디지털산업정보학회 논문지 제4권 제3호 - 2008년 9월

공공도서관 클러스터링을 위해 SAML 기반의 사용자통합인증 설계에 관한 연구

변 회 균* · 고 일 주**

A study of SSO design based SAML for public library clustering

Byeon, Hoi Kyun · Ko, Il Ju

〈Abstract〉

The user has to subscribe to the library so that user use the library service. User has to register at that in order to use of the nearby another library. Moreover, service such as the inter-library loan and returning my loan book to other library in which the mutual cooperation between the library is needed necessity. But it services due to the constraint condition because of the administrative or technical problems. In this paper excludes the administrative element. The web service model is forming the cluster based on the mutual cooperation between the technologically adjacent public library and provides the technologically necessary single sign-on (SSO) in order to support the additional service. The single sign-on of the library which is concluded by this model using the security information exchange standard (Security Assertion Markup Language : SAML), it is processed by XML base. In using this model, the loan information is confirmed in the attribution in return service library and the model can utilize for the return of loan book in other library. It designs the single sign-on about it.

Key Words : SSO, SAML, Clustering, Public Library

Ⅰ. 서론

정보에 원천이라 보면 도서관을 빼 놓을 수 없다. 도서관은 지식의 창고로서 인간의 역사를 고스란히 담고 있다. 과거에는 서가에 꽂혀있는 서가의 개념만이 존재하였으나, 다양한 매체의 발달과 인터넷 기술이 접목되어 디지털 도서관으로 점차 확장되고 있다. 이것은 직접 도서관을 방문해서만 여러 지식을 얻을 수 있던 방식에서 신기술의 발달과 인터넷의 장점을 이용하여 웹 서비스를 제공함으로써 오프라인 지식의 창고에서 시·공간의 제약에서 벗어나 온라인 서비스를 제공하고 있다.

도서관은 종류에 따라 공공도서관, 대학도서관, 학교도서관, 전문도서관 및 국립중앙도서관으로 구분하고 있다 이 중에 대학도서관과 공공도서관은 장서의 권수나 시설 면에서 규모가 크다. 한 대학 안에서도 중앙도서관을 비롯하여, 각 분교 도서관과 단과대학별 도서관들이 있고, 공공도서관도 시립, 구립, 정보화도서관, 어린이 도서관등 여러 도서관이 존재한다. 이미 외국에는 공공도서관이 교육 및 생활의

* 숭실대학교 정보과학대학원 디지털컨텐츠학과 석사과정
** 숭실대학교 미디어학과 교수(교신저자)

중심역할로서 확대되어 있고, 또한 국내에서도 복지시설의 확대에 힘입어 한 시·군 안에서도 여러 공공도서관이 새롭게 건립 또는 증축되고 있다. 이런 도서관의 확대는 분야별로 전문화 되거나, 서로 다양한 협정을 체결하여 사용자에게 차원 높은 서비스를 제공하기 위해 노력하고 있다.

대학 도서관인 경우, 중앙도서관을 중심으로 분교 도서관 및 각 단과 대학의 상호협력 서비스를 위해 도서를 관리 및 서비스 할 수 있는 도서관자동화시스템을 통합하여 구축함으로써 중앙도서관과 분교 및 단과 대학의 도서관에 통합서비스를 제공하고 있다. 하지만, 공공도서관인 경우 인근 도서관과의 상호 서비스를 위해 이와 같이 처리하기에는 행정적인 어려움과 비용에 따른 주체 및 예산확보 등의 어려움이 따를 수밖에 없다. 이를 해결하기 위해서는 행정적으로는 협정기관끼리 상호신뢰관계를 맺어야 하고, IT적으로는 사용자의 확인을 위해 통합인증이 가능토록 해야 하며, 필요한 부가서비스를 해줄 수 있는 방법을 찾아야 할 것이다.

기업에서는 다양한 업무시스템이 필요에 의해 독립적으로 개발되어 왔고, 비용절감과 운영의 편리성, 새로운 서비스 재창출을 위해 조직 내부시스템의 통합인증 및 통합서비스에 대해 고민을 해 왔다. 여러 S/W 시스템통합 회사들은 LDAP 이나 X.500 표준을 이용한 제품을 이용해 통합인증을 제공하거나, 직접 프로그램을 구현하여 한 시스템을 인증할 때 백그라운드로 여러 시스템에 로그인을 해두는 방식을 적용해 왔다.

기업에 적용했던 여러 표준들은 주로 기업 내의 단일 도메인 내에 통합인증을 구축하는 것에 용이하고, 용량이 적기 때문에 LDAP이나 X.500로 처리가 가능하나, 인터넷상의 보안문제나, 용량이 커질수록 처리속도 및 비용 등이 문제가 된다[1].

본 논문에서는 도서관을 중심으로 여러 공공도서관들의 사용자인증을 위해서 다중 도메인에서 통합인증을 처리할 수 있는 방법을 모색해 보고, 도서관 환경에 적용할 수 있는지 모델을 살펴본다.

사용자 통합인증을 위한 ID 연계기술로는 대표적으로 ID 관리를 통한 Liberty Alliance 방법과 SAML V2.0 방식이 있다[2]. SAML V2.0과 Liberty Alliance와 가장 큰 차이점은 인증의 병목현상이다. Liberty Alliance는 SP에서 IDP로 사용자에 대한 인증 정보를 요청하면 IDP는 해당 사용자의 IDP에서의 로컬 세션 상태에 관한 정보를 확인하고 인증된 상태인 경우 응답을 SP에 전달한다. 따라서 다른 사이트에 접근을 위해서는 또다시 IDP에 접근하여 인증을 수행하는 병목현상이 발생 될 수 있으나, SAML은 한번 인증을 받은 후에는 다른 사이트를 접속시 IDP를 통해 또다시 시도하지 않고 saml assertion 만을 확인하여 인증 처리를 한다. Liberty Alliance 방식은 연계된 네트워크 ID관리와 ID 기반의 서비스를 위한 공개 표준으로 개발되었고 활발히 연구되고 있으나[3], SAML V2.0이 Liberty Alliance 결과물을 수용하여 제정되었으므로 본 논문에서는 SAML을 이용한다. 또한 다른 분야에 적용한 ETRI 사례를 통해 통합인증을 위한 여러 기술을 살펴보고, 도서관간의 사용자통합인증을 처리하기 위한 설계를 제시한다.

