Federated Identities Update

Mine Altunay

October 3, 2019

Outline

- Goals
- Deliverables
- Available Resources
- Current Status

Goals

- Integrate Fermilab infrastructure with Federated identity and access tokens, i.e. replace certificates with tokens
- 2 sub-goals:
  1) Allowing external users access Fermilab resources (incoming)
  2) Enabling Fermilab users access external resources (outgoing)
- Goal #1 entails how to trust, recognize and process incoming identity and access credentials, determining the right authorization level from a user's access token.
- Goal #2 entails how to build and operate a system where we can generate identity and access tokens, how to distribute these tokens to our users, and which attributes to insert into the tokens.

Deliverables

Deliverables	Status	End Date
1. Architectural Design Document	In progress	Jan 2020
2. Selection of Token Issuer services and a contract with the hosting organization	In progress	July 2020
3. Decision over expressing group memberships	In progress	Nov 2019
4. A library plugin to process group membership attribute	Still researching	July 2020
5. Integrating Fermilab attribute repository Ferry with the selected Token Issuer interconnection services	Not started	Dec 2020
6. Integration of SciToken libraries with SCD services to process access tokens.	Not started	July 2021

Deliverables

Deliverables	Status	End Date
7. Token Translation Service	Not started	Aug 2021
8. Client-side tools to request and obtain tokens	Not started	Dec 2021
9. CERN account users can access DocDB and Fermipoint	Completed	Sept 2019
10: A Transition Plan to switch from certificates to access tokens.	Not started	July 2021

Effort and Resources

- Deliverables 4, 5, 6 and 8 will require significant effort from the SCD.
  - 4) A library plugin to process group membership attribute -- still in research mode
  - 5) Integrating Fermilab attribute repository Ferry with the selected Token Issuer interconnection services -- depends on #1 and #2
  - 6) Integration of SciToken libraries with SCD services to process access tokens -- not started
  - 8) Client-side tools to request and obtain tokens -- not started
- #6 will impact all service providers in SCD. Any service that uses certificates for authentication and authorization will need to integrate with SciToken libraries.
- #4 will require a python developer who understands the token schemas and Scitoken libraries

Effort and Resources

- #5 will require a developer (possibly python) who understands OAuth, OIDC, Ferry.
- #8 will require a python developer who understands the token schemas, and the OAuth OIDC flows
- All tasks require expertise and some background on federation technologies.
- Liz promised us 2 FTE. We need to spend this effort on highly technical developers who can handle federation technologies

Current Status

- Created the Project Scope document at https://fermipoint.fnal.gov/project/authfed/_layouts/15/WopiFrame.aspx?sourcedoc=/project/authfed/Project%20Documents/Fed%20Auth%20Scope%20Statement%20draft.docx&action=default
- Working on the Architecture document
- Arranging a series of meetings to disseminate information about the architecture and collect questions from the community
- We should form a list of stakeholders and invite them to these meetings.
- As a side note, work on the CCD side has been paused due to effort allocated to more urgent projects.

Current Status

- At this point, we are fairly confident that we will use the Token Issuer services (for creating access tokens) provided under the CILogon umbrella project at NCSA of Univ of Illinois.
- Building and maintaining our own Token Service is not our expertise and will cause us significant time and effort
- CILogon project at NCSA currently provides a OIDC Token Issuer with group attributes (ID token+group attribute), and LDAP server and a COManage service.
- If we make a request, they can also add 2 additional types of Token Issuers which can create: a) access tokens with groups and b) access tokens with authorization scopes.
- There are very good reasons for these different Token Issuer types due to WLCG Token Schema and being able to express group membership attributes.
- It will take far longer than 5 minutes to explain all this

Current Status

- CILogon subscription model:
- Basic Authentication Services (OIDC, X.509) -- Free
- Basic Multi-tenant Collaboration Management Services (COmanage, LDAP, OIDC Provider, InCommon SAML Provider, X.509 CA) - $1200 per year
- Full Service Production (dedicated service instances, add-on services, custom plugins, SAML proxy, SAML AA) - $20,000 per year
- We probably will need the full service production.