Deliverable Number:	D 5.2.1
Deliverable Title:	Survey on existing comparable systems and report on requirements and framework for single sign-on solution for common access to individual facility digital user office systems – Software package to handle integrated user registration

Delivery date:	30. 11. 2014 [month 33]
Leading beneficiary:	HZB
Dissemination level:	Report
Status:	done
Authors:	N. Leidel, HZB

Project number:	283883
Project acronym:	NMI3-II
Project title:	Integrated Infrastructure Initiative for Neutron Scattering and Muon Spectroscopy
Starting date:	1st of February 2012
Duration:	48 months
Call identifier:	FP7-Infrastructures-2010
Funding scheme:	Combination of CP & CSA – Integrating Activities

WP5 Integrated User Access

Report on single sign-on solution for common access to individual facility digital user office systems – Software packages to handle integrated user registration

N. Leidel, Helmholtz-Zentrum Berlin, Germany

Single sign-on (SSO) is a method that uses a single user action of authentication to allow an authorized user to access all related, but independent software systems or applications without being requested to log in again at each of them during a particular session.
It reduces the risk for the administrators to manage users centrally, increases user productivity by allowing mobility and allows users to access multiple services or applications after being authenticated just once. This doesn’t mean that the SSO system unifies account information for all services, applications and systems, rather it hides such a multiplicity of account information into a single account that the user needs to login. Once the user login, the SSO system generates authentication information accepted by the various applications and systems. The concept of SSO can be used within an Intranet, Extranet or Internet.

Pros

- Authenticate only once and access multiple resources
- Improved user productivity
- Ease of administration

Cons

- Potentially creates a single point of attack
- Can be very difficult to retrofit existing applications and infrastructures with an SSO solution

The core of a web browser-based SSO solution builds on a browser based authentication protocol. In principal three roles take part in the protocol: a client (C), an identity provider (IdP) and a service provider (SP). The objective of C, typically a web browser guided by a user, is to get access to a service or a resource provided by the service provider. The identity provider authenticates C and issues corresponding authentication assertions. Finally, SP uses the assertions generated by IdP to decide on C’s entitlement to the requested resource.

A large number of solutions for browser-based SSO are available: the OASIS Security Assertion Markup Language (SAML), Microsoft Passport, the Liberty Alliance project, the Shibboleth Initiative and OpenID are the most popular. The Web Browser SSO Profile of SAML 2.0 is the de facto standard in the business domain: SAML is a XML-based framework that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content. The definition of the XML-based language format determine the requirements for encoding security assertions as well as a number of protocols and bindings that prescribe how assertions must be exchanged in a variety of applications and/or deployment scenarios. Prominent software companies, including IBM, Novell, Oracle, and SAP, base their SSO implementations on SAML SSO. Google has developed an SAML-based SSO service for its popular web applications (namely Gmail, Google Calendar, Docs and Sites), called the SAML-based SSO for Google Apps. OpenID (OpenID Foundation) is a decentralized authentication protocol SSO solution more suited to Web 2.0 applications (*e.g.* blogs, wikis). It allows users to be authenticated by certain co-operating sites using a third party service. That means the user can log into multiple unrelated websites without having to register with their information over and over again. OpenID provides a framework for the communication that must take place between the identity provider and the client.

The OAuth protocol is an additional open standard for authorization. OAuth specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. For this reason important technical requirements for the standardized exchange of access permissions are given with numerous applications.
A fundamental criterion for SSO solutions is the integrability into an existing software and server environment. The main task is to find a solution with adaptable interfaces, which connects the individual digital user office applications. Attention should be paid in particular the supported standards by each SSO solution, identity services and applications on the network and in the cloud. Also privacy and confidentiality play an important role in evaluation a single sign-on system. The data integrity of browser-based SSO protocols critically relies on a number of assumptions on the trustworthiness of the principals involved and on the security of the transport protocol used to exchange data. In a single sign-on method requirements for complex passwords and encrypted registration procedures should be standard. If it were possible for an unauthorized person, to crack the central access, he would have access to all connected applications generally.

Social networks such as Facebook, Twitter and Google+ offer in the meantime also SSO solutions. The company NetIQ Social Access allows companies to offer their customers or partners to sign with any of the social log-ins. So the customers can use their credentials of a particular social network for the application.

There are a lot of different commercial and free solutions on the market. All these frameworks allow single sign-on to third-party websites and applications. Most of the programs support the established standard protocols for communication between the different sites. Some of the free, open source or academic SSO solutions are listed below.

