# Federated Access Management for Electronic Resourcesy the Taiwan Experience

**Naicheng Chang**

**Abstract**

*Currently, in Taiwan there is no demonstrable solution for access management to the many heterogeneous electronic resources that academic and university libraries provide for users, such as the full texts of electronic journals and books, electronic databases, among many others. Shibboleth has been developed in U.S.A. and the United Kingdom and has become an emerging solution to the access management of electronic resources in a growing number of developed countries. Our experience in starting a virtual federation by setting up an Identity Provider (IdP) at Academia Sinica and a Service Provider (SP) at the Chinese Geoscience Union (CGU), Taipei, a society which publishes a SCI journal entitled "Terrestrial, Atmospheric and Oceanic Sciences", as well as request Shibboleth-based service from some participating Shibboleth publishers like Elsevier, Springer and Thomson ISI, can provide valuable experiences to any library or organization wanting to start a Shibboleth federated access management for reference.*

***Keywords:*** Access Management, Authentication, Authorization

## 1. Introduction

Academia Sinica is Taiwan's preeminent research institution with a world-wide reputation. There are 18 libraries supporting research for twenty-four research institutes and seven research centers devoted mainly to three research disciplines: mathematics and physical sciences, life sciences, and the humanities and social sciences. Currently, the libraries provide approximately 25,000 electronic journal titles, 20,000 e-books for full-text access and 200 online databases. At present, there are four methods to access electronic resources in Academia Sinica. The first uses an IP address restriction, this method has its advantages; however, the restriction cannot meet the increasing need for off-campus access by users. Second, an IP address restriction using proxy-servers is available whereby with the help of an intermediate server, proxy-servers offer a virtual connection between the user and an IP-restricted resource and is unfortunately technically challenging for users. Third, a Virtual Private Network (VPN) method which has yet to be fully evaluated is now gradually replacing proxy-servers. Finally, there is individual registration of individual users to take advantage of individual resources. In addition, some otherwise unnoted privacy concerns arise as some users may not be willing to reveal their identities to a resource provider if the use of the material is commercially or politically sensitive. More typically, exchanges of personal data between the identity provider and a resource provider open opportunities for identity deception or theft [Garibyan, 2007].

In order to resolve the problems mentioned above, we initiated a Shibboleth implementation pilot project funded by the National Science Council, Taiwan.

7th International CALIBER-2009,
Pondicherry University, Puducherry, February 25-27, 2009

The reason we adopted Shibboleth is because the U.S.A. and the U.K. have been actively developing Shibboleth as a solution for access management to electronic resources since 2000 [Internet2][JISC: Shibboleth]. Shibboleth, an open source software under the development of Internet2/MACE (Middleware Architecture Committee for Education), has become an emerging global standard for access management to restricted electronic resources [Garibyan, 2007].

The aims of Shibboleth are to improve the way in which users access resources throughout the educational and research sectors. Specifically, the goal is to allow users to access internal and external resources seamlessly using a single, institutionally controlled identity. This will substantially reduce current problems in which users are restricted in some IP ranges or are required to maintain multiple passwords for multiple resources in multiple domains. Major benefits of Shibboleth include: (1) reducing the time needed to manage and access to protected resources such as sharing resources among several institutions and managing a large number of accounts; (2) increased security (Single SignOn - SSO – do not need to remember multiple passwords, acquire information about the users from reliable providers, etc.); and (3) interoperability with similar standard-based solutions. Shibboleth is based on SAML and is thus compatible with other SAML-based software[Internet2] [JISC: UK].

## 2. The first experience of implementing Shibboleth in Taiwan

As there is very limited knowledge about Shibboleth in Taiwan, for the first phase we joined the Meta Access Management System Tested Federation, MAMS), an Australian government backed initiative at Macquaire University, Sydney, as a federation member [Macquarie University] to gain more knowledge regarding Shibboleth' operation. We set up an IdP at the Library of the Institute of Earth Sciences, Academia Sinica (ASIES) to provide user information and authenticate our users as well as requesting Shibboleth-based access services from some participating Shibboleth publishers like Elsevier, Springer and Thomson ISI as we are their customers. The Chinese Geoscience Union, Taipei, a society with about 250 members and subscribers publishes a SCI journal entitled "Terrestrial, Atmospheric and Oceanic Sciences (TAO)" is also interested in how to go through Shibboleth operation to enforce access control to their resource and users and set up an SP at their site as well. In the second phase of our study, the Computing Center of Academia Sinica (ASCC) will play the role of issuing and managing certificates for our users. Our Shibboleth virtual federation will then be formed by implementing the IdP, SP and the 'Where Are You From (WAYF)"(ASCC).

