한국산학기술학회논문지
Vol. 12, No. 1 pp. 100-109, 2011

교육정보 통합 플랫폼 구현을 위한 통합 사용자 인증 서비스의 설계 및 구현

박정호[1*]
[1]서울디지털대학교 컴퓨터공학부

The Design and Implementation of Single Sign-On Service for Education-related Information Service Platform

Jung-Ho Park[1*]
[1]**Division of Computer Science & Engineering, Seoul Digital University**

요 약 본 논문은 개별적으로 사용자 인증 시스템이 구현된 16개 시·도교육청 교육정보서비스와 한국교육학술정보원의 교육정보서비스를 단일 사용자 인증을 통해 모두 이용할 수 있는 최적의 방안을 연구하여 도출한 것이다. 본 논문에서는 도출된 방안에 따라 통합 사용자 인증 서비스를 제공할 수 있는 시스템을 설계하고 구현함으로써 16개 시·도교육청과 한국교육학술정보원이 공동으로 운영 중인 전국교육정보공유체제의 교육정보 서비스 이용에 편리성을 도모하는 동시에 사용자 인증 관리의 효율과 안전을 기할 수 있는 방안을 마련하였다.

Abstract The study concluded that in order to achieve a single sign-on through the federation ID management method must be used among many other methods so to establish a combined approval service that gives access to education related information provided by the 16 city and provincial offices of education and the KERIS(Korea Education & Research Information Service). The federation ID management method allows the usage of authentication policy and enables transfer of ID information to other institutions through standardized processing. Therefore by establishing single sign-on through the federation ID management method allows individual city and provincial office of education to maintain the already existing approval services while combining user identification database.

Key Words : Single Sign-On, Education-related Information Service Platform

1. 서론

전국 16개 시·도교육청과 한국교육학술정보원(KERIS, Korea Education & Research Information Service)은 시·도교육청과 교육유관 기관, 그리고 교육 현장 등에서 생성되는 각종 교육용 자료를 한 번에 검색할 수 있도록 표준화된 교육 정보 메타데이터 형태로 디지털화된 교육자료를 공유·유통시키는 서비스로서 전국교육정보공유체제를 2002년 5월에 탄생시켰다. 이러한 전국교육정보공유체제는 16개 시·도교육청이나 한국교육학술정보원 등에서 개별 또는 분산 개발된 각종 교육정보를 공유하고 활용하는데 큰 역할이 되었으나, 2006년 말 개정된 저작권법에 따라 저작물의 공정한 이용을 확인할 수 있는 방안으로 각 시·도교육청이나 한국교육학술정보원 등에서 운영 중인 교육정보서비스에 대해서 사용자 인증을 개별적으로 구현하게 됨으로 인해 사용자가 전국교육정보공유체제를 통해 검색된 자료를 이용하기 위해서는 타 시·도에서 운영 중인 서비스에 다시 사용자 인증을 받아야 하는 상황이 발생하게 되었다. 따라서 전국교육정보공유체제를 통한 교육정보의 공유를 보다 활성화 시키고 저작물의 공정한 이용을 도모하기 위해서는 16개 시·도교육청과 한국교육학술정보원이 운영 중인 주요 교육정보

*교신저자 : 박정호(martinpark@paran.com)
접수일 10년 11월 02일 수정일 (1차 10년 12월 10일, 2차 11년 01월 09일) 게재확정일 11년 01월 13일

서비스에 대한 이용을 한 번의 사용자 인증만으로 가능하도록 하는 통합 사용자 인증(SSO, Single Sign-On) 서비스의 구현이 필요하게 되었다[1].

본 논문에서는 16개 시·도교육청과 한국교육학술정보원이 운영 중인 각 교육정보서비스에 대해서 사용자 인증 서비스의 구현 현황을 조사하고, 지금까지 국내외에서 연구된 주요 통합 사용자 인증 서비스 모델들을 비교·분석한다. 그리고 이런 비교·분석을 통해 16개 시·도교육청과 한국교육학술정보원의 모든 교육정보서비스를 효율적으로 운영하기에 가장 적합한 통합 사용자 인증 방안을 도출하고, 이를 바탕으로 하여 16개 시·도교육청과 한국교육학술정보원이 운영 중인 교육정보서비스를 단일 로그인/로그아웃으로 이용할 수 있도록 하는 통합 사용자 인증 서비스 시스템을 설계하고 구현한다.

2. 현황 조사·분석 및 통합 사용자 인증 모델 적용 검토

2.1 현황 조사 및 분석

16개 시·도교육청과 한국교육학술정보원의 교육정보화 시스템에 대한 사용자 인증 현황을 분석해 본 결과, 전반적인 문제점은 정책의 부재로 인해 발생된 문제들과 사용자 인증 시스템 구축이나 운영에 대한 지침이나 가이드라인 없이 각 시·도교육청이 개별적으로 인증 시스템을 구축해 온데서 발생되는 문제들, 그리고 사용자 신상 정보에 대한 보안 문제들로 크게 구분할 수 있다.

