IT Federation and Access Requests

Elizabeth Sexton-Kennedy

4th Meeting of the ICAC

February 9, 2021

Authentication Services at Fermilab

Benchmarking Against Other Host Labs

Comparison against CERN

CERN

- A Single Sign-On service with SAML, OIDC, and social logon
- Kerberos and LDAP services
- A Users Portal, where users can manage their own accounts.
- A Groups Portal
- An Applications Portal
- API for users, groups and applications management

FNAL

- A Single Sign-On service with SAML, OIDC~~, and social logon~~[4]
- Kerberos and LDAP services
- A Users Portal, where users can manage their own accounts.[5]
- A Groups Portal (Coming soon)[6]
- ~~An Applications Portal~~ Service Now[7]
- ~~API for users,~~ groups ~~and applications management~~[8]

Current Services

Fermilab Authentication Services Overview

- A Microsoft Active Directory domain for Windows servers, desktops, and laptops
- A MIT Kerberos realm for *nix-based servers, desktops, and laptops
- A LDAP service based on a Microsoft Active Directory domain
- A Single Sign-On service based on PingFederate
  - SSO Authentication can be LDAP, Kerberos, CILogon Certificates[1], InCommon IdPs[2], or Fermi Lightweight Accounts[3]

Related Services

- Eduroam federated authentication service for wireless access
- Multi-factor authentication based on RSA SecurID and Yubikey (PIV). MFA can be integrated with SSO and Active Directory as needed

Planned Enhancements – Multi-Factor Authentication

- Expand options for MFA in our SSO environment with the implementation of PrivacyIdea
  - Token options
    - PrivacyIdea supports both free and commercial tokens
      - Token selection is dependent on approval from CyberSecurity
      - End user can choose the token(s) they wish to use and self-register
- SSH Integration
    - SSH at the lab does not currently support MFA. To align with executive order requiring access to more systems enforce MFA, PrivacyIdea will make this easier to implement.
    - PrivacyIdea supports two methods for adding a second factor to SSH connections.

Planned Enhancements - Grouper

- Web based group management tool for central authentication services
  - Simplify end user activities
  - Using grouper to manage groups will reduce the number of people with administrative permissions in Active Directory.
- Will investigate consumption of group memberships from Ferry
  - Integrate into SSO assertions
  - CERN eGroup membership not released through the SAML assertions. It maybe possible to add VO information to the CernRoles field
  - Jeny Teheran is working with Paolo Tedesco from CERN and our AAI group

Planned Enhancements - Federation

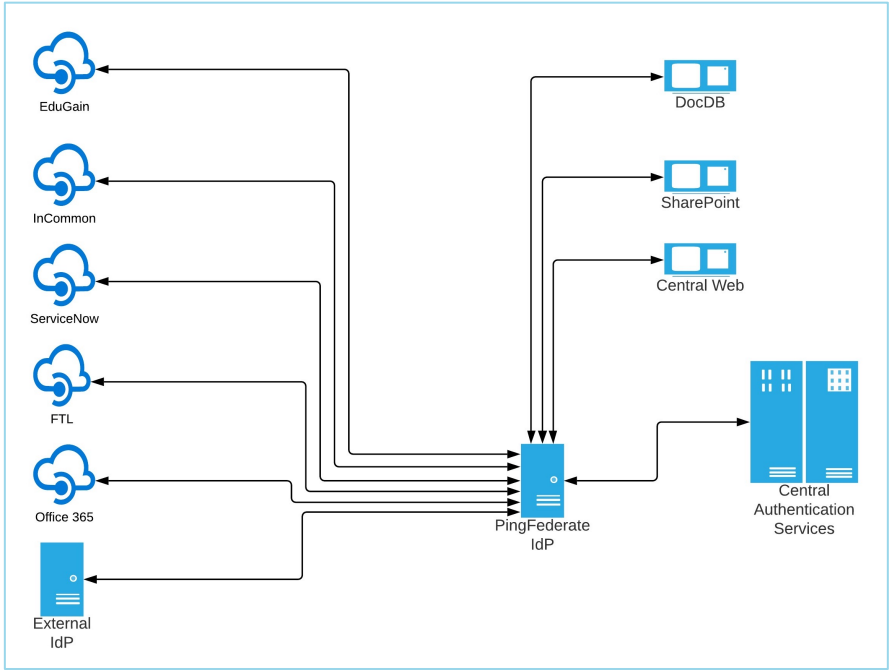
- An effort is underway to investigate allowing both OAuth and SAML access to Service Providers enabled for external federation. (Indico, DocDB, SharePoint, Central Web, etc)
- Enable Fermilab credentials for accessing EduGain and InCommon resources
  - Investigating use of a Shibboleth based Identity Provider service
    - Shibboleth – external federations
    - PingFederate – FNAL hosted service providers

5

Planned Enhancements - Federation

SSO Changes

- The current environment
  - PingFederate is used as the Identity Provider (IdP) for FNAL hosted Service Providers (SP), external SPs, and as the federation hub for external IdPs

