Shibboleth Authentication
For every question an answer:

• Why should I care about SAML?
• What is a Shibboleth?
• What is a Federation? Are we in one?
• How does it (Shibboleth) work?
• How do I get one of those?
• PennGroups!
SAML – Security Assertion Markup Language

A data format for exchanging authentication and authorization information.

There are many “flavors” of SAML. Shibboleth is one of those flavors.

Why is SAML important?

- It provides web application single sign-on (SSO).
- It allows an organization to exchange identity information with a trusted 3rd party.

You are already using Shibboleth
Shib·bo·leth  noun  \'shi-bə-ləθ

A word or way of speaking or behaving which shows that a person belongs to a particular group.

After speaking to multiple support technicians that can not help you...

[1] https://xkcd.com/806/
Federations

A federation is a group of providers that agree upon a standard (of operations, interactions, frameworks, goals etc...).
The InCommon Federation is the U.S. education and research identity federation, providing a common framework for trusted shared management of access to online resources. Through InCommon, Identity Providers can give their users single sign-on convenience and privacy protection, while online Service Providers control access to their protected resources.

There are 432 higher education participants.

There are > 2,000 services currently offered through InCommon.

We like InCommon members. We will find out why soon!

We have discussed ...

- SAML is a way to exchange identity information.

- Shibboleth is an implementation of SAML. Penn uses Shibboleth.

- InCommon is an Internet2 federation. Penn is a member of InCommon.
Shibboleth – How does it work?

IdP – Identity Provider
SP – Service Provider

1. An unauthenticated user attempts to access restricted content on the SP.
2. The SP generates an authentication request, and sends the request and the user to the IdP.
3. The IdP authenticates the user, and sends the authentication response, and the user back to the SP.
4. The SP verifies the IdP’s response. Checks the provided attributes, makes an authorization decision, and provides content as needed.
# Shibboleth - User Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Suppressible</th>
<th>Source</th>
<th>Definition</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Attributes that are available to all Service Providers</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eduPersonPrincipalName</td>
<td>No</td>
<td>PennCommunity</td>
<td>PennKey/PennName</td>
<td><a href="mailto:jbreen@upenn.edu">jbreen@upenn.edu</a></td>
</tr>
<tr>
<td>surname (sn)¹²³</td>
<td>Yes</td>
<td>Penn Directory</td>
<td>Surname</td>
<td>Breen</td>
</tr>
<tr>
<td>givenName¹²³</td>
<td>Yes</td>
<td>Penn Directory</td>
<td>Given Name</td>
<td>John</td>
</tr>
<tr>
<td>displayName²³</td>
<td>Yes</td>
<td>Penn Directory</td>
<td>Display Name</td>
<td>John Breen</td>
</tr>
<tr>
<td>Mail³</td>
<td>Yes</td>
<td>Penn Directory</td>
<td>E-mail Address</td>
<td><a href="mailto:jbreen@isc.upenn.edu">jbreen@isc.upenn.edu</a></td>
</tr>
<tr>
<td>eduPersonAffiliation</td>
<td>No</td>
<td>PennGroups</td>
<td>Affiliation</td>
<td>staff</td>
</tr>
<tr>
<td>eduPersonScopedAffiliation</td>
<td>No</td>
<td>PennGroups</td>
<td>Affiliation (scoped)</td>
<td>alumni</td>
</tr>
<tr>
<td><strong>Attributes that are available only by request</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employeeNumber</td>
<td>No</td>
<td>PennCommunity</td>
<td>PennID</td>
<td>10123072</td>
</tr>
<tr>
<td>eduPersonEntitlement</td>
<td>No</td>
<td>PennGroups</td>
<td></td>
<td>... Wait for it...</td>
</tr>
</tbody>
</table>

1. This information is pulled from Penn Directory. Users should update Penn Directory if they wish to correct the presentation of their name.
2. Other institutions may send more than 1 value for these attributes. We send only 1 value for each as provided by the user in Penn Directory.
3. Service providers should be aware this is user provided data and is not verified.

Shibboleth – Metadata

Metadata is configuration information for Identity Providers and Service Providers. It is required so Identity Providers and Service Providers know how to talk to each other.

```xml
<EntityDescriptor entityID="https://idp.pennkey.upenn.edu/idp/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <ds:X509Certificate>
      MIIDQDCCAiigAwIBAgIVAIW7U17BF4Oluf7KKej2n7iZo4sLMA0GCSqGSIb3DQEBCY
      VREplQZ1ZwSoTpxPhDq+6mzWGdyCyDdq2Nn4Qk0bMnsNvZj3svVJeBfiGiWe0xy1RO5prB/x5xli9fGaUdwE=
    </ds:X509Certificate>
  </IDPSSODescriptor>


</EntityDescriptor>
```
Shibboleth – SAMLRequest

```xml
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

    AssertionConsumerServiceURL="https://service.upenn.edu/Shibboleth.sso/SAML2/POST"

    Destination="https://idp.pennkey.upenn.edu/idp/profile/SAML2/Redirect/SSO"

    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">

    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

    https://service.upenn.edu/shibboleth

    </saml:Issuer>

</samlp:AuthnRequest>
```

The requesting service provider must identity itself, and let the identity provider know where to send the response to.

