FERMILAB-SLIDES-18-105-CD

Centralized Authorization in Non-Uniform Federation

Communities of Interest

Olga Terlyga

NLIT 2018

May 22, 2018

This manuscript has been authored by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy, Office of Science, Office of High Energy Physics.

Centralized Authorization

- Why do we care?

- What should we do?

(Semi) Open Science

Scientific process is based on free exchange of ideas.

Scientific collaborations require us to be more **open** than ever, while emphasis on cyber security puts pressure to become more **closed off**.

The role of IT is to enable exchange of ideas and data balanced with security concerns.

Non-Scientific resources

Exchange of information happens and is necessary in many other areas of Laboratory operations

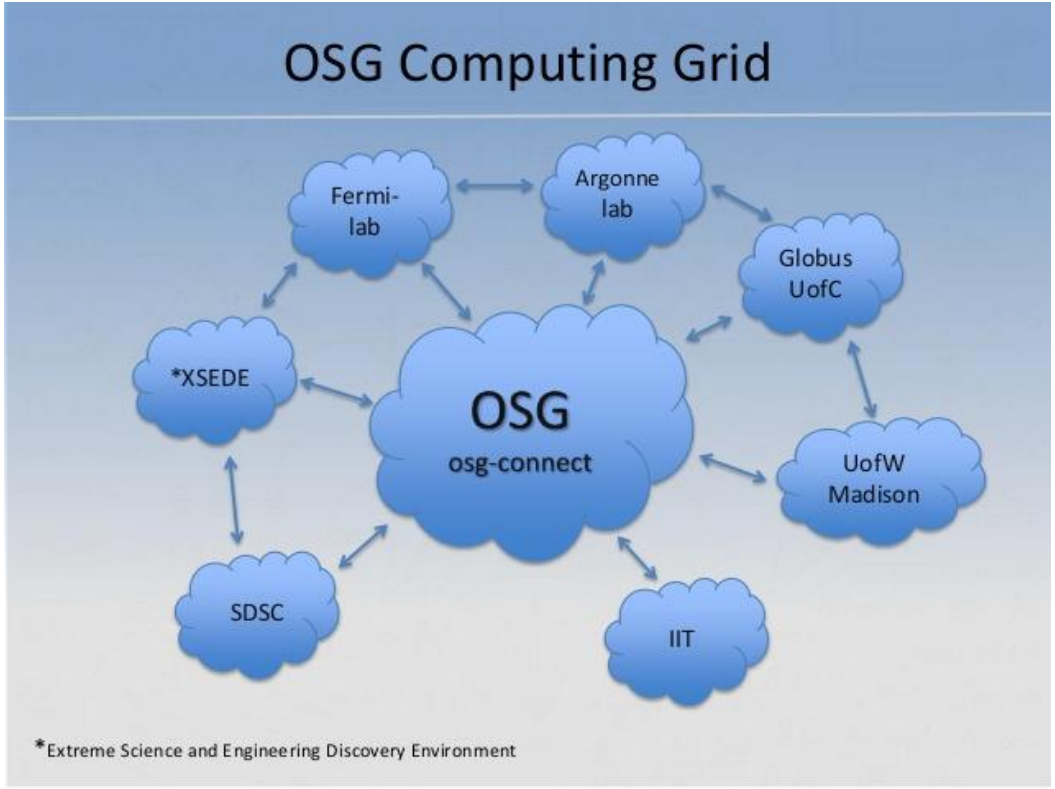
Global collaboration era

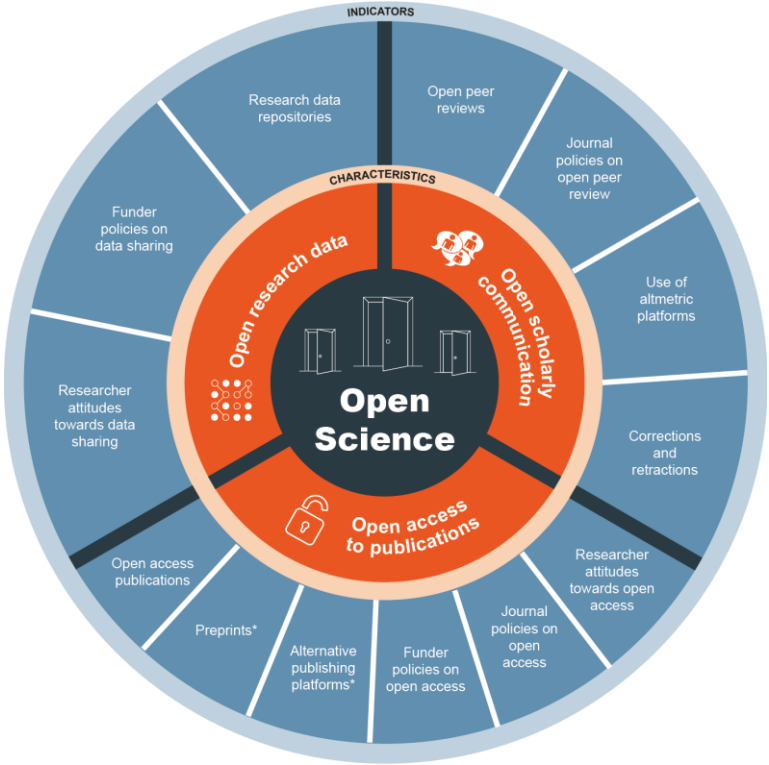
- Centro Brasileiro de Pesquisa...
- Aligarh Muslim University Hor...
- Fermilab
- University of Florida
- University of Geneva
- Universidad De Guanajuato
- Hampton University
- Massachusetts College Of Li...
- Indian Institute of Science Ed...
- Northwestern University
- Oregon State University
- Otterbein University
- Pontifical Catholic University ...
- University of Pittsburgh
- University of Rochester
- Rutgers–New Brunswick
- Tufts University
- University of Minnesota Duluth
- National University of Engine...
- Universidad Técnica Federico...
- Ewell Hall
- University of Oxford
- University of Mississippi
- University of Pennsylvania
- University of Wrocław

