스 제공자 인증 시스템에 신원 정보를 제공하고 신원 증명 정보를 발급받고 유지하고 사용한다. 서비스 제공자는 자신의 인증 및 사업적인 필요에 따라 인증 메카니즘, 인증 정책, 그리고 사용자 신원 속성(identity attributes) 등을 설계하고 사용자에게 일방적으로 따르도록 요구한다. 사용자는 서비스 제공자마다 다른 정책으로 운용되는 다수의 인증 시스템을 사용한다. 인터넷 기반의 서비스가 다양해짐에 따라 사용자는 더 많은 수의 서로 다른 인증 시스템을 사용하게 된다.

ISP 접속, 웹 서버 접근, 인터넷 쇼핑, 인터넷 전화, 인터넷 뱅킹, 모바일 인터넷 등 인증 요구 수준이 서로 다른 인터넷 기반 서비스의 확산은 서비스 제공자 중심의 고립형 인증 시스템 모델에서 인증 시스템 개발, 인증 시스템 운용, 그리고 사용자의 인증 시스템 사용 환경을 더욱 복잡하게 만든다. 특정 서비스 개발자는 별도의 신원 서버와 인증 장치를 포함하는 별도의 인증 시스템을 개발해야 하고, 유지하고 보수하고 운영해야 하므로 시간적 측면과 비용적 측면에서 낭비를 초래하고 있다. 사용자의 경우 인증 시스템 마다 신원 정보를 중복하여 제공하고 서로 다른 정책에 의해 발급되는 신원 증명 정보들을 유지하고 사용해야 하는 불편함을 감수해야 한다.

본 논문은 현재의 인터넷의 인증 시스템 환경의 문제점들을 구체적으로 분석하고, 이러한 문제점들을 개선하기 위해 시도되고 있는 Passport, OpenID, Liberty Alliance, PRIME 등 새로운 개념의 차세대 인증 시스템들의 장단점을 분석하고자 한다. 새로운 개념의 인증 시스템들에 대한 분석은 미래인터넷 환경에서 사용자들이 특정 서비스 환경에 적합한 새로운 개념의 인증 시스템을 선택하는 기준을 제시할 뿐만 아니라, 미래인터넷을 위한 인증 시스템 발전 방향을 제시한다.

본 논문의 구성은 다음과 같다. 제 2장은 현재 인터넷 인증 시스템 환경의 문제점을 구체적으로 분석하고, 제 3장은 최근에 시도되고 있는 새로운 개념의 차세대 인증 시스템들을 분석한다, 제 4장은 차세대 인증 시스템들의 장점과 단점을 분석하고, 제 5장에서 미래 인터넷 서비스 환경에서의 인증 시스템 연구 및 개발 방향을 제시하는 것으로 결론을 맺는다.

2. 현재 인터넷 인증 시스템의 문제점 분석

2.1 사용자 편의성 부족

현재의 인증 시스템 환경의 가장 큰 문제점은 사용자의 편의성 부족이다. 현재의 서비스 제공자 중심의 고립형 인증 시스템 환경의 사용자들은 다음과 같은 편의성 부족의 어려움에 직면해 있다[1, 2].

- 신원 증명 정보 관리의 어려움 : 사용자는 서로 다른 인증 정책을 사용하는 서비스 제공자의 요구사항에 맞는 사용자 이름/패스워드 등과 같은 신원 증명 정보를 사용해야 하므로 사용하는 서비스의 수에 따라 많은 수의 신원 증명 정보를 유지하고 사용해야 하는 어려움에 처해 있다.
- 신원 정보의 중복 및 반복적인 등록 : 서비스 제공자 중심의 고립형 인증 시스템 환경은 사용자가 특정 서비스를 사용하기 위해 서비스

제공자가 임의의 정책에 따라 설계한 신원 정보 체계에 따라 신원 정보를 등록해야 하고 해당 서비스 제공자가 발급하는 신원 증명 정보를 발급받아야 한다. 새로운 서비스를 사용할 때는 동일한 신원 정보를 포함하여 다시 해당 시스템이 요구하는 신원 정보를 반복적으로 등록하고 신원 증명 정보를 발급받아야 한다.

- 반복적인 로그인과 로그아웃 : 사용자는 각 서비스를 사용할 때 마다 로그인(login)과 로그아웃(logout)을 반복하고 처음 사용하는 서비스의 경우 신원 정보 등록과 신원 증명 정보 발급 절차를 수행한 다음 로그인을 해야 한다. 사용자가 다수의 서비스 제공자에 대해 동일한 신원 증명 정보를 사용하는 경우에도 반복적인 로그인과 로그아웃을 피할 수 없다

2.2 고비용 구조

현재 우리가 사용하고 있는 사일로(silo) 형태의 고립형 인증 시스템 모델은 서비스 제공자 마다 독자적인 인증 시스템을 개발하여야 하고 사용자의 신원 정보를 중복적으로 저장하고 관리하는 것이 불가피하다.

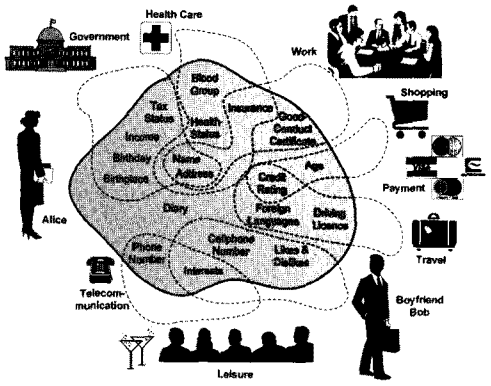
- 개발 측면 : 서비스 제공자 마다 신원 정보 서버, 인증 장치, 인증 클라이언트 등을 포함하는 독자적인 인증 시스템 개발은 많은 부분 중복 개발을 불가피하게 만들고 이에 따라 개발 비용 증가를 초래한다.
- 관리 측면 : 각 인증 시스템이 독자적으로 신원 정보를 안전하게 유지하고 관리하여야 하므로 이에 따른 시스템 구축 비용과 관리비용 증가가 불가피하다. 각 인증 시스템이 안전하게 신원 정보를 관리하고 있는 지를 감시하고 감사할 수 있는 체계를 구축하는 데에도 많은 비용과 노력이 소모될 수밖에 없다.

