Federated Identity Management at BNL

Fall 2020 HEPiX
October 12, 2020
Scientific Data and Computing Center (SDCC)
Shigeki Misawa

BROOKHAVEN NATIONAL LABORATORY
U.S. DEPARTMENT OF ENERGY
BROOKHAVEN SCIENCE ASSOCIATES

Background

Scientific Data and Computing Center (SDCC)

- Responsible for scientific computing at Brookhaven National Laboratory (BNL)
- Started as RHIC/ATLAS Computing Facility (RACF), supporting Nuclear and High Energy Physics experiments (NP/HEP)
- Expanding user community from groups outside of NP/HEP

SDCC Authentication Domain

- Provides authentication and authorization (AA) service for all non-grid systems/services managed by the SDCC
  - Web sites, Ssh Gateways, file service, compute servers
- Backends SDCC identity provider
- Permanent user name and uid assignment - Key feature
- Separate from the BNL campus AA service
  - Notable feature - user name and uid assignment is time limited. Keyed to the user's active status at BNL

Exciting Times for AAI at the SDCC

- SDCC identity management moved to Red Hat Identity Management Server (based on FreeIPA)
- New SDCC open source Keycloak based Identity Provider
- SDCC IdP joins the InCommon Federation
- NSLS-II requests single identity for users
- Dramatic increase in web sites requiring authentication and authorization services

SDCC Central Identity Management System

- Transition to new system completed December 2018
- Previous implementation
  - OpenLDAP - Authorization
  - MIT Kerberos - Two realms, providing authentication to two AFS cells
- New implementation
  - Red Hat IdM - Authentication and authorization (based on FreeIPA)
  - Single Kerberos realm - supporting existing two AFS cells
- Instituting new password policy, in progress now
  - Conform to new cybersecurity policy
  - 16 character minimum length
  - Continuous comparison with known compromised password list

New SDCC Identity Provider

- Based on Keycloak open source identity management system
- Backended by the SDCC central identity management system
- Online since June 2019
- Replaces legacy Shibboleth based facility single sign on IdP
  - Migration of web sites off Shibboleth IdP and SPs in progress
- Supports both SAML 2, OIDC, and OAuth 2
- New IdP is federated with InCommon (May 2020)
  - Provides federated identity for researchers at the SDCC
- Utilizes OTP capabilities included in Keycloak for multi-factor authentication (MFA) required by cybersecurity policy

Next Major AAI Challenge

- SDCC user population expected to more than double
  - Influx of users from the National Synchrotron Light Source II (NSLS-II) facility at BNL
- NSLS-II part of the BNL campus AA domain
- NSLS-II has requested single identity for their users
- BNL campus authentication
  - Based on Microsoft Active Directory
  - Utilizes Duo for multi-factor authentication
  - Operates an IdP federated with InCommon
  - AA service for VPN and Ssh gateways used by by NSLS-II users

Integrating NSLS-II into SDCC

- Plans for NSLS-II user integration at SDCC in development
- Short term plan
  - Place NSLS-II compute resources at SDCC within the BNL AA domain
  - Quantify extent of user name, uid, group name, and gid conflicts between BNL and SDCC AA domains
  - Implement mechanism to prevent the creation of new conflicting identities
  - Develop a plan to eliminate existing conflicts
- Long term plan
  - Currently investigating options ranging from federation to unification
  - Major issue - MFA for non-web services
  - Web services solved by federation with BNL IdP

