

Federated Identity & AAI @SDCC

Mizuki Karasawa
09/22/2020

Agenda

- Federation & Benefits
- Authentication domains/Federation in BNL & SDCC
- Authorization Systems for Federated IDs
- Federation Challenges & AAI models
- IdP & SP & AuthN (SAML vs OIDC vs OAuth2)
- IdP Proxy Architecture & Examples
- SP Proxy Architecture & Examples
- Summary & Questions

What is Federation

Federation Benefits

- Avoid the needs to get separate accounts at different institutions
- One account (ex, BNL AD or SDCC) to access local & external sources in other Laboratories & Universities and vice versa
- Save time & resource, delegates hassles of vetting accounts
- Streamline the federated research access
- Enable global collaboration

Research and Scholarship (R&S) Federation

- * Large-scale identity federations cross the regions:
 - InCommon in US
 - eduGain in Europe
 - *APAN in APAC*
 - Inter-federation
- * InCommon in US:
 - Establish standards for participation, technical interoperability
 - Provide community-based governance
 - ~1000 universities, laboratories, institutions, etc
- * These allow identities from any federation members to be used at relying parties
 - Using SDCC accounts at other participated institutions ex, Fermilab or CERN
 - Access the SDCC resources using Fermilab IDs

SDCC Federated IdP w/ InCommon

CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

Sign in with your CERN account

Reminder: you have agreed to comply with the CERN computing rules, in particular OCS. CERN implements the measures necessary to ensure compliance.

Use credentials

Username or Email address Password

Remember Username or Email Address [Need password help ?](#)

Use one-click authentication

[Sign in using your current Windows/Kerberos credentials \[autologon\]](#)
Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC (Firefox help here).

[Sign in using your CERN Certificate \[autologon\]](#)
You can get a CERN certificate on the CERN Certification Authority website.

Use strong two factor authentication [show]

Sign in with a public service account

[Facebook, Google, Live, etc.](#)
Authenticate using an external account provider such as Facebook, Google, Live, Yahoo, Orange.

Sign in with your organization or institution account


[eduGAIN](#)

Why is my **Brookhaven**

- Brookhaven National Laboratory
- Brookhaven National Laboratory - SDCC.BNL.GOV

Related sites

- [Need password help ?](#)
- [Create/Check your account](#)
- [EduGain disclaimer settings](#)
- [Service Desk +41 22 76 77777](#)
- [Computing Status Board](#)




Log in to use Globus Web App

Use your existing organizational login

e.g., university, national lab, facility, project

- Brookhaven National Laboratory
- Brookhaven National Laboratory - SDCC.BNL.GOV

Or



Select an Identity Provider

Brookhaven National Laboratory - SDCC.BNL.GOV

- Brighton Young University
- Brighton and Sussex Medical School
- Brighton Hove & Sussex 6th Form College
- British & Irish Modern Music Institute (BIMM)
- British Library
- British Universities Film & Video Council
- Bmo University of Technology
- Brock University
- Brockenhurst College
- Brookhaven National Laboratory
- Brookhaven National Laboratory - SDCC.BNL.GOV**
- Brooklands College
- Brooksby Melton College
- ...

Campus Level Authentication Domains & Federation

- Managed/Operated by lab-level Information Technology Division(ITD)
- ITD enterprise services (ex, Office365, PeopleSoft, VPN, PASS etc)
- Runs Federated IdP w/ InCommon/eduGain backed by central campus Active Directory (AD) account system (~5000 accounts)
- Duo for MFA external, non-MFA internal

Scientific Authentication Domain & Federation

- A scientific computing provider, supports multi-experiment
- Operates scientific computing facility/non-enterprise level (ex, SSH gateway, NX, Interactive Nodes, Web applications/services including BNLBox, Invenios&Zenodo, Drupal, Jupyterhub)
- ~2000 accounts distinct from ITD AD (no deletion of the user accounts, data is preserved)
- **Recently established federated IdP with InCommon, backed by IPA systems**
- **OTP for MFA external, non-MFA internal**
- **Inter-connect with ITD system to allow users use AD +/- SDCC**

Authorization Systems for Federated IDs

CILogon:

Provides an integrated open source identity and access management platform for research collaborations, combining federated ID management (Shibboleth, InCommon), handles authentication (AuthN), but nothing more.

What about support for collaborations, distributed projects, multi-institutional experiments?

