

Federated Identity at BNL: Enabling global collaboration

John Hover <jhover@bnl.gov>

Scientific Data and Computing Center

BROOKHAVEN
NATIONAL LABORATORY

 U.S. DEPARTMENT OF
ENERGY

Overview

- Orientation/Context
- Components/Terminology
- The InCommon federation
- CILogon
 - Relationship to InCommon, other federations
- COManage:
 - What it does
 - Genesis, other use cases
- Authorization
- Federating services:
 - Plugins, OIDC, SAML
- KeyCloak
- Challenges
- Issues for Admins

Orientation

Federation: *Trusting* other organization(s) to verify username+password

- E.g. Travelocity allowing Google ID login.
- In this case, Google is a federation of 1.
- **Service provider** trusts that the next time the ID is used, it is the same person.
- **User** trusts Google not to divulge unneeded info.

Value for Users:

- Avoids the need to get separate computing accounts at different institutions.
- One login and password for all.

Value for Service providers:

- Delegates hassle of vetting accounts, automatically suspends departed users.

Orientation (2)

Federation vs. Single-Sign-On (SSO)

- SSO means you type password once--other apps notice that you're already logged in (via browser cookies).
- SSO happens naturally with federations, but not vice-versa

Authentication (AuthN) vs. Authorization (AuthZ)

- Who you are vs. what you're allowed to do.
- A driver's license doesn't make you a member at the country club.

Components/Terminology

Identity provider:

- The organization where the user has an account.
- Runs an IdP (ID Provider endpoint)

Service provider:

- The organization where a web-based application is run.

Directory:

- Lookup service to find endpoints.
- Where Are You From (WAYF)

InCommon

The US Research & Scholarship (R&S) identity federation.

- ~900 universities, companies, laboratories, institutes, museums, etc.
- Establishes standards for participation, technical interoperability.
- Issues cryptographic tokens for mutual validation.
- Distributes metadata about all endpoints.
- Transparent community-based governance.