SAML에서 인증을 제공하는 Identity Provider를 IdP라 하고, 서비스를 제공하는 Service Provider를 SP라고 할 때, 이들 간에 단일 인증 절차를 명시하고, 한 IdP와 다수의 SP 간의 단일인증 시나리오를 제시하고 이에 맞도록 설계 한다.

2장 관련연구에서는 도서관의 통합인증에 대한 설명과 본 논문에 적용한 SAML 프로토콜, 그리고 이를 활용한 ETRI의 사례를 분석하고, 3장에서는 본 논문에서 제안하는 SAML기반의 사용자통합인증에 대해 설명하며, 4장 결론으로 끝을 맺는다.

Ⅱ. 관련연구

2.1 도서관의 통합인증

본 논문에서는 대표적인 공공도서관과 대학도서관의 사례를 중심으로 살펴본다.

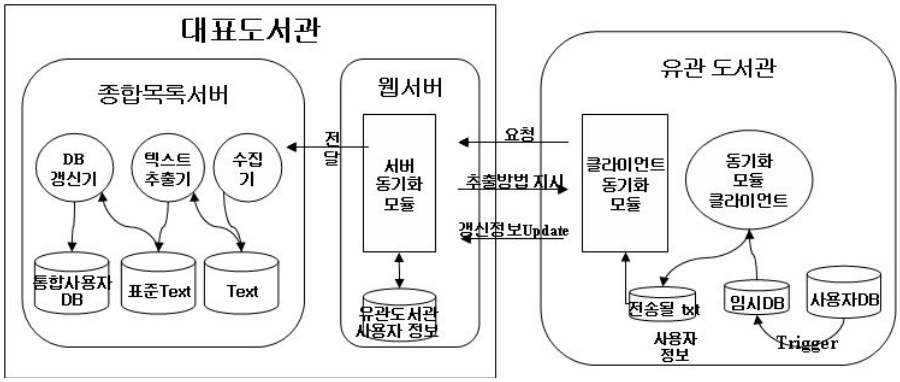
공공 도서관들 간에 통합인증을 구축한 사례는 흔하지 않지만, 시립도서관의 경우 중앙도서관(또는 대표도서관)을 놓고 분관으로 처리하여 시립이하 작은 도서관까지를 사용자통합을 하여 처리하는 방식을 취하고 있다. 또는 통합인증은 아니지만 일부 서비스를 위해 사용자의 일부정보와 관련된 정보를 수집하는 방식을 취하기도 한다. 전자의 경우 상위기관의 도서관에서 하위기관의 도서관을 함께 통합구축함으로서 한 시스템에 각각 도서관들의 사용자 DB를 하나로 구축하고, 프로그램에서 중앙도서관 이외의 도서관은 분관 개념으로 처리하기 때문에 이는 상·하 도서관 구분이 명확하고, 한 예산으로 사업을 진행해야만 가능하다. 또한 통합과정에서 발생하는 여러 문제를 동시에 해결해야 하는 어려움이 존재한다. 후자는 도서관 중에서 상위 개념의 도서관이 있는 경우, 각 하위 도서관과 약정을 맺고 각 도서관의 사용자 DB를 정기적으로 수집하여 상위 도서관 사용자 DB에 쌓는 방식이다. 이는 수집기간 사이의 동기화 문제와 사용자 DB 수집에 따른 개인정보외부 유출될 가능성이 존재하기 때문에 구조적 문제를 안고 있다.

대학도서관들 간의 통합인증도 상황은 거의 비슷하나 공공도서관보다는 더 좋은 편이다. 한 대학 내에서는 이미 중앙도서관과 분관개념이 존재하여 사용자 DB의 통합이 가능할 수 있고, 인근 대학 간에 협정을 맺은 후에 자기도서관에 없는 도서를 협정을 맺은 타 대학에서 복사 또는 대출 받을 수 있도록 상호대차서비스를 활용하기 위해 오프라인 상으로 사용자 정보를 확인하여 처리하는 경우가 있다.

사용자 통합은 SSO(Single Sign on)를 구축하기 위해서는 우선적으로 이루어져야 하며, 각 도서관에 이미 구축된 사용자테이블을 하나의 테이블로 통합 과정을 거치게 된다. 이는 각 도서관이 같은 종류의 솔루션을 이용할 경우와 다른 종류의 솔루션을 이용할 경우에 따라 절차가 다르다. 같은 솔루션을 사용한다면 사용자테이블 스키마가 동일하므로, 각각의 사용자 테이블의 레코드를 합하고, 혹시라도 중복될 수 있는 중복가입자를 찾아낸다. 주민번호를 가지고 있다면 작업이 쉬우나, 정보시스템 구축운영기술지침에 따라[4], 점차 주민번호 정보를 가지고 있는 경우가 적으므로 사용자성명과 전화번호 또는 사용자성명 및 주소 등의 정보로 매핑 한다. 이렇게 만든 사용자통합DB를 이용하여 모든 서비스는 사용자 인증 및 권한 부여를 할 수 있도록 변경한다. 만약, 서로 다른 솔루션을 사용한다면 훨씬 더 복잡한 처리를 진행해야 한다. 앞에서 설명한 중복가입자 처리를 진행하고, 각 사용자에게 부여한 각종 코드(신분, 권한 등)를 맞추어야 하고, 데이터 값의 속성들도 변환하여 처리하여야 한다. 이러한 작업 시 가장 발생하기 쉬운 문제로 사용자의 유일한 식별번호(주민번호 등)가 없기 때문에 사용자 중복가입자처리가 쉽지 않다. 또한 시스템이 다른 경우 사용자정보 관련 코드매핑이 쉽지 않으며, 통합할 도서관이 많을수록 매핑작업에 많은 시간 및 비용이 소요된다. 하지만 이와 같은 문제에도 한번 사용자통합을 한 이후에는 하나의 시스템으로 서비스되므로, 여러 도서관에 원활한 서비스를 이용할 수 있기 때문에 최근 여러 시립도서관이 이와 같은 작업을 하고 있는 추세이다.

사용자 통합은 각 기관의 독립적인 시스템을 유지하면서, 통합인증을 처리할 수 있는 방법이다. 하지만 사용자 DB를 수집해야한다는 문제로 개인정보보호차원에서 보안이 요구되며 점차 수집되는 정보를 최소화 하고 있다. 다음의 예는 동기화 통신모듈을 통해 사용자정보를 수집하는 방식을 설명한다.