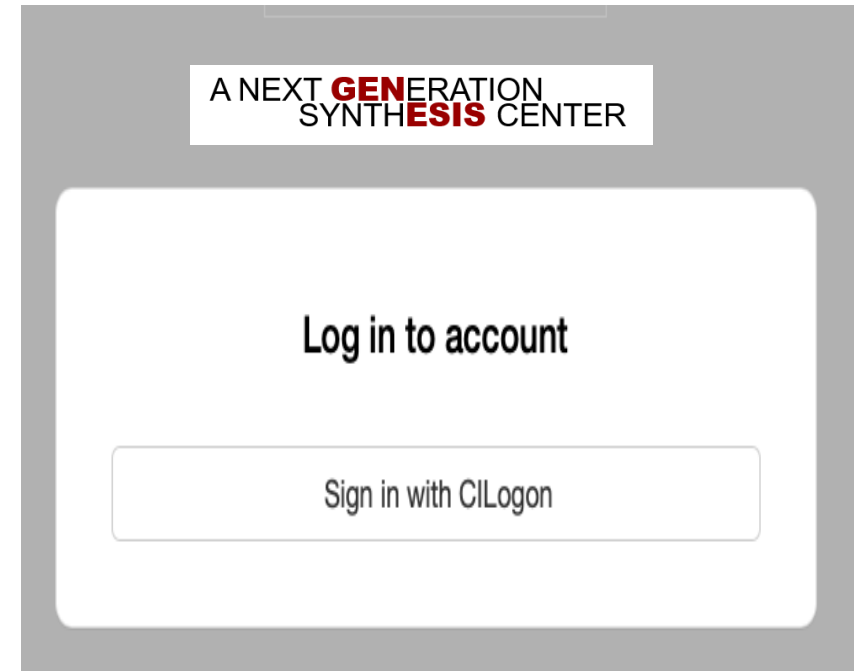
COManage ("Collaborative Organization Manage"):

Fills the need for CiLogon, support fine-grained authorization (AuthZ)

- User invitation, enrollment, email validation, suspension
- Group and Role assignments
- Delegation of group administration and invitations
- Self-service OIDC application registration
- Fine-grained attribute releases via CiLogon during authentication

AuthZ System Example w/ CoManage: ex. CSI Invenio/Genesis

- CSI Admin sends an invite to users for enrollment
- User receives an invite, signing in using federated id with home institution account
- Admin places users in authorization groups
- Invenio checks user group OIDC claims and makes authorization decision



Federated ID Use Cases @SDCC:

- CSI Invenio/ Genesis
- EIC Zenodo
- Covid-19-archieve: Custom Zenodo based digital repository
- USATLAS Drupal CMS
- *Jupyterhub: DCDE Project, developing strategies for collaborations for higher assurance level, possibly using OneID (another federation platform for DOE labs)*

Inter-Connect w/ BNL AD: BNLBOX

SDCC

Username

Password

Log In

BNL Active Directory

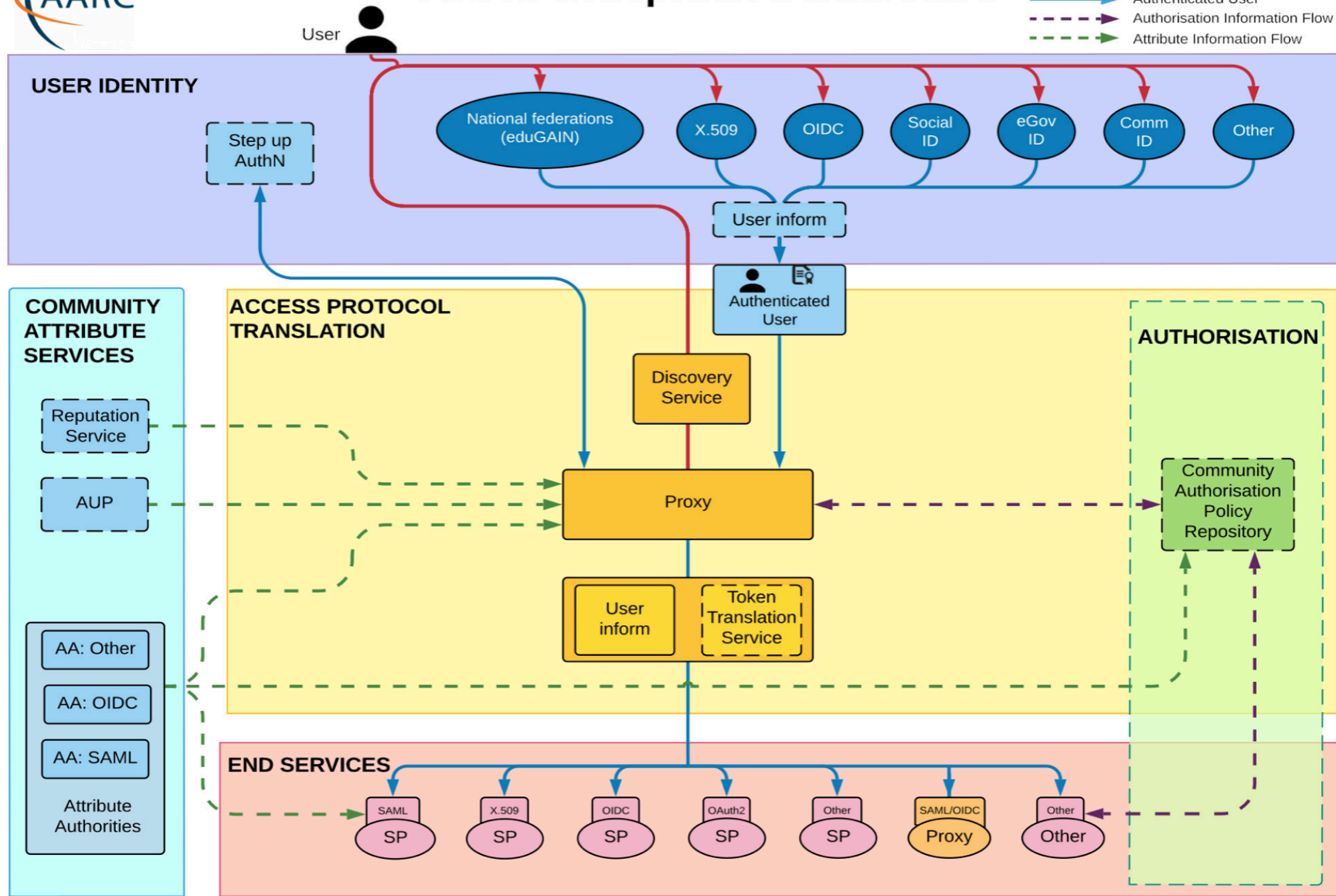
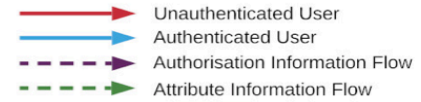
Note:

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

Federation Challenges & AAI Models



AARC Blueprint Architecture

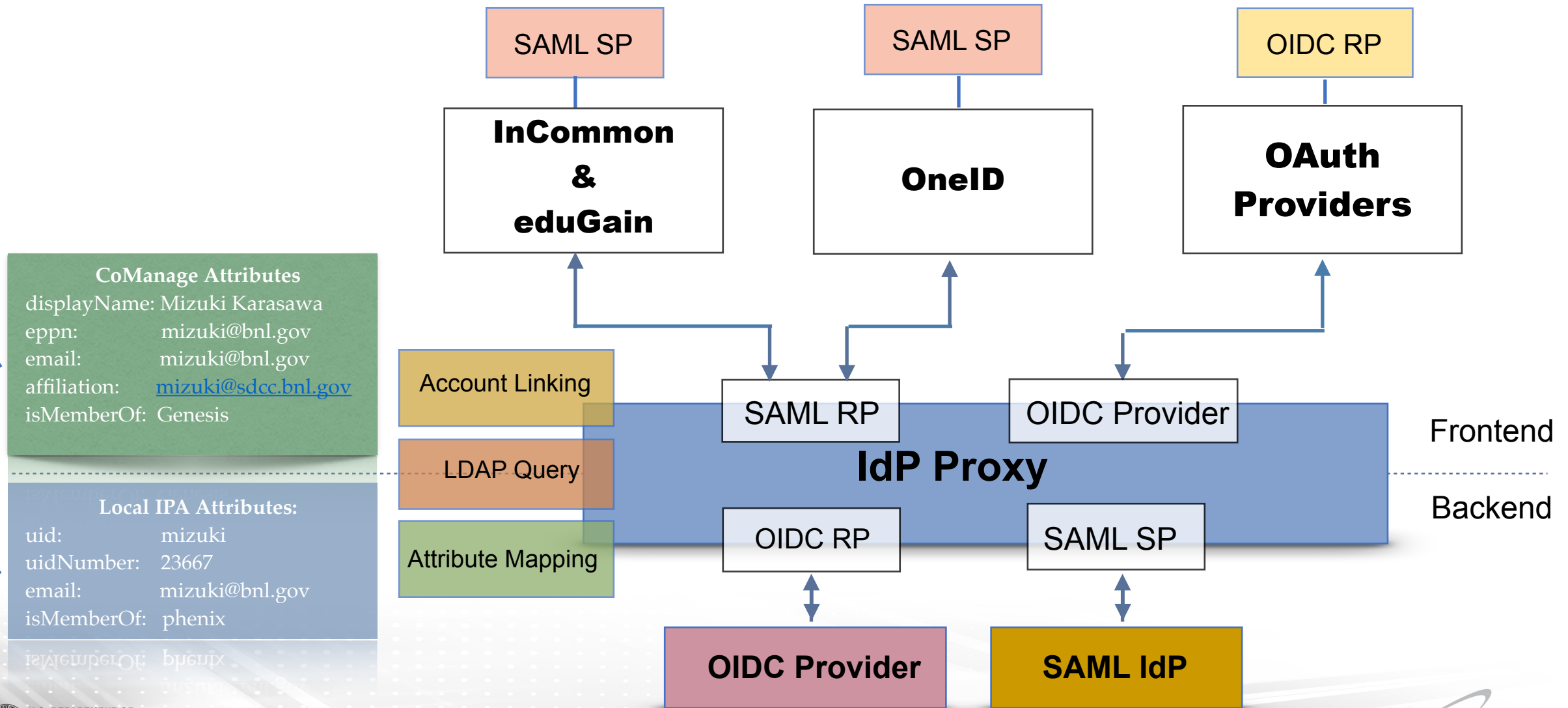


Authentication and Authorization for Research and Collaboration (AARC)
<https://aarc-community.org>

SSO & IdP/SP/Authentication Protocols

- SSO: Single Sign-On, enter the login credential once, access all of the applications within the Domains & Realms
- IdP : Identity Provider, the source for validating user identities in federated identity system
- SP : Service Provider, initiates SSO