이 가운데 정책의 부재로 인해 발생된 문제들로는 우선 시·도교육청별로 통합 사용자 인증 서비스를 구축하면서 통합 사용자 인증 대상으로 선정한 서비스들 각기 다르다는 것이었고, 사용자 ID(identity) 관리 정책의 부재로 인하여 ID 발급절차나 휴면계정 관리 정책 등이 상이했다. 예를 들어, 한국교육학술정보원이 운영하고 있는 에듀넷의 경우에는 회원가입을 하는데 있어서 약관동의, 실명인증, 상세정보입력, 가입완료의 절차를 거치는 반면, 특정 시·도교육청이 운영하고 있는 교육정보화 서비스의 경우에는 약관동의나 실명인증 절차 없이 단지 회원정보 입력만으로 회원가입이 가능했다. 또한 회원자격에 따라 교육정보화 서비스가 제공하는 정보나 자원을 제한하는 교육정보 자원 접근 정책도 모든 시·도교육청이 개별적으로 정하였기 때문에 어떤 시·도교육청의 서비스에서는 교사용으로 만들어진 정보를 학생이나 학부모 회원자격으로도 이용할 수 있는 반면, 다른 어떤 시·도교육청의 서비스에서는 학생이나 학부모 회원자격으로 교사용 정보를 이용할 수 없도록 하고 있었다. 실명인증의 경우에도 대다수 시·도교육청에서는 미성년자인 학생에 대해서는 미성년자에 대한 실명인증을 제공하는 기관이 없다는 이유로 실명인증을 실시하지 않고 있었으나 한국교육학술정보원의 에듀넷 서비스 같은 경우에는 보호자 동의서와 함께 주민등록등본이나 의료보험증 사본을 팩스나 이메일로 접수받아 실명인증 처리를 대신하고 있었다. 이와 같이 회원 관리 정책이 없거나 온라인 교육정보화 서비스를 제공하는 기관별로 상이한 정책을 운영하는 데서 오는 불일치는 전국적인 통합 사용자 인증 서비스를 구현하는 데 있어서 뿐만 아니라 시·도교육청이 개별적으로 통합 사용자 인증 서비스를 구현하는 데 있어서도 큰 걸림돌로 작용하고 있었다. 따라서 향후 전국적인 통합 사용자 인증 서비스를 구현하기 위해서는 우선 통합 사용자 인증 서비스를 제공하고자 하는 대상 서비스에 대한 기준을 정립하고 그 기준에 따라 SSO 대상 서비스를 선정하도록 할 필요가 있다. 또한, 표준 ID 관리 정책을 수립하여 모든 시·도교육청의 교육정보서비스가 일관된 정책으로 사용자 ID를 관리하여야 하고, 시·도교육청 및 한국교육학술정보원이 제공하고 있는 교육정보 자원에 대한 접근 정책도 수립하여 회원자격별로 접근할 수 있는 정보자원에 대한 한계를 명확하게 하여야 한다. 그리고 실명 인증에 있어도 정책적 기준을 제시하고 모든 시·도가 그 기준에 준해 실명인증을 하도록 하여야 할 것이며, 더불어 교사의 신분을 확인하는 방법이나 미성년자의 실명확인 방법도 강구하여야 한다[2,3].

사용자 인증 시스템 구축이나 운영에 대한 지침이나 가이드라인 없이 각 시·도교육청과 한국교육학술정보원이 개별적으로 인증 시스템을 구축해 온데서 발생되는 문제들 가운데 가장 큰 것은 우선 시·도교육청별로 다른 사용자 인증 시스템을 구축하여 운영하고 있다는 것이며, 더불어 시·도교육청에 따라 개별적으로 구축된 통합 사용자 인증 서비스 시스템 역시 상이하여 시·도교육청 간에 상호 호환성을 가지지 못한다는 점이다. 이러한 문제로 인하여 이미 개별적으로 통합 사용자 인증 서비스를 구축한 시·도교육청에서는 향후 전국적인 통합 사용자 인증 서비스가 구축될 경우 이미 기 구축되어 있는 시·도교육청의 통합 사용자 인증 서비스 시스템에 대한 변경을 최소화할 수 있는 방안으로 이루어지기를 희망하고 있는 상황이었다.

2.2 통합 사용자 인증 모델 유형 및 적용 사례 검토

2.2.1 통합 사용자 인증 모델의 유형

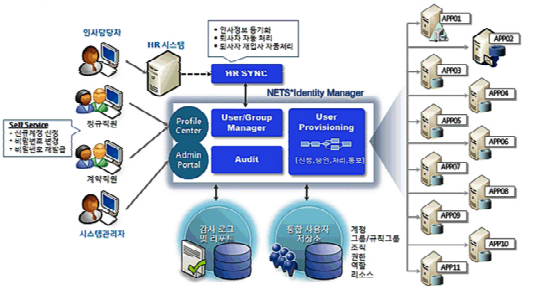
인터넷 환경에서 이용되는 통합 사용자 인증에 대한 국내외 기술은 그 기술적 유형으로 분류해 볼 때 중앙 집중형 SSO 모델, 사용자 중심형 SSO 모델, ID 연계형 SSO 모델로 크게 구분할 수 있다.[4] 이 세 가지 모델 가운데 첫 번째인 중앙 집중형 SSO 모델은 주로 Enterprise idM (identity Management) 솔루션들이 채택하고 모델로 국내 기업에서 통합사용자 인증 서비스를 구현할 때 가장 많이 채택하고 있는 형태이다[5,6].

두 번째 모델인 사용자 중심형 SSO 모델은 사용자가 ID 제공 사이트(IdP, ID Provider)에 ID를 등록하고 이를 지원하는 서비스 제공 사이트(SP, Service Provider)에 로그인을 시도하면 두 사이트 간에 인증정보를 교환한 후 서비스를 제공하는 방식으로 사용자가 직접 개인정보 및 ID 사용정책을 통제하는 것을 기본사상으로 하고 있다.

세 번째 모델인 ID 연계형 SSO 모델은 각 웹사이트가 타 웹사이트와의 연동을 위한 연계 ID의 제공을 통해 통합 사용자 인증을 구현하는 방식이다. 이때 통합 사용자 인증에 참여하는 개별 사이트에서는 여전히 ID 생성을 담당하며 필요에 따라 사용자의 개인정보를 보유하게 된다. 이러한 ID 연계형 모델은 신뢰를 기반으로 웹사이트들을 연계하여 서비스한다는 의미에서 CoT(Circle of Trust)-based 방식이라고도 불린다.

2.2.2 통합 사용자 인증 모델의 유형별 적용 사례

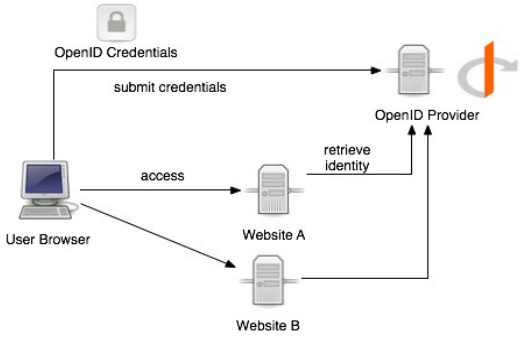
(1) 중앙 집중형 SSO 모델 적용 사례



[그림 1] 이랜드 그룹의 중앙집중형 SSO 구축 사례
(출처: http://www.nets.co.kr)