<그림 1>에서 유관도서관은 사용자가 회원가입 또는 수정에 따른 처리가 발생할 때 이 정보를 임시DB로 저장하고, 동기화모듈(서버, 클라이언트)이 유관도서관 사용자 정보를 수집한다. 이 변경된 사용자 정보를 XML 형식의 text파일로 수집하여 서버로 전달되어 지고, DB 갱신기를 통해 통합사용자DB로 저장한다. 이렇게 수집된 통합사용자DB는 사용자가 대표도서관에 로그인 시 소속도서관의 정보와 ID를 입력하면 인증을 가능케 할 수 있다. 하지만 이와 같이 공공 또는 대학 도서관들의 수집 방식은 개인정보 유출의 위험성을 내포하고 있으며, 사용자 DB의 신규, 수정, 삭제 시에 필요 데이터를



<그림 1> 사용자 DB 수집 구성도

주기적으로 송신해야 하므로 필요 없는 네트워크 트래픽을 발생한다. 또한 반영 주기에 따른 상호간의 데이터 불일치가 생길 수 있으며, 전송된 데이터가 DB에 정확히 반영되었는지에 대한 트랜잭션 관리가 어렵다. 이와 같은 문제점으로 대표도서관 로그인시는 통합인증이 가능하나, 유관도서관으로 로그인한 경우는 다른 유관도서관으로 통합인증은 어렵다.

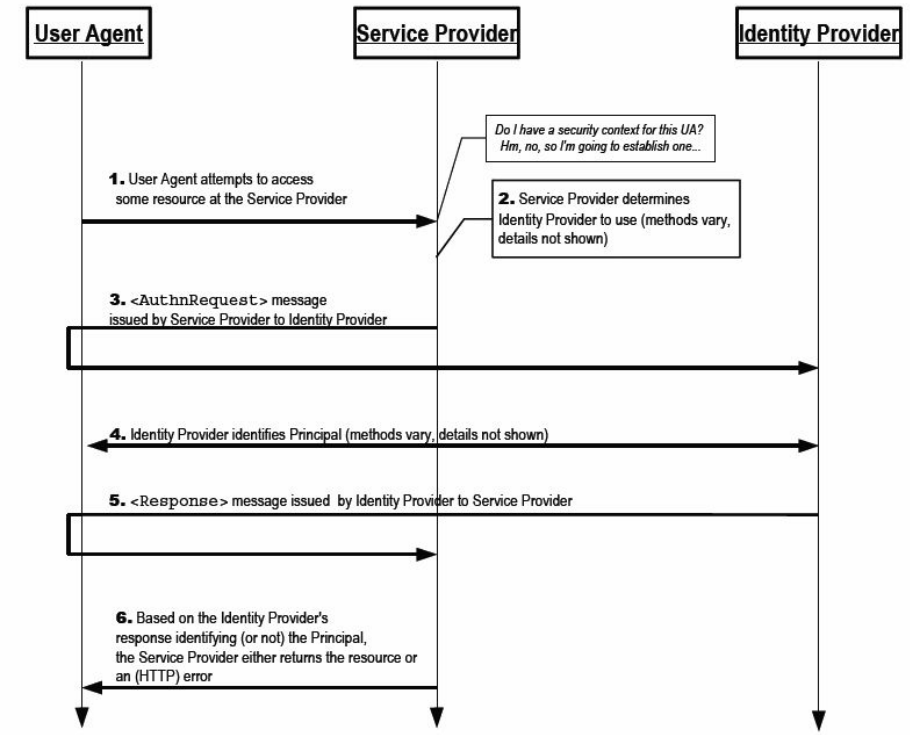
2.2 SAML 프로토콜

SAML은 인터넷상의 비즈니스 보안 정보교환용이며 사용자 인증, 자격, 속성정보의 교환을 위한 XML기반의 표준 언어이다. 이것은 OASIS(Organization for the Advancement of Structured Information Standards)의 Security Service Technical Committee에서 개발되었으며[1], 2002년 11월에 SAML V1.0 표준을 제정하였고 2003년 9월에는 V1.0을 보완한 V1.1을 제정하였다. SAML V1.1은 많은 업체에 의해 구현되어, 공공, 교육, 산업 분야에서 큰 성공을 거두었다. SAML V2.0은 Liberty Alliance와 Shibboleth 의 연구 결과물을 수용하여[5], SAML V1.1에 ID 연계 기능을 통합하여 2005년 3월에 제정된 통합 표준이다.

SAML은 사용자, 기기 또는 구분이 가능한 모든 개체들에 대한 인증 및 승인 정보를 교환하는 것을 가능하게 하기 위해 XML의 부분적인 집합들을 사용하여 시스템이 주장기반 주체의 인증 요청을 허용하거나 거부하는 Request-response protocol 을 정의한다. Assertion은 주체에 관한 특정 사실에 대한 선언으로 세 가지의 주장으로 정의된다.

첫 번째 Authentication 주장으로 주체가 이전에 특정한 방법(패스워드, 하드웨어 토큰 또는 X.509 공개 키 등)으로 인증되었다는 것을 나타낸다. 그리고 두 번째 Authorization 주장은 주체가 자원 접근을 허용하거나 거부해야 함을 나타내며, 세 번째 Attribution 주장은 주체가 갖는 속성들을 나타낸다.

<그림 2>는 SAML의 기본적인 템플릿을 보여주고 있으며,[6] 보안적인 측면에서는 단일인증을 구현하기 위해 키 교환방식이나, 쿠키 그리고 SAML 같은 토큰기반의 프로토콜이 있다[7]. 키 교환방식은 사용자 인증단계를 키 교환이나 키 확인 단계부터 시작하기 때문에 사용자 응용프로그램은 암호화와 사용자 인증을 위한 새로운 키를 사용하거나 검증된 키를 사용하는 특징이 있다. 그러나 쿠키들은 때때로 동일한 세션 키를 가지고 암호화되기 때문에 공격자가 단 하나의 쿠키에 대한 세션 키를 찾는다면 시스템내부의 모든 사용자의 쿠키들이 취약해질 수 있다. 또한 브라우저 내의 쿠키들은 플러그인이나 다른 방법을 통해 도난당할 수 있으며, 스푸핑(spoofing) 공격을 당할시 쿠키가 다른 도메인들로부터 개별적인 서