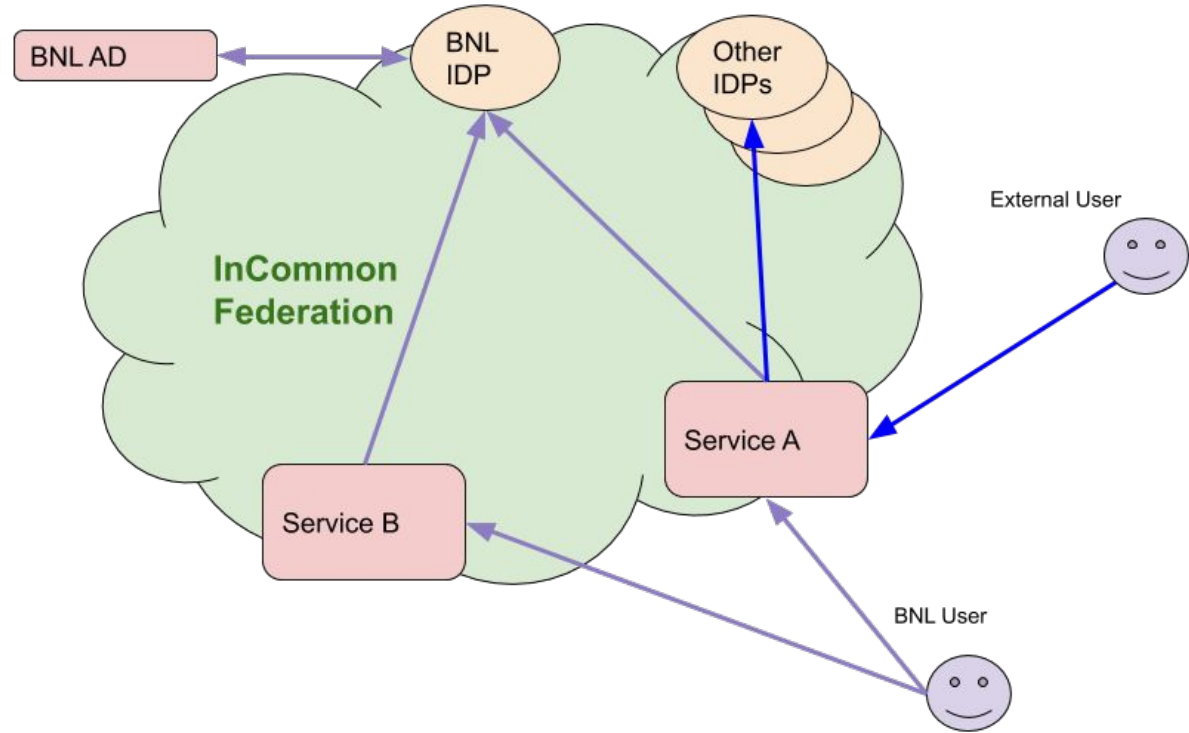
<https://www.incommon.org/>

Native InCommon

Service registered
directly with
InCommon

CONS:
SAML-only

Service provider must
"join" InCommon (not
trivial)



CILogon

InCommon is based on the SAML protocol (2005).

Many universities/institutions created SAML-based campus SSO.

But, many services now support **OAuth/OIDC** (2012).

OIDC/OAuth is used by Google, WordPress, Yahoo, Facebook, Microsoft, Github, and PayPal...

CILogon ("Cyber Infrastructure Logon") is a **bridge** to InCommon and other federations, that allows the use of OAuth/OIDC with InCommon identities.

- Also other ID sources: InCommon, eduGAIN, Google, GitHub, and ORCID
- These are configurable by service.
- The CILogon is an Internet2 project.

<https://www.internet2.edu/products-services/trust-identity/>

<https://www.cilogon.org/home>

Other Federations/ Identity Sources via CILogon

eduGAIN:

- European "federation of federations".
- Each country has its own national federation.
- eduGAIN identities usable in US via CILogon