- Authentication Protocols (SAML vs. OAuth vs. OIDC)
 - SAML : An open standard for exchanging authentication & authorization data between parties SP & IDP, XML based for security assertions
 - OAuth : An open standard for access delegation, authorize users w/ access token exchange to the access of the data w/o giving the password
 - OIDC : An extension of OAuth, an JWT that includes assertion of identity on top of the access

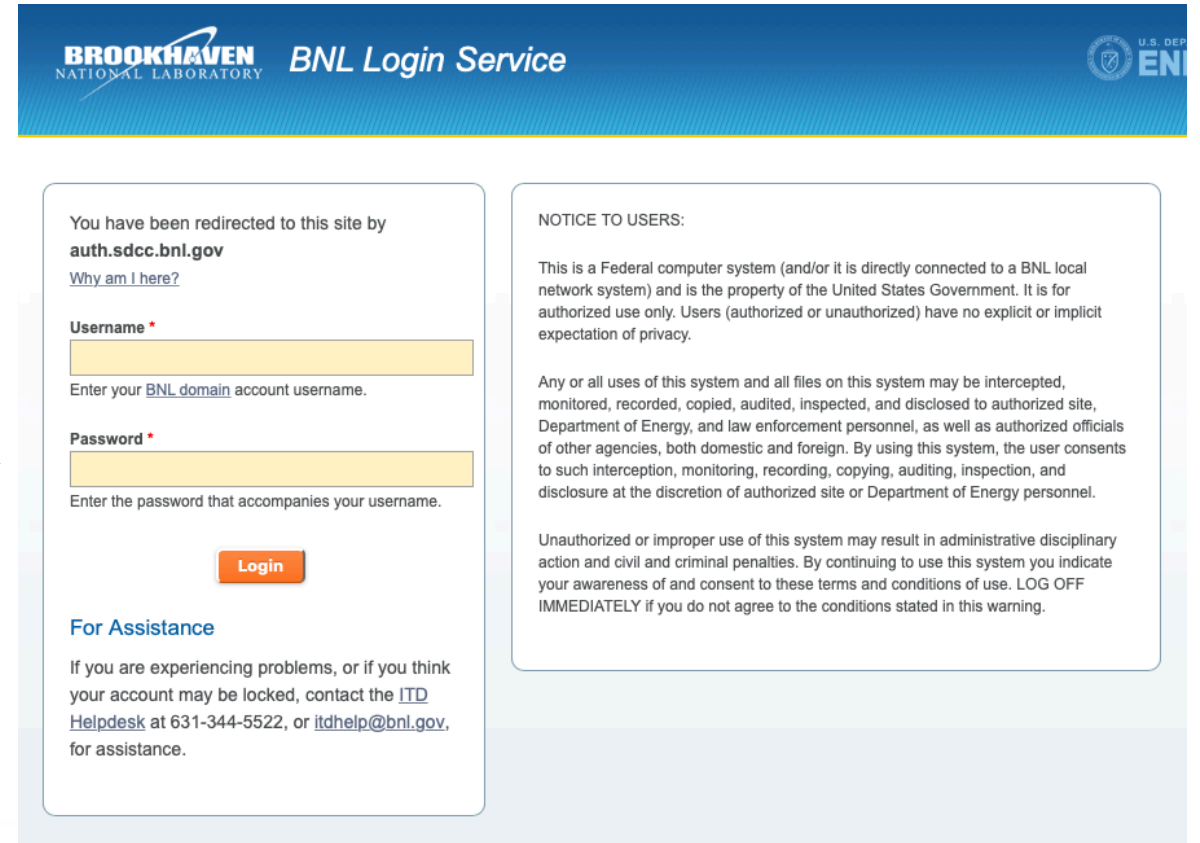
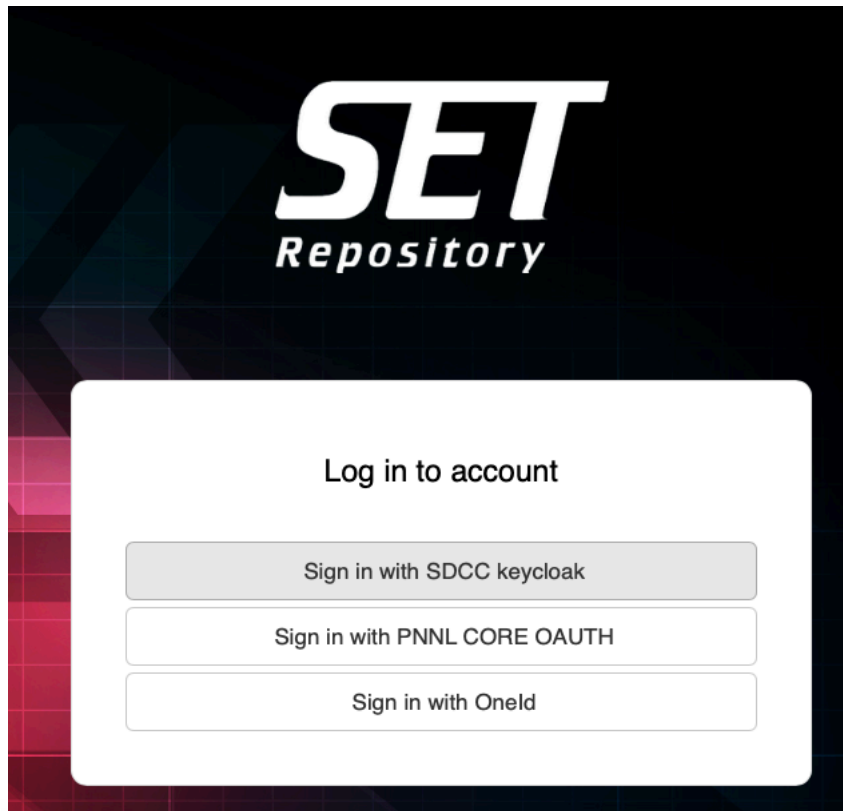
IdP Proxy Architecture @SDCC



