Shibboleth and Federated Identity Management

Mark Scheible
Manager, Identity and Access Management
OIT – Security & Compliance

Introduction

Shibboleth is a system designed to exchange **attributes** across realms for the primary purpose of **authorization**. It provides a secure framework for one organization to transmit attributes about a ***web-browsing individual*** across security domains to another institution.

In the primary usage case, when a user attempts to access a resource (Service Provider - SP) at a remote domain, the user's own home security domain can send certain information about that user to the SP site in a trusted exchange. These attributes can then be used by the resource to help determine whether to grant the user access to the resource. The user may have the ability to decide whether to release specific attributes to certain sites by specifying personal Attribute Release Policies (ARP's), effectively preserving privacy while still granting access based on trusted information.

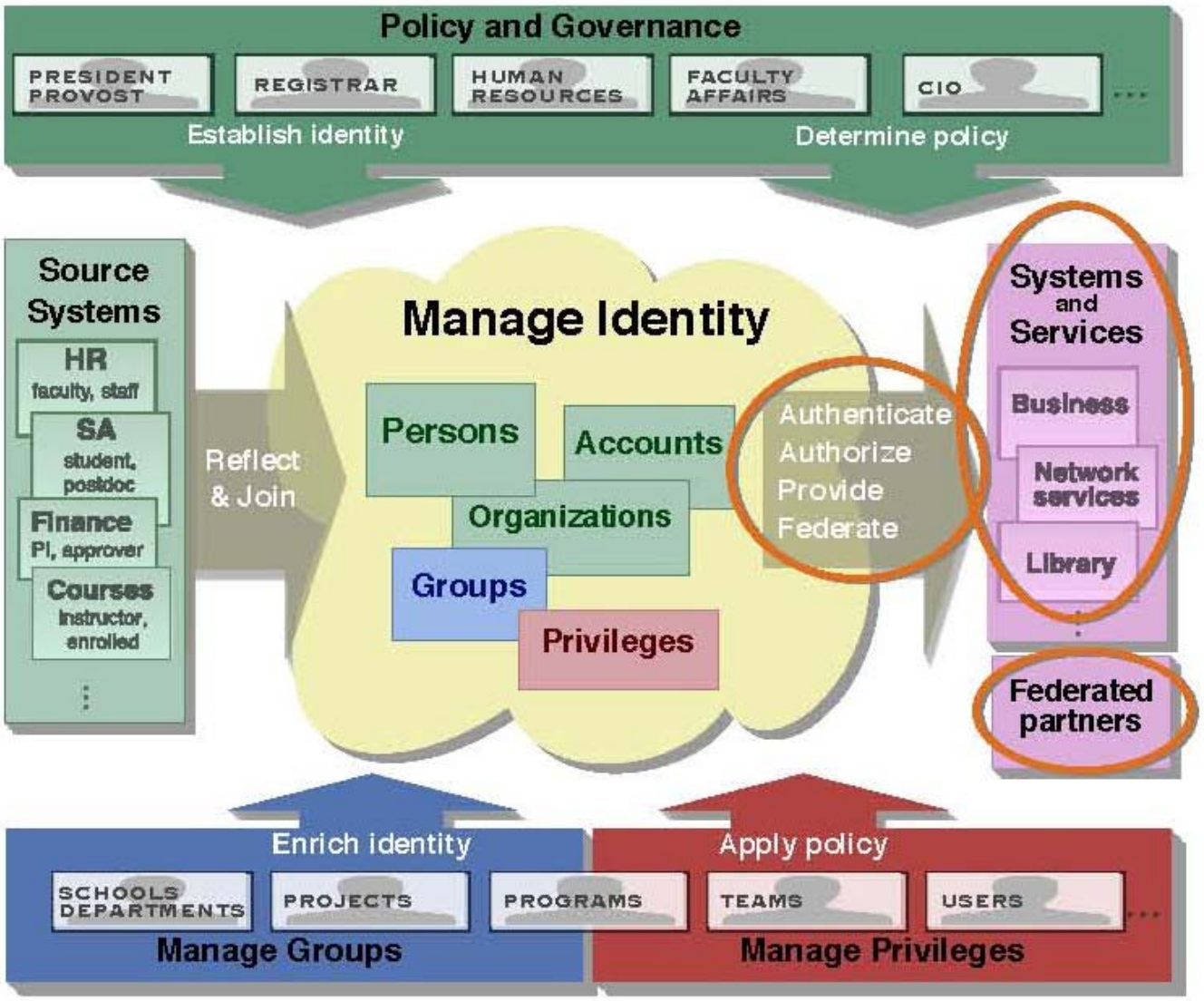
Introduction, continued

Shibboleth has two major halves:

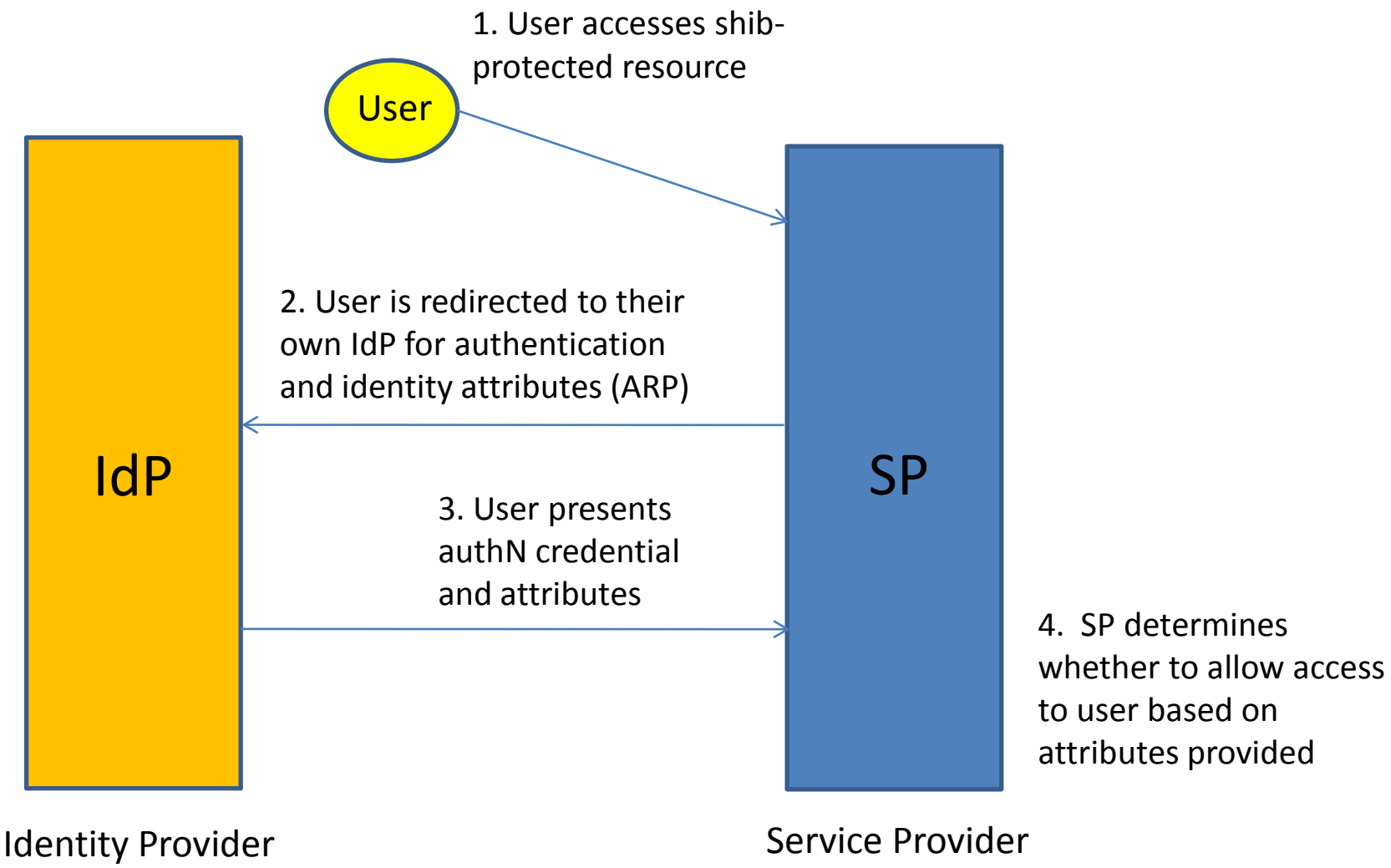
- an *identity provider* (IdP) and
- a *service provider* (SP)