AA Services for Web

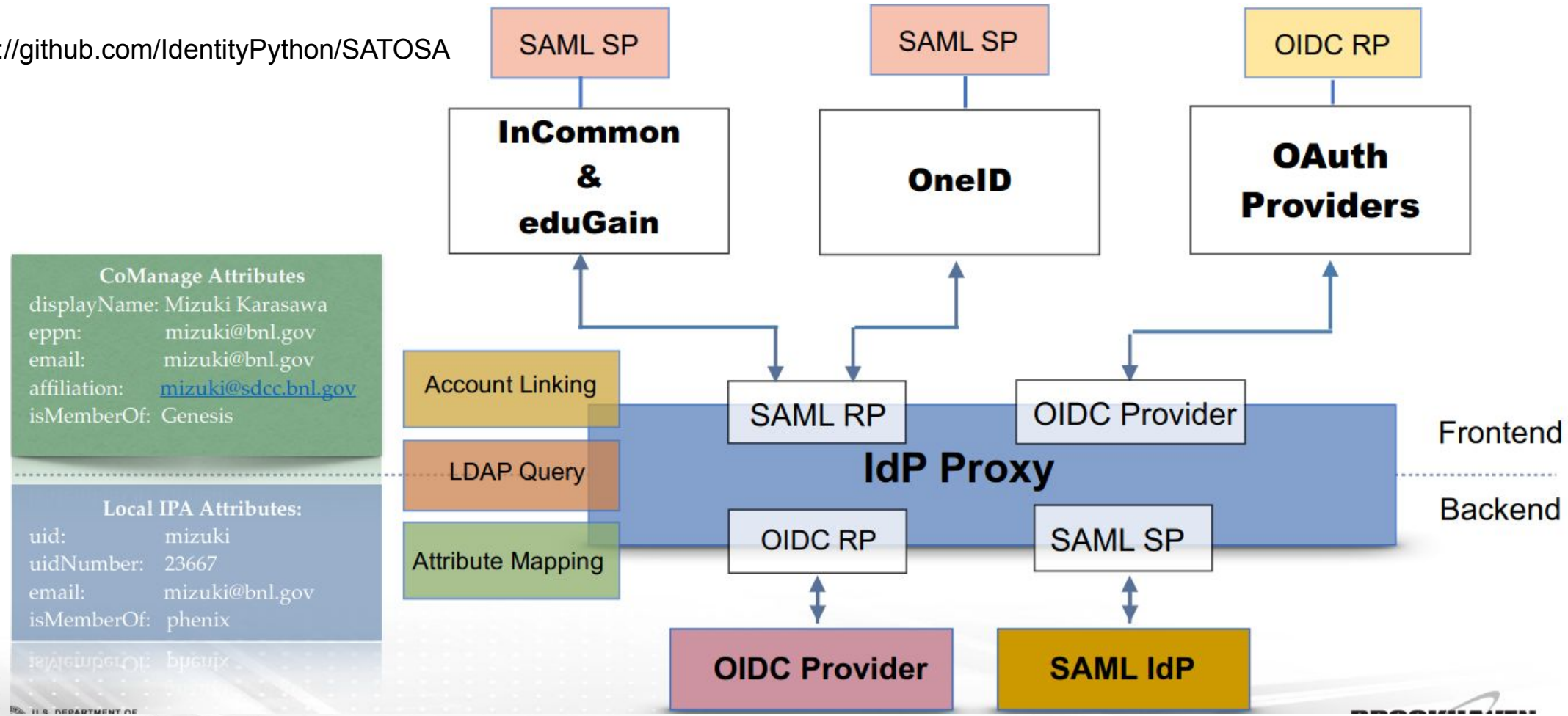
- Increase in demand for centralized AA services for web based applications
- Dramatic increase in demand for federated identity capability
- Need to address multiple AA issues to satisfy demand
  - Support OIDC relying parties, in addition to SAML service providers
  - Support for applications using “legacy” AA mechanisms
  - Provide an authorization solution for web applications
  - Support a range of applications requiring different “levels of assurance”

AA Design Patterns in Use

- IdP Proxy
  - SATOSA proxy
  - Keycloak identity brokering
- SP Proxy
  - w/ Delegation of Authentication
  - Relieves web application of authentication details
  - Web application receives user identity from SP proxy
- CiLogon/CoManage
  - Fine grained authorization (AuthZ)