IdP Proxy Benefits

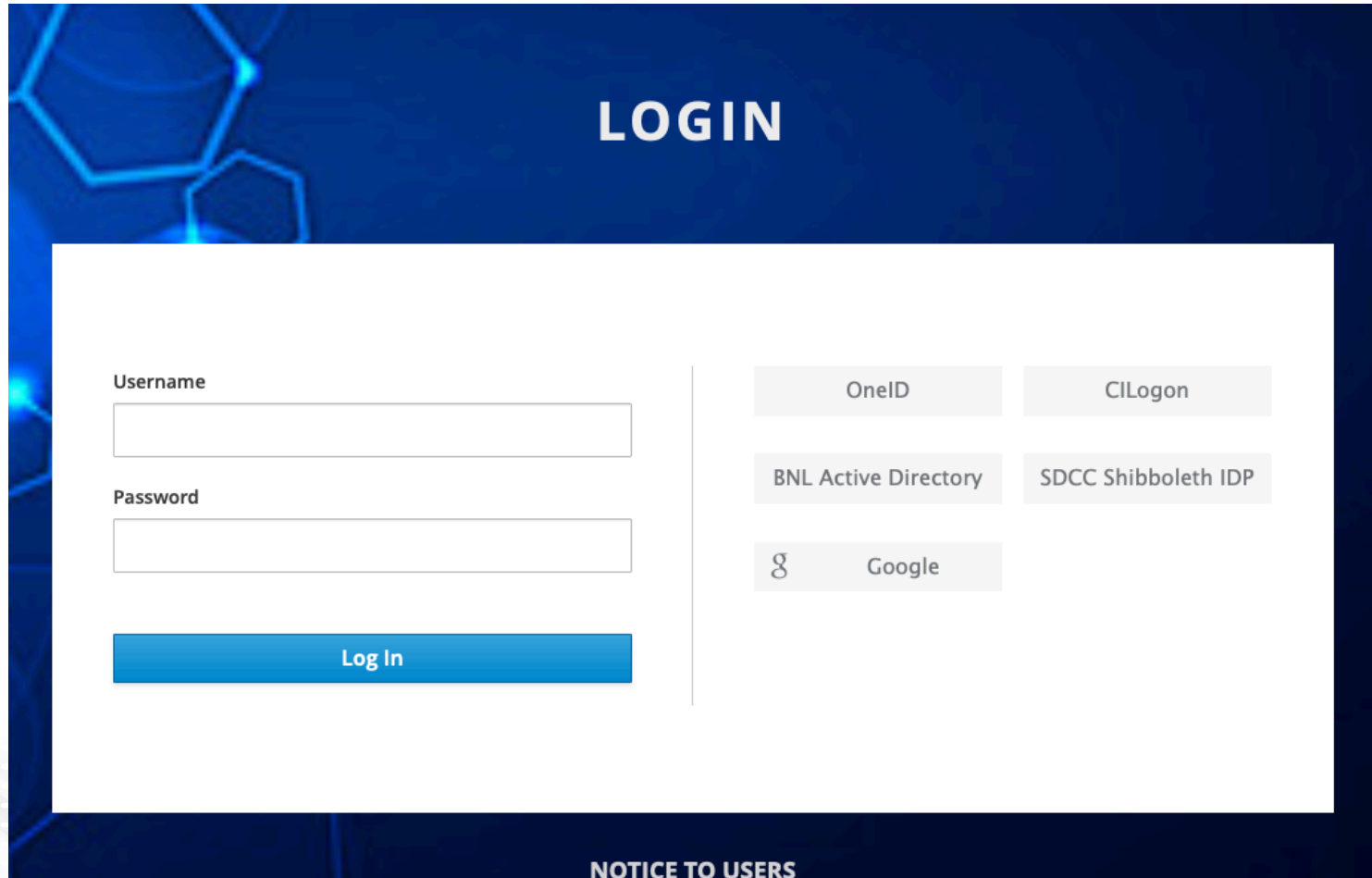
- Options for federation & Social Providers integration
- DS (Discover Service)
- Attributes Manipulations
- Account Linking
- Interoperability among SP & IdPs