The identity provider supplies information about users to services and the service provider consumes information about users to make authorization decisions whether to allow access to its resource.

Identity Management



How's it Work? (simplified)



Benefits

•Enable Single Sign-on to On- and Off-site Managed Services
One organizational ID and password to access all on- and off-campus resources

Shibboleth was developed specifically to address the challenges of controlling access to multiple resources offered by an institution, third-party providers, or both. In the past, each resource required a separate ID and password. This makes life complicated for the user and opens security and workload concerns for the institution.

•Build and Manage Locally, Access Globally
Use your existing identity management system for access to all resources

Account management is provided by your existing campus Identity Management infrastructure; Shibboleth leverages that system. You define a user's relationship with your institution. Shibboleth delivers this information so that a web-based service – hosted on- or off-campus – can make an access control decision

•Protect Your Data and Users' Privacy
Release only the essential information about your users

Shibboleth is the only SAML-based federating software that does not require the release of user identities. Your campus sends only the data needed for authorization. If the criterion for access is current enrollment in a particular biology course, that is the only information sent. The data is delivered just-in-time and governed by your institution's privacy policy. However, if the service provider needs personal information or an identity, and this is acceptable with the organizational policy, Shibboleth can be configured to send that, too.

Benefits, continued

•Partner with your Service Providers
Time-saving features for you and your resource provider

Shibboleth can substantially reduce the risk and time involved in offering services. In the past, IT departments sent large files of identity data to a service provider to create and update separate accounts. Using Shibboleth, the service provider

- o **receives fresh, accurate account information** each time the user accesses the resource
- o **saves time and reduces risk** by not having to maintain campus identity and account stores that age and must be updated
- o **controls access** to its protected services without the concerns of potential identity data spills or misconfigured IP-based access methods
- o **saves money** by reducing the integration work when adding new customers and troubleshooting multiple account IDs and passwords
- o **enables personalization** by providing a persistent but anonymous identifier so the browser experience can be customized based on the individual's history with your service while maintaining his or her privacy

•Ease Your Federation Participation
Adding new partners is a breeze

Shibboleth was developed with federations and their operational requirements in mind. Information associated with federation membership and trust can be updated automatically, as often as you'd like. And once you implement Shibboleth, adding a new partner can take just minutes.

Benefits, continued

•Provide Access to the Federal Government Applications
E-Authentication is coming and Shibboleth will lead the way

The Federal E-Authentication Initiative has approved a Shibboleth plug-in to work with their federation. The software is currently supported by the National Institutes of Health which is a member of the U.S. InCommon Federation.

•Play Well with Others
Shibboleth is standards based – it gets along with everyone

Interoperability is extremely important in a federated world, where commercial sites and U.S. government agencies might use different federating software. Shibboleth offers multi-protocol support that ensures it will interoperate with other commercial implementations. These protocols include OASIS SAML (versions 1.0, 1.1, and 2.0), protocols and extensions for Microsoft's Active Directory Federation Services and, in the future, CardSpace.™

•Create Opportunities
Resource providers will appreciate the fine-tuned access control.