ORCID

- Guaranteed unique research/scholarship identities.
- <https://orcid.org/>

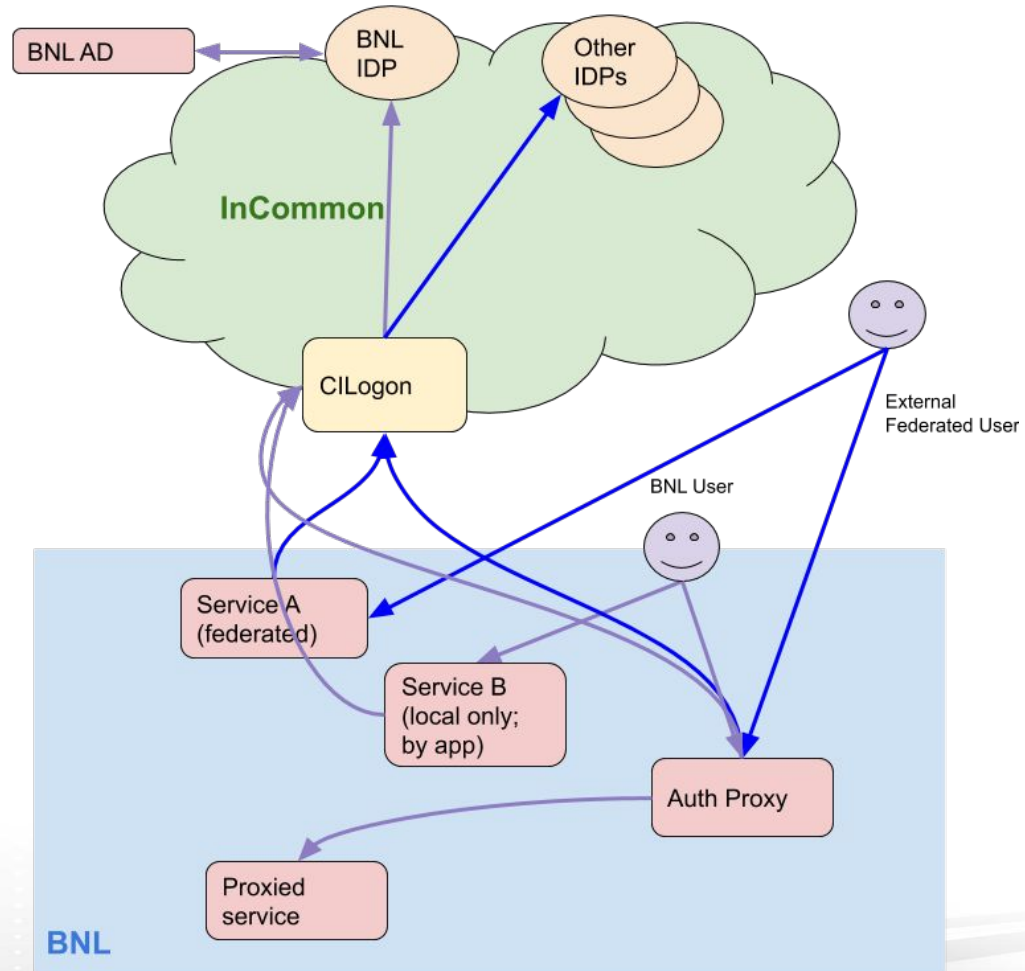
Google, Github

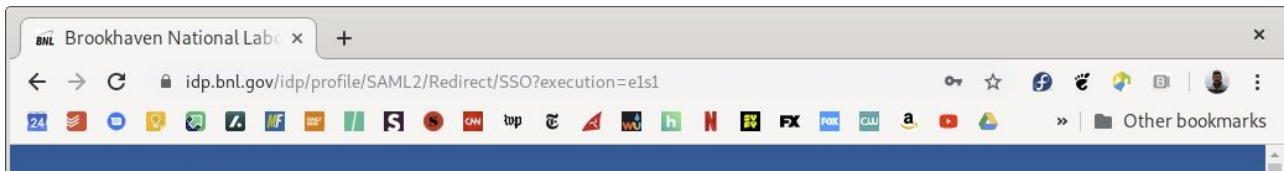
CILogon Bridged

Services registered with CILogon.

Uses **OIDC/OAuth** as protocol.

To InCommon
CILogon is simply another *service*.





BROOKHAVEN NATIONAL LABORATORY *BNL Login Service*

set (CILogon = CILogon facilitates secure access to CyberInfrastructure (CI).)
You have been redirected to this site by **CILogon**
[Why am I here?](#)

Login to CILogon
Username *

Enter your [BNL domain](#) account username.

Password *

Enter the password that accompanies your username.

For Assistance
If you are experiencing problems, or if you think your account may be locked, contact the ITD

NOTICE TO USERS:
This is a Federal computer system (network system) and is the property of the United States Department of Energy, and law of other agencies, both domestic and foreign. Use of this system is authorized only for the purpose intended and in accordance with the expectation of privacy.
Any or all uses of this system are monitored, recorded, copied, and disseminated to the United States Department of Energy, and law of other agencies, both domestic and foreign, to such interception, monitoring, disclosure at the discretion of authorized personnel.
Unauthorized or improper use of this system is prohibited and may result in civil and criminal penalties. Your awareness of and consent to these terms is required. If you do not agree, please do not use the system. IMMEDIATELY if you do not agree.

Home x +

Address bar: jupyter05.sdcc.bnl.gov:8000/user/jhover@bnl.gov/tree?

jupyter

Files Running IPython Clusters

Select items to perform actions on them.

	Name ↓	Last Modified	File size
0	/		
<input type="checkbox"/>	bin	a month ago	
<input type="checkbox"/>	compiler_compat	a month ago	
<input type="checkbox"/>	conda-meta	a month ago	
<input type="checkbox"/>	condabin	a month ago	
<input type="checkbox"/>	data	6 months ago	
<input type="checkbox"/>	doc	a month ago	
<input type="checkbox"/>	envs	3 hours ago	
<input type="checkbox"/>	etc	a month ago	
<input type="checkbox"/>	git	3 months ago	
<input type="checkbox"/>	include	a month ago	
<input type="checkbox"/>	lib	a month ago	
<input type="checkbox"/>	libexec	a month ago	
<input type="checkbox"/>	man	a month ago	
<input type="checkbox"/>	mkshrc	a month ago	

COManage

CILogon + InCommon handles authentication (AuthN), but nothing more.

This is OK for many applications. But what about support for fine-grained *authorization* (AuthZ)? What about support for collaborations, distributed projects, multi-institutional experiments?

COManage ("Collaborative Organization Manage") fills this need for CILogon.

COManage is a web application

- User invitation, enrollment, email validation, suspension
- Group and/or role assignments
- Delegation of group administration and invitations
- Self-service OIDC application registration
- Fine-grained attribute release via CILogon during authentication.

Member Enrollment

Prospective members can be sent invitations by group admin.

Users log in using their federated identity and are added to the correct group(s).

