A modern approach to SSO at the RACF/SDCC

Jamal Irving
<jamal@bnl.gov>

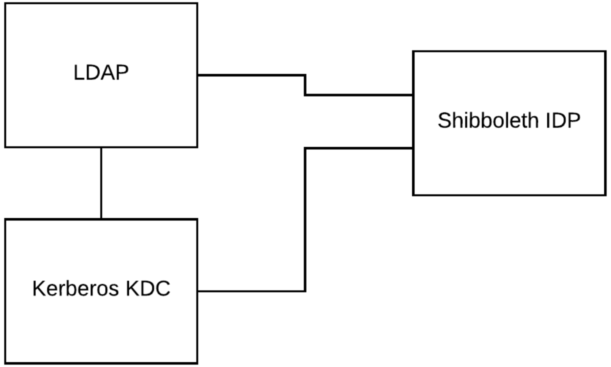
70 YEARS OF DISCOVERY
A CENTURY OF SERVICE

U.S. DEPARTMENT OF ENERGY

BROOKHAVEN NATIONAL LABORATORY

Current RACF/SDCC Infrastructure

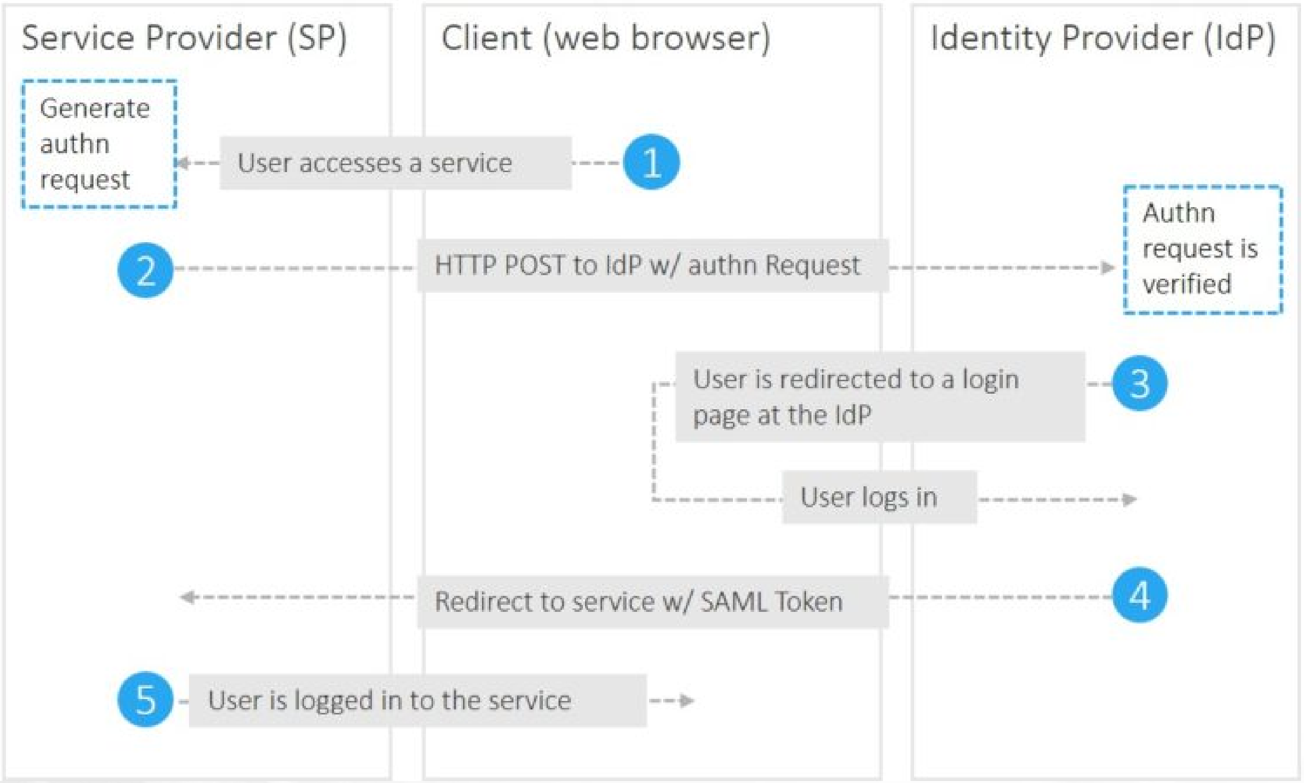
- LDAP server
  - Source of truth for user account information
  - Holds user public keys, groups, etc.
- Kerberos KDC
  - Kerberos version 5
  - Consists of 3 Kerberos realms
- Shibboleth
  - Provides browser based single sign on
  - Shibboleth identity provider corresponding to each realm



Why move to a single authentication infrastructure?