중앙 집중형 SSO 모델을 사용한 통합 사용자 인증 서비스의 구현은 그림 1에 나타낸 이랜드 그룹의 구축 사례와 같이 통합계정관리(Enterprise idM) 솔루션을 이용하여 어플리케이션에 산재되어 있는 사용자의 계정과 속성, 역할, 권한을 통합 관리하고 사용자 프로비저닝, 사용자 계정 및 권한 승인, 사용자 셀프-서비스, 관리자 권한 위임을 포함한 계정관련 프로세스를 자동화한다. 따라서 중앙 집중형 SSO 모델을 사용하게 되면, 계정 정책의 일관된 적용과 계정 관련 활동 감사를 통해 보안 위험을 감소시킬 수 있는 동시에 감사 요구에 대한 처리를 실시간으로 처리할 수 있다. 그러나 중앙 집중형 SSO 모델은 사용자 계정 관리와 관련된 모든 프로세스가 통합계정관리 시스템에 집중되기 때문에 통합계정관리 시스템이 다운되면 그 통합계정관리 시스템에 종속되는 모든 어플리케이션들이 동시에 영향을 받아 이용을 할 수 없게 된다. 그렇기 때문에 중앙 집중형 SSO 모델을 채택하여 통합 사용자 인증 서비스를 구현할 때는 L4 스위치(Layer 4 Switch) 장비를 사용하여 통합계정관리 서버를 이중화로 구성함으로써 부하 및 장애에 대비하여야 한다.

(2) 사용자 중심형 SSO 모델 적용 사례

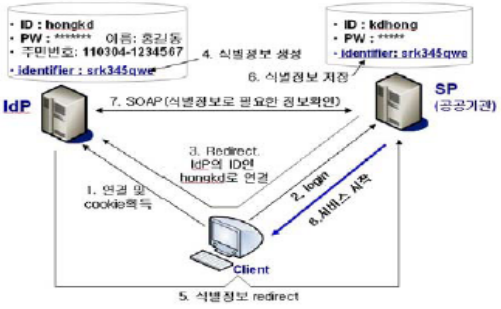


[그림 2] 사용자 중심형 SSO인 OpenID 인증 방법
(출처:http://www.devx.com/opensource/Article/37692)

사용자 중심형 SSO 모델의 대표적인 사례로는 OpenID를 들 수 있다. OpenID는 그림 2에 나타낸 것과 같이 사용자가 사전에 OpenID Provider에 등록해 놓은 하나의 ID로 OpenID 인증 프로세스가 적용된 모든 서비스에 별도의 가입 없이 로그인 되는 프로세스를 정의한다. OpenID를 사용하는 사용자들은 자신의 온라인 ID를 관리하기 위해 개개의 서비스에 의존할 필요가 없으며, 어떤 웹 서비스이든 웹 주소(URL, Uniform Resource Locator)로 표기된 ID를 통해 로그인이 가능하다. 따라서 OpenID 인증 프로세스가 적용된 서비스에는 사용자가 자신의 이름이나 주소 등을 계속 입력할 필요가 없으며, 사용자 자신이 사용하던 ID와 암호를 분실할 위험이 없다. 또한 웹 사이트를 운영하는 사업자의 입장에서는 회원가입 화면이 필요 없고, 사용자의 ID와 암호를 관리하는 데 드는 비용을 절감할 수 있다. 그러나 OpenID는 가벼운 인증 레벨단의 사용을 목적으로 설계되었기 때문에 신뢰성 및 보안성에 대한 문제점들이 제기되고 있다. OpenID는 스팸(spam), 피싱(phishing) 공격에 취약하다는 지적을 받고 있으며, 이외에도 인증키 암호화 방식, 모순

된 인증 유효주기 등이 문제로 대두되고 있다.

(3) ID 연계형 SSO 모델 적용 사례



[그림 3] ID 연계형 SSO 모델을 적용한 행정자치부의 통합 ID 관리체제 시범구축 사례[2]

ID 연계형 SSO 모델을 사용한 통합 사용자 인증 서비스의 구현 사례로는 그림 3에 나타낸 것과 같은 행정자치부의 통합 ID 관리체제 시범 구축 사례가 있다. 이 경우, 사용자는 IdP(Identity Provider)를 이용하여 별도로 가입한 SP(Service Provider)의 개인정보를 관리할 수 있는 기능을 지원한다. 따라서 사용자는 처음에 한번은 개인 신원 확인을 위해 동사무소를 방문하여 신분증을 제시하고 개인의 ID와 암호를 IdP 서버에 등록하여야 한다. 이후 사용자가 자신의 PC에서 어떤 공공기관의 웹 사이트(SP)에 접속하여 서비스를 이용하려고 하면, 클라이언트(client) 프로그램은 행정자치부에서 관리하는 IdP 서버에 연결하여 쿠키(cookie)를 획득한 후 다시 그 공공기관의 웹사이트(SP)에 획득한 쿠키와 함께 로그인 시도를 하게 된다. 그러면 그 공공기관의 웹사이트(SP)는 사용자의 쿠키를 IdP 서버에 redirect함으로써 사용자 자신이 처음에 IdP 서버에 등록해 놓은 ID로의 연결을 확인하게 된다. 이때 IdP 서버의 DB(Database)에는 영구 식별정보(identifier)가 생성되고, 이 식별 정보는 클라이언트(client)를 거쳐 그 공공기관의 웹사이트(SP)로 redirect된 후, 그 공공기관의 웹사이트(SP)의 DB에 사용자의 local ID와 함께 저장하게 된다. 이후 공공기관의 웹사이트(SP)는 식별정보를 이용하여 IdP 서버에게 사용자가 요청한 서비스에 대한 권한이나 자격 등을 확인하고 승인처리가 되면 사용자가 요청한 서비스를 제공하게 된다. 이와 같이 ID 연계형 기반의 SSO 모델을 적용한 통합 ID 관리체계에서는 IdP 서버에 비해 상대적으로 보안이 약한 SP가 관리하고 있는 개인의 ID 정보가 유출되어도 IdP 서버가 관리하는 주민등록번호를 비롯한 개인의 신상 정보가 유출되지 않기 때문에 개인정보를 좀 더 안전하게 보관할 수 있게 된다.[2] 또한 새로운 공공기관의 웹사이트를 SP로 추가하고자 할 경우에도 기존의 인증 체제를 온전히 유지하면서 비교적 간단하게 통합 사용자 인증 서비스를 제공할 수 있다.