IdP Proxy Example



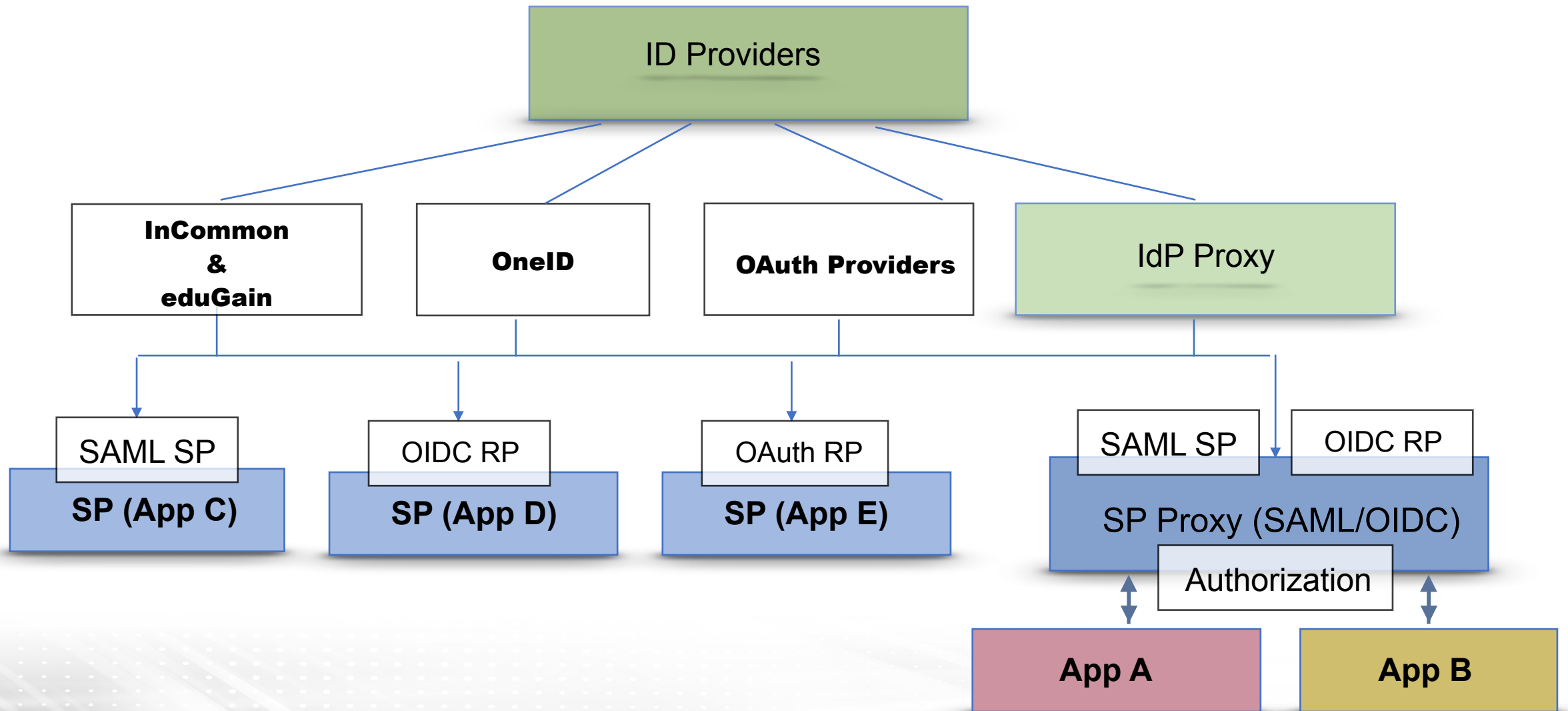
Possible Extended Federation Options

- OneID, ORCID, Google, LinkedIn, etc



The screenshot shows a login interface with a dark blue background and a white central panel. At the top of the panel, the word "LOGIN" is displayed in white. Below this, there are two input fields: "Username" and "Password". To the right of these fields, there are several buttons for different authentication methods: "OneID", "CILogon", "BNL Active Directory", "SDCC Shibboleth IDP", and "Google". A blue "Log In" button is positioned below the input fields. At the bottom of the white panel, the text "NOTICE TO USERS" is visible.

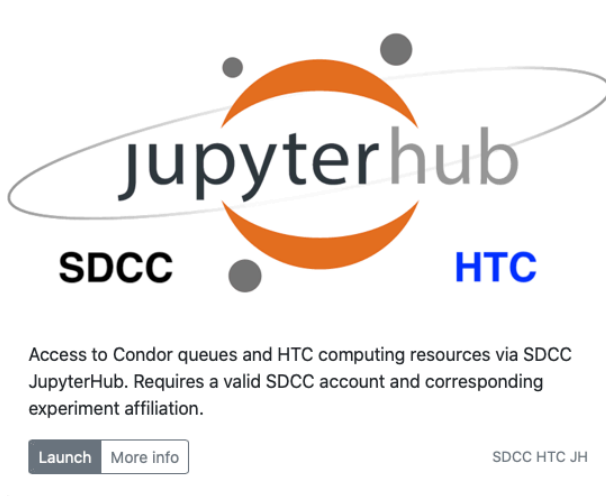
SP Proxy Architecture @SDCC



SP Proxy Benefits

- Offload the AuthN/AuthZ off Apps/Services