- Reduce the number of passwords users need to worry about.
  - A number of users have more than one account
- Reduce the number of Kerberos instances we have to maintain.
- Having one source of truth simplifies the user login work-flow.
- Helps to eliminate some of the lingering technical debt we have had for some time.

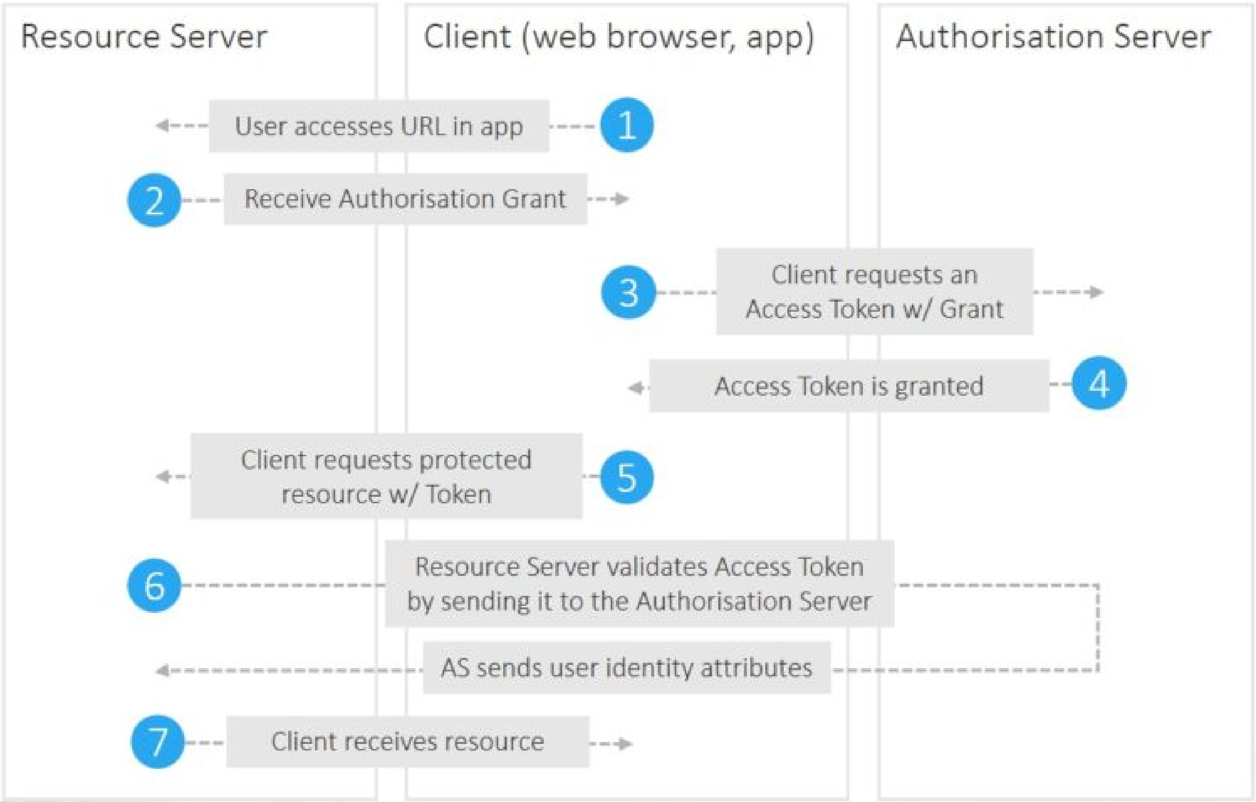
SAML 2.0 Flow



Service Provider (SP)
Client (web browser)
Identity Provider (IdP)
Generate authn request
1
User accesses a service
2
HTTP POST to IdP w/ authn Request
Authn request is verified
3
User is redirected to a login page at the IdP
User logs in
4
Redirect to service w/ SAML Token
5
User is logged in to the service