2.3 통합 사용자 인증 모델 비교 분석

2.3.1 비교 요소

교육정보서비스에 통합 사용자 인증 모델을 적용하고자 할 경우에는 현재 독립적으로 운영되고 있는 기존 환경을 고려하여 가능한 한 개발 비용과 노력을 적게 들이면서 운영상 많은 장점을 가지는 모델을 선택하는 것이 바람직하다. 따라서 본 논문에서는 개발적 측면과 운영적 측면을 고려하여 앞서 설명한 세 가지 모델을 비교하기로 하였다. 개발적 측면에서의 비교 요소는 DB 어플리케이션 통합 개발 작업에서 일반적으로 수행하는 작업 요소와 유사하기 때문에 '인증 DB 작업', '어플리케이션 수정', '인증 서비스 개발 작업'이라는 세 가지 작업 요소를 선택하였다. 그리고 운영적 측면에서의 비교 요소는 '사용자 정보 관리의 효율성', '인증 정책 관리의 일관성', '인증 서비스의 응답 속도', '보안성', '서비스의 안정성' 등을 선택하였다. 손태식, 이상하, 유승화, 김동규는 "단일 인증 시스템의 인증 기법과 인증 모델 분석"이라는 연구를 통해 사용자 관리의 효율성과 정책관리의 일관성, 보안성, 안정성을 중심으로 여러 통합 사용자 인증 모델의 특징을 비교하여 설명한 바 있다[7]. 그리고 구희정, 홍충선, 강명수, 이길행의 "SAML 기반의 사용자와 OSS 간 안전한 정보교환을 위한 관리시스템", 최진탁의 "Single Sign-On을 이용한 인증 관리 기법에 관한 연구" 등에서는 통합 사용자 인증 모델의 성능을 비교하기 위한 요소로 인증 서비스의 응답속도를 사용하였다[8,9].

본 논문에서는 통합 사용자 인증 모델의 객관적 비교를 위하여 통합 사용자 인증 서비스의 개발적 측면에서의 세 가지 비교 요소와 통합 사용자 인증 서비스의 운영적 측면에서의 다섯 가지 비교 요소를 모두 사용하여 앞서 설명한 세 가지 통합 사용자 인증 모델을 비교하였으며, 그 비교 결과를 표 1과 표 2에 나타내었다.

개발적 측면의 세 가지 비교 요소들 가운데 인증 DB 작업 항목은 통합 사용자 인증 서비스를 구축함에 있어서 사용자 인증 데이터를 어떤 형태로 수집하여 DB를 구축하는가를 검토하여 비교한다. 어플리케이션 수정 항목은 통합 사용자 인증 서비스를 구현하는 데 있어서 관련 어플리케이션 프로그램에 대한 수정 요구가 상대적으로 많고 적음을 비교한다. 인증 서비스 개발 작업 항목은 통합 사용자 인증 서비스를 개발하는 데 있어서 각 모델 별로 어떠한 작업들이 필요한 지를 열거해서 비교한다.

[표 1] 개발적 측면에서의 통합 사용자 인증 모델 비교

항목	중앙 집중형 모델	사용자 중심형 모델	ID 연계형 모델
인증 DB 작업	기존 사용자 정보 통합 및 이관하여 통합 DB 구축, 인증 DB 수정 작업 많음	ID Provider 를 구축한 후 사용자 정보를 재수집, 인증 DB 수정 작업 많음	기존 인증 DB에 연계 정보만 추가 인증 DB 수정 작업 적음,
어플리케이션 수정	많음	적음	적음
인증 서비스 개발 작업	많은 시간과 비용이 소모됨. - 서비스 인증 DB 분석 - 통합 정책 수립 - 통합 인증 DB 재구축 - 기존 정보 이관 - 서비스 인증 로직 수정	많은 시간이 소모되지 않으나 많은 비용이 소모됨. - 서비스 인증 로직 분석 - OpenID Consumer 적용 - OpenID Provider 구축	많은 비용과 시간이 소모되지 않음. - 서비스 인증 로직 분석 - 연계 기능 추가 - 연계 서버 구성

[표 2] 운영적 측면에서의 통합 사용자 인증 모델 비교

항목	중앙집중형 모델	사용자 중심형 모델	ID연계형 모델
사용자 정보 관리의 효율성	효율성이 낮음 (관리자가 모든 사용자 정보를 직접 관리)	효율성이 높음 (사용자가 직접 관리)	효율성이 보통 (통합 사용자 인증에 관한 사용자 정보만을 사용자가 직접 관리)
인증 정책 관리의 일관성	일관된 인증정책 적용 및 사용자 정보 관리 용이하나 타 서비스에 대한 추가가 용이하지 않음.	일관된 인증정책 적용 및 타 서비스에 대한 추가가 용이	표준 기반 타서비스와의 연계 용이, 서비스별 다양한 인증 정책 적용 가능하지만 일관된 인증 정책 적용이 어려움
응답 속도	응답 속도 빠름	응답 속도가 중앙집중형 보다는 느리나 ID 연계형 보다는 빠름	응답 속도가 중앙집중형 보다 응답속도가 평균 40% 정도 느림
보안성	보안성 우수	보안성이 떨어짐 (피싱공격에 취약)	보안성 우수
안정성	안정성 떨어짐 - 통합 DB 부하 증가, - 통합 DB 장애 시 로그인 불가	안정성 떨어짐 - OpenID Provider 장애시 로그인 불가	안정성 우수

운영적 측면의 다섯 가지 비교 요소들 가운데 사용자 정보 관리의 효율성 항목은 개인정보를 관리하는 주체가 누구이며 통합 사용자 인증 서비스를 위한 개인정보 관리가 상대적으로 얼마나 효율적인가를 비교한다. 그리고 인증 정책 관리의 효율성 항목은 일관된 인증 정책 적용이 가능하며 타 서비스와의 연계가 용이한 가를 비교한다. 응답 속도 항목은 사용자 인증에 소모되는 시간을 비교한다. 보안성 항목은 사용자의 개인정보가 해킹으로부터 취약한 지를 비교한다. 안정성 항목은 통합사용자 인증 서비스가 사용자 증가나 어플리케이션 증가 등으로 인해 부하가 늘어나도 안정적으로 서비스될 수 있으며 장애 발생 시 빠른 복구가 가능한 가를 비교한다.

