

Federated ID/SSO @BNL's SDCC

Mizuki Karasawa

10/2019 for HEPiX

BackGround

- ❖ RACF (RHIC and ATLAS Computing Facility) now became SDCC (Scientific Data and Computing Center)
- ❖ Under the mission to share Scientific Computing Resource / Staff, to help support any computing needs for other departments cross lab-wide
- ❖ Emerging computing needs for new applications and collaborative tool services, require various types of authentications including federated ID authentication externally (use non-BNL institution account for authentication) and internally (use different account sources ex, BNL AD)
- ❖ Managing Kerberos Servers / Shibboleth IDPs (experiment-based) inherited from RACF became difficult.
- ❖ Shibboleth SSO implementation in RACF is outdated

2 Types of Systems, 2 Types of Accounts Federation Status

- ❖ Brookhaven Lab-wide Active Directory Account managed by ITD (Information Technology Division), used for Employee time management, Payroll, Enterprise applications such as Exchange, Share Point, One Cloud etc...Lab-level SSO enabled by Shibboleth and an InCommon participant for federation
- ❖ Scientific computing accounts managed by SDCC (Science Data Center Computing), hosted under open-source OpenLDAP / IPA, provides unix accounts to the operating systems, integrated to open-source projects and research programs etc. A cost-saving model. SSO enabled but not a InCommon participant

User Account Conversion from OpenLDAP -> IPA

- ❖ Replaced OpenLDAP with IPA (completed by the end of 2018)
- ❖ Converted experiment-based Kerberos Realms into one single Realm under domain dc=sdcc,dc=bnl,dc=gov, use ldap groups to manage experiments membership info for authorization
- ❖ Removed the needs for maintaining experiment specific Kerberos servers, Shibboleth IDPs etc, IPA now becomes a true single source of identify management system
- ❖ IPA comes with OTP feature for MFA auth, adds security features for Gateways access, Web-Services protection, interactive NX sessions etc

Shibboleth or Keycloak?

- ❖ OAuth / OIDC / SAML Support
- ❖ MFA OTP token Support
- ❖ Ease of application & client management
- ❖ Utilize Apache `mod_auth_openidc/mod_auth_mellon` for SP implementation