- Leverage Central IAM(Identity and Access Management) Systems
- Eliminate the needs for managing users in local applications
- Comply with Cyber policies
- Security

SP Proxy Example A: Jupyterhub



jupyterhub
SDCC HTC

Access to Condor queues and HTC computing resources via SDCC JupyterHub. Requires a valid SDCC account and corresponding experiment affiliation.

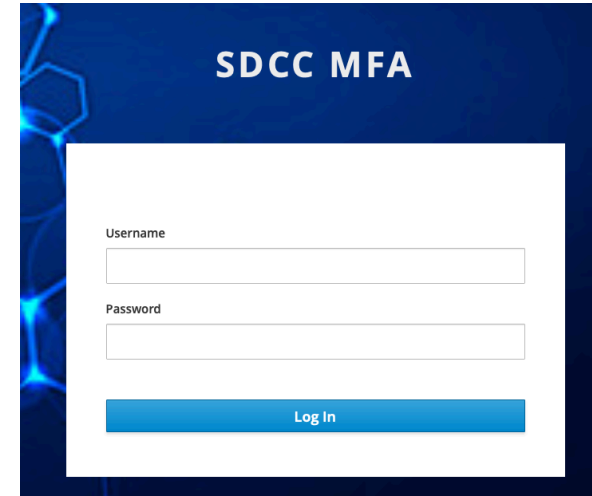
[Launch](#) [More info](#) SDCC HTC JH



jupyterhub
SDCC HPC

Access to Slurm scheduling and GPU computing resources on the IC and KNL clusters via JupyterHub. Requires a valid SDCC account and computing resource allocation.

[Launch IC](#) [Launch KNL](#) [More info](#) SDCC HPC JH

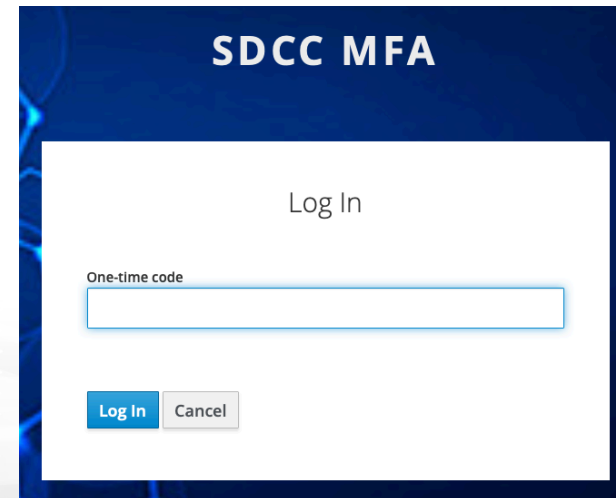


SDCC MFA

Username

Password

[Log In](#)