2.3.2 비교 검토 결과

중앙 집중형 SSO 모델을 현 교육정보 서비스를 위한 통합 사용자 인증모델로 적용하려면 기존의 각 시·도교육청 산하 교육정보원에서 자체적인 정책에 의해 수집한 사용자 인증 정보와 개인정보를 한 곳에 모아야 한다. 그러나 이를 위해서는 각 교육정보서비스에 가입하고 있는 사용자들로부터 개별적인 동의를 구해야하고 각 시·도교육청 별로 상이한 ID 관리 운영 정책에 대한 합의가 이루어져야 한다. 그리고 실제 통합에 대한 합의가 이루어진다고 해도 일관된 인증 정책과 사용자 정보 관리가 가능하다는 장점에 비하여 많은 구축 비용과 시간이 필요하며 통합 사용자 인증 DB에 대해 전체 서비스 의존도가 높아지는 단점이 있어 현 교육정보 서비스 환경에 적합하지 않다.

사용자 중심형 SSO 모델에서는 각 서비스에 대해 사용자 인증을 할 때만 IdP를 이용하고 사용자 속성 정보는 각 서비스 별로 관리한다. 하지만 이렇게 사용자 중심형 SSO 모델의 IdP에서 교육정보서비스에 필요한 개인 정보를 모두 관리할 경우에는 프로토콜만 사용자 중심형에서 사용하는 프로토콜을 쓰는 형태일 뿐 사용자 인증 DB는 중앙 집중형 모델과 마찬가지로 IdP에 통합된 형태로 구축되어야 한다. 그렇기 때문에 사용자 중심형 SSO 모델도 통합 사용자 인증 서비스를 구현하는 과정에서 중앙 집중형 모델과 동일한 문제점을 가지게 된다. 물론 사용자 중심형 SSO 모델의 IdP에서 인증만을 담당하게 할 경우, 인증에 대한 일관된 정책 적용이 가능하고 기존 어플리케이션에 대한 사용자 인증 변경 또한 용이하다는 장점도 있다[10]. 그러나 사용자 ID가 URL 형태로 바뀌어 사용자가 불편을 느낄 수 있으며, 기존에 이용하던 계정을 그대로 이용할 수 없어 모든 사용자가 다시 새로운 ID를 발급받아야 한다. 그리고 개인정보의 흐름을 사용자 판단에 맡기게 되므로 교육정보 서비스를 위해 제공

된 개인정보가 사용자의 판단에 의해 타 서비스에도 동일하게 제공될 수도 있다. 이에 따라 피싱 공격 등에 의해 개인정보가 노출될 위험이 따른다.

ID 연계형 SSO 모델의 경우는 개발적 측면에서 기존의 인증 체제를 온전히 유지하면서 비교적 간단하게 통합 사용자 인증 서비스를 구축하여 제공할 수 있다는 장점이 있다[11,12]. 또한 인증 과정이 어느 한 서버에서 집중되지 않기 때문에 사용자 인증 서버에 대한 서비스 의존성이 낮아지게 마련이며, 그로 말미암아 통합 사용자 인증 서비스를 보다 안정적으로 제공할 수 있다[13]. 반면, 인증 방법이 각 서비스별로 상이하여 일관된 인증 정책 적용이 쉽지 않으며, 응답 속도가 타 모델에 비하여 40%정도 느리다는 단점이 있다[8]. 그러나 ID 연계형 SSO 모델은 기존의 시・도 별로 독립적으로 운영되고 있는 교육정보서비스에 대하여 각 시・도 교육정보원의 통제권을 보장할 수 있다.

이상의 비교 검토를 통해 본 연구에서는 16개 시·도교육청과 한국교육학술정보원이 운영 중인 교육정보 서비스를 위한 통합 사용자 인증 서비스 구현에 ID 연계형 SSO 모델을 적용하기로 결정하였다. 비록 ID 연계형 SSO 모델이 세 모델 가운데 응답 시간이 가장 느리나 개발적인 측면에서 기간과 비용을 줄일 수 있고, 운영적인 측면에서도 안정성, 보안성, 통제권 보장 등 다양한 장점을 가질 수 있기 때문이다.

3. 통합 사용자 인증 서비스 설계

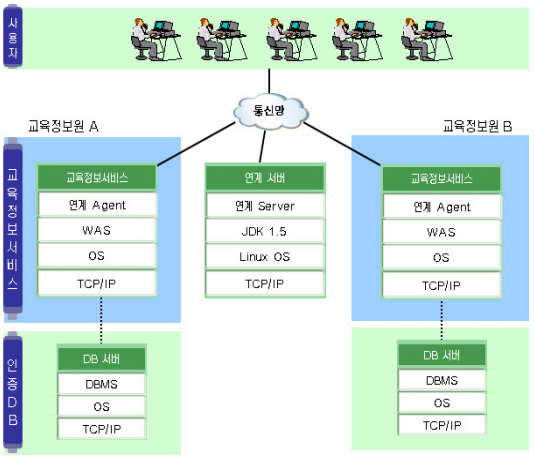
3.1 통합 사용자 인증을 위한 정책 수립

본 논문에서는 16개 시·도교육청과 한국교육학술정보원이 개별적으로 운영 중인 교육정보서비스들을 ID 연계 기반으로 통합 사용자 인증을 구현하기 위하여 다음과 같은 세부 정책들을 수립하였다.

