Federated Identity and Access Management for Research Collaborations
Outline

- Research Collaboration IAM Needs
- Federated Identity for Authentication
- SAML Federations
- Hands-on with SAML
- Hands-on with OpenID Connect (OIDC)
Research Collaboration IAM Needs
What Is A Collaboration?

- A cross-organizational collection of people who come together for a particular interest
- Virtual Organizations (VOs) are one type of Collaboration
  - Here the terms can be used interchangeably
Characteristics of a Collaboration

- Participants from many institutions
  - Some with federated identities
  - Some with social identities (Google, etc)
  - Some with no identities
- One institution often hosts collaboration infrastructure
What A Collaboration Needs

- **Common Tools**
  - Wikis / Document Repositories
  - Mailing Lists
  - Calendaring / Scheduling

- **Domain Specific Tools**
  - Application portals
  - Analysis workflow tools
  - Data viewers
Types of Collaborations

- Large pseudo-enterprises (e.g., big science) with a long time frame
- Researchers from a dozen schools working together on a fixed-duration project
- Members of the community partnering with a University to provide a service
- A handful of people from different departments within the same institution
Collaboration Identity Management Processes

- **Identity Infrastructure**
  - Onboarding / Offboarding / Lifecycle Management
    - Transfers and Account Linking
  - Group Management

- **Attributes to drive authorizations**
  - Managed by academic institutions / cloud ID providers
  - Managed by the collaboration
Regardless of size, the basic IdM need remains the same:

1. Grant access to services when needed
2. Remove access when done
Identity Management Infrastructure

● Authentication / Credentialing Services
  ○ External: Federated, Social
    ■ Proxies, Gateways, Direct Integration
    ■ Discovery Services
  ○ Internal: Kerberos, LDAP
  ○ User-Centric: SSH Keys, Certificates
  ○ Multi-factor: RSA, Google Auth, Duo, U2F
Identity Management Infrastructure

● Lifecycle/Access Management and Authorization
  ○ Person Registry
    ■ Identity Matching / Linking
  ○ Group Registry

● Provisioning and Application Integration
  ○ Directory Services
  ○ Messaging Services
Federated Identity for Authentication
Federated Identity Definition

"...the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems."

"...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 administration."

Use Your Federated Identity

- Browse to https://wiki.refeds.org/
- Click "Log in"
- Search for your home organization name
- Click on your home organization name
- Authenticate to your home organization identity provider
- Verify you are "logged in" to the REFEDs wiki
No Federated Identity?

Cannot find your home organization?

- Use a social identity (Google, Facebook, Twitter...)
- Or sign up for a (free) federated identity
- Try NCSA: https://go.ncsa.illinois.edu/idp-guest
- Or try United ID: https://unitedid.org/
  - Requires a second factor like Google Authenticator on your phone
What just happened?

- Used identity from one security domain (home organization) to access resources from another security domain (REFEDs)
- Pre-established trust between the identity provider (home organization) and the service provider (REFEDs wiki)
- Leveraged SAML protocol
  - Security Assertion Markup Language
  - Facilitates federated web browser single sign-on (SSO)
  - Most common (today) protocol in higher ed and research
SAML Federation
The Role of Federations

- Enable us to scale up to 1000s of IdPs and SPs
- Publish digitally signed SAML metadata containing public keys, endpoint URLs, and other info about IdPs and SPs
- Set standards for SAML attributes, levels of assurance, etc.
- Provide support and training
InCommon: The US R&E Federation

- [https://www.incommon.org/](https://www.incommon.org/)
- Over 800 participants and growing: [https://www.incommon.org/participants](https://www.incommon.org/participants)
- 400+ IdPs / 3000+ SPs: [https://incommon.org/federation/info/all-entities](https://incommon.org/federation/info/all-entities)
- Becoming an InCommon Member: [https://www.incommon.org/join](https://www.incommon.org/join)
eduGAIN: Global InterFederation

- InCommon joined eduGAIN in 2016
  https://www.incommon.org/edugain/
- Enables SAML metadata exchange across federations, with per-entity opt-in/opt-out
eduGAIN: Global InterFederation

eduGAIN Policy Framework requires:

- Primarily serve the interests of the R&E sector
- Provide a point of contact for technical issues
- Provide processes for handling complaints and incidents
- Have a published Metadata registration practice statement
- http://www.edugain.org
- https://technical.edugain.org/
SAML Metadata

- InCommon metadata includes US IdPs/SPs plus international IdPs/SPs from eduGAIN:
  https://incommon.org/federation/metadata.html
- SAML metadata interoperability enables secure, scalable federation between IdPs and SPs
SAML Metadata

- SAML metadata is a digitally signed XML document that establishes trust in the federation:
  
  http://md.incommon.org/InCommon/InCommon-metadata.xml
  
  https://spaces.internet2.edu/display/InCFederation/Metadata+Signing+Certificate
<EntityDescriptor entityID="https://idp.ncsa.illinois.edu/idp/shibboleth">
  <IDPSSODescriptor errorURL="https://idp.ncsa.illinois.edu/error" protocolSupportEnumeration="...">
    <Extensions>
      <shibmd:Scope regexp="false">ncsa.illinois.edu</shibmd:Scope>
      <mdui:UIInfo>
        <mdui:Display Name xml:lang="en">National Center for Supercomputing Applications</mdui:Display Name>
        <mdui:Description xml:lang="en">National Center for Supercomputing Applications</mdui:Description>
        <mdui:PrivacyStatementURL xml:lang="en"></mdui:PrivacyStatementURL>
        <mdui:Logo height="100" width="148" xml:lang="en">
          ...</mdui:Logo>
      </mdui:UIInfo>
      <KeyDescriptor use="signing">
      </KeyDescriptor>
    </Extensions>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://idp.ncsa.illinois.edu/idp/profile/SAML2/Redirect/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://idp.ncsa.illinois.edu/idp/profile/SAML2/POST/SSO"/>
  </IDPSSODescriptor>
  <Organization>...</Organization>
  <ContactPerson>...</ContactPerson>
</EntityDescriptor>
<EntityDescriptor entityID="https://cilogon.org/shibboleth">

<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <Extensions>...</Extensions>
  <KeyDescriptor>...</KeyDescriptor>
  <AssertionConsumerService Binding="..." Location="https://cilogon.org/Shibboleth.sso/SAML2/POST"/>
  <AttributeConsumingService index="1">
    <ServiceName xml:lang="en">CILogon</ServiceName>
    <ServiceDescription xml:lang="en">...</ServiceDescription>
    <RequestedAttribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
    <RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
    <RequestedAttribute FriendlyName="eduPersonTargetedID" Name="urn:oid:1.3.6.1.4.1.5923.1.1.10" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
    <RequestedAttribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
  </AttributeConsumingService>
</SPSSODescriptor>

<Organization>...</Organization>
<ContactPerson>...</ContactPerson>
</EntityDescriptor>
Hands-on with SAML
SAML Web Browser SSO: Protocol Overview

1. Request target resource
2. Redirect to SSO Service
3. Request SSO Service
4. (Discover the IdP)
5. Redirect to SSO Service
6. Request Assertion Consumer Service
7. Request target resource
8. Respond with requested resource

Trace Your SAML SSO Flow

- Install SAML tracer Add-on for FireFox
  - SAML DevTools extension for Chrome is also available
  - Other tools useable but involve more work
    - LiveHTTPHeaders
    - Safari Web Inspector
    - Fiddler
    - Often combined with https://www.samltool.com/
Trace Your SAML SSO Flow

- Open SAML tracer
- Browse to https://wiki.refeds.org
- Click "Log in" to kickoff SAML SSO flow
- Authenticate and complete SAML SSO flow
- Examine SAML exchanges using SAML tracer
SAML SP Authentication Request

```xml
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
ID="_3c59c65a242980ba8200dd31d48b2b9a"
IssueInstant="2016-08-12T16:27:34Z"
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://spaces.internet2.edu/shibboleth</saml:Issuer>
  <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- SAML entityID
- Every SP and IdP has unique entityID
- Best practice is URL syntax
- Older practice is URN
SAML SP Authentication Request