<그림 2> SAML 시나리오

버들에게 보내져야 한다는 요구를 기술할 방법이 없기 때문에 쿠키의 목적지 제어를 방해할 수 있다.[8]

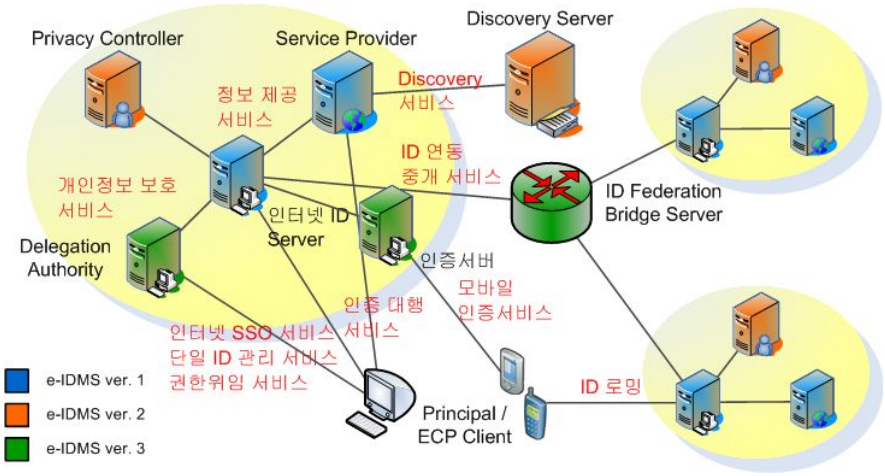
SAML은 단일 인증 후에 신뢰된 보안 도메인들 사이에서 사이트 접근을 용이하게 하는 적합한 표준이기 때문에 쿠키 기반의 단일인증 솔루션 이상의 장점을 갖는다. 특히, 토큰 역할을 하는 artifact는 보안 도메인 내에서 생성되고 사용자 인증을 위한 다른 보안 도메인들에 보내진다. 다른 보안 도메인에 보내진 artifact는 원래의 보안 도메인에 반환되고 사용자 인증 후 제거된다. 따라서 artifact를 이용한 단일인증 메커니즘을 통해 세션 키가 노출되는 문제와 브라우저에서 토큰들이 도난당하는 문제를 해결할 수 있고 artifact가 Uniform Resource Locator(URL)에 첨부되어 사용자의 인증정보를 담고 있는 메시지를 목적지로 전송하기 때문에 목적지 제어에 대한 문제점을 해결할 수 있다[9].

SAML의 1.0 과 1.1 프로파일은 SSO를 제공하기 위해 POST 또는 artifact bindings 2가지만 사용하였다. 하지만 SAML2.0은 더욱 확장되어 여러 조합이 가능하다. 즉 SP 또는 IdP에 의해 시작된 SSO 프로토콜은 HTTP Redirect, HTTP POST 그리고 HTTP artifact bindings의 조합으로 이루어진다[10].

2.3 ETRI SAML 적용 사례

공공기관 통합ID 관리시스템에 대한 사례로 ETRI 솔루션의 구조를 보면 ID 관리시스템인 e-IDMS를 단계별로 개발하여 진행되었으며, 본 논문에서는 version 3를 표본으로 분석하였다[11].

e-IDMS의 특징은 표준규격을 준용하였으며, 중앙 집중적인 정책관리 지원하고, 강화된 보안서비스를 제공했



<그림 3> e-IDMS 구성

다. 그리고 e-IDMS는 ID-중앙집중식의 SSO를 지원하고 있다. 이는 위에서 언급한 것처럼 관리적인 편리성은 좋다. 하지만, IDSP에서만 관리가 가능하여, 모든 사이트에 기본 로그인이 IDSP에서 먼저 처리하므로 인증에 대한 IDSP의 시스템, 소프트웨어 및 네트워크 등에 대한 신뢰성 및 만족할만한 성능을 제공해야 되는 부담이 있다.

e-IDMS의 구성을 보면 IDSP와 Privacy Controller, 가입자 웹브라우저, Discovery Server, ID Federation Bridge Server로 구성되어있다.

IDSP(인터넷 ID Server)는 인터넷 ID 관리 서비스를 제공하는 메인 시스템으로 인증, 개인정보 관리, 개인정보 열람 등의 서비스를 제공한다. 타 도메인의 서비스 제공자가 운영하는 인터넷 ID Server와 연결되어 로밍 서비스를 제공하기도 한다.

Privacy Controller는 인터넷 ID 관리 서비스에서 개인정보 유통을 제어하는 서버이다. 개인정보 제공자는 공개되는 정보에 대한 허가를 Privacy Controller에게 질의한다. Privacy Controller는 가입자가 자신의 개인정보 제어 정책을 쉽게 관리할 수 있도록 해주는 인터페이스를 제공한다. 프라이버시 도메인 관리자 또한 정보의 유통을 제어할 수 있다.

e-IDMS의 가입자는 IE나 Mozilla 등과 같은 기본 브라우저만으로 e-IDMS에 접근하며 서비스를 제공받을 수 있다. 가입자는 브라우저를 통해, 가입, 개인정보 관리, 개인정보 보호 정책 관리 등의 기능을 수행하게 된다.

Discovery Server는 ID 정보를 제공하는 AP(Attribute Provider)가 제공하는 정보를 등록하고, ID 정보를 소비하는 AC(Attribute Consumer)가 ID 정보 제공자를 검색하는 기능을 제공한다. SP는 자신이 ID 정보를 제공할 때는 AP 역할을 수행하고, 다른 AP에서 제공하는 ID 정보를 사용할 때는 AC의 역할을 수행한다.

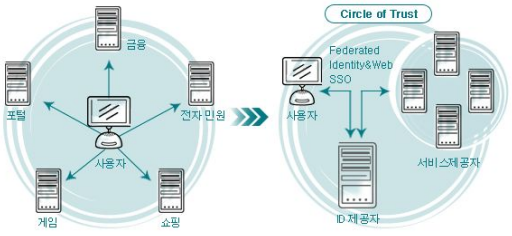
마지막으로 ID Federation Bridge Server는 여러 CoT가 존재할 때 이들 간의 ID Federation을 통해, SSO와 ID 정보 서비스를 제공하려면, 개별 CoT간 신뢰 관리와 ID 연계가 선행되어야 한다. CoT가 여러 개 존재하면, CoT간 신뢰 관리와 ID 연계가 매우 복잡해지게 된다. ID Federation Bridge Server는 이들 신뢰 관리와 ID 연계가 쉽게 제공할 수 있도록 하여 시스템의 확장성을 제공한다.