2.3 확장성 및 유연성 부족

현재 인증 시스템 환경에는 다양한 인증 프로토콜(authentication protocol), 검증 프로토콜(validation protocol), 어써션 프로토콜(assertion protocol), 그리고 프로비져닝 프로토콜(provisioning protocol)이 사용되고 있으나 대부분의 프로토콜들은 웹 서비스, 인터넷 접속 서비스, 모바일 인터넷, 인터넷 뱅킹 등 특정 환경에서 특정 서비스를 위해 특정 수준의 인증 서비스 제공에 적합하게 개발되었다. 따라서 기존의 프로토콜 체계에 따라 구축된 인증 시스템을 새로운 환경에서 새로운 서비스에 적합한 새로운 수준의 인증 서비스 제공에 적용하기가 매우 어렵다. 예를 들어 사용자 뿐만 아니라 장치 인증에 널리 사용되고 있는 PKI(Public Key Infrastructure) 인증서 기반의 상호 인증은 공개 열쇠 암호화 처리가 가능한 고성능 장치에 적합하게 개발되었다. 이러한 PKI 인증서 기반의 상호 인증 시스템을 새롭게 구축되는 IoT(Internet of Things) 센서 등 저성능 인터넷 장치로 확장하여 사용하기가 현재로서는 사실상 불가능하다. 뿐만 아니라 PC 등 인증 빈도가 높지 않은 환경에 적합한 PKI 인증서 기반의 상호 인증 시스템을 통신 장치(라우터, 스위치 등)의 패킷 소스(출발지) 인증 등 보다 동적인 환경으로 확장하기엔 패킷 처리 성능에 지나친 부담 초래하여 사용하기가 어렵다. 따라서 이와 같은 새로운 환경의 새로운 인증 서비스를 위해 기존 인증 시스템과 다른 별도의 인증 메카니즘과 프로토콜 개발이 불가피해진다. 또한 기존 인증 시스템에 보다 강한 인증을 위한 새로운 기능(multi-factor authentication)을 추가하기가 어렵고 서로 다른 인증 요구사항을 가지는 다양한 사용자/장치를 적절하게 수용하기가 어려운 문제를 안고 있다.

2.4 프라이버시 보호 체계 미흡

많은 종류의 인터넷 서비스를 사용하는 사용자는 [그림 1]과 같이 자신이 인지하지 못하는 상태에서 자신의 많은 개인 정보가 인터넷에 노출되는 환경에서 생활하고 있다[3].



[그림 1] 사용자의 신원 정보 노출 상황

- 불필요한 개인 정보 요구 : 현재 인터넷 인증 환경에서 대부분의 사용자는 서비스 이용 수준에 관계없이 서비스 제공자가 요구하는 모든 정보를 제공해야 한다. 예를 들어 주소 정보의 경우 물건 또는 우편물을 배송할 경우에만 필요한 정보이지만 많은 경우 물건 또는 우편물의 배송 요청과 무관하게 사용자의 관련 정보를 요구한다. 그리고 단순한 서비스 이용의 경우에도 익명이 아닌 반드시 실명 확인을 거치도록 요구하는 경우가 많다.
- 서비스 제공자 인증의 어려움 : 대부분의 기존의 인증 시스템들은 서비스 제공자에 의한 사용자 인증에 초점을 맞춰 개발되었기 때문에 사용자가 서비스 제공자를 인증하기가 어렵다. 대부분의 서비스 제공자는 사용자에 의한 서비스 제공자 인증 방안을 지원하지 않는다. 설령 인증서에 의한 상호 공개 열쇠 기반의 인증 메카니즘등을 통해 서버 인증 방안을 지원한다 할지라도 대부분의 사용자는 기술적인 이해도 부족 또는 사용상의 어려움 등으로 인해 사용할 수 없는 현실이다.
- 신원정보 수집, 유지, 그리고 이용에 대한 사용자 통제 체계 미흡 : 대부분의 서비스 제공자는 자신이 원하는 신원 정보 수집에 대한 일괄적인 동의를 요구하고 동의하지 않는 경우 서비스를 제공하지 않는다. 많은 경우 동의 절차 자체가 생략되기도 한다. 또한 대부분의 경우 사용자는 수집된 자신의 개인 정보가 서비스 제공자에 의해 어떻게 관리되고 있는 지에 대해 파악할 수 없고 단지 서비스를 이용하기 위해서는 믿을 수밖에 없는 것이 현실이다. 더욱이 사용자는 수집된 자신의 개인 정보가 어떻게 사용되고 있는 지를 파악하기는 더욱 어렵다.