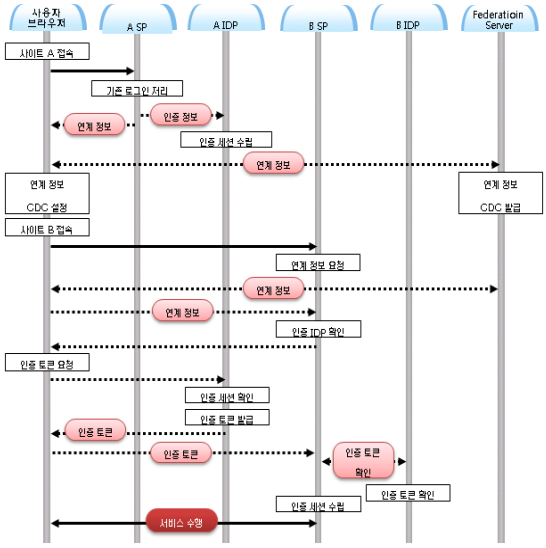
- 사용자는 각 시·도교육청이나 한국교육학술정보의 교육정보 서비스에서 사용하던 ID를 변경이나 재가입 없이 그대로 사용하여 로그인할 수 있게 한다.
- 통합 사용자 인증을 위한 서비스들 간의 연계는 시스템 관리자에 의한 강제적인 사용자 계정 연계가 아닌 서비스를 이용하는 사용자가 필요에 따라 사용자가 직접 계정 연계를 처리할 수 있도록 한다.
- 연계가 이루어지는 교육정보 서비스에 이미 다른 곳에서 로그인한 사용자의 또 다른 ID가 존재할 경우에는 이에 대한 변경 및 추가 없이 사용자의 ID 연계 정보만을 생성하도록 한다.
- 생성된 ID 연계 정보는 기존 교육정보 서비스 관리 체제 내에서 관리하지 않고 기존 교육정보 서비스 단위로 추가되는 연계 에이전트(agent)와 중앙의 연계 서버(server)에 의해 별도로 관리되도록 한다.
- 각 시·도교육청의 교육정보 서비스에서는 정책적 결정에 따라 연계 에이전트가 처리할 연계 정책을 설정하도록 한다.
- 중앙의 연계 서버에서는 서비스 간 연계 여부를 통합하여 관리하도록 한다.
- 각 연계 에이전트에서는 사용자의 로그인이 처음 일어날 경우 사용자의 크레덴셜(credential) 정보를 확인한 후 인증 세션을 수립하도록 한다.
- 이미 로그인된 사용자에 대해서는 연계 서버를 거쳐 처음 로그인하였던 교육정보서비스의 연계 에이전트로부터 인증 세션의 수립 여부를 확인받은 후 다른 교육정보 서비스에서 인증되도록 함으로써 기존 인증 체계에 변경이 없도록 한다.
- 각 연계 에이전트에서는 사용자 연계 현황을 조회할 수 있는 기능을 제공하도록 한다.

3.2 시스템 구성

16개 시·도교육청과 한국교육학술정보원이 운영 중인 교육정보 서비스들 간의 통합 사용자 인증을 구현하기 위한 사용자 인증 서비스 시스템의 구성은 그림 4에 나타낸 것과 같이 각 교육정보 서비스에 대해 연계 에이전트를 추가하고, 이 연계 에이전트들 간 메시지 처리 및 연계 정책을 관리하는 연계 서버를 별도로 두는 형태를 가진다. 따라서 통합 사용자 인증에 참여하게 되는 각 교육정보 서비스는 웹 어플리케이션 서비스(WAS, Web Application Service) 위에 연계 에이전트가 추가로 설치되는 것 이외에 다른 변경이 없게 된다. 각 교육정보서비스를 위해 사용되었던 기존의 사용자 인증용 데이터베이스들은 특별한 변경 없이 그대로 사용하게 된다. 연계 서버는 중앙에 별도의 서비스 시스템으로 구축되며, 연계 에이전트와 연계 서버 간에는 TCP/IP(Transmission Control Protocol/Internet Protocol) 프로토콜을 기반으로 한 인증 토큰 메시지가 전달되게 된다.



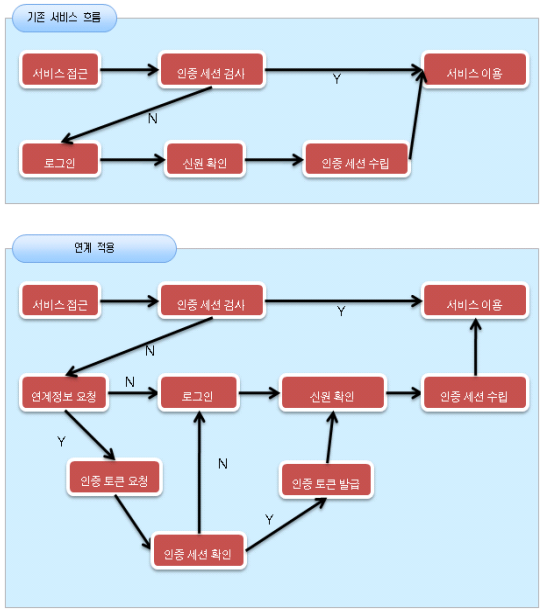
[그림 4] 통합 사용자 인증을 위한 시스템 구성



[그림 5] ID 연계 흐름도

3.3 연계 프로토콜 설계

연계 프로토콜에서는 사용자 인증을 담당하고 사용자의 개인정보를 관리하는 IdP(Identity Provider)와 IdP로부터 받은 인증 정보를 확인하고 서비스를 제공하는 SP(Service Provider)를 정의한다. 또한, 2개 이상의 IdP가 존재할 때 원하는 IdP에게 인증 정보를 요청하기 위한 정보를 관리하고 이러한 연계 정책을 관리할 수 있는 연계 서버를 정의한다. 연계 프로토콜에서는 SAML(Security Assertion Markup Language) v2.0 기반의 메시지와 프로토콜을 사용하여 그림 5에 나타낸 것과 같이 ID 연계 프로토콜을 재설계하였다.[12] 기존 서비스와 ID 연계를 적용한 서비스 간에 인증 흐름은 그림 6에 나타낸 것과 같이 달라지게 된다.



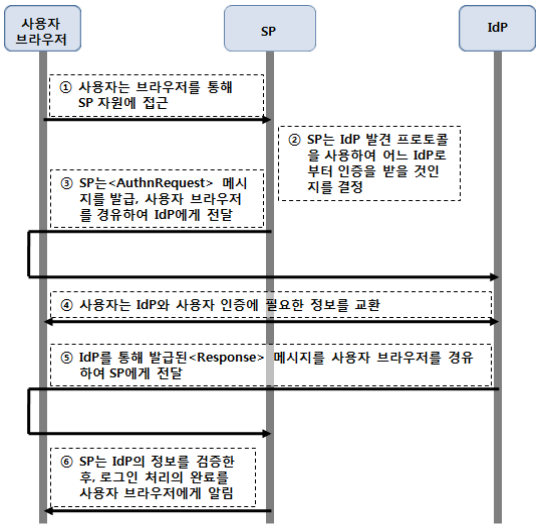
[그림 6] 기존 서비스와 연계 적용 서비스간의 인증 흐름 절차 비교

3.3.1 단일 로그인 절차 설계

사용자가 SP자원에 접근 하려 하거나 또는 IdP에 접근할 때, 사용자는 자원에 대한 인증을 IdP를 통해 받아야 한다. 이때 IdP는 Service Provider와 약속된 인증 정보를 만들어야 한다. 그리고 Service Provider는 IdP에서 제공하는 인증 정보를 가지고 사용자를 인증 할 수 있다. 단일 로그인이 이루어지는 세부적인 절차는 다음과 같다. (그림 7 참조)