```xml
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
    Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
    ID="_3c59c65a242980ba8200dd31d48b2b9a"
    IssueInstant="2016-08-12T16:27:34Z"
    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://spaces.internet2.edu/shibboleth
    </saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- Timestamp
- Prevent replay attacks
- Most systems tolerate some clock skew
SAML IdP Response

```xml
<saml2p:Response
  Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
  ID="_a7a2a544baf52cc9bf3e58e485249fde"
  InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
  IssueInstant="2016-08-12T16:27:36.448Z"
  Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml2:Issuer
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    https://idp.uwm.edu/idp/shibboleth
  </saml2:Issuer>
  <ds:Signature
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    SNIP
  </ds:Signature>
  <saml2p:Status>
  </saml2p:Status>
  <saml2:EncryptedAssertion
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    SNIP
  </saml2:EncryptedAssertion>
</saml2p:Response>
```

- entityID of the IdP
SAML IdP Response

<
saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
ID="_a7a2a544baf52cc9bf3e58e485249fde"
InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
IssueInstant="2016-08-12T16:27:36.448Z"
Version="2.0"
 xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
<saml2p:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
 https://idp.uwm.edu/idp/shibboleth
</saml2p:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
 SNIP
</ds:Signature>
<saml2p:Status>
</saml2p:Status>
<saml2p:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
 SNIP
</saml2p:EncryptedAssertion>
</saml2p:Response>

● Status is Success
● Could have been Failure
SAML IdP Response

```xml
<saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
ID="_a7a2a544baf52cc9bf3e58e485249fde"
InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
IssueInstant="2016-08-12T16:27:36.448Z" Version="2.0"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        https://idp.uwm.edu/idp/shibboleth
    </saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        SNIP
    </ds:Signature>
    <saml2p:Status>
    </saml2p:Status>
    <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        SNIP
    </saml2:EncryptedAssertion>
</saml2p:Response>
```

- Timestamp
- Prevent replay attacks
- Most systems tolerate some clock skew
SAML AuthnStatement

```
<saml2:AuthnStatement AuthnInstant="2016-08-13T18:42:47.925Z"
SessionIndex="_6e20e8085b98cab86ef99af6b9489b9" >
<saml2:SubjectLocality Address="75.86.142.120" />
<saml2:AuthnContext>
  <saml2:AuthnContextClassRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
  </saml2:AuthnContextClassRef>
</saml2:AuthnContext>
</saml2:AuthnStatement>
```