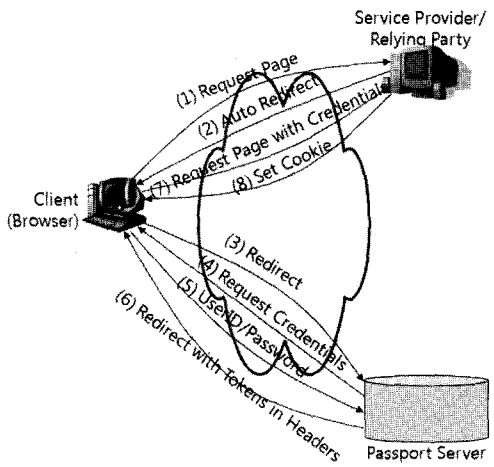
3. 차세대 인증 시스템

최근에 들어와서 이러한 문제들을 해결하기 위해 차세대 인증 시스템을 위한 많은 연구 개발 노력들이 진행되고 있다. 차세대 인증 시스템 개발을 위한 노력은 단일 인증 시스템으로의 통합, 서비스 제공자 중심(service provider centric)의 기존 인증 시스템에서 사용자 중심(user centric)의 인증 시스템으로의 전환, 인증 시스템간 연동을 통한 연방형 인증 시스템 환경 구축, 프라이버시 보장형 인증 시스템 개발 등에 집중되어 왔다. 통합 인증 시스템 개발을 위한 대표적인 시도는 마이크로소프트사의 Passport 인증 시스템과 그 후속 시스템인 Live ID 시스템을 들 수 있다. 사용자 중심의 인증 시스템 개발의 대표적인 시도는 OpenID Foundation의 OpenID 시스템을 들 수 있다. 연방형 인증 시스템 환경 구축을 대표적인 시도는 Liberty Alliance의 연방형 신원 관리 시스템(Federated Identity Management System)을 들 수 있다. 프라이버시 보장형 인증 시스템 구축은 EU의 PRIME과 PrimeLife 프로젝트를 들 수 있다.

3.1 Passport

Passport 인증 시스템은 마이크로소프트에서 서비스 제공자 중심의 고립형 인증 시스템 환경에서 발생하는 편의성 부족과 고비용 구조 문제를 해결하고 사용자의 신원 정보를 안전하게 관리하기 위하여 개발된 웹 기반의 통합 인증 시스템이다[4].

Passport 시스템에서는 사용자의 모든 신원 정보가 마이크로소프트에 의해 관리되는 Passport 서버에 등록되고, 유지되고, 관리된다. 그리고 사용자가 Passport 인증 시스템을 사용하는 서비스 제공자(Passport 인증 시스템의 RP(Relying Party))에 로그온하고자 하는 경우 해당 사용자에 대한 인증 요구는 사용자의 웹 브라우저를 경유하여 Passport 서버에게 전달되고, 모든 인증 서비스는 Passport 서버에 의해 통합적으로 제공된다. [그림 2]는 Passport 인증 시스템의 동작 절차를 보여준다.



[그림 2] Passport 인증 시스템의 동작 절차

(1) 웹 브라우저 사용자가 Passport 인증 시스템을 사용하는 서비스 제공자의 특정 웹 페이지의 접근을 요청한다.

(2),(3) 서비스 제공자는 해당 사용자를 Passport 서버에게 인증을 위해 Redirect한다.

(4) Passport 서버는 해당 사용자 웹 브라우저와 보안 채널(SSL/TLS)을 설정하고 로그인 페이지를 제공한다.

(5) 사용자는 보안 채널을 통해 사용자 이름과 패스워드를 입력한다.

(6) 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 서버가 다시 Passport 서버를 방문할 때 로그인 절차를 생략하기 위해 사용된다.

(7) 암호화된 인증 정보와 함께 웹 페이지 요청 메시지가 서비스 제공자에게 전달된다.

(8) 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.

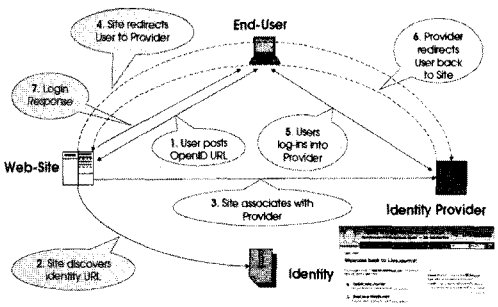
3.2 OpenID

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 사용자 중심 인증 시스템이다[5]. OpenID 사용자는 자신의 브라우저를 통하여 접근하고자 하는 임의의 OpenID 지원 웹 사이트(Relying Party, RP라 함)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(OpenID Provider, OP라 함)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.

OpenID 인증 시스템의 동작 절차는 [그림 3]과 같다[6].

(1) 사용자가 UA(웹 브라우저)를 사용하여 목표 웹 사이트(RP)에 접근하면 OpenID 지원 웹 사이트는 사용자가 OpenID URL을 입력할 수 있는 인터페이스를 제공하고, 사용자는 자신의 OpenID URL(또는 XRI)를 입력한다.

(2) 목표 웹 사이트(RP)는 사용자가 입력한 OpenID URL을 기초로 Yadis 프로토콜 또는 HTML 기반의 발견 메카니즘을 사용하여 OP의 URL을 발견한다.



[그림 3] OpenID 인증 시스템의 동작 절차

(3) OP의 URL을 발견한 RP는 OP와의 안전한 메시지 교환을 위해 보안 채널(DH 알고리즘 등)을 설정한다. 만약 보안 요구사항이 높지 않은 환경에서 사용되는 OpenID 인증 시스템이라면 이 과정은 생략될 수 있다.

(4) RP는 사용자의 접근 요청을 발견된 OP에게 redirect함으로써 해당 OpenID에 대한 인증을 의뢰한다.

(5) 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 이미 로그인 상태에 있으면 이 과정은 생략될 수 있다. OpenID 인증 시스템은 기본적으로 RP에 대한 신뢰 여부를 사용자가 판단하게 한다.

(6) OP는 OpenID에 대한 인증 결과를 담은 어써션을 서명된 redirect 메시지로 해당 RP에게 전달한다.

(7) RP는 OP로부터 수신한 redirect 메시지의 서명을 확인하고 인증 결과를 확인한다. 인증 결과가 성공이면 RP는 해당 사용자에 대해 인가 작업을 수행한다. 이 과정에서 RP는 OP에게 해당 사용자에 대한 추가적인 신원 정보를 요청할 수 있다.

3.3 Liberty Alliance

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 결성하였다. Liberty Alliance는 다음과 같은 구체적인 목표를 가지고 있다[7].