The screenshot shows a web browser window with the URL `registry.cilogon.org/registry/co_enrollment_flows/index/co:5`. The page title is "Enrollment Flows" and the breadcrumb is "Home > SDCC > Enrollment Flows". The interface includes a left sidebar with navigation options: People, Groups, Email Lists, Jobs, Servers, Configuration, and Collaborations. The main content area displays a table of enrollment flows with columns for Name, Status, Petitioner Enrollment Authorization, and Actions. The table lists various templates and active flows, such as "Account Linking (Template)", "Additional Role (Template)", "Conscription With Approval (Template)", "Copy of Invitation (Template)", "COU:csi-invenio Registration: Invitation", "Invitation (Template)", "SDCC Registration: Invitation", and "SDCC Registration: Self Signup With Approval".

Name	Status	Petitioner Enrollment Authorization	Actions
Account Linking (Template)	Template	CO Person	Edit Duplicate Delete
Additional Role (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Conscription With Approval (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Copy of Invitation (Template)	Template	CO or COU Admin	Edit Duplicate Delete
COU:csi-invenio Registration: Invitation	Active	CO or COU Admin	Begin Edit Duplicate Delete
Invitation (Template)	Template	CO or COU Admin	Edit Duplicate Delete
SDCC Registration: Invitation	Active	CO or COU Admin	Begin Edit Duplicate Delete
SDCC Registration: Self Signup With Approval	Suspended	Authenticated User	Edit Duplicate Delete

Groups and Roles

Many separate projects can be supported in a single COManage instance.

Users and attributes are published into a dedicated LDAP instance...

The screenshot shows a web browser window with the URL `registry.cilogon.org/registry/co_groups/select/co:5`. The page title is "SDCC" and the logo "COManage™" is visible in the top right. The left sidebar contains navigation options: People, Groups, Email Lists, Jobs, Servers, Configuration, and Collaborations. The main content area is titled "Manage John Hover Group Memberships" and displays a table of group memberships.

Home > SDCC > My Population > CO Person > Manage Group Memberships

Manage John Hover Group Memberships

Name	Description	Open	Status	Actions
CO:admins	SDCC Administrators	Closed	Active	<input checked="" type="checkbox"/> Member <input checked="" type="checkbox"/> Owner
CO:COU:csi-invenio:admins	csi-invenio Administrators	Closed	Active	<input checked="" type="checkbox"/> Member <input checked="" type="checkbox"/> Owner
CO:COU:csi-invenio:members:active	csi-invenio Active Members	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:COU:csi-invenio:members:all	csi-invenio Members	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
CO:members:active	SDCC Active Members	Closed	Active	<input checked="" type="checkbox"/> Member <input type="checkbox"/> Owner
CO:members:all	SDCC Members	Closed	Active	<input checked="" type="checkbox"/> Member <input type="checkbox"/> Owner
csi-c3d	csi c3d	Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner
csi-genesis	CSI Genesis Invenio Demo	Closed	Active	<input checked="" type="checkbox"/> Member <input checked="" type="checkbox"/> Owner
testgroup		Closed	Active	<input type="checkbox"/> Member <input type="checkbox"/> Owner

SAVE

Display 25 records per page

Application Registration

Application admins can set up new endpoints via self-service interface.

The screenshot shows a web browser window displaying the 'OIDC Clients' management page in the SDCC (Service Discovery and Configuration Center) interface. The page title is 'OIDC Clients' and the breadcrumb is 'Home > SDCC > OIDC Clients'. A navigation sidebar on the left includes links for People, Groups, Email Lists, Jobs, Servers, Configuration, and Collaborations. The main content area features a table of registered OIDC clients, each with a Name, Client ID, and Actions (Edit and Delete). A '+ Add a New OIDC Client' button is located in the top right corner of the table area.