The issuer must be a unique name to identify the service provider, it is the entityID that defines the requesting service. An entityID must be a URI, it is strongly recommended that it is a URL.

[1] https://spaces.internet2.edu/display/InCFederation/Entity+IDs
Shibboleth – SAMLResponse

<
sam1:Attribute
    FriendlyName="eduPersonPrincipalName"
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6">
    <sam1:AttributeValue xsi:type="xs:string">jbreen@upenn.edu</sam1:AttributeValue>
</sam1:Attribute>

<
sam1:Attribute
    FriendlyName="eduPersonAffiliation"
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1">
    <sam1:AttributeValue xsi:type="xs:string">staff</sam1:AttributeValue>
    <sam1:AttributeValue xsi:type="xs:string">employee</sam1:AttributeValue>
</sam1:Attribute>

<
sam1:Attribute
    FriendlyName="eduPersonEntitlement"
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7">
    <sam1:AttributeValue xsi:type="xs:string">businessServices:apps:qualtrics:qualtricsIsc</sam1:AttributeValue>
</sam1:Attribute>

eduPersonPrincipalName (EPPN) - EPPN is the eduPerson equivalent of a username. It is not an e-mail address.

eduPersonAffiliation - high-level expression of the relationship of the user to the university.

eduPersonEntitlement - Entitlements represent an assertion of authorization to something. Generally, they should be simply compared as strings to access-control expressions in the application.

The integration is usually easier!

We most likely already have your metadata, or will shortly after it is published.

InCommon Members have a common understanding of affiliation data.

We can get metadata in an automated way including updates (metadata refresh). This makes maintenance and key rollover easier.

“Respect for Privacy of Identity Information”
Members must adhere to the participation agreement.
E-Mail us.
weblogin-help@isc.upenn.edu

We will point you towards our online documentation:
http://www.upenn.edu/computing/weblogin/shibboleth/attribute.html

We will usually setup a phone call to discuss (~30 minutes).

We want your metadata, and you will need ours!

We will set things up in our staging environment and test. We want the stakeholders to test as well.

We will push things to production.... And test again! +24 - 48 hours after we receive confirmation that things are well in staging.
Shibboleth – Things to think about

When will users lose access to the service?
This is dependent on affiliation changes in Penn Community.
Make sure your choices are informed by “long-term” use of the resource.

Be careful which data you are using for authorization.
Some data is: suppressible, and/or user controllable.

Keep your vendor honest.
Make sure your vendor does not allow hijacking of accounts on the basis of user controlled attributes.

No matter how you integrate you must consider privacy.
Authorizations Choices

- Use affiliation Data. Affiliation data changes quickly/automatically.

- Use PennGroups (eduPersonEntitlement).
  Consider the coarseness of your entitlement group in regards to privacy.

- Use a Vendor supplied interface to load user data (side load).
Shibboleth - User Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Suppressible</th>
<th>Source</th>
<th>Definition</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Attributes that are available to all Service Providers</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eduPersonPrincipalName</td>
<td>No</td>
<td>PennCommunity</td>
<td>PennKey/PennName</td>
<td><a href="mailto:jbreen@upenn.edu">jbreen@upenn.edu</a></td>
</tr>
<tr>
<td>surname (sn) ¹ ² ³</td>
<td>Yes</td>
<td>Penn Directory</td>
<td>Surname</td>
<td>Breen</td>
</tr>
<tr>
<td>givenName ¹ ² ³</td>
<td>Yes</td>
<td>Penn Directory</td>
<td>Given Name</td>
<td>John</td>
</tr>
<tr>
<td>displayName ² ³</td>
<td>Yes</td>
<td>Penn Directory</td>
<td>Display Name</td>
<td>John Breen</td>
</tr>
<tr>
<td>Mail ³</td>
<td>Yes</td>
<td>Penn Directory</td>
<td>E-mail Address</td>
<td><a href="mailto:jbreen@isc.upenn.edu">jbreen@isc.upenn.edu</a></td>
</tr>
<tr>
<td>eduPersonAffiliation</td>
<td>No</td>
<td>PennGroups</td>
<td>Affiliation</td>
<td>staff alumni</td>
</tr>
<tr>
<td>eduPersonScopedAffiliation</td>
<td>No</td>
<td>PennGroups</td>
<td>Affiliation (scoped)</td>
<td><a href="mailto:staff@upenn.edu">staff@upenn.edu</a> alumni @upenn.edu</td>
</tr>
<tr>
<td><strong>Attributes that are available only by request</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>employeeNumber</td>
<td>No</td>
<td>PennCommunity</td>
<td>PennID</td>
<td>10123072</td>
</tr>
<tr>
<td>eduPersonEntitlement</td>
<td>No</td>
<td>PennGroups</td>
<td></td>
<td>... Wait for it... ...</td>
</tr>
</tbody>
</table>

(1) This information is pulled from Penn Directory. Users should update Penn Directory if they wish to correct the presentation of their name.

(2) Other institutions may send more than 1 value for these attributes. We send only 1 value for each as provided by the user in Penn Directory.

(3) Service providers should be aware this is user provided data and is not verified.

Next Up: PennGroups