MINERVA collaboration

Fermilab

Global collaboration era

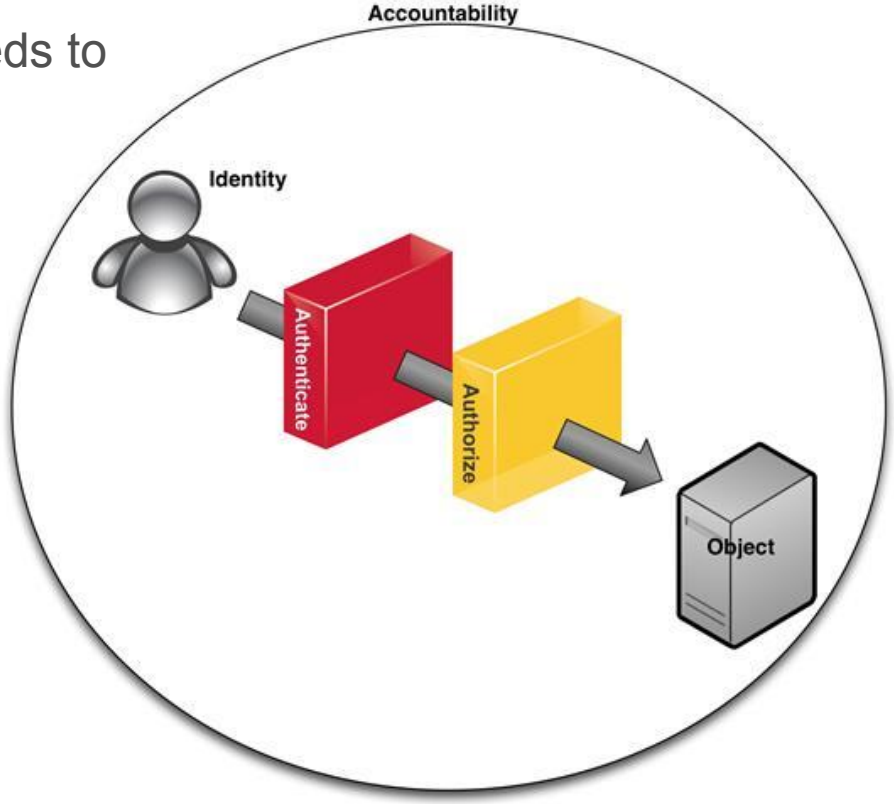




Fermilab

Access = Authentication + Authorization

Access **always** needs to be managed



Even open science is not 100% open

Fermilab

On Premise => More Control

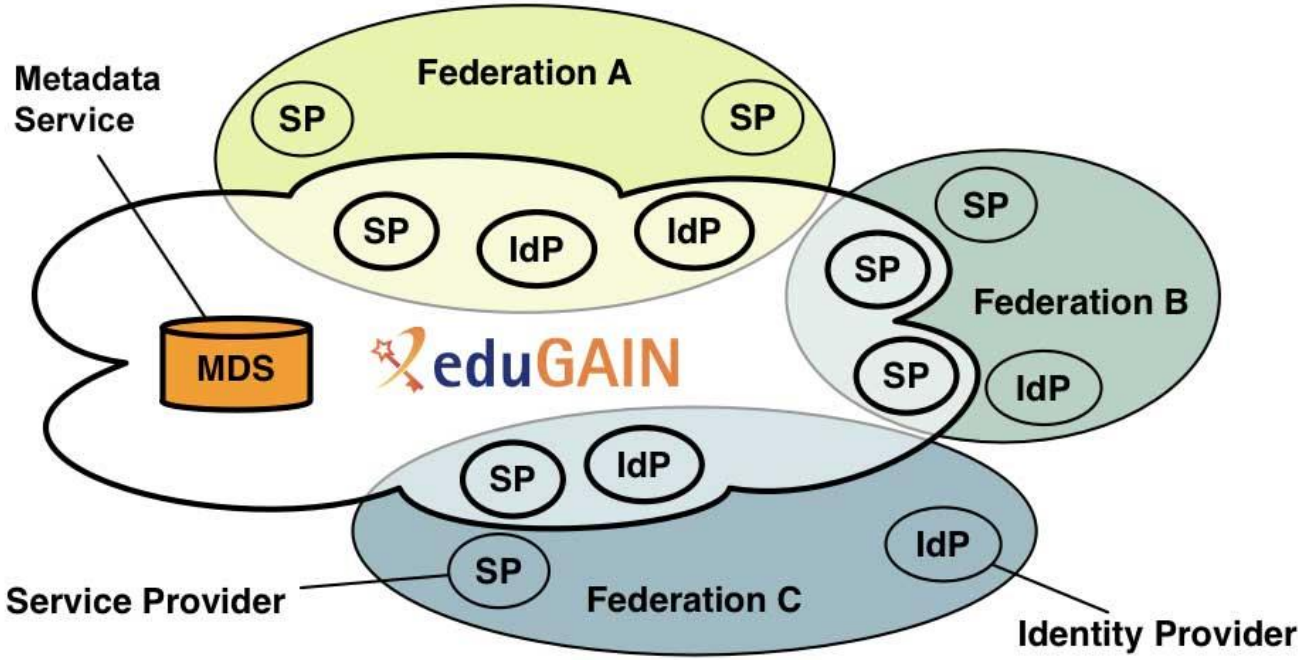
- On premise authentication
  - Typically Single Sign-On
  - Maybe LDAP
  - …
- On premise authorization
  - Active Directory Security groups
  - Individual Service Provider's Database
  - Identity Management
  - …

On Premise => Constraints

- Users don’t want to maintain another set of credentials
  - Passwords
  - Usernames