ETRI에서는 e-IDMS를 적용하여 공공기관 통합 ID 관리시스템에 적용하고 있다. 여기서 공공기관 통합 ID 관리 시스템은 행정업무 효율화와 민원서비스 개선 등을 위한 전자정부의 자치단체 정보화사업의 일환으로 대전광역시에서 현재 진행되고 있다. 이처럼 통합 ID 사용으

로 인해 사용자는 연계기관 홈페이지와 통합ID를 연결시킴으로써 통합ID를 사용가능하며, 사용자는 통합ID만 기억하면 연계홈페이지 사용할 수 있다. 또한 ID/암호는 물론 모든 온라인상 개인정보를 국제표준에 따라 암호화시킴으로써 안전하게 보호되며, 사용자는 연계홈페이지에 개인정보 공개범위를 선택할 수 있다. 통합 ID관리는 ID 관리서비스와 ID 정보제공서비스를 제공한다.

ID 관리서비스는 통합ID(Identity Service Provider)가 가입자의 ID를 관리하는 서비스이다. 가입자는 이 서비스를 통해 하나의 가입자 ID를 등록하며 통합ID에 가입한다. 가입 후, 사용자는 자신의 모든 개인 정보를 등록, 수정, 관리할 수 있다. 또한 가입자는 통합ID에 저장된 개인 정보를 이용하여, 통합ID에 등록된 연계사이트를 자유롭게 사용할 수 있게 된다. 그리고 ID 정보제공서비스는 통합ID가 신상정보, 비신상정보 및 Credential로 구성된 가입자의 속성정보를 관리하며, SP의 요청시 SP에게 속성 정보를 제공하여 주는 서비스이다. 또한 가입자가 본인의 정보를 변경할 때, 관련된 모든 SP의 정보를 자동으로 갱신하여 주는 서비스를 제공한다. SP는 별도의 관리 없이도 가입자의 최신 정보를 이용할 수 있게 된다.

<그림 4>는 인터넷상에서 안전하고 편리한 전자거래 활성화를 촉진하고 공공기관이 운영하는 다양한 웹 사이트에 산재된 사용자 ID와 개인정보를 안전하게 보호·관리할 수 있도록 대전광역시 통합 ID관리시스템을 시범 구축하여 제공하려는 관리시스템 구성도이다[12].



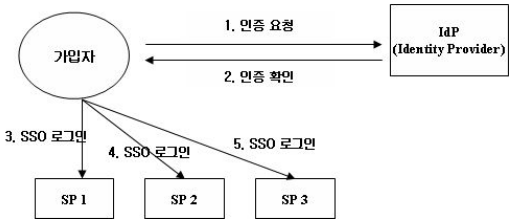
<그림 4> 대전광역시 통합ID 관리시스템

Ⅲ. 도서관에서 SAML적용

3.1 적용 방법

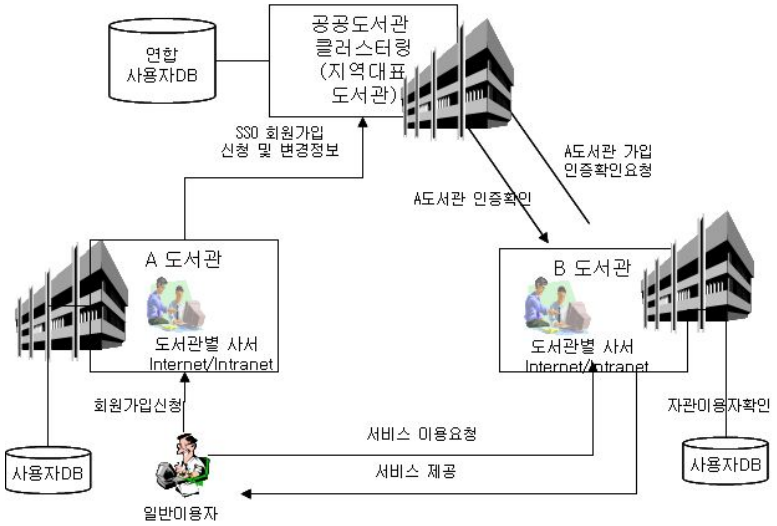
앞에서 언급했듯이 SAML은 여러 도메인에서 ID 통합 관리나 인증처리 표준을 위한 방식에 이용된다. 따라서 각각의 개별 도메인을 가지고 있는 공공도서관 간의 통합인증에 SAML을 어떻게 적용할지 설명한다.

사용자가 원하는 실제 서비스를 제공하는 SP가 사용자의 모든 정보 관리를 IdP에 일임하면, IdP는 관리를 대행하고 SP가 필요하다고 요청할 경우 해당 사용자의 속성정보(주민등록번호, 주소, 전화번호 등)를 제공하여 주는 서비스이다. 또한 사용자가 본인의 정보를 변경할 때, 관련된 모든 SP의 정보를 자동으로 갱신해 주는 서비스를 제공한다. SP는 별도의 관리 없이도 가입자의 최신 정보를 이용할 수 있게 된다. 신뢰 관계에 있는 모든 파트너 사이트들을 한 번의 인증으로 이용할 수 있도록 IdP에서 사용자에게 제공하는 기능이다[13]. 즉 사용자가 한 번의 인증 후, 추가적인 인증 없이 모든 파트너 사이트의 서비스를 이용할 수 있게 되는 것이다. 아래 <그림 5>은 단일 인증의 동작 예를 보인다. 사용자가 우선 IdP에 로그인을 하게 되면 SP 1,2,3 에 로그인 할 때는 단일 인증 기능을 통해 별도의 인증 절차 없이 자동으로 로그인하게 된다.



<그림 5> IdP와 SP 처리방식

공공도서관에 경우, 2006년10월4일자로 공포된 도서관 및 독서진흥법 전부 개정 법률안에 따라 전국 시도별로 지역대표도서관을 설립하게 되어 있다[14]. 도서관법(전부 개정 2006.10.4 법률 제8029호)에 지역대표도서관



<그림 6> 도서관 SSO 처리방식

의 설립 안이 있으며, 전국 시도별로 16개가 지정되어 있으며, 지역 대표 도서관은 시·도 단위의 종합적인 자료의 제공 및 수집, 정리, 보존을 하며, 지역의 공공도서관 지원과 협력 사업을 수행한다. 또한 도서관 업무에 관한 조사 연구를 수행하고 지역의 자료수집 지원 및 다른 도서관으로부터 이관 받은 자료를 보존한다. 그리고 국립중앙도서관의 자료 수집활동 및 도서관 협력사업 등에 대한 지원과 지역대표도서관으로서 필요한 업무 등을 처리하는 역할을 한다[15].