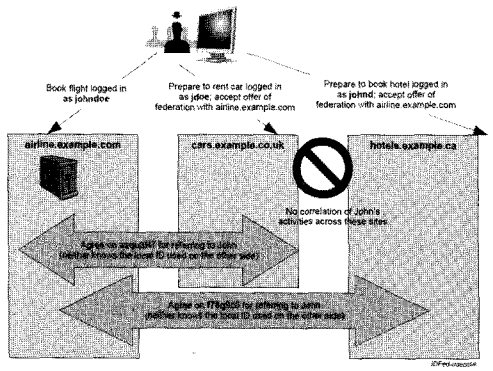
- 사용자들이 자신들의 신원 정보의 프라이버시 보호와 보안 유지를 가능하게 한다.
- 사업자들이 제 3자의 개입 없이 자신들의 고객 관계 정보를 유지하고 관리할 수 있게 한다.
- 다수의 서비스 제공자로부터 비집중형(decentralized) 인증에 기초한 개방형의 단일 사인온(single sign-on) 표준을 제공한다.
- 현재와 미래의 모든 네트워크 접속 장비를 지원할 수 있는 네트워크 신원 기반구조(network identity infrastructure)를 만든다.

이러한 목표들을 성취하기 위해 Liberty Alliance는 신뢰 동아리(Circle of Trust, CoT)와 신원 연방화(identity federation) 개념을 개발하였다. CoT는 상호 사업적인 협약을 통해 신뢰 관계를 형성한 Liberty 아키텍처를 따르는 서비스 제공자(Service Provider, SP)들과 신원 제공자(Identity Provider, IdP)들의 연방(federation)이다[8].

CoT에서 서비스 제공자(SP)는 사용자에게 서비스 그리고/또는 상품을 제공하는 실체이다. SP는

프라이버시 보호 등을 위해 일반적으로 자체적인 인증 및 인가 메카니즘을 가지고 있지만 단일 사인온 서비스와 신원 정보의 안전한 관리 등을 위해 CoT내의 신원 제공자(IdP)에게 신원 관리 서비스를 의존한다. CoT의 신원 제공자(IdP)는 SP들이 CoT에 가입할 수 있도록 사용자에 대한 신원 관리 서비스를 대신 제공하는 실체이다. IdP는 신원 서비스 제공 과정에서 사용자의 프라이버시가 보호될 수 있게 하고 신원 정보가 안전하게 전달되도록 보장한다. 사용자는 기존의 웹 브라우저 등을 사용하여 믿을 수 있는 특정 IdP 통해 같은 CoT 내 또는 다른 CoT의 서비스 제공자들을 단일 사인온 방식으로 편리하게 접근할 수 있고, CoT 내의 SP들의 신원 정보 관리와 프라이버시 보호 등을 신뢰할 수 있다.

사용자의 신원은 다수의 서비스 제공자들이 해당 사용자를 참조하기 위해 사용하는 식별자와 신원 속성들에 대해 서비스 제공자들간의 합의에 의해 연방화 될 수 있다. 한 사용자의 신원은 연방화 과정에서 SAML(Security AssertionMarkup Language)[9] 어써션으로 상호 공유되고, 연방화 과정에서 생성된 공유 이름 식별자를 통해 연방 도메인 내의 다른 서비스 제공자(신원 서버)의 인증 결과를 SAML 어써션으로 상호 공유할 수 있다. [그림 4]의 예의 경우 사용자(Jone Doe)는 현재 airline.example.com에서 johndoe 사용자 이름으로 비행기표를 예약하고 있다.

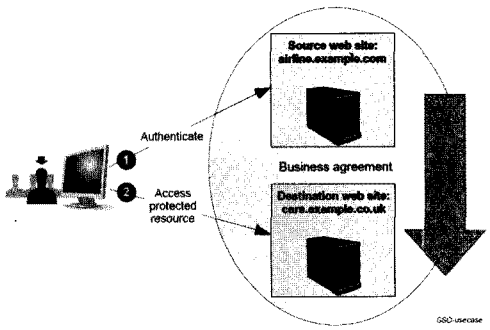


[그림 4] 신원 연방화(identity federation) 예

그런 다음 John은 cars.example.co.uk 사이트에서 렌트카를 예약하고자 한다. cars.example.co.uk 사이트는 사용자 John에게 지역 신원(jdoe)을 신원 서버 파트너 사이트인 airline.example.com와의 연방화에 동의하는 지 확인한다. John이 동의하면 cars.example.co.uk 사이트는 John에 대한 신원 정보를 포함하는 SAML 어써션 요청 메시지를 신원 서버 사이트인 airline.example.com에 전송한다.

airline.example.com 사이트는 John을 인증하고 새로운 필명(azqu3H7)을 생성하여 SAML 어써션 응답 메시지를 cars.example.co.uk 사이트에 전송한다. 이후 cars.example.co.uk 사이트와 airline.example.com 사이트는 John을 참조하기 위해 필명(azqu3H7)을 공동으로 사용하게 된다. 동일한 방식으로 johnd 사용자 이름을 사용하는 hotels.example.ca 사이트는 airline.example.com 사이트와 SAML 어써션 요청 및 응답 메시지 교환을 통해 연방화하고 John을 참조하기 위해 새로운 필명(f78q9c0)을 생성한다. 연방화된 사용자가 특정 사이트(cars.example.co.uk 또는 hotels.example.ca)에 접속하는 경우 각 사이트에서 인증 작업을 수행할 필요 없이 신원 서버 파트너 사이트(airline.example.com)의 인증 결과를 공유할 수 있다.

Liberty Alliance의 가장 대표적인 응용은 다중 도메인 웹 단일 사인온(web single sign-on) 서비스이다. 단일 사인온 서비스는 [그림 5]에서와 같이 사용자가 신원 서버 역할을 수행하는 하나의 웹 사이트(airline.example.com)에 로그인하고 있으면 해당 사이트와 신원 정보 공유를 상호 합의한 다수의 웹 사이트의 다른 웹 사이트(cars.example.co.uk)를 접속할 때 다시 로그인할 필요가 없도록 한다. 이 경우 신원 서버 웹 사이트는 해당 사용자의 신원 정보를 접속하고자 하는 목표 웹 사이트에게 SAML 어써션으로 안전하게 전달하고, 신원 서버 웹 사이트를 믿는 목표 웹 사이트는 SAML 어써션의 인증 결과를 확인함으로써 별도의 신원 검증 과정 없이 제한된 자원의 접근을 허용한다.