The Shibboleth architecture diagram we use to delineate our Shibboleth virtual federation is a modification of the original schematic provided by the Swiss Education and Research Network (SWITCH)[SWITCH] and Klingenstein [Klingenstein]. In the diagram, there are four components: (1) the user is a research fellow from Academia Sinica, who tries to gain online access to an article available at Science Direct, Elsevier; (2) the libraries of Academia Sinica as IdP with which the user is registered; (3) The SP as Elsevier, Springer, Thomson ISI, CGU which provides restricted resources and has an access control system to decide whether the user should be allowed to access the resources, and if, yes, at what level; (4) The "Where Are You From" (WAYF)

service, a centralized service operated on behalf of a Shibboleth Federation. Here the "WAYF" is MAMS at the first phase of our study and will be replaced by Academia Sinica Grid Computing Certification Authority [Macquarie University].

There are also four stages for the user to complete for his or her access as indicated in the diagram. In stage 1, the user connects to the resource and is redirected to the appropriate organization; second, the user makes a selection for his/her home organization; third, the user authentication at his/her home organization ascertained; and finally, access to resource is approved [SWITCH].

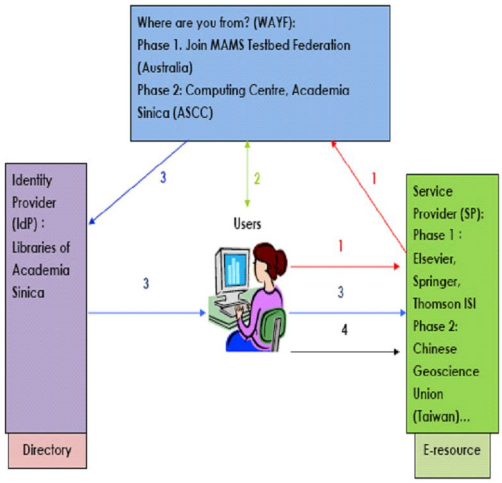


Diagram-1. Shibboleth architecture diagram used in this pilot project (modified from the diagrams provided by SWITCH and Klingenstein).

Concerning the technology for software installation, as a library representing the IdP, we here will just mention the IdP environment that we set up. We adopted SuSe Linux 10.0 version for the operating system and installed Shibboleth version 1.3c at our IP domain name: idprovider.earth.sinica.edu.tw. We also set up our user database using Lightweight Directory Access Protocol (LDAP).

Can the Shibboleth method of access management resolve the current problems mentioned earlier? Using Shibboleth, the benefits for the users include: (1) needing to sign on only once to various protected resources; (2) no IP restriction for access; (3) no need to remember different usernames and passwords; (4) privacy protection because only the users' attributes are released from the IdP to the SPs, who roughly know where the user is from; and (5) the same methodology of access to resources from inside or outside the subscribing institution's network, particularly useful for multi-site institutions without a homogenous network. The advantages for the library are: (1) a cost reduction in password support; (2) the scale of the users is under control; and (3) different categories of users are able to access different levels of resources.

Who can authenticate users? A federation must be established within the trust of IdPs, SPs and the entity who issues users' certificates. As a library intending to initiate a federation or join a federation, it is important to know the entity which authenticates users and deploys signed site metadata, which must be in a federation and recognized by the publishers. Taking Elsevier as an example, they prefer a trusted commercial Certificate Authorities (CAs), with whom Elsevier coordinates the use of certificates and agrees on attributes to be used. For Elsevier, in effect, the entity should (1) host and manage federation metadata in Shibboleth 1.3 format on http://, and compile and sign correctly and appropriately; (2) define what entitlements attribute is released by the IdP's attribute authority; and (3) validate which commercial CA that Elsevier can be used for secure back-channel communication or supply them with the appropriate certificate if it should be of a proprietary nature [De Vries, 2008].