Name	Client ID	Actions
BNL SDCC Keycloak	cilogon:/client_id/5113835ebb02fe4317599bbdec8441b4	Edit Delete
BNL Test	cilogon:/client_id/5a447b99f7eb80de3a80e9d01511aae4	Edit Delete
cilogontest	cilogon:/client_id/3dacbf0addcc7449ebdb0305f285d885	Edit Delete
cilogontest2	cilogon:/client_id/3c207505f1915002b44423a0d11ff01	Edit Delete
comanagekeycloak	cilogon:/client_id/222cea90c21ba1dd1a9197603e40b65c	Edit Delete
genesis	cilogon:/client_id/1edaded29a1f24314c5d695f7b3d242e	Edit Delete
inveniotest07	cilogon:/client_id/3b1220a922c3844659e45c7fc40a1ae2	Edit Delete
inveniotest08	cilogon:/client_id/8f16cba50d1bcf2da7c7f37e21f75d1	Edit Delete
inveniotest09	cilogon:/client_id/3877809a6968d37a6570262db0e905ea	Edit Delete
inveniotest10	cilogon:/client_id/73cf186f8a6800e25a106439ac7c99ec	Edit Delete

Adding an Application

Add a New OIDC Client

registry.cilogon.org/registry/oa4mp_client/oa4mp_client_co_oidc_clients/add/co:5

Home > SDCC > OIDC Clients > Add OIDC Client

Add a New OIDC Client

Name *
The client Name is displayed to end-users on the Identity Provider selection page

Home URL *
The Home URL is used as the hyperlink for the client Name

Callbacks *
The redirect_uri parameter must exactly match a callback URL

URL

[+ Add another Callback URL](#)

Scopes *
Information on scopes

openid

profile

email

org.cilogon.userinfo

LDAP to Claim Mappings
Information on LDAP to claim mappings

[+ Add a LDAP to Claim Mapping](#)

ADD

Authorization sequence

When authentication is performed against an COManage-registered app, CILogon

1. Queries the CO-specific LDAP instance.
2. Adds relevant COManage attributes to the login token e.g:

```
{'sub': 'http://cilogon.org/serverA/users/166926',  
'idp_name': 'Brookhaven National Laboratory',  
'eppn': 'jhover@bnl.gov',  
'iss': 'https://cilogon.org',  
'aud': 'cilogon:/client_id/5ea8818a26318a9dc03d8a1f82bef34a',  
'acr': 'https://refeds.org/profile/sfa',  
'idp': 'https://idp.bnl.gov/idp/shibboleth',  
'name': 'Hover, John',  
'isMemberOf': ['CO:members:all', 'CO:members:active', 'CO:admins', 'bnl'],  
'given_name': 'John',  
'family_name': 'Hover',  
'email': 'jhover@bnl.gov'}
```

3. The application can then make Authorization decisions based on the presence/absence of group membership...

Site-level brokers: KeyCloak, SimpleSAMLPhP

Yet another layer!!

KeyCloak:

- Can function as both an OIDC and SAML identity provider.
- Redhat supported, community-based open source project.
- Often used for site-based SSO. But can *also* redirect to external authentication sources like CILogon, allowing, e.g.:

Application -> KeyCloak -> CILogon -> InCommon

SDCC is moving toward a KeyCloak-based layout for all our internal services.

SimpleSAMLPHP:

- BNL ITD uses this for their site-level SSO
- Also federate out to CILogon, Google, etc.

KeyCloak Login

Local SDCC
accounts, BNL AD,
InCommon
federation, or Google

Configurable on a
per-service basis.

BROOKHAVEN
NATIONAL LABORATORY | Scientific Data and
Computing Center

LOGIN

Username


Password

Log In

Federated ID

BNL Active Directory

SDCC Shibboleth IDP

 Google

Note:

- * Use left pane for SDCC Account Login
- * Use right pane for non SDCC Account Login