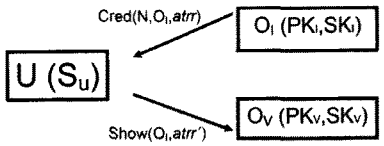


[그림 5] 단일 사인온 서비스 사용 예

3.4 PRIME

PRIME(Privacy and Identity Management for Europe) 프로젝트는 2004년부터 2008년까지 4년 간 EU의 FP6 프로그램의 일환으로 프라이버시 보호가 강화된 신원 관리 시스템을 시연하기 위해 진행되었다. PRIME 프로젝트에는 IBM 취리히 연구소를 주축으로 유럽의 20개 기관이 참여하였으며 현재의 FP7 프로그램에서도 PrimeLife 프로젝트로 계속 진행되고 있다. PRIME 프로젝트의 목표는 사용자가 자신의 신원 정보에 대한 제어권을 가지고 신원 정보의 노출을 최소화하면서 정보 서비스를 안전하고 편리하고 신뢰적인 방법으로 사용할 수 있는 신원 관리 시스템의 실현 가능성을 보이는 것이다[10].

PRIME 프로젝트는 온라인 서비스 이용 과정에서 개인 신원 정보의 노출을 최소화하기 위해 기존의 실명 인증서를 사용하는 대신 IBM 취리히 연구소에서 개발한 필명 인증서(pseudonymous certificate) 기반의 익명 신원증명 기법인 IDEMIX (Identity Mixer)를 사용한다[11, 12]. [그림 6]에서와 같이 익명 신원증명 시스템에서 사용자(U)는 항상 자신의 마스터 비밀 열쇠(S_U)에 근거하여 생성되는 필명(N)으로 신원증명서(credential) 발급 기관(O_I)이 자신의 비밀 열쇠(SK_I)로 서명한 익명 신원증명서(anonymous credential) 또는 필명 인증서(pseudonymous certificate)를 발급받는다.



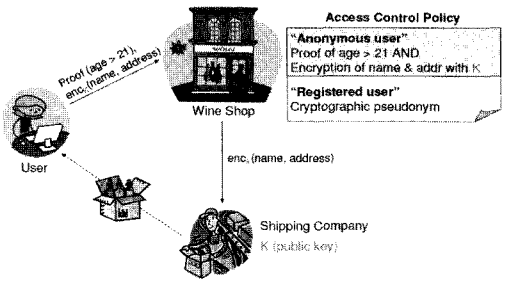
[그림 6] 익명 신원증명 시스템 프로토콜

익명 신원증명서는 사용자가 등록한 필명(N), 발급 기관(O_I), 그리고 사용자 신원 속성(attr)들을 포함한다. 익명 신원증명서를 발급받은 사용자는 자신의 신원을 확인하고자 하는 확인 기관(O_V)에게 자신의 실명과 발급받은 신원증명서의 내용(속성) 전체를 보여주는 대신에 다음과 같은 사실을 무지식 증명(zero-knowledge proof) 기법을 통해 확인 기관(O_V)에게 확신시켜준다.

- 발급 기관(O_I)가 필명(N)과 사용자 신원 속성(attr)들에 대해 서명한 신원증명서를 보유하고 있다.
- 발급 기관(O_I)이 서명한 필명(N)이 확인 기관(O_V)에서 사용하고 있는 자신의 필명과 동일한 비밀 열쇠(S_U)에 근거하여 생성된 자신(U)의 것이다.
- 신원증명서의 속성들의 일부 또는 전부에 대해 적용된 계산(arithmetic), 비교(comparative), 그리고 논리(logical) 연산이 참(true)이다.

따라서 사용자는 익명 신원증명 기법을 통해 [그림 7]과 같이 WineShop에 자신의 신원 정보가 모두 누출되는 신원증명서(인증서)를 보내는 대신 자신이 와인을 구매할 수 있는 연령(age > 21)임을 증명할 수 있다. 뿐만 아니라 이 과정에서 사용자는 확인 기관(O_V)에게 자신의 실명 등 자신의 실제 신원을 노출하지 않음으로써 확인 기관(O_V)이 사용자(U)를 전혀 식별할 수 없는 익명성(anonymity)을 보장한다. 이와 같은 익명성 보장은 확인 기관(O_V)이 사용자에 대해 허가 없이 개인 정보를 수집하고 가공하는 것을 원천적으로 차단할 수 있다. 만약 사용자(U)와 발급 기관(O_I)이 1회용 필명

(transactional pseudonym)을 사용하는 경우 확인 기관(O_V)은 동일한 사용자가 다시 방문하더라도 이를 인지할 수 없다.



[그림 7] 익명 신원증명 시스템 활용 예

PRIME 프로젝트의 IDEMIX 익명 신원증명 시스템은 사용자가 자신이 암호화한 메시지가 가지고 있는 특성을 메시지의 노출 없이 제3자(확인 기관)에게 확인시킬 수 있는 확인가능 암호화(verifiable encryption) 기법을 적용하였다. [그림 7]에서 보는 것처럼 사용자는 자신의 이름과 주소를 물류 회사(ShippingCompany)의 공개 열쇠(K)로 확인가능 암호화 기법으로 암호화하여 보내고, 확인 기관은 사용자의 이름과 주소를 알 수 없는 상태에서 단지 암호화된 메시지가 사용자의 이름과 주소가 정확하게 포함되어 있다는 특성만 확인한 다음 암호화된 메시지를 물류 회사(ShippingCompany)에게 전달한다. 따라서 사용자는 불필요하게 자신의 이름과 주소 정보가 WineShop에 노출되는 것을 차단할 수 있다.