- "How" the subject authenticated
- SAML2 defines a few standards
- Almost always see "PasswordProtectedTransport" in higher ed and research
  - Effectively "login and password over TLS"
- Higher ed and research community working on new international standards
  - e.g., https://refeds.org/profile/mfa
SAML AttributeStatement

```xml
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="sn" Name="urn:oid:2.5.4.4" NameFormat=SNIP>
    <saml2:AttributeValue>Basney</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" NameFormat=SNIP>
    <saml2:AttributeValue>James Basney</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="givenName" Name="urn:oid:2.5.4.42" NameFormat=SNIP>
    <saml2:AttributeValue>James</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat=SNIP>
    <saml2:AttributeValue>jbasney@illinois.edu</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```
Hands-on with OpenID Connect (OIDC)
OpenID Connect: Introduction

- Third gen OpenID (after OpenID 1.0 and OpenID 2.0)
- Adopted by Amazon, Google, Microsoft, and many others
- Auth layer on top of OAuth 2.0 authz framework (RFC 6749)
- Adds new token type: ID Token
- Adds new OAuth resource: UserInfo
- Standard claims in ID Token and UserInfo response
- Defines scope values for requesting claims
- Specifications: https://openid.net/connect/
# SAML and OIDC: Terminology

<table>
<thead>
<tr>
<th>SAML</th>
<th>OIDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider (IdP)</td>
<td>OpenID Provider (OP)</td>
</tr>
<tr>
<td>Service Provider (SP)</td>
<td>Relying Party (RP)</td>
</tr>
<tr>
<td>Attributes</td>
<td>Claims</td>
</tr>
<tr>
<td>Attribute Bundle</td>
<td>Scope</td>
</tr>
<tr>
<td>Authentication Assertion</td>
<td>ID Token</td>
</tr>
</tbody>
</table>
OpenID Connect: Standard Claims

- `sub`
- `email`
- `email_verified`
- `phone_number`
- `phone_number_verified`
- `address`

- `scope: openid`
- `scope: email`
- `scope: phone`
- `scope: address`
- `scope: profile`

- `name`
- `given_name`
- `family_name`
- `middle_name`
- `nickname`
- `preferred_username`
- `profile / picture`
- `website`
- `gender / birthdate`
- `zoneinfo / locale`
- `updated_at`
OpenID Connect: Protocol Overview

1. The RP (Client) sends a request to the OpenID Provider (OP).
2. The OP authenticates the End-User and obtains authorization.
3. The OP responds with an ID Token and usually an Access Token.
4. The RP can send a request with the Access Token to the UserInfo Endpoint.
5. The UserInfo Endpoint returns Claims about the End-User.

Source: https://openid.net/specs/openid-connect-core-1_0.html
Use Google OIDC

- Google OIDC documentation is at
  https://developers.google.com/identity/protocols/OpenIDConnect
- We'll use the Google OAuth playground at
  https://developers.google.com/oauthplayground/
We request 3 standard scopes.
Next we get the tokens.
We'll use the tokens from the response.
eyJhbGciOjJSUzI1NiIsImtpZCI6IjVkYmE5NDFiODMOMWNjMWM5NTk2NmI3MDgyMDk2YWVIY2Odc3NDc3OTgi
fQ.eyJpC3MiOiJoHRwczovL2FjY291bnRzLmRvb2d
sZS5jb20iLCJhdF9oYXNoIjoidnoxeUI4NHzCRmyS
FQweHN0azJNdyyIsImF1ZCI6IjEzNzgwMDY1MzYxNS1
wZnI0bm9ocm9wcWVIz0cDdqNzFbnRhWxrcXJ1M
y5hcHBlmdvb2dsZXVzZXJjbj25QZ050LmNvbSi3InN
1YiI6IkEpMjIwODQxMTI0TA1NjUyMzczMIIsImVtY
WlsX3ZlcmlmaWkVjip0cnVLCLJhenAoiIiXz4cMDA
2NTM2MTUtcGZyN5vaHJvCHF1YmZwdHA3ajcxaw5GZ
Gisa3FyDFmuYXbc5nyb29nbGV1c2VvY29udGVudC5
jb20iLCJoZCI6InNwaGVyaWNhbG9yd2dyb3VwLmNvb
Si3ImVtYWlsIjoic2tvcmFuZGFAC3BoZXJpY2FsY29
3Z3JvdxAnYzI2tiwiaWF0IjoNDc0NjUzNzIwLCJle
HAiOjE0NzQ2NTUzNTJ9.IyYX-
Pgr9HYeAQwLnCcOn8f_dhHXftPWSvT85Yf5pBoK_e
_KUf1W-uVkc28XquHsdjseyz8j7_WFYfNv5Qx3Q8h-
xylygDO3pTHrrQmtDas_Hk2UjD5MkP7SahIzs9cHQ
HoUsPkd2JaC1StNo6o2WJuddZKDZ_nxAJZtu2_YP3QP
nNHMz80xBuwVjOlgO9Pl28YxvPBcCRup5wjBGj5r
p9gy65oITim5i5rnZKdh4wYX2ErznUNKc19eb1yREW1

Use the access token to query Google for user info

```
export ACCESS_TOKEN=ya29.CjNnA0sBU6up4orY7ZrKGdvbdKYuePnAa7p

curl -H "Authorization: Bearer $ACCESS_TOKEN"
    https://www.googleapis.com/oauth2/v3/userinfo
```
Result will look similar to this:

```json
{
    "sub": "102208411259056523752",
    "name": "",
    "given_name": "",
    "family_name": "",
    "picture": "https://lh3.googleusercontent.com/-XdUIqdMkCWA/AAAAAAAAAAI/AAAAAAAAC/tYsrscbv5M/photo.jpg",
    "email": "skoranda@sphericalcowgroup.com",
    "email_verified": true,
    "hd": "sphericalcowgroup.com"
}
```
SAML and OIDC Hands-On Exercises (Handout)
Wrap Up

● Hands on with SAML and OIDC
● CI projects use federated identity and access management to support distributed collaborations
● R&E institutions operate SAML IdPs in large federations
● More info: https://trustedci.org/iam

This material is based upon work supported by the National Science Foundation under grant number 1547272. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.