1. Free SSO

Accounts & SSO framework - code.google.com/p/accounts-sso
It is a free software licensed under LGPL 2.1. This framework is made for Linux and POSIX platforms. It consists of a set of components and libraries which implement an account manager for a user's online accounts and a single sign-on daemon which handles the authentication to the remote services on behalf of the client applications.

Facebook Connect – facebook.com
In the year 2008 Facebook launched the SSO system Facebook Connect. User can use their facebook account for authentication on other partner websites. Applications which are connected with FC can use user data outside of Facebook itself. Log in with Facebook cannot be used by users in locations that cannot access Facebook (*e.g.* China).

IBM Enterprise Identity Mapping
This framework from IBM is available free of charge on all IBM server platforms. It allows the mapping of different user IDs on various applications to a single identity.

Microsoft account – account.live.com
It is a SSO web service developed and provided by Microsoft that allows users to log into many websites using a single set of credentials.

Mozilla Persona - developer.mozilla.org/en-US/Persona
The Mozilla Foundations developed a open decentralized cross-browser login system for the web. The system works on all major browsers. The functionality is based on the BrowserID protocol.

OpenID Connect

OpenID Connect enables clients to verify the identity of the end-user based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner. Protocol based on OAuth 2.0.

2. Open source SSO

Central Authentication Service (CAS) - www.jasig.org/cas
It is an open source single sign-on protocol and server/client implementation. CAS validates the user's authenticity by checking username and password against a database. If the authentication succeeds, CAS returns the client to the application, passing along a security ticket. The application then validates the ticket by contacting CAS over a secure connection and providing its own service identifier and the ticket. CAS then gives the application trusted information about whether a particular user has successfully authenticated.

CoSign single sign on - weblogin.org
This open source project was made to provide the University of Michigan with a SSO system. It can operate on multiple computer platforms.

Distributed Access Control System (DACS) - dacs.dss.ca
DACS provides a modular authentication framework under an open source license that supports an array of common authentication methods and a rule-based authorization engine that can grant or deny access to resources.

Enterprise Sign On Engine - esoeproject.qut.edu.au
ESOE is standards based and open source SSO cross-platform system. The core server system is developed in Java while connectivity to services is achieved through provided SAML service provider software.

FreeIPA - freeipa.org
FreeIPA is an open source identity management project with the company Red Hat as developer.

JOSSO – josso.org
Java Open Single Sign On (JOSSO) is an open source Java and SAML based software for user authentication and authorization and can be used as a SSO solution for web applications.

OpenAM - openam.forgerock.org

An open source access management is provided by OpenAM formerly known as OpenSSO. It contains multiple options and methods for SSO.

WSO2 Identity Server - wso2.com/products/identity-server
With the implementation of the open source software package WSO2 Identity Server a SSO solution via several standardized protocols can be used.

3. Academic SSO

eduGAIN - edugain.org
eduGAIN is a service that interconnects the participating identity federations. They agree on a set of common standards and policies which ensure interoperability. eduGAIN is therefore also called an interfederations service. Its goal is to enable Pan-European Web Single Sign On (Web SSO) for members of the research and education community. It uses the SAML 2.0 technology.

Umbrella - umbrellaid.org
A specialized solution in the photon community already exists with the Umbrella project. It is commonly developed within several EU projects such as EuroFEL, PaNData project and the CRISP. The work is supported by the European Commission under the 7th Framework programme.
Umbrella based on the Shibboleth architecture. Shibboleth is an open source software package for web single sign-on across or within organizational boundaries. Shibboleth finds application especially in the area of science and teaching. Many major content providers support Shibboleth-based access. The software implements widely used identity standards, like the OASIS Security Assertion Markup Language (SAML), to provide a federated single sign-on and attribute exchange framework. Umbrella provides an EU-wide and persistent user ID. A user authenticates with his or her organizational credentials, and the organization (or identity provider) passes the minimal identity information necessary to the service provider to enable an authorization decision. Umbrella is already successfully established at several European synchrotron facilities. It is based upon the local user office structure.

Conclusion

There are multiple factors to consider when deciding on the SSO solution you need. Open source or free solutions are preferred, because licensing issues are removed. The vast number of possible identity management provider makes a detailed individual evaluation essential. Any institution will need to consider what aspects are important to them and pick their solution accordingly.

Of particular interest to the neutron community is whether the solution picked will work together with the different individual user offices. For this purpose the Shibboleth architecture of the Umbrella initiative seems to be the best candidate to fit these needs. They already demonstrated the successful implementation of the system at several digital user offices of European synchrotron facilities. Hence an integration of the Umbrella project in the NMI3 community seems to be the most appropriate SSO solution. By this conclusion to develop a software prototype to demonstrate an integrated user registration within this activity seems not appropriate.