IT Federation and Access Requests

Elizabeth Sexton-Kennedy

4th Meeting of the ICAC

February 9, 2021

Fermilab Physical and Logical Access

Policy Evolution Backdrop

- No one will deny that cyber attackers have become more numerous and more sophisticated. Some are even state actors…
- Government owned facilities have become a target.
- My vision is that we counter this by “circling the wagons”
  - Information for public consumption has to be vetted as safe to release
  - If it is not for the public, it is restricted to a group. There is safety within the group
  - Of course, this means we have to identify you
  - Leads to privacy concerns
- Easiest for Fermilab – allow access to fully vetted users/associatiates
- Difficult for users/associates to obtain and retain these credentials
  - In a meeting with Spokespeople, I was told to concentrate on streamlining renewals
  - Requirements are only going to get harder, HPD12 for instance
- All of this is affected by privacy concerns

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    - Any place the previous answer is no longer applicable (e.g. previous Fermilab point of contact is no longer at the lab)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.

Additional Enhancements

- Better communication
  - Set expectations for how much time people should set aside for filling out these forms.
  - Document where it is possible to save state and come back later.
- 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.

Authentication Services at Fermilab

Benchmarking Against Other Host Labs

Comparison against CERN

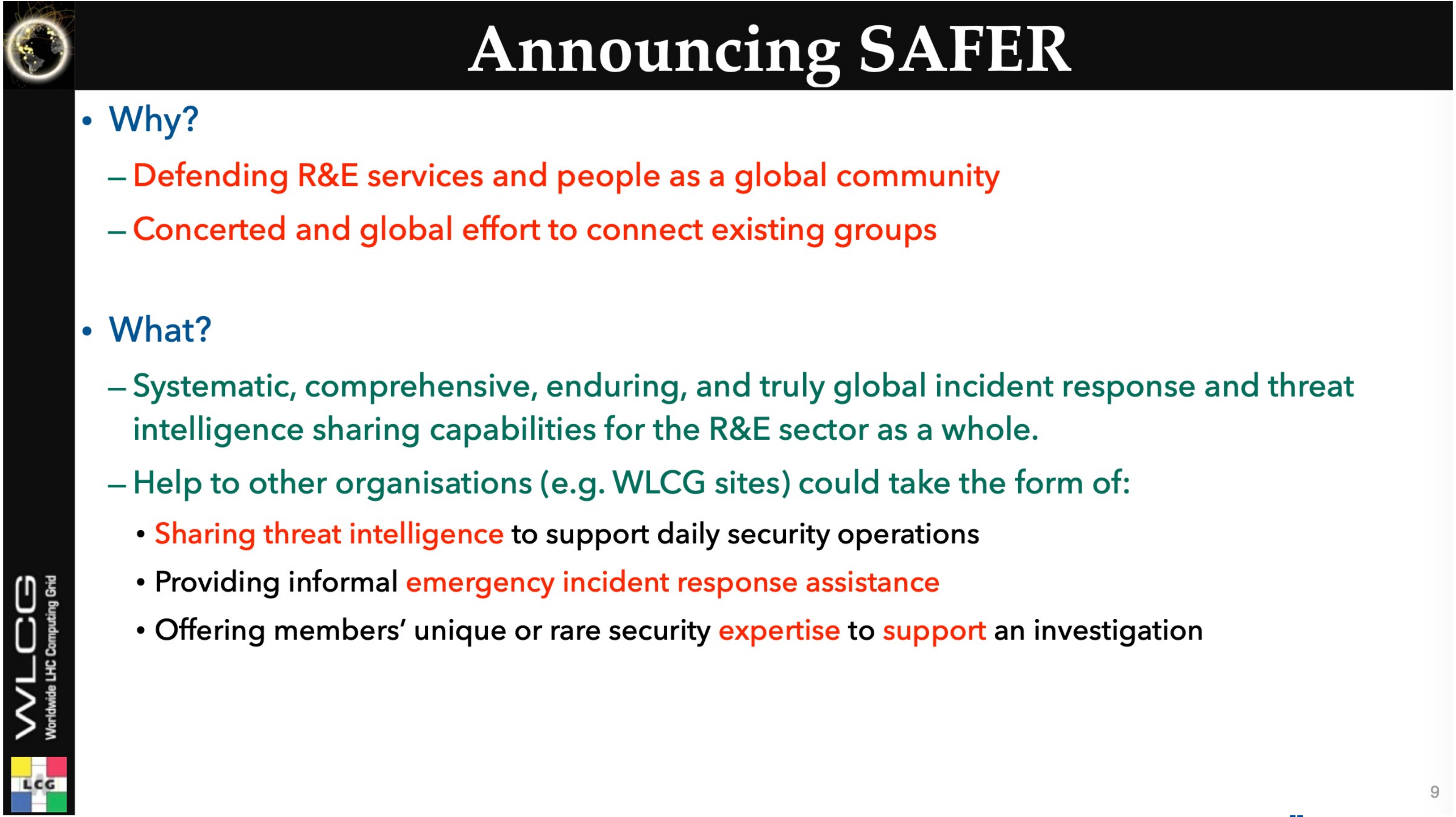
CERN

- 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

WLCG SAFER program

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]