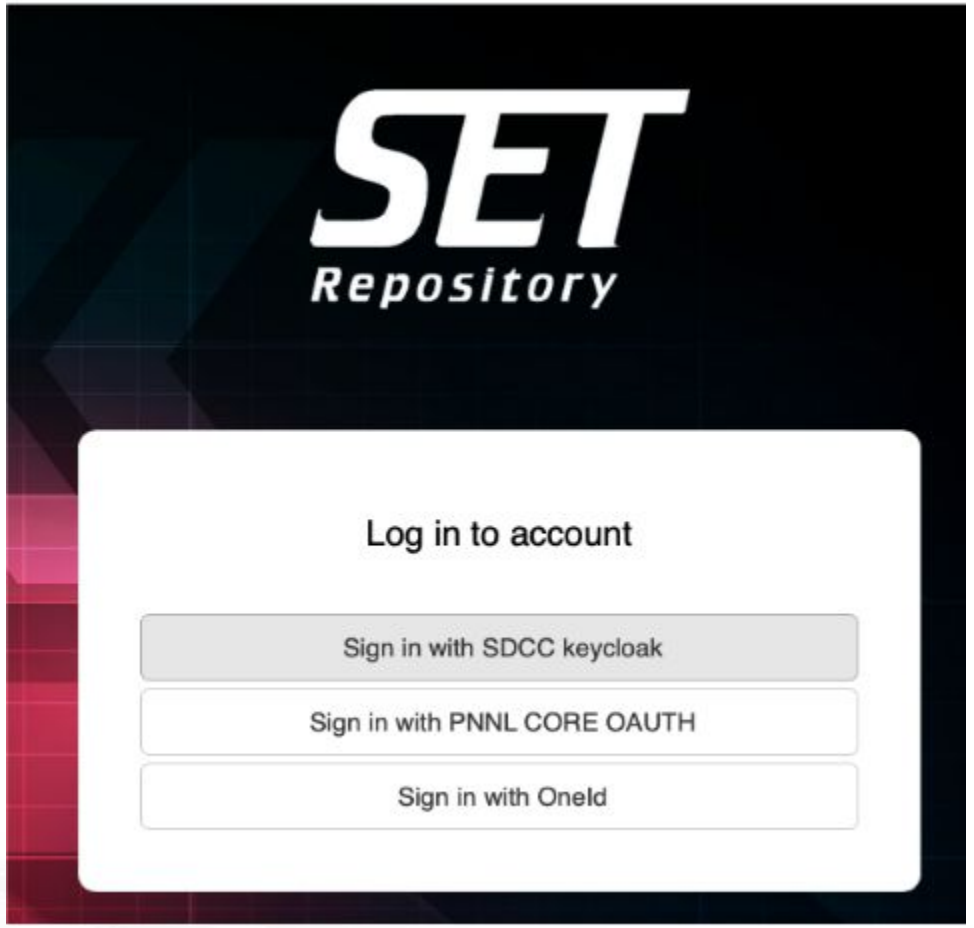
SATOSA Proxy

https://github.com/IdentityPython/SATOSA



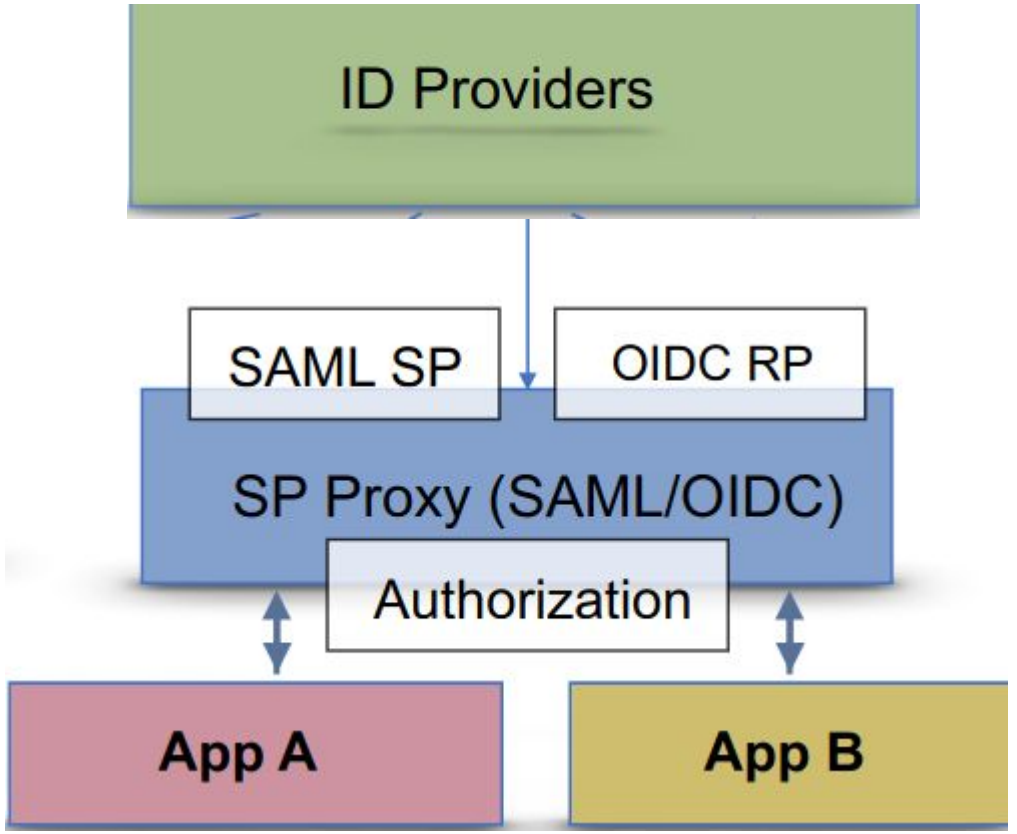
KeyCloak Identity Brokering

- SET Project archives
  - Application is an OIDC client
  - Accepts authentication via SAML and OIDC IdP
  - Keycloak translates between SAML IdPs and OIDC client
- BNLBox local cloud storage
  - BNLBox application is SAML SP
  - Keycloak enables access to BNLBox with BNL or SDCC IdP credentials