이 지역대표 도서관이 IdP역할을 하고, 그 지역의 공공도서관이 SP역할을 한다면 SAML을 이용한 SSO를 처리하여 지역대표도서관의 역할을 수행할 수 있다.

<그림 6>에서 보면 일반이용자가 A도서관에 회원가입신청을 하고, 이는 A도서관 이용자DB에 저장되며, SSO 회원가입신청을 할 때 이에 따른 정보가 지역대표도서관에 저장된다. 이 일반이용자가 같은 신뢰기관의 B도서관 서비스를 요청시에 B도서관은 지역대표도서관의 정보를 확인하여, A도서관 로그인사용자를 확인하고, 해당 서비스를 제공한다.

이는 ETRI사례와는 달리, ID관리를 지역대표도서관에만 위임을 하는 것이 아니라, 기존의 로컬도서관에 기본적인 인증을 인정하고, 추가적으로 SSO를 인증할 때 지역대표도서관의 통합인증을 처리한다.

3.2 설계

구체적으로 지역대표도서관이 IdP 역할을 하고, 그 지역 도서관을 각각 A, B 도서관이라고 가정할 때, 각각의 도서관은 직접 가입한 사용자정보만을 가지고 있고, IdP 지역대표도서관은 A와 B도서관의 사용자정보가 통합되어 있다고 본다. 이 때 지역대표도서관이 IdP의 역할을 하기 위해서는 ID관리를 위한 추가테이블을 설계를 해야 한다. 기본적으로 Id의 통합을 위한 테이블과 각 소속도서관의 ID정보, 세션을 위한 정보들이다.

<표 1>은 ID 통합을 위한 테이블로 Key_ID(통합사용자 ID) 는 IdP_IdInfo 의 Primary key이며, 유일한 값이다. 이 테이블은 각 도서관 별 사용자의 정보가 통합된 테이블이며, 각 사용자별로 유일한 레코드로 존재한다. 사용자ID, 비밀번호(암호화된 값), 사용자명, 주소를 관리한다. 여기서 비밀번호는 타 소속도서관에서 로그인을 시도하는 경우나, IdP로 직접 로그인을 할 경우 필요한 속성 값이다.

<표 1> IdP ID정보 테이블

Key_ID	사용자 ID	비밀번호	사용자 명	주소
lee9890	lee989	aeAxF	Lee	경기도 군포시 산본동 125-4
Tom0909	Tom09	EpEJA	Tom	경기도 군포시 수리동 658-8

<표 2> IdP 소속도서관 정보ID테이블

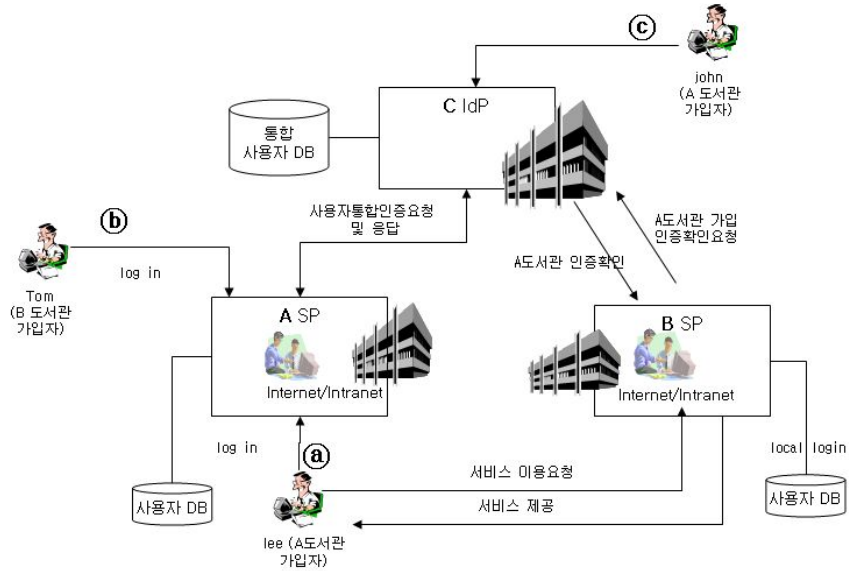
개별 ID	소속 도서관번호	Key_ID	사이트명	대출 등록번호
lee989	21008	lee9890	www.sanbonlib.or.kr	A00012, A92012
LeeJin	21010	lee9890	www.orkumlib.or.kr	C000128, C000859, C068821, C096840
Tom09	21009	Tom0909	www.surilib.or.kr	B006652, B008865
tomSon	21008	Tom0909	www.sanbonlib.or.kr	A02052, A82014, A00312

<표 2>는 소속도서관의 ID정보를 위한 테이블로 개별 ID와 소속도서관번호가 IdP_SubscribeId의 Primary Key 이다. 이 테이블은 소속도서관인 SP에서 로그인한 ID를 가지고 Key_ID를 얻을 수 있으며, 소속도서관의 공유정보(대출등록번호)가 포함되어 있다. 한 사람이 이미 여러 도서관에 등록된 경우, 도서관 기준으로 해당 도서관에 대한 사이트명, Key_ID 및 공유정보 등을 관리한다. 또한 소속도서관에서 대출이 처리될 때에 이 IdP_SubscribeId 테이블의 대출등록번호를 변경해 준다.