- Ubisecure diagram

OAuth 2.0 Flow



1 User accesses URL in app

2 Receive Authorisation Grant

3 Client requests an Access Token w/ Grant

4 Access Token is granted

5 Client requests protected resource w/ Token

6 Resource Server validates Access Token by sending it to the Authorisation Server

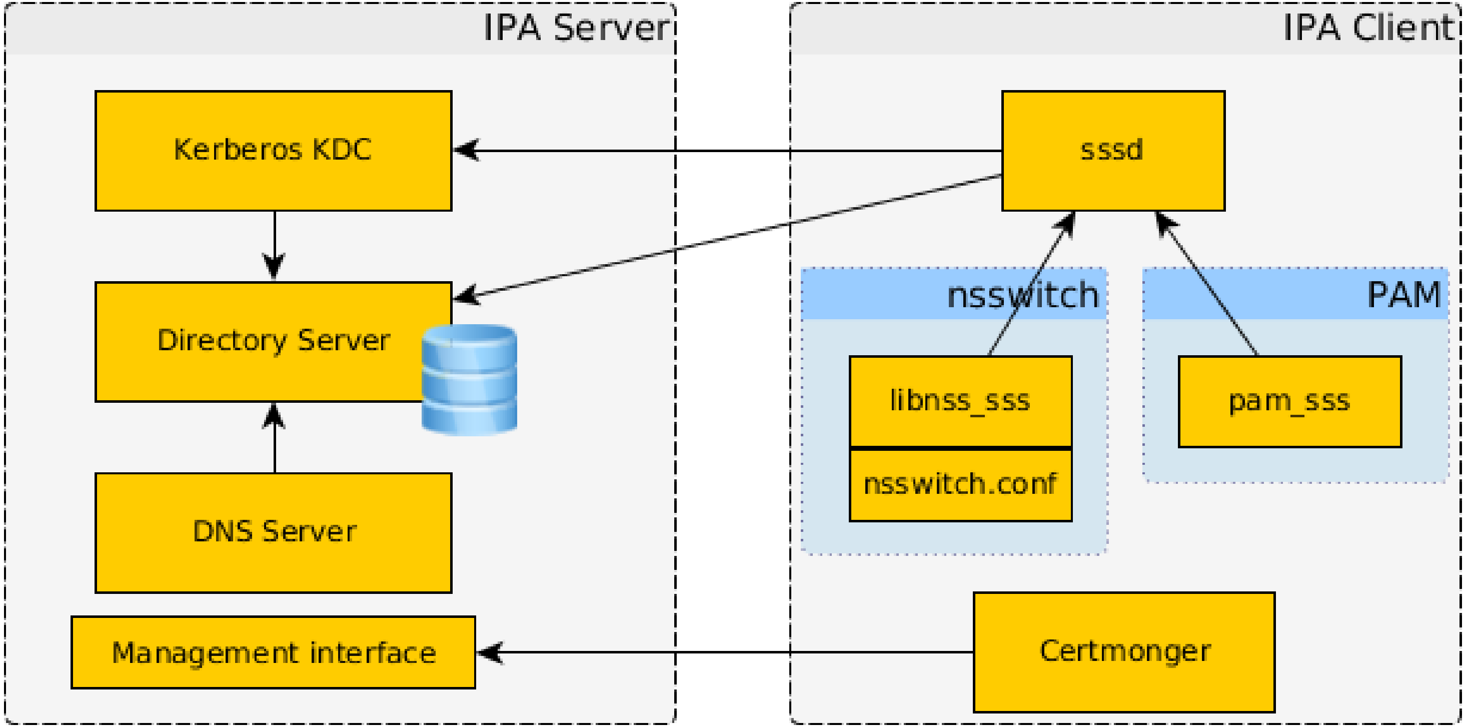
AS sends user identity attributes

7 Client receives resource

- Ubisecure diagram

Newer SSO approach

- In the process of replacing our current LDAP, Kerberos, and shibboleth instances with FreeIPA
- FreeIPA
  - Open source solution that brings LDAP, Kerberos, and identity management policies together
  - “Active Directory” for linux
- Keycloak
  - Identity management web application that supports Oauth/SAML protocols to facilitate SSO


IPA Server
Kerberos KDC
Directory Server
DNS Server
Management interface
IPA Client
sssd
nsswitch
libnss_sss
nsswitch.conf
PAM
pam_sss
Certmonger

Reasons to modernize

- Administrative burden gets reduced
- Implement open source projects that are backed by commercially viable companies
  - Ensures less down time for users b/c we are deploying production quality products
- Potential future to tie into a cross forest active directory environment
- Increase authentication strength by enabling TOTP 2FA

Modern User applications RACF/SDCC must support

Modernization Steps

- Identify parts of the old authentication and authorization system that are still needed vs. things that are obsolete. [user account attributes]
- Create a test bed infrastructure to implement proof of concepts.
- Copy all user account info from legacy LDAP infrastructure to IPA
- Set a cut off date, where all new user accounts get created in the new IPA Kerberos database

Modernization Next Steps

- Ensure that all existing users of the legacy Kerberos realms create a new password on the new IPA Kerberos database.
- New password creation can be done in 2 ways:
    - Self Service portal, which authenticates user against legacy Kerberos realm and prompts user to set up a new password.
    - Command line option, which allows a user to authenticate to a ssh gateway via their public key. User will then be able to execute a custom script which will allow them to set their new password.

Future Plans

- RACF/SDCC self hosted applications that are used within photon sciences could possibly be opened to users who do not have BNL accounts.
- Configure Keycloak to support
  - Incommon federation
  - Orcid id

Reference Links

- https://www.freeipa.org/page/Documentation
- https://www.keycloak.org/documentation.html
- https://wiki.shibboleth.net/confluence/#all-updates
- https://www.ubisecure.com/uncategorized/difference-between-saml-and-oauth/
- https://orcid.org/
- https://www.incommon.org/federation/

Questions?

Questions? Comments?

jamal@bnl.gov