① 사용자는 브라우저를 통해 SP의 자원에 인증을 거치지 않은 채로 접근한다.
② SP는 사용자의 인증을 처리할 IdP를 IdP 발견 프로토콜을 통해 결정한다.
③ SP는 <AuthnRequest> 메시지를 만들어내고 사용자 브라우저를 통해 IdP에게 전달한다.
④ 사용자는 IdP를 통해 인증을 하게 된다.
⑤ IdP는 <Response> 메시지를 생성하고 사용자 브라우저를 통해 SP에 전달하게 된다. <Response> 메시지 안에 담긴 정보는 인증 에러 또는 사용자의 인증 정보들이 담겨 있다.
⑥ SP는 IdP가 사용자 브라우저를 통해 보낸 메시지를 통해 사용자가 처음 접근했던 자원에 대해 인증을 처리 할 것인지 에러 메시지를 보낼 것인지에 대해

결정이 가능하다.



[그림 7] 단일 로그인 절차

3.3.2 단일 로그아웃 절차 설계

통합 사용자 인증 서비스를 구현하는 과정에서 가장 중요하게 여겨지는 것이 단일 로그인의 구현이지만, 이것 못지않게 중요한 것이 단일 로그아웃이다. 사용자는 단일 로그인을 통해 여러 서비스를 자동 인증 받아 이용하다가 서비스의 이용을 중단할 수 있다. 이 경우, 통합 사용자 인증 서비스는 단일 로그인 과정을 통해 연결된 모든 서비스 세션들을 자동적으로 종료시켜야 한다. 따라서 본 연구에서는 이를 위해 그림 8에 나타낸 것과 같이 SAML의 단일 로그아웃 프로토콜을 기반으로 단일 로그아웃 절차를 설계하였다. 본 연구에서 구현한 단일 로그아웃의 세부적인 절차는 다음과 같다.

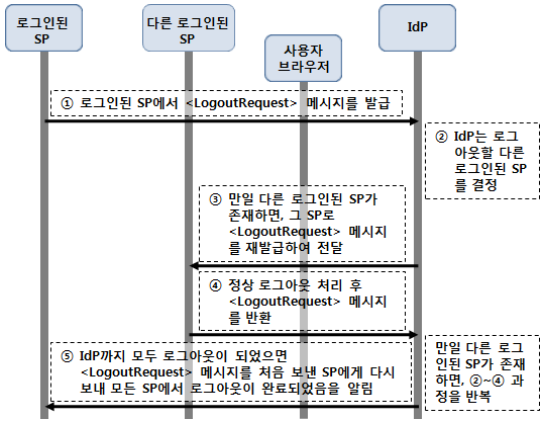
① <LogoutReqeust> 메시지를 통해 로그인된 SP들은 단일 로그아웃 또는 서비스 종료가 되었음을 IdP에게 알린다. 이 요청은 SP와 IdP 간에 직접 요청하는 형태로 구현되거나 SP와 IdP 간에 사용자 브라우저를 통해서 간접적으로 전달되는 형태로도 구현될 수 있다.

② IdP는 <LogoutRequest> 메시지 안에 포함된 정보를 가지고 세션의 종료를 결정한다. 만약 단일 로그인이 일어나지 않은 경우에는 자신의 세션만을 종료 하게 된다.

③ IdP는 <LogoutRequest> 메시지를 재생성하고 다른 단일 로그인이 된 서비스에 <LogoutRequest>메시지를 전달한다.

④ 다른 단일 로그인된 서비스는 IdP를 통해 전달받은 <LogoutRequest> 메시지를 통해 자신의 세션을 종료하고, <LogoutResponse> 메시지를 IdP에게 전달한다.

⑤ IdP는 다른 단일 로그인 된 서비스로부터 전달 받은 <LogoutResponse> 메시지를 통해 다른 서비스들의 로그아웃이 정상 처리됨을 확인한 후에 처음 <LogoutRequest> 메시지를 요청한 SP에게 정상 로그아웃 처리가 되었음을 알리는 <LogoutResponse> 메시지를 전달한다.



[그림 8] 단일 로그아웃 절차

4. 결론

본 논문에서는 개별적으로 사용자 인증 시스템이 구현된 각 시·도교육청 교육정보서비스와 한국교육학술정보원의 교육정보서비스를 단일 사용자 인증을 통해 모두 이용할 수 있는 최적의 방안을 연구하고 설계함으로써 전국교육정보공유체제를 통한 교육정보 서비스 이용에 편리성을 도모하는 동시에 사용자 인증 관리의 효율과 안전을 기할 수 있는 방안을 제시하였다.

본 연구가 진행되기 이전까지 이미 여러 시·도교육청에서는 해당 시·도교육청에서 운영 중인 교육정보서비스들을 단일 사용자 인증으로 서비스하기 위하여 사용자 인증 정보를 가지고 있는 데이터베이스들을 하나로 통합하거나 사용자 인증 시스템들 간에 쿠키 정보나 세션 정보를 교환하는 방법을 통해서 통합 사용자 인증 서비스를 구현하였다. 그러나 이렇게 각 시·도교육청에서 개별적으로 진행된 통합 사용자 인증 서비스는 그 구현 방법이 모두 상이하여 타 시·도에서 구현된 사용자 인증 서비스는 물론 통합 사용자 인증 서비스와도 호환되지 못하

는 문제점을 가지고 있었다. 또한, 16개 시·도교육청 산하 교육정보원이나 교육과학연구원 등을 방문하여 설문조사를 실시한 결과 대다수 시·도가 전국적인 통합 사용자 인증 서비스가 구현될 경우 시·도에서 이미 개별적으로 구축 운영 중인 통합사용자 인증 서비스의 변경을 최소화할 수 있는 방안으로 이루어지기를 희망하였으며, 기존에 각 시·도가 보유하고 있는 사용자 신상정보 데이터베이스에 대한 통제권을 각 시·도가 그대로 유지하기를 원하였다.