Announcing SAFER

- Why?
  - Defending R&E services and people as a global community
  - Concerted and global effort to connect existing groups
- What?
  - Systematic, comprehensive, enduring, and truly global incident response and threat intelligence sharing capabilities for the R&E sector as a whole.
  - Help to other organisations (e.g. WLCG sites) could take the form of:
    - Sharing threat intelligence to support daily security operations
    - Providing informal emergency incident response assistance
    - Offering members' unique or rare security expertise to support an investigation

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]
  - Currently we trust CERN and DOE IdPs

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 – unspecified timeline

Planned Enhancements – Inbound Federation

- An effort is underway to investigate allowing both OAuth and SAML access to Fermilab Service Providers enabled for external federation. (Indico, DocDB, SharePoint, Central Web, etc)
- Goal: CMS/DUNE collaborator would be recognized by Fermilab services as having access to their respective collaboration’s information.
- Issue: Federated Identities from CERN do not contain VO information
- CERN eGroup membership not released through the SAML assertions
    - Jeny Teheran is working with Paolo Tedesco from CERN and our AAI group
- Will investigate a number of options to solve this, to date there is no clear option, all have pros and cons

Planned Enhancements – Outbound Federation

- 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

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.

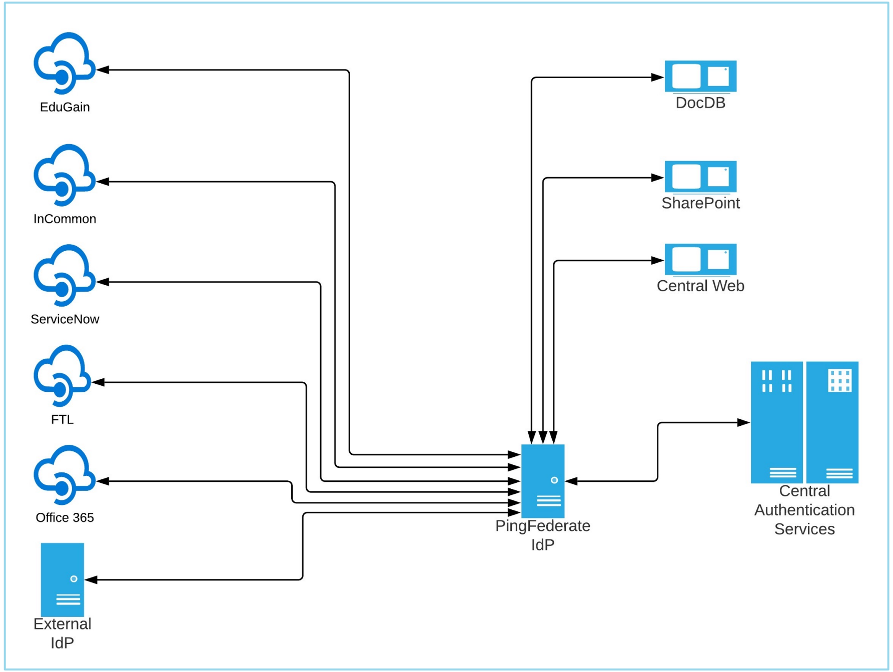
Planned Enhancements – Multi-Factor Authentication

- 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.

Backup

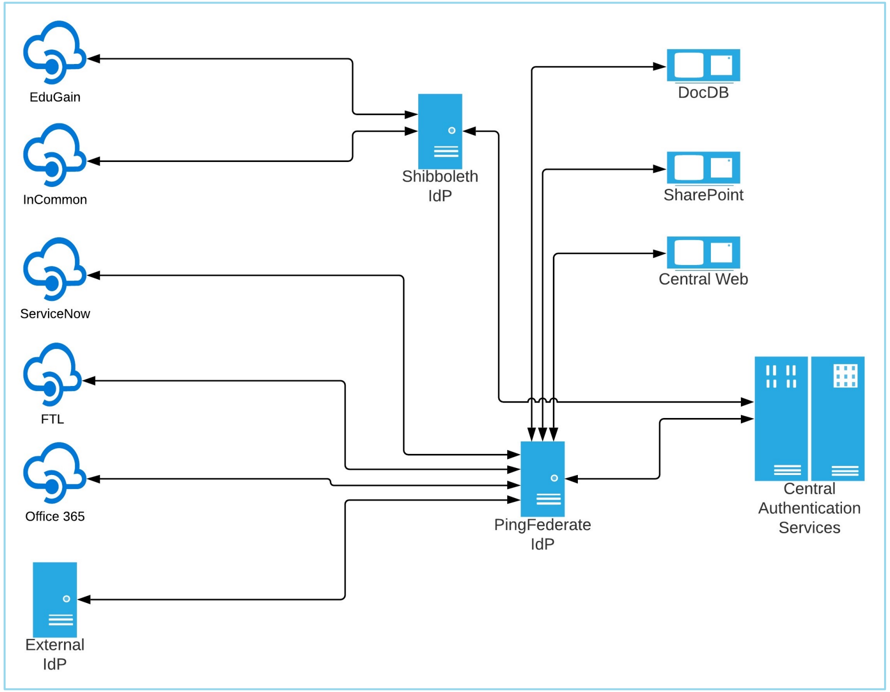
Planned Enhancements - Federation SSO Changes

- 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



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


EduGain
InCommon
ServiceNow
FTL
Office 365
External IdP
Shibboleth IdP
DocDB
SharePoint
Central Web
PingFederate IdP
Central Authentication Services