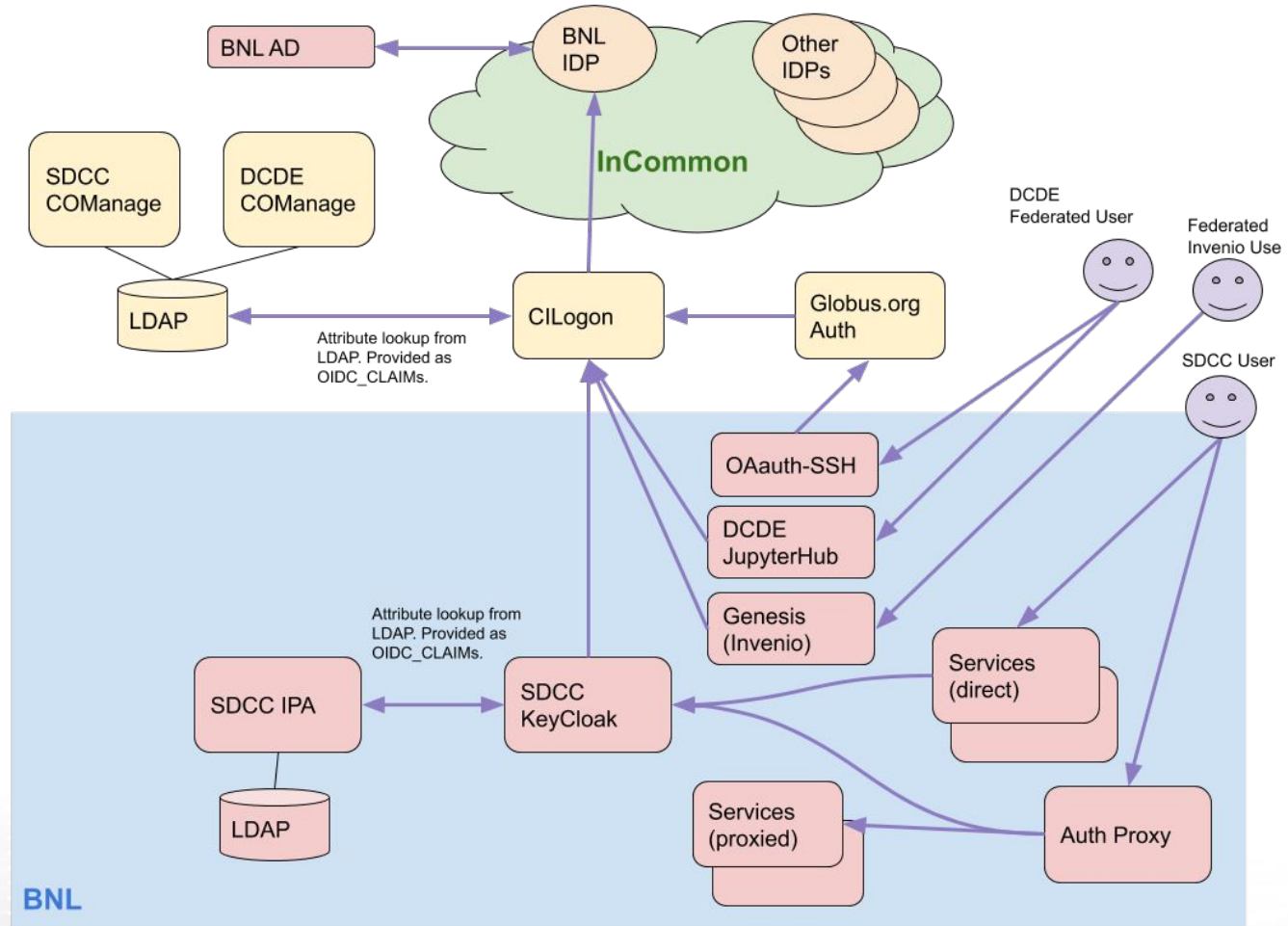
NOTICE TO USERS

Current SDCC Layout

Pilot projects directly federating with CILogon/COManage. Plugins doing AuthZ.

Shared cloud-based COManage instances.

KeyCloak bridging to InCommon, using BNL IDP, ready to use rest of InCommon.



Challenges with Federated ID

- Non web-based services.
 - Each IDP has its own web page layout, meaning a browser is needed for the user to enter their info.
- Any service that requires a local UNIX account context
 - What user should a *federated* user run as??
- For DOE labs, strict cybersecurity standards have made adoption slow.
 - Currently being approved for general usage.
 - Still potential issue with foreign national status for some applications.
- Multi-Factor Authentication
 - Used by banks, other secure services. E.g. access code texted to your phone.
 - BNL uses Duo
 - InCommon currently adding requirement that institutions include an attribute declaring whether a login was done with or without MFA.
- Integration of Globus...

Issues/Questions for Service Administrators

Do you need fine-grained authorization?

- Does the application have built-in management (e.g. Indico)?
- If not, COManage may be necessary.

Native Plugins vs. Authenticating Proxy

- If an application has a native OIDC plugin, it can be directly registered with COManage.
- If an application has a native SAML plugin, it *could* be directly federated in InCommon (without CILogon).
- Any application that can use REMOTE_USER variable can be placed behind an *authenticating proxy*. The proxy is the CILogon client and only allows access after auth.