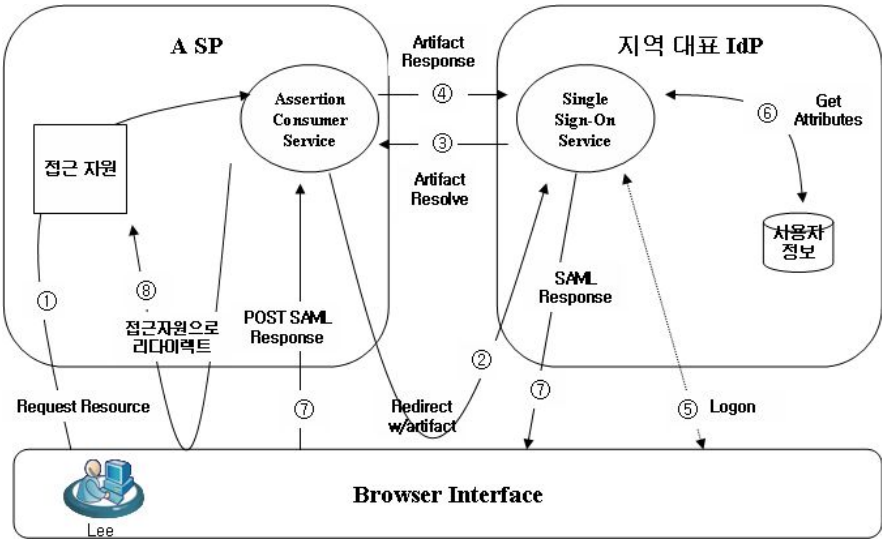
<표 3> IdP session 정보 테이블

Key_ID	클라이언트IP	Session key	접속시간
lee9890	192.168.100.216	98a8c0812	2008-04-24 07:11:25+0900
Tom0909	101.23.12.65	eda1923e76	2008-04-24 08:30:56+0900

<표 3>은 세션을 위한 테이블로 현재 로그인한 session 정보를 가지고 있으며 또한 세션정보를 관리하



<그림 7> SSO 로그인



<그림 8> SP 로그인 시나리오

기 위해 사용자가 통합인증을 한 경우, IdP에 클라이언트 IP, Session Key, 접속시간, Flag를 기록한다. Session Key 값은 Key_ID와 접속시간을 조합하여 만든 key값으로 세션 정보 확인 값으로 활용한다.

<그림 7>의 전체적인 로그인 절차를 보면 ⓐ 경우는 A도서관 가입자이면서 A도서관에 로그인을 하는 경우이며, ⓑ 경우는 B 도서관 가입자이면서, A도서관에 자원을 이용하려고 하는 경우이며, ⓒ 경우는 A 도서관 가입자가 직접 지역대표도서관으로 로그인하는 경우이다.

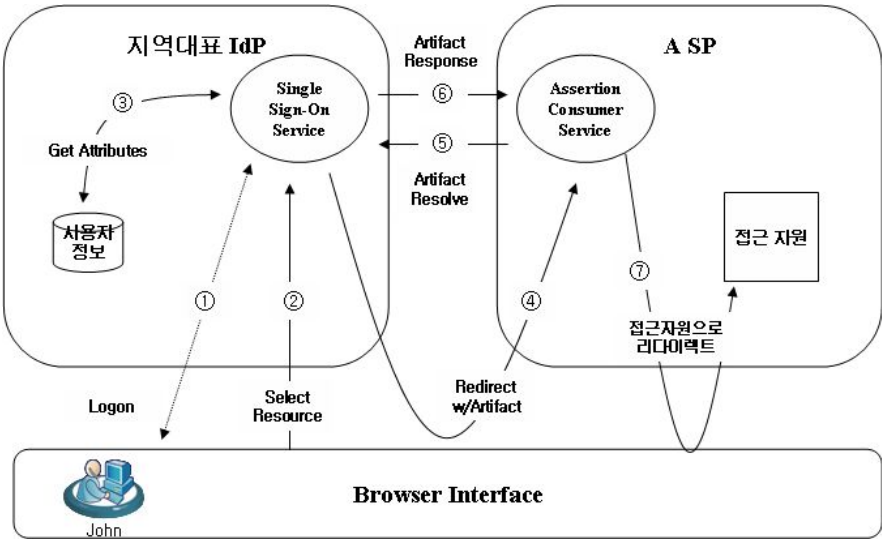
ⓐ, ⓑ 경우는 이미 앞에서 설명한 것처럼 SP-Initiated SSO: Artifact/POST 경우로 처리할 때 시나리오는 <그림 8>과 같다.

사용자 Lee는 보호된 A SP의 자원에 접근하기 위해 인증을 요청한다. 이때, 사용자는 해당 사이트에 로그온 되어 있지 않으므로, A SP는 자체 인증을 처리한다. Lee는 자관 사용자이므로 인증에 성공하고, 통합 인증 요구 시 인증을 다루기 위한 Assertion Consumer Service로 이동한다.

A SP는 인증요청을 생성하고 artifact를 만든다. A SP는 지역대표 IdP의 SSO 서비스에 사용자의 브라우저를 통해 artifact를 포함한 HTTP redirect를 보낸다.

SSO 서비스는 SAML artifact로부터 로컬인증 ID를 추출하고 SP's Artifact Resolution Service에 artifact를 포함한 SOAP으로 SAML artifact-resolve message를 보낸다.

SP의 ARS는 이전에 생성한 인증요청을 포함한 SAML메시지를 보낸다. 이때, SP에서 전달한 개별ID와 사이트정보를 가지고 IdP_SubscribeId 테이블에서 Key_ID 값을 구한다. 이 값을 가지고 IdP_sessionInfo 테이블에 이미 생성된 값이 있는지 확인하고, 일치되는 값이 없으면 Session Key값을 생성하고, 새로운 레코드를 생성한다. 만약 사용자가 SP에서 로그온 되어 있지 않거나, 또는 IdP사이트에 아직 로그온 되어 있지 않은 경우, 개별ID값이 없으므로, IdP에서 재 인증을 요구하는 화면을 요청하고, IdP는 자격(ID와 비밀번호)을 요구하고 사용자가 입력된 값을 IdP_IdInfo 에서 사용자ID와 비밀번호를 확인하고, 이에 따른 Key_ID 값을 가지고 이전 경우와 같이 처리하여 로그온 한다.



<그림 9> IdP 로그인 시나리오

사용자의 추가적인 정보는 SAML 응답에 포함시키기 위해 사용자정보를 검색한다.(이 속성들은 IdP와 SP사이에 사전에 정의된 부분이다)

IdP의 SSO 서비스는 인증 assertion과 IdP에서 정의한 개별ID, 대출등록번호 등의 속성을 포함한 SAML응답을 가진 브라우저에게 HTML form을 돌려준다. 브라우저는 자동적으로 SP에게 HTML form을 돌려준다. 그리고 서명과 assertion이 타당하면, SP는 사용자의 통합인증세션이 성립되며, A SP 화면으로 이동한다. 만약, A SP에서 개별로그아웃을 하여도, IdP로 재 로그인 할 때 세션정보가 남아 있으면, ⑤과정인 IdP의 Logon 을 하지 않고, 바로 A SP의 화면으로 돌아온다.