4. 차세대 인증 시스템들의 장단점 분석

4.1 Passport 인증 시스템 장단점 분석

Passport 인증 시스템은 현재의 고립형 인증 시스템 환경을 완전 통합형으로 전환하기 위한 거의 최초의 시도였으며 초기에는 어느 정도 성공하였다. Passport 통합 인증 시스템은 다음과 같은 몇 가지 장점을 제공한다. 첫째, Passport 인증 시스템은 사용자로 하여금 자신의 신원 정보를 Passport 서버에게 한번만 등록하면 되도록 하기 때문에 서비스 제공자 중심의 고립형 인증 시스템 환경에서 반복적인 신원 정보 등록의 문제점을 해결한다. 둘째, Passport 인증 시스템을 사용하는 서비스 제공자들을 접근하고자 할 때 첫 번째 서비스 제공자에서 한번만 로그인하면 다음부터는 로그인 절차를 반복적으로 수행할 필요가 없는 단일 사인온(Single Sign-On) 서비스를 제공함으로써 사용자 편의성의 획기적으로 제고한다. 셋째, 사용자의 신원 정보가 신뢰할 수 있는 마이크로소프트에 의해 관리되는 Passport 서버에 유지되고 관리되므로 신원 정보 노출 위험이 획기적으로 감소된다.

이러한 장점에도 불구하고 Passport 인증 시스템이 인터넷 환경에서 광범위하게 사용되지 못한 이유는 다음과 같다. 첫째, Passport 인증 시스템을 사용하려면 사용자의 신원 정보 등록 및 유지, 신원 증명 정보 발급, 검증 등 인증 관련 모든 서비스가 마이크로소프트에 의해 통제되는 중앙 집중 시스템(Passport 서버)에 의존하여야 한다. 따라서 마이크로소프트와 이해관계가 있는 서비스 제공자와 사용자들이 마이크로소프트에 의해 완전히 통제되는 Passport 시스템을 사용하는 것을 꺼려할 수밖에 없다. 이해관계가 있는 서비스 제공자와 사용자들은 당연히 자신들의 통신에 마이크로소프트가 중간에 참여하는 것을 원하지 않는다. 둘째, Passport 서버에 의한 중앙 집중형의 인증 시스템은 당연히 확정성(scalability)의 문제에 직면할 수밖에 없다. Passport 서버를 분산 형태로 유지하더라도 마이크로소프트 단일 회사에 의해 인터넷 규모의 확장성을 시의적절하게 지원하는 것은 어려운 문제이다. 이러한 문제점으로 인해 결국 마이크로소프트는 인터넷의 인증 시스템을 목표로 출범한 Passport 인증 시스템 확산 정책을 철회하고, 현재에는 Live ID로 이름을 변경하여 마이크로소프트의 온라인 서비스들과 파트너들을 위한 인증 시스템으로 사용하고 있다.

4.2 OpenID 인증 시스템 장단점 분석

OpenID 인증 시스템은 사용자로 하여금 자신이 원하는 OP(OpenID Provider)에 신원 정보를 등록하고 OpenID를 할당받은 다음 RP(Relying Party)인 어떤 웹 사이트에서도 사용할 수 있게 한다. 따라서 OpenID는 사용자 편의성과 비용적인 측면에서 여러 가지 장점을 제공한다. 먼저 OpenID 인증 시스템은 사용자가 선택한 특정 OP에 등록한 동일한 OpenID를 OpenID를 지원하는 모든 웹 사이트에서 사용할 수 있게 하므로 사용자가 사이트별로 별도의 신원 증명 정보(예 : 사용자 이름/패스워드)를 유지하고 사용해야 하는 불편함에서 해방될 수 있다. 그리고 OpenID는 SSO(Single Sign-On) 서비스를 제공하므로 OP에서 한번 로그인하면 다른 웹 사이트를 접근할 때 마다 로그인하는 불편을 없애준다. 뿐만 아니라 사용자는 자신의 신원 정보를 OP에 한번만 등록하면 되기 때문에 반복적이고 중복적인 신원 정보 등록의 불편 문제도 해결한다.

OpenID 인증 시스템은 기본적으로 기존의 사용자 웹 브라우저를 그대로 사용할 수 있게 하므로 OpenID 사용자를 위해 추가적인 개발 비용을 요구하지 않는다. 그리고 서비스 제공자인 웹 사이트의 경우에도 자체적인 인증 시스템의 개발과 유지 및 관리 필요 없이 간단한 URL(또는 XRI) 형태의 OpenID를 지원하고 HTTP 기반의 OP와의 통신만 지원하면 되므로 개발과 유지 및 관리가 간단해지는 장점이 있다. 사용자가의 신원 정보의 유지와 인증 작업이 OP 한곳에서만 이루어지는 OpenID 인증 시스템은 신원 정보에 대한 보안 유지와 사용자 통제를 보다 용이하게 하여 프라이버시 보호를 강화할 수 있는 측면이 있다.

이와 같은 여러 가지 장점에도 불구하고 Open ID 인증 시스템은 RP와 OP에 대한 신뢰 문제로 인해 발생하는 몇 가지 문제점으로 인해 현재 높은 신뢰도를 요구하는 서비스에 응용되지 못하고 있다. 기본적으로 OpenID 인증 시스템은 OP와 RP, 그리고 사용자간에 신뢰 인프라스트럭처 구축에 관한 어떤 사항도 정의하지 않으므로 상호간에 대한 신뢰 문제는 전적으로 상호간 인터페이스의 구현에 달려 있다. 예를 들어 어떤 OP의 경우 사용자 등록 시에 사용자 신원 정보의 진위 여부를 엄밀하게 심사하고 또 어떤 OP는 사용자 신원 정보 진위 여부에 대한 심사를 전혀 하지 않을 수도 있다. 따라서 OP의 인증 서비스에 의존하는 웹 사이트인 RP는 임의의 OP가 발급한 OpenID를 신뢰하기가 어려울 수 있다. 이것이 현재 구글, 마이크로소프트, AOL, 야후와 같은 대형 서비스 제공자들이 단지 OP 역할만 수행할 뿐 임의의 다른 OP가 발급한 OpenID를 사용하는 RP 역할을 수행하지 않는 이유이다.