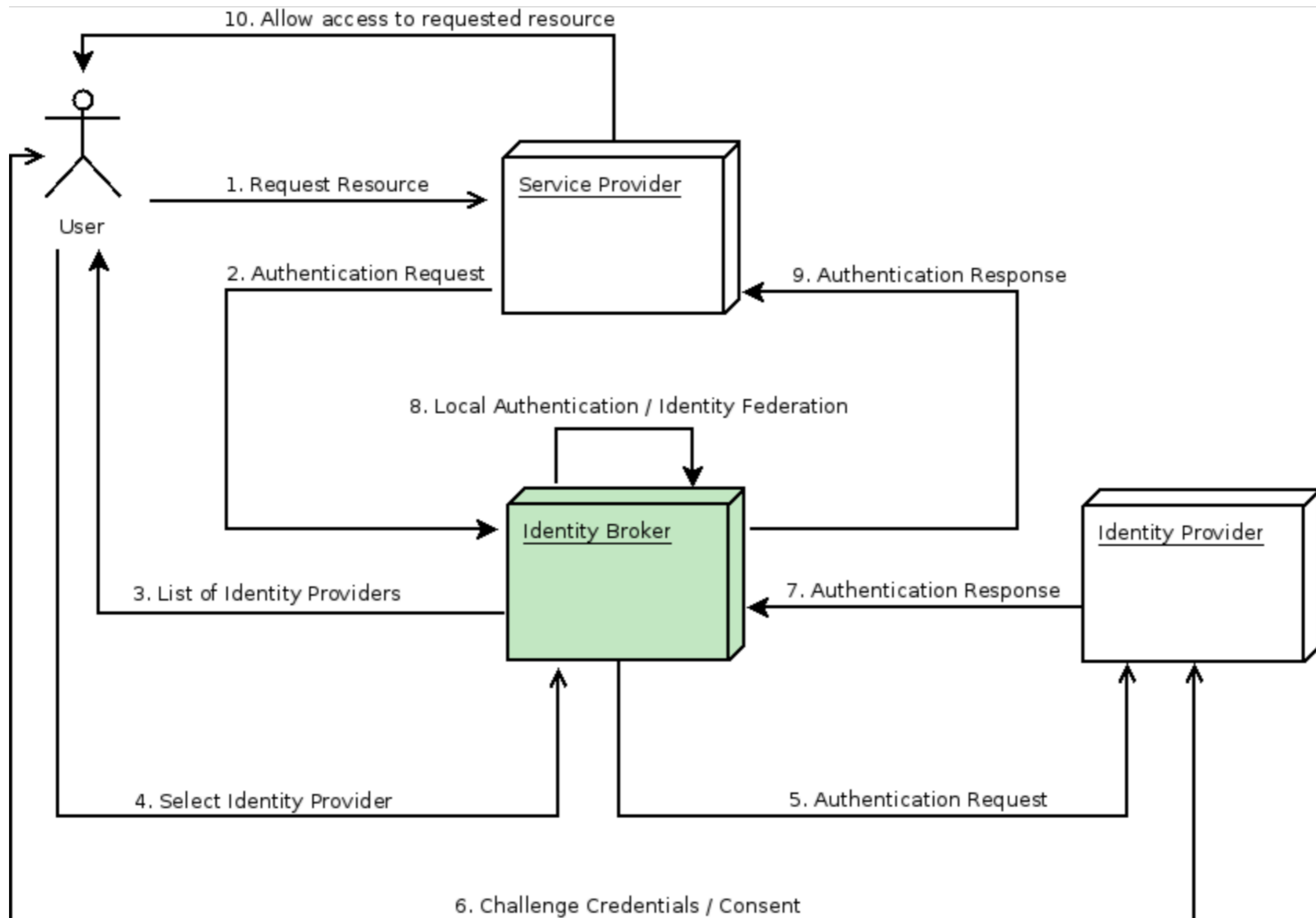
Keycloak

- ❖ Upstream of Redhat SSO, well maintained
- ❖ JBOSS / Wildfly based Application
- ❖ Broker to other IDPs and become centralized IDP hub
- ❖ Linking feature to map accounts to single identity
- ❖ Provides Authorization Layer
- ❖ Flexibility of federation internally and externally

Brokering Feature

- ❖ Federated IDPs (ex, CILogon - SP / DS in InCommon)
- ❖ OAuth IDPs (ex, Google, Facebook, Github..etc)
- ❖ Other IDPs (ex, BNL AD SAML IDP)

A Glance of Brokering...



Centralized & Distributed IDP Models:

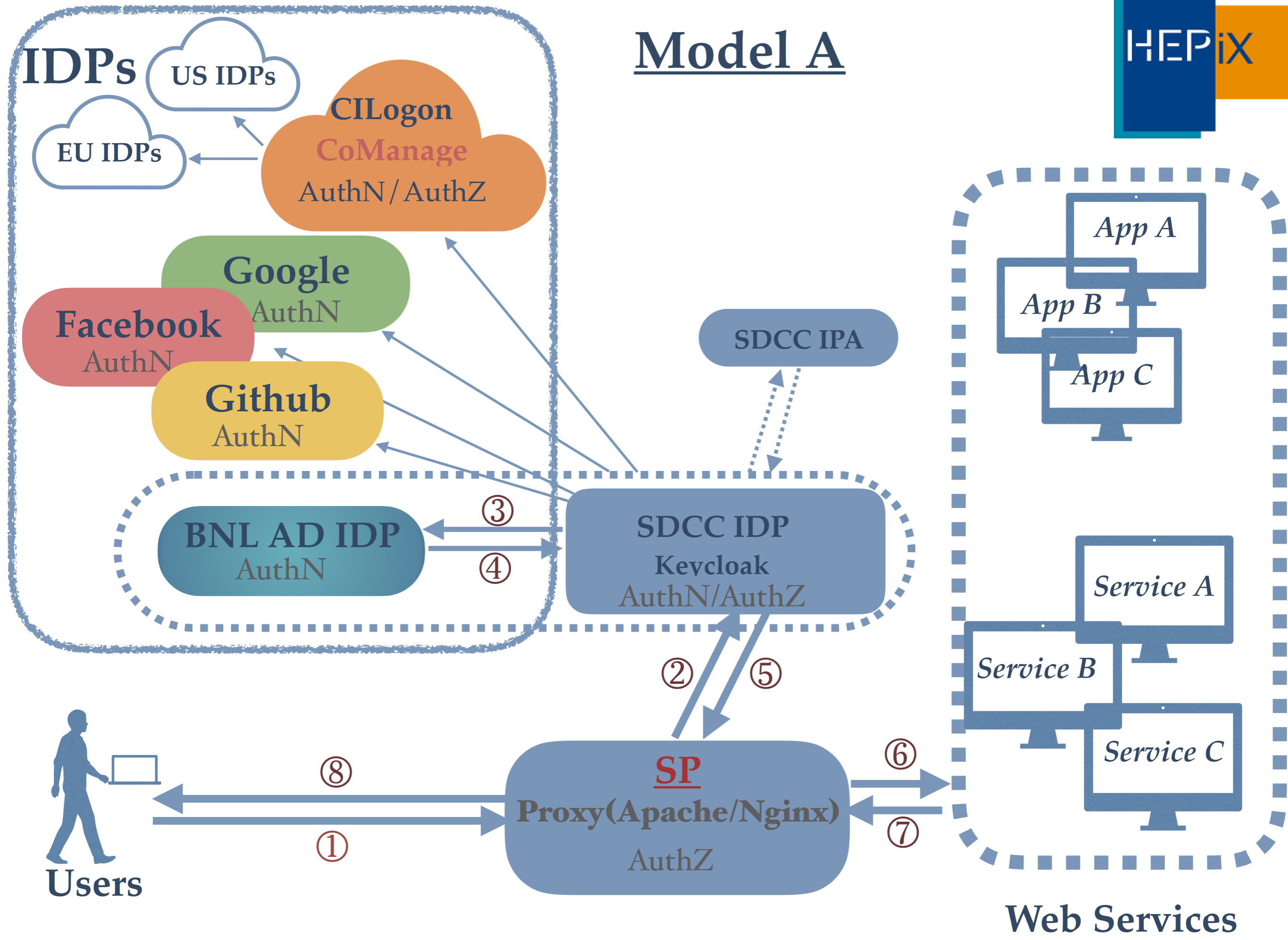
- ❖ Model A: Centralized IDPs + Web Proxies as SP + Apps / Services access
- ❖ Model B: Centralized IDPs + Direct Access to Application SP
- ❖ Model C: Distributed IDPs + Direct access to Application SP

Note:

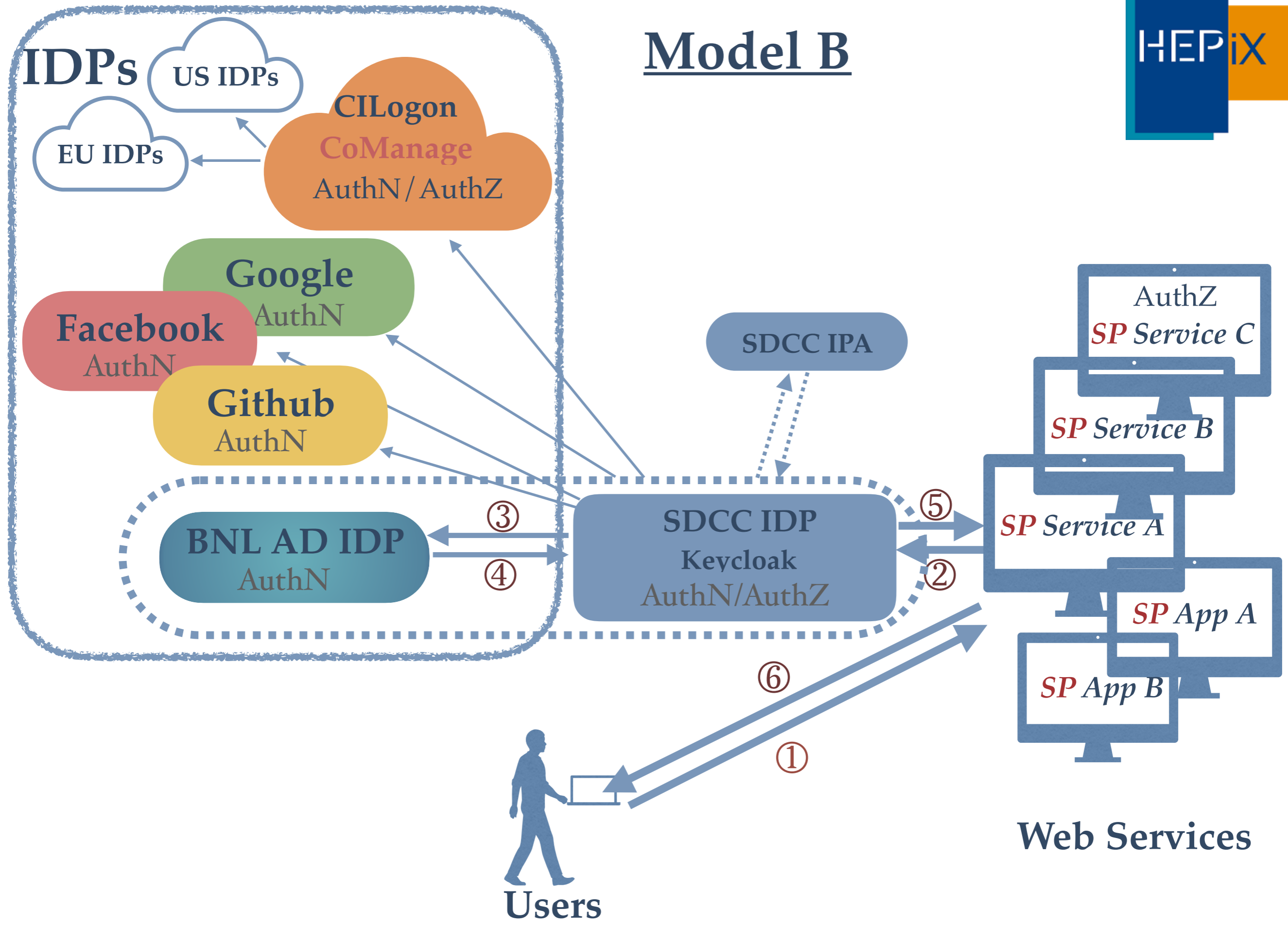
* *Blue Color* indicates the locally managed resources

* AuthN = Authentication / AuthZ = Authorization

Model A



Model B



Example of Model A & B:

Username

Password

Log In

Note:

* Use left pane for SDCC Account Login

* Use right pane for non SDCC Account Login

Federated ID

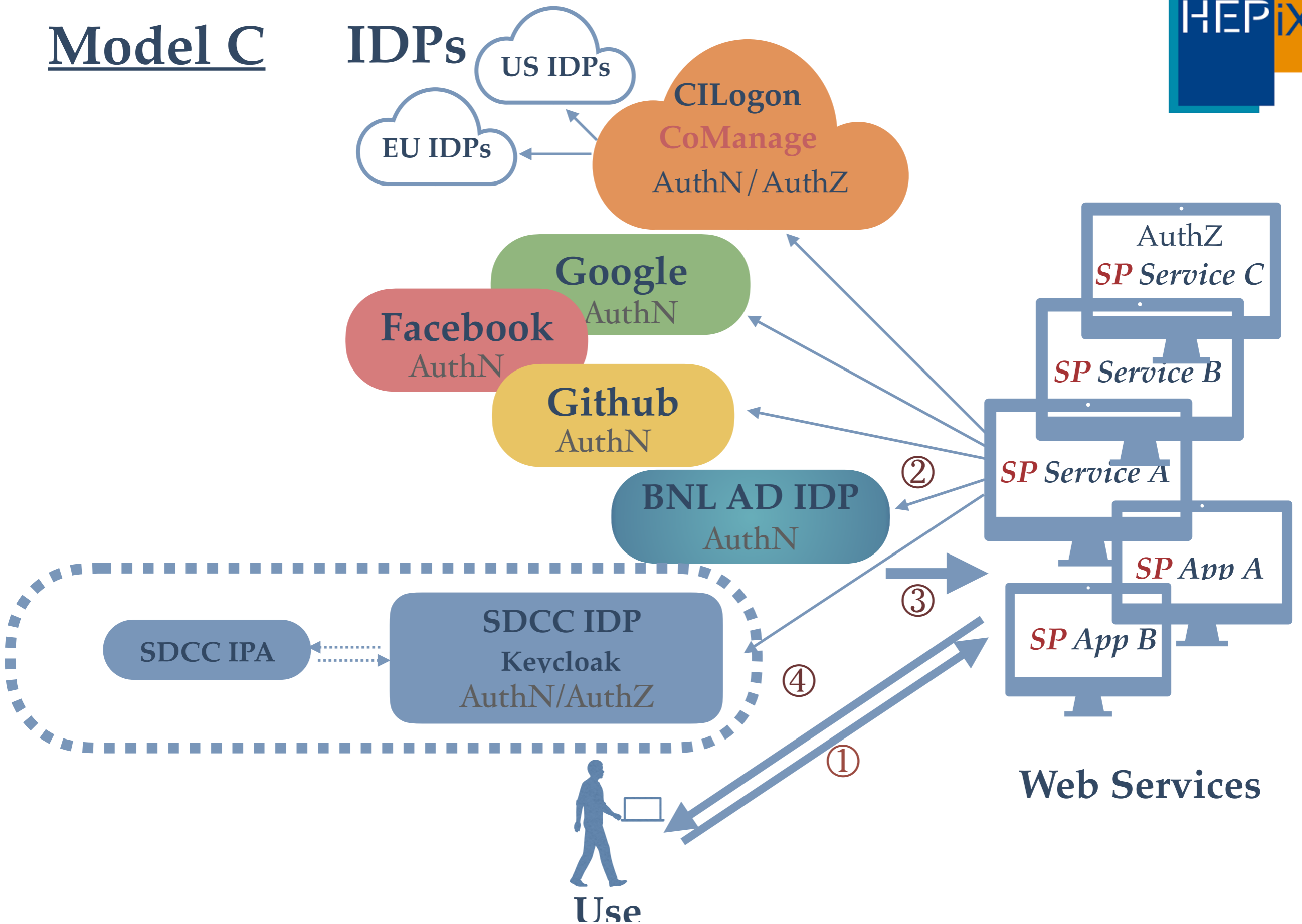
BNL Active Directory

SDCC Shibboleth IDP



Google


Model C



Example of Model C:

Log in to account

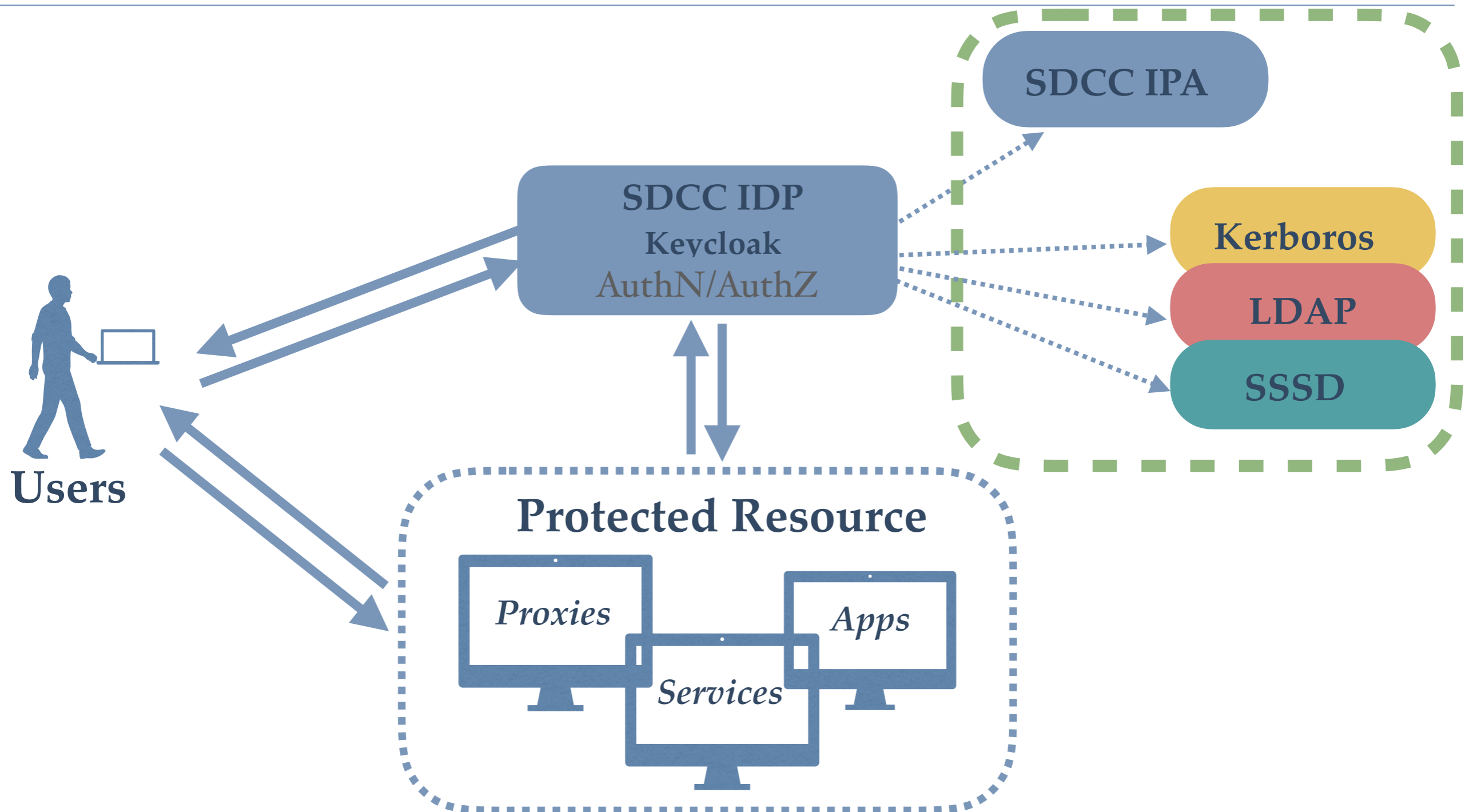
Sign in with ORCID

 Sign in with GitHub

Sign in with SDCC keycloak

Sign in with CILogon

Federation in Premises:



Linking Feature

- ❖ Link various accounts to single identity (similar approach seen in Indico, Invenio etc)
- ❖ Map Federated user accounts to local unix accounts, useful for programs (ex, Jupyterhub) require a local unix account.

Authorization

- ❖ **CoManage**:(ex, use CILogon for Federated ID Authentication)
- ❖ **Keycloak**:
 - Role-based local to Keycloak or mapped from IPA
 - Roles can be assigned per Client/Realm
 - Maps external providers attributes (ex, CoManage) to local Keycloak

Note:

* Realm is a grouping concept for apps / services who have the same AuthN requirements.

Application Support

- ❖ Invenio Instances (BNL AD +DUO)
- ❖ Jupyterhub (SDCC+ OTP)
- ❖ BNLBox (SDCC + BNL AD)
- ❖ Mattermost (SDCC now + CILogon Federated ID later)
- ❖ Ticketing
- ❖ BNL Indico
- ❖ CMS (Drupal, WordPress, Plone etc)
- ❖ Gitlab/Gitea?
- ❖ SDCC Web sites
- ❖ Experiments' Web Sites
- ❖ Etc.....

Note: Ones w/o underline is to be complete...

Issues/Improvements

- ❖ No SSO cross Realms
- ❖ IPA based OTP non-working, as a workaround, use OTP local to keycloak

Moving Forward...

- ❖ SDCC join InCommon as a standalone IDP?
- ❖ Locally hosted CoManage?

Questions?