How many components can make an access management federation? An access management federation could be as small as what we now have and can be as large as a national or international federation. It should at least have an IdP with users and SP which provide resource(s) as well as an Authentication system.

## 3. Discussion

Taking into account the experience of the SWITCHaai federation which spent 4 years from pilot to a production federation and the UK federation which used 2 years to the stage of a working federation, we would like to propose a national and international liaison plan which covers three phases. We suggest to start with a common federation in Academia Sinica for testing purposes to look the same way as we would want a production federation to look. And then we suggest moving to phase two which could be set up as a national federation in Taiwan through the leadership of the government. The third phase is to initiate a confederation to connect countries in the Asia Pacific area. We give it a name: Asia Pacific Shibboleth COlaboration (APSCO). What benefits does a confederation have? Certainly, resources and services sharing is one more benefit in that international take-up secures the future of development and support, and also saves money through work in partnership.

Given the differences in national law and licensing preferences, we expect there would be harsh challenges and potential risks. Davies and Shreeve [2007] pointed out that possible challenges of a common global infrastructure could be in two aspects: technical and policy. In order to build up a common global infrastructure, technically, a common language is required to communicate among federations. Security Assertion Markup Language (SAML) is the one currently that has been globally accepted. There are more challenges such as the management of metadata. If one looks at the policy issues of inter-federation interoperability, the challenges are much more difficult than the technical aspects. Taking the example of the preparation of agreements between federations for the establishment of confederations, this involves setting up of rules about joining for IdPs and SPs; the obligations of the federation operator; the mechanisms and practices for data protection and so on. And to achieve the level of successful interoperability, very possibly it has to cross numerous legislative barriers from different nations. In short, this involves issues of whether federation members from the confederation are willing to adhere to rules to establish a trust relationship.

## 4. Conclusion

At present, Academia Sinica has tens of self-established and valuable databases, yet these databases are distributed among different research institutes and centers and do not have a proper access management protocol. Based on our prototype used at the libraries of Academia Sinica, we will recommend the Shibboleth access management system to the Academia Sinica authorities to create our own inter-organizational federation to first integrate our self-established and subscribed databases and e-resources and provide a single sign-on ability for users. Hopefully we can extend our federation over time to other Taiwanese institutions. Although there would be long-term challenges ahead, yet we do believe that a geographic international federation like APSCO should be the future trend of Shibboleth development for institutions in the Asia Pacific area.

## References


1. **Davies, Claire and Shreeve, Matt.** Federated access management: international aspects. Surrey: Curtis+Cartwright, 2007.
2. **E-mail communication with Ale DE VRIES,** Elsevier's Senior Product Manager, Platform & content. 27 June 2008.
3. **Garibyan, M.**: Building a national federated access management infrastructure (the U.K. experience), the ITE 2007 Conference in Yerevan, 21-23 May 2007.
4. **Internet2:** Shibboleth: a project of the Internet2 middleware initiative. Internet2. Available at http://shibboleth.internet2.edu (Accessed on 22/121/2008).
5. **JISC:** Shibboleth: connecting people & resources briefing (version 2), Joint Information Systems Committee. Available at http://www.jisc.ac.uk/publications/publications/pub_shibboleth.aspx (Accessed on 02/11/2008).
6. **JISC:** U.K. federated access management, Joint Information Systems Committee. Available at http://www.jisc.ac.uk/federation (Accessed on 02/11/2008).
7. **Klingenstein, N.:** Shibboleth 2.0: finally. Trans-European Research and Education Networking Association. Available at http://tnc2008.terena.org/core/getfile.php?file_id=401 (Accessed on 09/12/2008).
8. **Macquarie University** – Sydney: MAMS: Meta Access Management System :Tested Federation. Available at http://www.federation.org.au/FedManager/jsp/index.jsp(Accessed on 02/11/2008).
9. **Switch**: Serving Swiss Universities. Available at http://www.switch.ch (Accessed on 05/12/2008).


## Acknowledgement

Financial support for this research from the National Science Council, Taiwan, under the grant NSC 96-2413-H-036-001 is gratefully acknowledged.

## About Author

**Mr. Naicheng Chang,**
General Education Center, Tatung University,
No.40, Sec. 3, Jhongshan N. Rd. Taipei, Taiwan 104