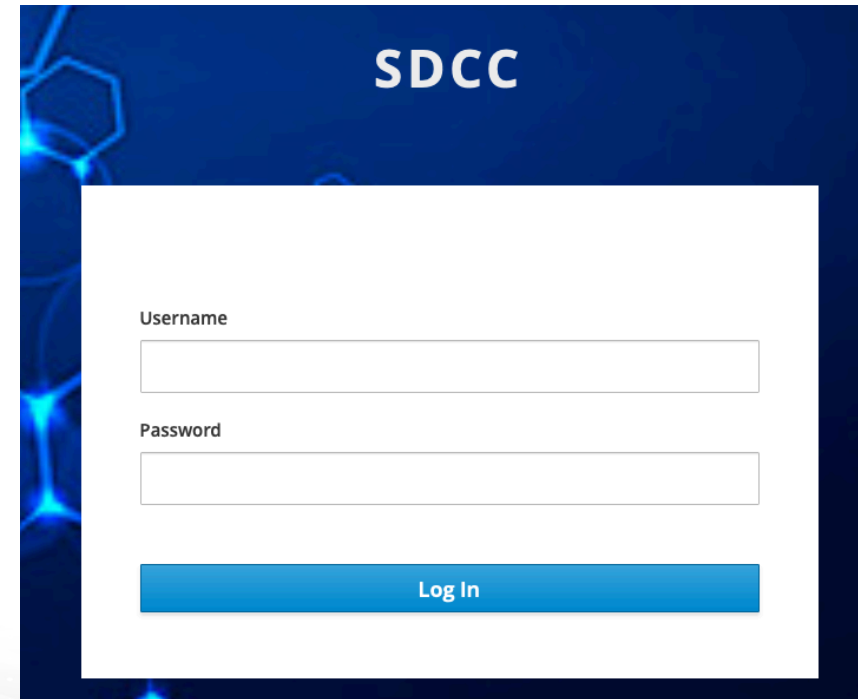
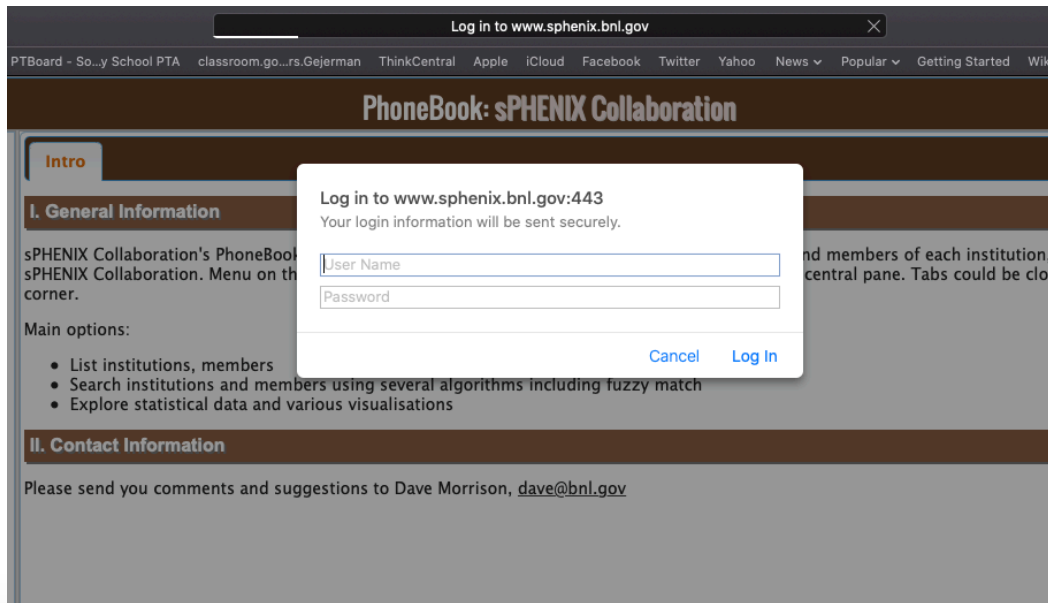
SDCC MFA

Log In

One-time code

[Log In](#) [Cancel](#)

SP Proxy Example B: Phonebook



Looking for utilizing AAI for your applications?

Lot to take in, but don't be overwhelmed by the technology, rather ask:

- Does the application need protection? - *Determine the need for AuthN*
- **Who** are the collaborators accessing the protected sources? - *Determine IdP authentication sources & providers*
- Can application inherit identity via REMOTE_USER? - *Determine SP model*
- **What** protocol can application handle? - *Determine the authentication protocols among SAML/OIDC/OAuth*
- Does it require authorization? - *Determine AuthZ*
- **Where** is entitlement data for AuthZ? - *Determine authorization model*

Questions?