Shibboleth's attribute-based approach provides the ability to implement fine-grained access control and allows more licensing options. You and your service provider can control access by department, major or by any other criteria. Using a similar technique, the software also enables personalization of services without releasing identity or sacrificing privacy.

Use Cases (Examples)

- iTunes U content creation and use (instructor / student)
- Library Services
- Moodle (Learning Management System)
- NSC (National Student Clearinghouse)
- Google Apps for Education
- National Institutes for Health (NIH)
- National Science Foundation (NSF)

Federations

"The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly, and without the need for completely redundant user [account] *administration" - Wikipedia*

Current Federations:

- UNC Identity Federation (UNC-GA)
- InCommon Federation
- NCTrust Federation
- "NC State Federation"

A *More Technical* Workflow between IdP and SP

FlowsAndConfig

Added by Nate Klingenstein, last edited by Scott Cantor on Sep 21, 2009 (view change)

How it All Fits Together

Shibboleth has two major halves: an identity provider (IdP), and a service provider (SP). The identity provider supplies information about users to services, and the service provider gathers information about users to protect resources. In the typical use case, a web browser accesses a protected resource, authenticates at their identity provider, and ends up back at the resource logged in. How does this actually happen, and how does it fit with IdP and SP configuration? What other pieces are involved?

Technical Workflow, Continued

Step 1: User Accesses Protected Resource

A user tries to access a protected resource, causing Shibboleth to intercept the request. The resource locations to protect can be defined in the web server configuration itself, such as httpd.conf, or in shibboleth2.xml in the <RequestMap>.

The SP will select a session initiator to use based on this protection configuration, which in turn figures out which IdP the user will authenticate with and what protocols to use. The providers signal their profile preferences to one another through metadata. It might supply a text entry box, send the user to a discovery service (DS), or redirect the user to a common IdP. That depends on where the users accessing the application will come from, and what is the most appealing interface choice.

Step 2: User Authenticates to the IdP

An authentication request is issued by the SP to the IdP with the format based on the profile they choose to speak. The authentication request is placed in the browser, and the user is redirected back to the right endpoint at the IdP. The IdP examines the request and decides how it would like to authenticate the user based on configuration for this SP in relying-party.xml and authentication in general in <LoginHandler> and login.config. The user is redirected off to the right login handler, authenticates through the method selected, and comes back to the profile handler with their username set.

Technical Workflow, Continued

Step 3: IdP issues Response to SP

The IdP now uses the principal's name, the SP, and the profile spoken to decide what information to send the SP and how to wrap it.

First, the IdP gathers a set of attributes for the user through the attribute resolver. It collects user data from all the backend sources, transforms it if necessary, and attaches encoders to each attribute.

These attributes are shuffled along to the attribute filter, which constrains the set of information sent in the response. The set of attributes released most often depends on the SP and the principal. This protects the user's privacy. The resulting information could be as little as "someone authenticated successfully", or reveal any attribute you can imagine.

The user's information is all wrapped up into a message with the encoders attached earlier, typically in a SAML 2.0 assertion. This assertion is signed with the IdP's key and encrypted with the SP's key for security and privacy. The assertion is placed into a message and the user is redirected to the SP carrying it along.

Step 4: Back to the SP

The user ends up at an assertion consumer service at the SP. It unpacks the message, decrypts the assertion, and performs several security checks. If everything's in order, then it will extract attributes and other information from the message. Attributes are translated into local environment or header variables using the SP's attribute extractor.

The SP can then enforce rules itself or just pass along the attributes to the application to use however it requires.

Questions ?

References

OIT IAM Shibboleth Home Page:
http://oit.ncsu.edu/iam/shibboleth-and-federated-identities

Shibboleth Home Page:
http://shibboleth.internet2.edu/

InCommon Federation Home Page:
http://www.incommonfederation.org/index.cfm