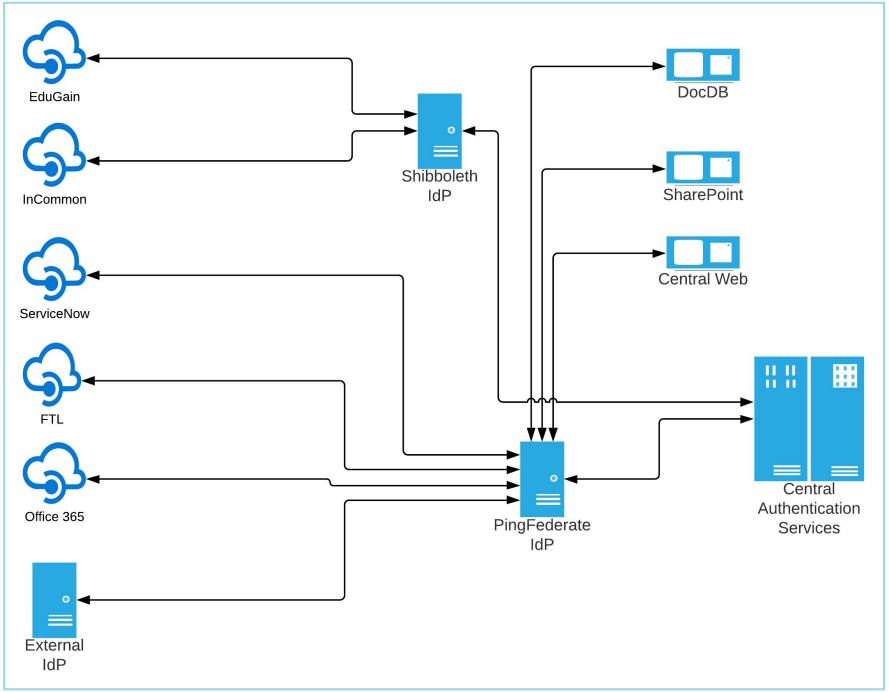


Fermilab

6

Planned Enhancements - Federation SSO Changes

- The proposed environment
  - PingFederate is used as the IdP for FNAL hosted SPs, and as the federation hub for external IdPs
  - A Shibboleth based service is provisioned to act as the IdP for FNAL identities for SPs in external federations



Fermilab

Fermilab Physical and Logical Access

Fermilab Access Renewal Process

The access renewal request is done in two parts:

- **ServiceNow** – User requests a renewal, answers a number of questions, uploads CV and submits the request
- **FermiWorks** – User receives a notification to complete their request in FermiWorks. Logs into FermiWorks (with a separate username and password), answers some PII questions, uploads a picture of an identity document, and confirms that they have read several policy/training documents.

Currently, a renewal request asks the same questions as a new access request, with no pre-filled answers.

- This is largely because when this process was deployed, there were many new US Federal government and DOE requirements, resulting in most people not having answers to the required questions in any of our systems.

Now that the request process has been in place for a while, we are looking into streamlining renewals for users who:

- Have active access to Fermilab (onsite or offsite)
- Can log in to ServiceNow using their Services account, so they are authenticated at the time of submission

Potential Form Enhancements

- ServiceNow form
  - Pre-fill most answers from the previous request. User will have an option of changing any of them.
  - Exceptions – questions that will need to be answered each time:
    - Citizenship
    - New access dates
    - CV (?)
    - Any place the previous answer is no longer applicable (e.g. previous Fermilab point of contact is no longer at the lab)
- FermiWorks form
  - Some of the questions may be skipped if the previous access request is less than a year old.

Potential Additional Improvements

- Better communication
  - Set expectations for how much time people should set aside for filling out these forms.
- Better help for people who forgot their password
  - Access to Password reset tool with other credentials than RSA/YubiKey token. (e.g., CILogon)
  - Instructions added to the password reset tool for how to change FermiWorks password.
- SSO for FermiWorks
  - This has had some technology roadblocks but is under active consideration.

Question 1 - Tokens **AND** X509 proxies

- The GlideinWMS infrastructure could send either token's or x509 proxies to CE's depending on what they require. Our factory/fronend will be configured to send the appropriate credential to make sure we don't lose access to any sites. These are "infrastructure" credentials (aka NOT user tokens/proxies).
- That gets a glidein started that can then authenticate back with that credential to accept a job. A user job then with user credentials would run in that slot. This credential is only used for example to transfer data files in or out of the job. Whether using an x509 proxy or a token, the credential is contained in a file. You of course must have a client available that can use the credential you have but that could be provided via cvmfs or even possibly in the job tarball. But if there is a need, we can send both a token and an x509 proxy with a job so the user job could use either/both within the job.
- Mine confirms there is no deadline for when we have to stop issuing certificates. We can keep generating them as long as we need them.
- We need to test whether sending tokens and certificates together would break any European sites. We don’t expect it will.
  - Officially we’ll be ready to test in 3mo.
  - Ken is actively working on it.