이러한 조사 결과를 바탕으로 본 논문에서는 통합 사용자 인증을 구현하는 여러 방법들 가운데 ID 연계 관리 방식으로 16개 시·도교육청과 한국교육학술정보원의 교육정보서비스에 대한 통합 사용자 인증 서비스를 설계하였다. 본 논문에서 설계를 통하여 제시한 ID 연계 기반의 통합 사용자 인증 방식은 여러 기관들이 독자적인 인증 정책을 사용할 수 있도록 하면서 다른 기관과는 표준화된 절차로 ID 정보를 교환하도록 한다. 따라서 본 논문에서 제시한 ID 연계 관리 방식을 사용하여 통합 사용자 인증 서비스를 구현하게 되면, 이미 여러 시·도교육청에서 개별적으로 기 구축해 놓은 통합 사용자 인증 서비스의 구현 내용을 변경하지 않아도 될 뿐만 아니라 사용자 신상정보 데이터베이스를 하나로 통합할 필요가 없기 때문에 통합 사용자 인증 구현에 따른 비용과 노력을 줄일 수 있다.

한편, 본 연구에서는 중앙 집중형 SSO 모델과 사용자 중심형 SSO모델로 통합 사용자 인증을 구현하는 경우에 비해 ID 연계형 SSO 모델로 통합 사용자 인증이 성능적으로 얼마나 더 우수한 지는 분석하지 않았다. 사실 통합 사용자 인증 서비스의 구현은 어떠한 방식으로 구현되든 사용자 입장에서 처음에 한번 가입한 이후 통합사용자 인증이 제공되는 모든 사이트에 별도의 가입 절차가 필요치 않다는 데 공히 편리함을 느끼게 된다. 그러나 ID 연계형 SSO 모델은 다른 두 모델에 비해서 로그인을 처리하는데 있어서 더 많은 시간을 필요로 한다. 앞으로 더 편리한 통합 사용자 인증이 구현되기 위해서는 빠른 로그인 시간을 보장하면서 사용자 가입 절차를 줄일 수 있어야 한다. 향후 연구에서는 세 모델별 성능 비교를 위한 평가 지표를 수립하고, 이러한 평가 지표를 기반으로 각 모델별 성능을 분석하는 연구를 통해 보다 편리한 통합 사용자 인증을 구현하는 방안을 제시할 계획이다.

참고문헌

[1] 조영섭, 진승헌, “Digital Identity 관리 기술 현황 및 전망”, 전자통신동향분석 제22권 제1호, 2월, 2007.

[2] 유재형, 다중 도메인 간 SSO 실현을 위한 통합 Identity 관리기술 분석, KNOM Review, Vol. 10, No. 1, 8월, 2007.

[3] 오해석 외, 전자정부 서비스 사용자 인증 및 권한 관리 레벨화 방안 연구, 한국정보사회진흥원 연구보고서, 9월, 2007.

[4] 송정환, 강연정, 장환석, “인터넷 ID 관리를 위한 서비스 모델 제안”, 정보보호학회논문지 제18권 제4호, pp. 143-152, 8월, 2008

[5] 최향창, 김현, 박해룡, 전길수, 이형효, “개인정보 DB 관리기술의 보안 요구사항 연구”, 정보보호학회지 제18권 제2호, pp. 76-86, 4월, 2008

[6] 최향창, 이용훈, 노봉남, 이형효, 조상래, 진승헌, “ID 관리 시스템에서의 프라이버시 보호”, 정보보호학회지 제14권 제6호, pp. 82-93, 12월, 2004.

[7] 손태식, 이상하, 유승화, 김동규, “단일 인증 시스템의 인증 기법과 인증 모델 분석”, 정보보호학회지 제11권 제4호, pp 87-100, 8월, 2001

[8] 구희정 외, “SAML 기반의 사용자와 OSS간 안전한 정보교환을 위한 관리시스템", KNOM Review, Vol, 7, No. 2, 12월, 2004.

[9] 최진탁, “Single Sign-On을 이용한 인증 관리 기법에 관한 연구”, KSIAM IT series Vol. 10, No.1, pp. 61-69, 2006.

[10] 진승헌 외, “Digital Identity Management 2008년 기술백서”, 한국전자통신연구원 SW콘텐츠연구부문 정보보호연구본부 디지털ID보안연구팀, 10월, 2008.

[11] 조영섭, 진승헌, “OASIS SAML (Security Assertion Markup Language) V2.0 고찰 및 활용”, 한국멀티미디어학회지 제10권 제1호, 3월, 2006.

[12] 김성훈, 김인호, 김홍근, 김윤정, “웹 2.0과 ID 관리 기술 전망”, 한국정보보호진흥원 CSO Briefing, 6월, 2007.

[13] 원유재 외, “XML 기반의 통합 인증·인가 시스템 개발”, 정보통신부, 5월, 2003.

[14] 염흥열, 이재승, “웹 2.0 보안 기술 동향 및 표준화 추진 방향”, IT Standard & Test TTA Journal, No. 117, 5월6월, 2008.

[15] 조상래, 진승헌, “사용자 중심의 ID 관리를 위한 디지털 ID 공유 프레임워크”, 전자통신동향분석 제23권 제6호, pp.102-111, 7월, 2008.

[16] Security Assertion Markup Language (SAML) V2.0 Technical Overview, Working Draft 21. Feb 2007

[17] 박정호 외, “교육정보 통합 플랫폼 구현을 위한 통합 사용자 인증 방안에 관한 연구”, 한국교육학술정보원, 12월 2008.

[18] 유인태 외, “차세대 모바일 환경에 적합한 ID 관리

기술 연구”, 한국정보보호진흥원, 12월 2008.

박 정 호(Jung-Ho Park) **[정회원]**

- 1987년 2월 : 성균관대학교대학원 전자공학과 (통신공학석사)
- 1998년 8월 : 성균관대학교대학원 전자공학과 (통신공학박사)
- 1987년 1월 ~ 1992년 5월 : 삼성종합기술원 전자기기연구소 주임연구원
- 2004년 3월 ~ 현재 : 서울디지털대학교 컴퓨터공학부 조교수

<관심분야>
정보통신, 컴퓨터교육