Summary...

Lots to take in, but don't get overwhelmed by the technology. Rather ask:

- Is your service capable of federation?
- Does it already have relevant authN capabilities (SAML, OIDC, remote_user)?
- Can federation allow you to do more with the same admin effort, or the same with less admin effort?
- Who do you want to allow to use it?
- How fine-grained do permissions need to be?
- Is MFA required?
- Does it have special restrictions that must be enforced?

References

<https://www.internet2.edu/>

<https://www.incommon.org>

<https://www.cilogon.org/home>

<https://www.internet2.edu/products-services/trust-identity/comanage/>

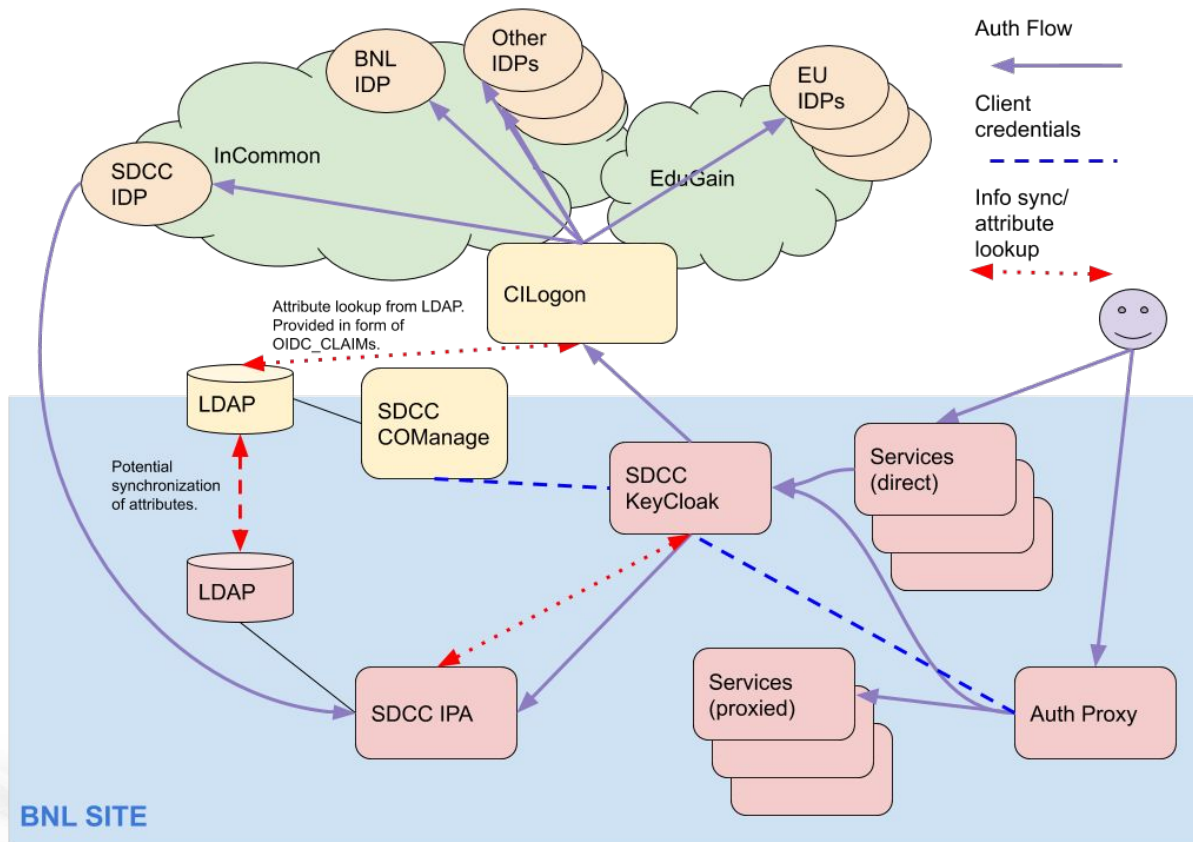
<https://www.keycloak.org/>

<https://simplesamlphp.org/>

<https://openid.net/connect/>

Discussion & Questions...

Extra Slides



One Possible Future...

KeyCloak as broker.
Bridging to CILogon,
OneID.
Service-by-service auth
choice.

COManage for group
admin.

OIDC as standard
protocol; supporting
SAML where needed.

