Shibboleth

“Shibboleth is the standard federated authentication and attribute query service protocol in the higher education. It was designed from the ground up to support the pseudo-anonymous login scenarios required by the libraries.

Shibboleth has strong support from the Internet2. It is also on a converging path with similar commercial efforts (Liberty Alliance)."

— Taken from EDIMIassumptions.doc found on AIS website

Shibboleth Resource

- Shibboleth Set Up Guide on the UCLA IAMUCLA site
- ISIS to Shibboleth Migration Help Center
- The Official Internet2 Shibboleth Site
- Internet2 Shibboleth Support

Deprecated Pages

- Shibboleth Target Deployment Guide for v1.2.1

Presentations Related to Shibboleth

- Slides from the January 30, 2007 ISIS/Shibboleth Technical Information Session
- Slides from the September 18, 2007 Campus Web Publishers presentation
- A very cool series of demos of how Shibboleth works
  Produced by SWITCH, this is probably the best set of online demonstration/explanation of how Shibboleth works

---

More information about Shibboleth and ISIS, taken from a post by Albert Wu to the ISISdev mailing list:

1. What is Shibboleth?
2. Why haven’t you rolled out Shibboleth to a broader group?
3. Which is better for me, ISIS or Shibboleth?
4. What about authorization? How will that be handled?
5. How might I use data returned from Shibboleth to perform authorization?
6. What does a user see when he/she logs into a Shibboleth enabled application?
What will my Shibboleth-enabled application be able to see about that user?

1. What is Shibboleth?
-————————————-

Shibboleth (http://shibboleth.internet2.edu/) is standards-based, open source middleware software which provides Web Single SignOn (SSO) across or within organizational boundaries. It is open source and is developed and support by the Internet2 Middleware Group.

Shibboleht IS the next version of ISIS.

We have in the past two years, been preparing to evolve ISIS to a standards-based protocol. Shibboleth is the right fit. Shibboleth has been adopted by many institutions throughout the world as their web single sign-on service of choice. It has been adopted by UC as its federated Single Sign-on solution.

We are in fact operating a fully functioning Shibboleth Identity Provider (that would be the “server” side of the service) parallel to the curent ISIS 5 interface. The two are integrated. Applications can choose to use either API and get single sign-on across applications using either.

At this time, we are working with several early adopters on deploying Shibboleth. They include CCLE, Paul’s Plone site, MyEvents.ucla.edu, UCLA GRID, and our own sites.

2. Why haven’t you rolled out Shibboleth to a broader group?
-————————————————————————————

There are several considerations.

First, we are ourselves learning how to deploy a Shibboleth-enabled application. Since we didn’t write the sofware, there is a fair amount of learning to do.

Second, Shibboleth does not offer the exact same set of features ISIS does. In particular, it has a different concept of session management. We need to better understand how that impacts the applicaitons.

Third, transitioning from the current ISIS API to Shibboleth will require a fair amount of work. We want to minimize that work as much as possible for you all. To do that, we are using the pilot program to develop a series of support materials and to try streamline the set up process as much as possible before we make everyone jump through unnecessary hoops.

The good news is that we are just about there. Stay tuned. :-)

3. What are the differences between ISIS and Shibboleth, and Which is better for me?
-——

These are the key differences between ISIS and Shibboleth:

- ISIS is a home grown system with a proprietary API. Shibboleth is developed based on SAML (http://en.wikipedia.org/wiki/SAML)

- ISIS is only used within UCLA. Shibboleth is used at a significant number of institutions. More significantly, Shibboleth enables member of one instution to use his/her credential to log in to services at another institution. Imagine using your UCLA Logon ID to log into a UCOP, or UC Berkeley application. It's happening. :-)

- To use ISIS, you need to write code to call the ISIS Web Serivce. Internet2 provides standard "client" (called Service Provider) modules for Apache and IIS. These SP modules handle all communications between your server and the Shibboleth Identity Provider. Any information returned is presented to your application in the HTTP headers. So all your application needs to be able to do is to read HTTP headers. On top of that, if you only have static pages, the Shibboleth SP modules have enough logic built-in that it can controll access to static documents by simply editing configuration files.

- ISIS can only provide a fixed set of user attributes. Shibboleth is designed to be able to flexible return any arbitrary number of attributes, AND be able to control the release of those attributes in a very granular fashion.

Which one is better? Generally speaking, if you are launching a new application, I'd seriously consider using Shibboleth. After all, eventually, we will phase the current ISIS API out in favor of Shibboleth. That won't happen for a couple of years, but if your new application will be around for at least 2 years, now may be the time to move onto Shibboleth. We are still a couple of months away from fully ramped up to support a large number of adopters, but if you are interested and have an active project, we want to work with you.

Besides, while there is significant set up (at least for the first time), there is far less coding involved on your part. It may just shorten your deployment window.

Reason for not going to Shibboleth now:

a. You already have a set of working ISIS applications, and you have no immediate plans to launch new projects/rewrite your applications.

You have very specific session management requirements, and you can't change those requirements in the short term. Shibboleth works differently. It may require some rethinking how session management is done

c. You want to wait till the full set of support material is available. :-)

4. What about authorization? How will that be handled?
-————————————————————————————

At least for web applications, we expect authorization data will come through the Shibboleth attribute response packets. As a user logs into your application and runs through the shibboleth authentication sequence, the shibboleth SP module eventually fires attribute requests against the IdP. The IdP in turn returns any attribute the SP requests AND has the authorization to see.

The technical framework for this service is available now. Our main problem is the availability of data, and lining up proper support for managing the release of attributes. Keep in mind that AIS does not have the authority to arbitrarily release data. The business offices (e.g., Registrar's Office for student data, CHR/Payroll for employee data) need to be involved in the process.

Our main challenge now is to come up with a scalable mechanism for the offices to efficiently manage the release of sensitive data. That process is ongoing. We have a significant permission management system proposed in the UTIPP2 funding cycle. Whether we get the funding to proceed there will significantly determine the types of services we can offer moving forward.

5. How might I use data returned from Shibboleth to perform authorization?
-————————————————————————————————————-

Shibboelth attributes returned to your application are presented as name/value pairs in the HTTP header. You simply read the headers and parse out the data you are looking for. Specifically for authorization data, they are returned in the form or affiliation values or entitlement values.

For example, if we had the proper data, we may assert me as:

eduPersonScopedAffiliation = affiliate@ucla.edu,employee@ucla.edu, staff@ucla.edu,alum@ucla.edu

Note that attributes can contain multiple values. Also note that the "@ucla.edu" part is the scope of the value. so "employee@ucla.edu" means "employee of UCLA".

As I mentioned in 4., whether we receive funding significantly impacts how much we expand this moving forward. In theory, we can assert any amount of details about a person that we have data for. In fact, paired with a permission management tool for the security administrators, we can assert any custom authorization attributes the administrators might set…

6. What does a user see when he/she logs into a Shibboleth enabled application?
What will my Shibboleth-enabled application be able to see about that user?
-——-

The best way to explain this is for you to log in to a live Shibboleth-enabled application.

If you want to see what the application sees in the header, try this little diagnostic application:

https://whoa.mi.ais.ucla.edu

7. How can I contact AIS if Shibboleth appears to be problematic?
-——-

“AIS help desk does not check emails over the weekend. A different group answers the help desk phone during evenings and on weekends. They route calls to the appropriate party for production outage issues. The AIS help desk extension is x66951.” (Albert Wu 09/30/2007)

Revision #20
Created 2006-05-13 17:39:44 UTC by Kellar, Paul
Updated 2010-08-27 20:35:16 UTC by Lu, John