RP에 대한 신뢰 인프라 부재는 피싱(phishing)과 같은 더 큰 보안 문제와 연결될 수 있다. OpenID 인증 시스템에서 OpenID를 지원하는 웹 사이트인 RP에 대한 신뢰 여부는 전적으로 사용자의 판단에 의존한다. 즉, RP에 대한 신뢰 정도를 판단해서 사용자에게 알려주는 어떤 서비스도 OpenID는 정의하지 않는다. 따라서 OpenID의 개념에 익숙하지 않는 사용자가 임의의 악의적인 RP를 접근하는 경우 해당 RP는 사용자를 OpenID의 정상적인 OP가 아닌 자신이 위조한 OP로 라다이렉트(redirect)하여 사용자의 신원 증명 정보(예 : 사용자 이름/패스워드 등)를 가로챌 수 있다. 또한 OP는 사용자가 접근한 모든 웹 사이트에 대한 기록을 유지할 수 있기 때문에 악의적인 OP에 의한 사용자의 웹 사이트 접근 기록이 유출되는 프라이버시 문제가 발생할 수도 있다.

4.3 Liberty Alliance 인증 시스템 장단점 분석

Liberty Alliance의 연방형 신원 관리 시스템의 장점은 사용자 신원 정보를 별도의 중앙 집중적인 시스템에 유지하고 관리할 필요 없이 사용자 편의성을 제고하고, 서비스 제공자(SP)에 대한 신뢰도를 제고하며, SP들의 유지 및 관리 부담을 축소한

다는 점이다. Liberty Alliance의 연방형 신원 관리 시스템은 독립적으로 운영되는 기존 및 새로운 서비스 실체(IdP, SP)들을 상호 신뢰적으로 연방화하여 단일 사인온과 단일 사인아웃 서비스 제공함으로써 사용자 편의성을 제고한다. 또한 사용자는 신뢰할 수 있는 IdP와 신뢰 동아리(CoT)를 형성하고 있는 SP들을 신뢰할 수 있는 장점이 있다. 그리고 SP들도 자신의 서비스 제공에 반드시 필요한 신원 정보만 관리하고 나머지는 IdP로부터 아웃소싱(outsourcing)할 수 있기 때문에 신원 정보의 유지 및 관리와 새로운(보다 강력한) 인증 서비스 구현 등에 대한 부담에서 벗어날 수 있다.

Liberty Alliance 연방형 신원 관리 시스템은 이러한 여러 가지 장점을 가지고 있지만 몇 가지 단점도 가지고 있다. 연방형 신원 관리 시스템의 첫 번째 문제점은 확장성(scalability) 문제이다. 기본적으로 서비스 실체(SP, IdP)간의 신뢰 동아리(CoT) 구축이 전제되어야 하고 신뢰 동아리 구축은 서비스 실체들간의 기술적인 안전 채널 구축과 구체적인 사업적인 계약 관계를 포함하므로 연방형 신원 관리 시스템에 많은 서비스 실체들을 포함하는 것이 어렵다. 특히 많은 수의 사용자가 서비스 제공자로 참여하는 P2P(peer-to-Peer) 환경에서는 이러한 문제가 더욱 어려워진다. 두 번째 문제점은 연방형 신원 관리 시스템의 복잡성이다. 사용자는 어떤 IdP에 어떤 SP들을 연방화시킬 것인지 일일이 판단하고 결정해야 한다. 이러한 작업은 많은 SP를 사용하고 다수의 IdP가 존재하는 경우 사용자를 복잡하게 만들고 특히 다수의 CoT의 연합 환경에서는 더욱 복잡해진다. 세 번째 문제점은 IdP에 의존적인 프라이버시 보장 문제이다. 우선 Liberty Alliance에서 IdP에 대한 신뢰 여부는 전적으로 사용자가 결정하는 문제이다. 그리고 IdP는 기본적으로 사용자에 대한 신원 정보를 관리하고 연방화된 SP들에 대한 사용자의 모든 접근 기록을 관리한다. 따라서 IdP가 사용자 신원 정보를 악의적으로 또는 사고로 노출하는 경우 사용자의 프라이버시 정보가 심각하게 침해될 수 있다.

4.4 PRIME 인증 시스템 장단점 분석

PRIME 프로젝트는 실제 환경에서 사용할 수 있는 인증 시스템 또는 신원 관리 시스템을 개발하기보다 사용자의 프라이버시를 최대한 강화할 수 있는 방안을 적용한 시스템에 대한 시연에 목표를 두고 진행되었기 때문에 사용 관점에서 장점과 단점을 분석하기는 적절하지 않다. 그러나 다음과 같은 점들은 앞에서 다룬 다른 인증 시스템과 차별화되는 PRIME 프로젝트만이 제공하고 있는 장점이다.

- 익명 통신 채널(anonymous communication channel), 익명 신원증명(anonymous credential), 그리고 확인 가능한 암호화(verifiable encryption) 기법을 통한 개인 정보 노출 최소화
- DHP(Data Handling Policy) 협상을 통한 개인 정보 관리에 대한 구체적인 사용자 개입
- 개인 정보 관리 규칙 준수 의무 강제화

그러나 PRIME 프로젝트가 개인 정보 노출을 최소화하기 위해 도입한 익명 통신 채널, 익명 신원증명, 그리고 확인 가능 암호화 기법들은 모두 매우 복잡한 처리 과정을 요구하므로 실제 환경에 적용하기 위해서는 성능 문제, 대역폭 문제 등을 해결할 수 있는 새로운 기술 개발이 앞으로도 지속적으로 이루어져야 한다. 또한 PRIME 시스템은 사용자 시스템과 서비스 제공자 시스템이 대칭적인 구조를 가지고 있기 때문에 모든 사용자 시스템이 PRIME의 복잡한 구조를 처리할 수 있어야 한다. 따라서 IoT(Internet of Things)와 같이 경량 단말 장치와 같은 환경에서는 기본적으로 사용하기가 어려울 것으로 예상된다. 또한 모든 사용자 장치가 PRIME 구조를 지원할 수 있도록 개발되어야 하므로 기존 시스템과의 호환성을 유지하기 어려운 문제도 PRIME 시스템을 실체 환경에 적용하는 데에 걸림돌이 될 것으로 판단된다. 뿐만 아니라 단일 사인온과 단일 사인아웃과 같은 인증 결과 공유 기능과의 통합 문제 등도 PRIME 프로젝트가 향후에 해결해야할 과제이다.