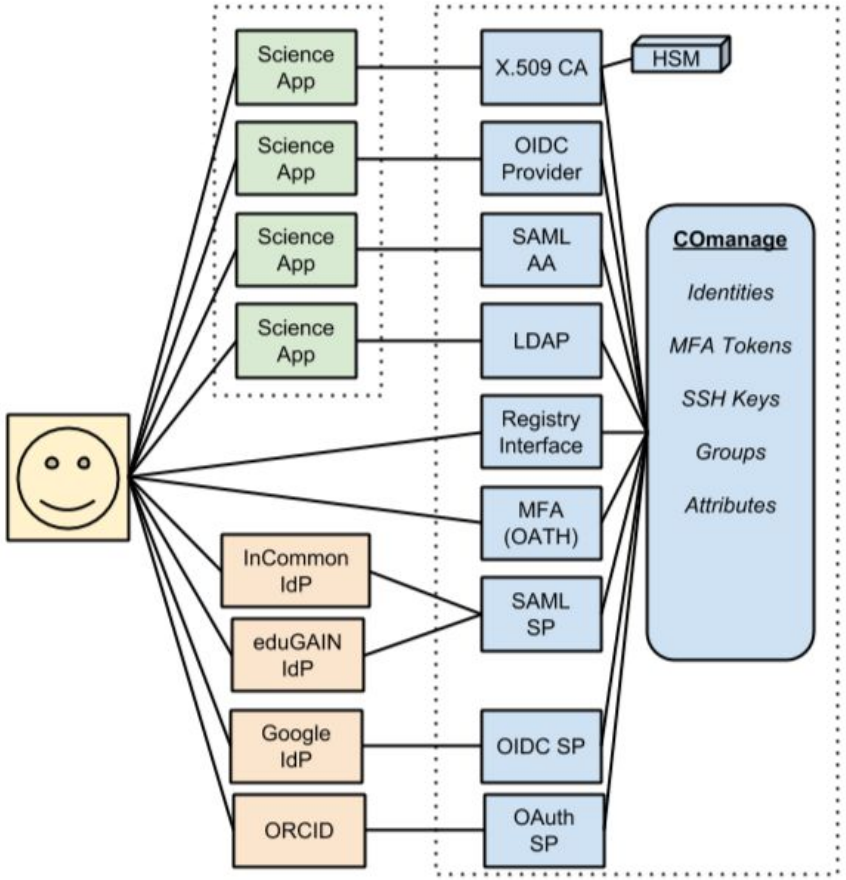
SP Proxy

- Application delegates authentication to SP proxy
  - Application receives user identity from SP proxy
  - mod_auth_openidc used for OIDC
  - mod_auth_mellon used for SAML
- Applications utilizing SP proxy
  - SDCC Jupyter
  - sPhenix, Phenix, and EIC Phonebooks
  - Facility monitoring, configuration management and other SDCC internal website