ⓒ 경우는 이미 앞에서 설명한 것처럼 IdP-Initiated SSO : Artifact 로 시나리오는 <그림 9>와 같다.

사용자 John은 IdP로 로그온 해야 하며, 보호된 SP의 자원에 접근하기 위해 먼저 IdP에 로그인을 한다. 로그인이 성공된 후에 IdP_sessionInfo 에 정보를 추가하고, SSO를 요청한다. 이 때 John은 그 사이트에 로그온 되어 있지 않아야 한다. 선택적으로, IdP는 사용자정보로부터 개별ID, 대출등록번호 등의 속성을 검색한다.

지역대표 IdP의 SSO 서비스는 assertion을 생성하고, artifact를 만들고, SP's ACS에게 브라우저를 통해 artifact를 포함한 HTTP redirect를 보낸다.

ACS는 SAML artifact로부터 SourceID를 추출하고, 지역대표 IdP의 ARS에 artifact-resolve message를 보내며, ARS는 이전에 생산된 assertion을 포함한 SAML artifact 응답메시지를 보낸다. 만약 서명과 assertion이 타당하면, A SP는 사용자의 세션이 성립된다. 그리고 접근자원화면으로 이동한다.

<그림 9>의 시나리오에서는 타 도서관 서비스를 이용하기 위해, 통합인증과 자기 소속도서관의 대출정보공유를 보여준 예이다. 도서관의 경우, 각 사용자 마다 개인의 서비스를 위해 대출/반납정보, 개인부가서비스를 위한 MyMenu 등을 관리하고 있다. 따라서 IdP 소속도서관 정보ID 테이블(IdP_SubscribeId)을 확장한다면 다른 서비스에 이용할 수 있다.

Ⅳ. 결론

도서관에서 제공하는 서비스는 주로 도서대출 및 자관도서관에 소장하고 있는 콘텐츠서비스에 국한되어 있다. 만약 도서관 간의 연계만 이루어진다면, 차원 높은 서비스를 제공할 수 있다. 특히, 도서관 간에 시도하려고 하는 상호대차나 타관자료반납서비스 같은 것은 시·공간적인 제약을 벗어나 사용자를 편리하게 할 뿐 아니라, 신규 서비스이용자를 확대할 수 있는 계기가 될 것이다.

본 논문에서 본 바와 같이 지역대표도서관을 중심으로 그 산하 공공도서관 및 작은 도서관등이 사용자 통합인증이 되고, 이에 따른 유관서비스를 위한 정보를 공유한다면, 공공도서관의 입장에서는 사용자 관리에 따른 비용 절감과 콘텐츠 공유를 통해 소량의 구입비용으로 활용성을 극대화할 수 있으며, 지역도서관을 분야별로 발전시켜 다양한 분야의 서비스를 제공할 수 있다. 또한 빠른 도서 반납을 통해 도서회전율 극대화하고 효율적인 예산수립과 활용이 가능하게 된다. 그리고 사용자 입장에서도 이 같은 서비스를 활용가능하다면 개별 도서관에 대한 개별 회원가입 및 관리가 필요 없고, 인근 지역도서관의 모든 서비스를 공간적 제약 없이 활용할 수 있으며, 여러 도서관의 콘텐츠를 하나의 서비스로 이용 할 수 있다.

참고문헌

[1] 김철, "LDAP를 이용한 SSO 인증 시스템의 설계에 관한 연구", 자연과학연구소논문지, 제10권 제1호, 2005, pp.141-146.

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

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

[4] 정보시스템의 효율적 도입 및 운영 등에 관한 법률 제 7조에 의거 "정보시스템의 구축·운영기술지침", 정보통신부고시, 제37호, 2006.

[5] Shibboleth, http://shibboleth.intenet2.edu

[6] http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf, 2005, pp.15-16.

[7] SAML Tokens and Claims, http://msdn2.microsoft.com/en-us/library/ms733083.aspx.

[8] V. Semar, "Single Sing-O Using Cookies for Web Applications", Proceedings, IEEE 8th International Workshops on Enabling Technologies, Infrastructure for Collaborative Enterprises (WET ICE '99), 1999, pp.158-163.

[9] 정종일, 유석환, 신동규, 신동일, 차무홍, "SAML을 이용한 그리드와 웹 서비스 보안을 위한 자바 기반 Single Sign-On 라이브러리의 설계 및 구현", 정보처리학회논문지C, 제12-C권 제3호, 2005, pp.341.

[10] Ping Identity, PingFederate 5 Getting Started Manual, 2008, pp.36~47.

[11] 조영섭, 진승헌, 문필주, 정교일, "ID 연계 기반의 인터넷 ID Management System", 전자공학회논문지, 2004, pp.6-10.

[12] 대전 공공기관 통합ID 관리의 소개, http://www.idsp.go.kr/idp_service/guide/idsp-01-01.jsp.

[13] 문홍서, "웹 서비스 환경에서의 SAML 기반 단일 인증 시스템의 설계 및 구현", 2005, pp.16-17.

[14] 의안정보시스템, 도서관및독서진흥법 전부개정법률안, http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=036702.

[15] 도서관 및 독서진흥법, 전부개정 2006.10.4 법률 제8029호.

■ 저자소개 ■

변 회 균
Byeon, Hoi Kyun

2008년 6월~현재
오롬윈 솔루션사업부 본부장
2008년 8월 숭실대학교 정보과학대학원
디지털컨텐츠학과(공학석사)
1993년 2월 인하대학교 전산계산학과(이학사)

관심분야 : Library Contents, Semantic Web
E-mail : hkbyeon@korea.com

고 일 주
Ko, Il Ju

2003년 3월~현재
숭실대학교 미디어학과 조교수
1997년 숭실대학교 대학원
전산학과(공학박사)
1994년 숭실대학교 대학원
전산학과(공학석사)
1992년 숭실대학교 전산학과(학사)

관심분야 : 감성인식, 콘텐츠공학, 멀티미디어
정보검색 등
E-mail : andy@ssu.ac.kr

논문접수일 : 2008년 7월 11일
수 정 일 : 2008년 8월 10일
게재확정일 : 2008년 8월 20일