5. 결론 및 향후 연구

인증 시스템은 인터넷 환경에서 다양한 서비스를 안전하고 효과적으로 제공하는 데에 중심적인 역할을 수행한다. 그러나 현재의 인터넷 인증 시스템 환경은 신원 증명 정보 관리의 어려움과 반복적인 등록 및 로그인에 따른 사용의 편의성 부족, 개발과 관리 측면에서의 고비용 구조, 확장성과 유연성 부족, 그리고 개인 정보에 대한 프라이버시 보호 체계 미흡 등의 여러 가지 문제점들로 인해 인터넷 서비스 활성화의 장애가 되고 있다. 이러한 문제점들을 개선하기 위해 최근에 통합적인 인증 시스템인 Passport, 사용자 중심의 경량 인증 시스템인 OpenID, 기존 인증 시스템들을 포함하는 독립적인 인증 시스템들의 연방화를 통해 단일 사인온과 단일 사인아웃 등의 효율적인 인증 서비스를 제공하는 Liberty Alliance의 연방형 인증 시스템, 그리고 익명 신원증명 기법과 확인가능 암호화 기법 등을 적용하여 프라이버시 보호가 강화된 PRIME과 같은 차세대 인증 시스템 개발이 활발하게 진행되어 왔다. 이러한 차세대 인증 시스템들은 기존 인증 시스템 환경의 문제점들의 특정 부분 해결에 초점을 두고 개발되었기 때문에 <표 1>과 같이 각각 장점과 단점을 가지고 있다.

〈표 1〉 차세대 인증 시스템 비교 분석 요약

인증 시스템	장점	단점
Passport	◦ 단일 서버 ◦ SSO ◦ 서버 보안 신뢰	◦ MS 서버 의존 ◦ 확장성 결여
OpenID	◦ 선택한 소수의 서버 ◦ SSO ◦ 간단한 개발 ◦ 사용자 제어 용이	◦ 신뢰 인프라스트럭처 부재 ◦ 피싱 등 보안에 취약 ◦ 악의적인 OP에 의한 프라이버시 문제
Liberty	◦ 분산 SSO ◦ 신뢰 인프라스트럭처 ◦ SP 개발 부담 경감	◦ 확장성 결여 ◦ 시스템 복잡성 ◦ IdP에 의존적인 프라이버시
PRIME	◦ 개인정보 노출 최소화 ◦ 사용자에 의한 개인정보 통제 ◦ 개인정보 관리 규칙 강제 준수	◦ 성능과 대역폭 문제 ◦ 사용자 시스템 개발 복잡 ◦ SSO 기능 미지원

본 논문의 차세대 인증 시스템에 대한 분석 결과는 인터넷 사용자들이 차세대 인증 시스템을 선택하는 데에 기준을 제시할 뿐만 아니라 미래 인터넷 서비스 환경에서 인증 시스템에 관한 연구와 개발 방향을 제시하는 데 의미가 있다. 본 논문의 분석 결과를 통하여 우리는 미래 인터넷 서비스 환경을 위한 인증 시스템은 다음과 같은 방향으로 지속적으로 연구되고 개발되어야 함을 알 수 있다.

- 특정 시스템에 의존하지 않고 서로 다른 플랫폼 기반의 인증 시스템을 사용하되 서로 간에 글로벌 상호동작성(interoperability)을 제공할 수 있어야 한다.
- SSO(Single Sign-On)를 포함하여 보다 편리한 사용자 인터페이스를 지원해야 하고, 기존 서비스 환경에 쉽게 적용할 수 있어야 한다.
- IoT 환경 등 새로운 인터넷 환경과 새로운 서비스를 효과적으로 지원할 수 있는 확장성과 유연성을 제공할 수 있어야 한다.
- 개인정보 노출 최소화를 포함하는 프라이버시를 최대한 보호할 수 있어야 한다.
- 사용자가 신뢰할 수 있는 서비스 환경을 제공할 수 있어야 한다.

참 고 문 헌

[1] Audun Josang and Simon Pope, "User Centric Identity Management", *AusCERT Conference*, 2005.

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

[3] PrimeLife, "Requirements and concepts for identity management throughout life", *http://www.primelife.eu*, 2009.

[4] David, P. K. and D. R. Aviel, "Risks of the Passport Single Signon Protocol", IEEE Computer Networks, 2000.

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

[6] Dimitry Stogov, "Enabling OpenID", *IZEND/PHP Conference and Expo,* 2007.

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

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

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

[10] PRIME Consortium, "PRIME Architecture V3", http://www.prime-project.eu, 2008.

[11] PRIME Consortium, "PRIME Framework V3", http://www.prime-project.eu, 2008.

[12] Jan Camenisch and Ekc Van Herreweghen, "Design and Implementation of the IDEMIX Anonymous Credential System", Proc. of 9th ACM Conference on Computer and Communication Security, 2002.

◈ 저 자 소 개 ◈

박 승 철 (scpark@kut.ac.kr)

서울대학교 계산통계학과에서 학사, KAIST 전산학과에서 석사, 그리고 서울대학교 컴퓨터공학부에서 박사학위를 취득하고 현재 한국기술교육대학교 컴퓨터공학부 부교수로 재직 중이다. 현재 브로드밴드 네트워크, P2P 스트리밍, 네트워크 보안 등을 연구 중이며, 관심분야는 멀티미디어 통신, 네트워크 보안, 미래인터넷 등이다.