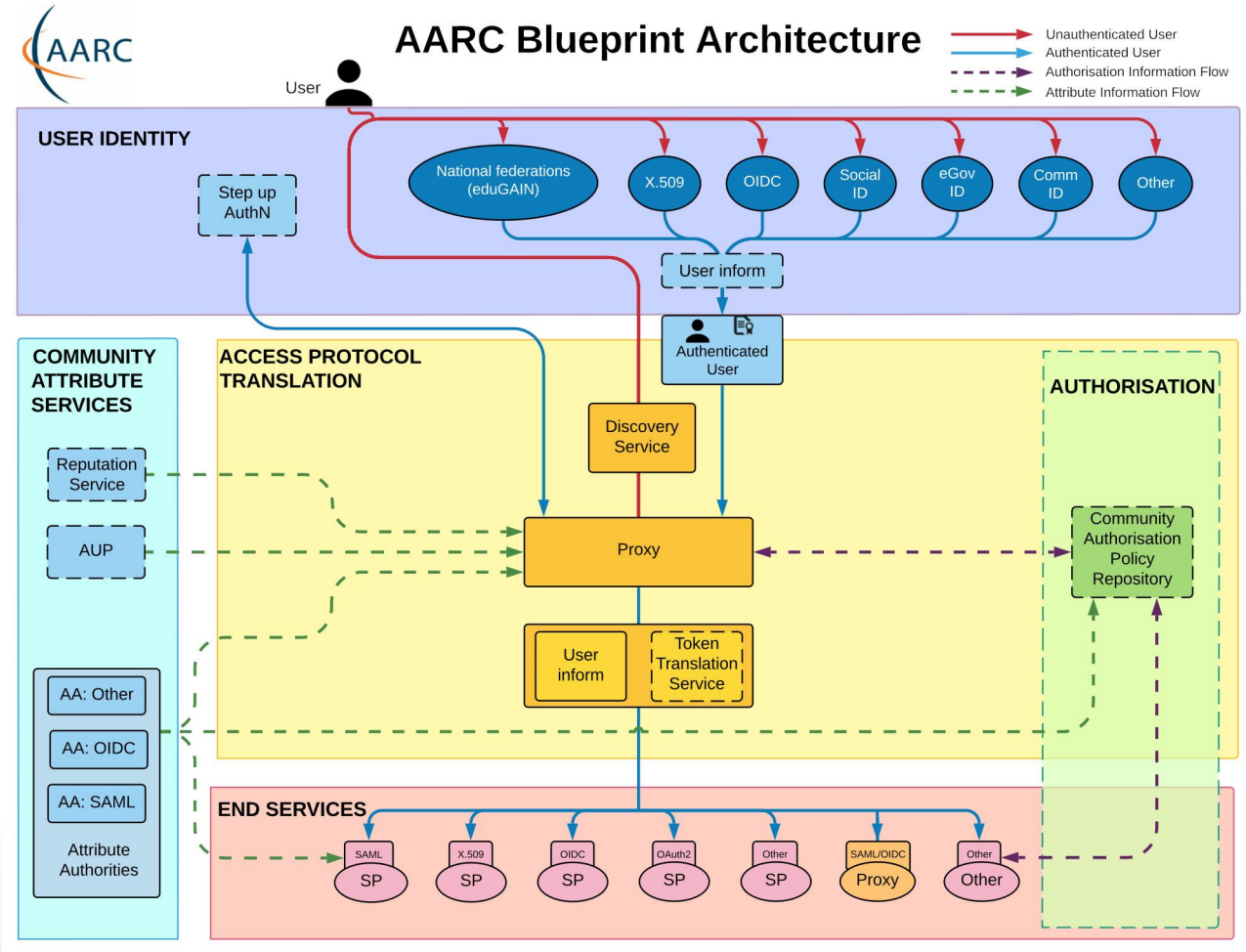
Use of CoManage for Authorization

- Cloud and local CoManage servers tested
- Cloud based CoManage for authorization for Inventio/Zenodo
  - Also for management of AuthZ groups
  - CiLogon used for authentication
  - Used by Genesis, EIC, and BNL internal Covid-19 Invenio/Zenodo archives
- US Atlas Drupal base web site
  - Manage authorization for write access
  - Authentication with CERN, SDCC, or BNL IdPs



Baseny, et. al., International Symposium on Grids & Clouds 2019, ISGC2019

AARC Blueprint as Reference Architecture



Future work

- BNL and SDCC AA interoperability
- Common MFA solution for Keycloak and FreeIPA
  - Necessary to allow the user to use the same MFA mechanism for all services, web and non-web based.
- Federation with non-InCommon id providers
  - US Department of Energy OneID
  - ORCID ID
  - Social Platforms - Google, Facebook, LinkedIn
- Possible MFA for non-web authentication, beyond ssh keys, at SDCC

Contacts

For more information on Federated Identity, identity providers, and service providers at the SDCC contact

- Mizuki Karasawa mizuki@bnl.gov