  - Registration process
- Admins don’t want to maintain another set of credentials
  - Expirations dates
  - Source of truth
  - HR involved in registration process
  - Short lived accounts
  - Price?

Federation

Each person is uniquely identified within organization and within Federation



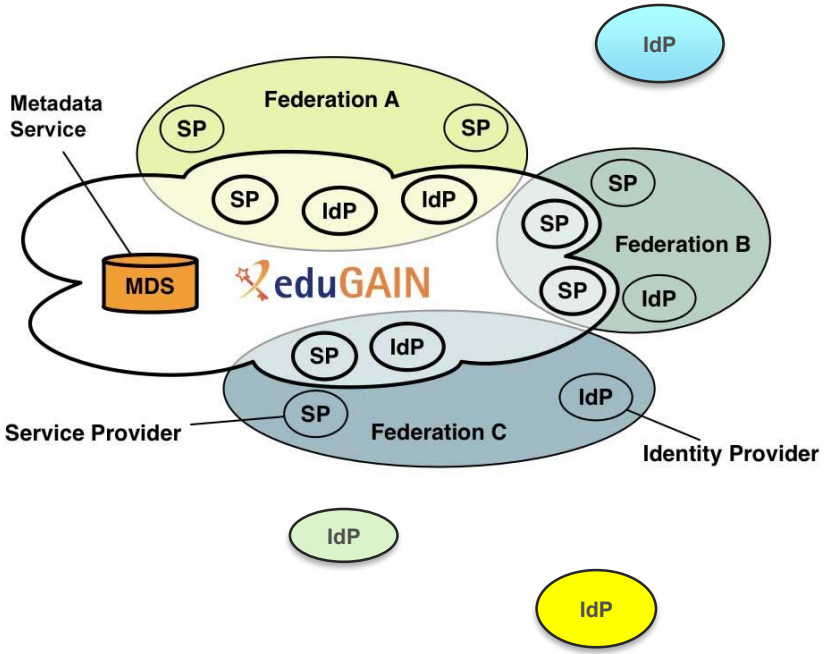
Federations in eduGAIN	
Members	51
Voting-only Members	5
Candidates	13
Entities in eduGAIN	
All entities	4654
IdPs	2711
SPs	1947
Standalone AAs	6

Fermilab

Federation

Invaluable collaboration tool!

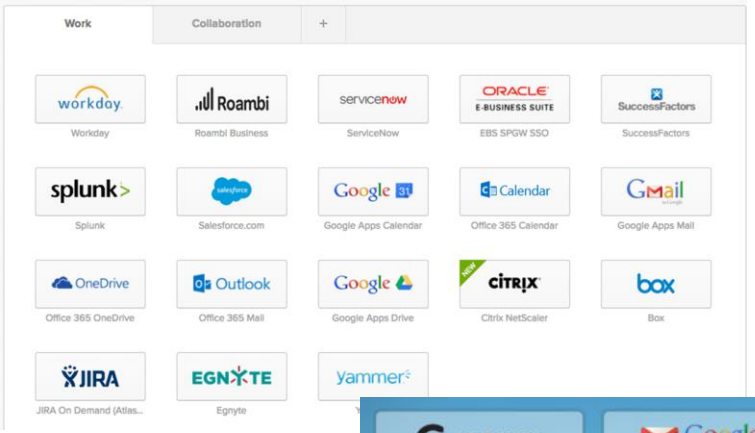
- Placing every SP in federation is not practical
- Each SP maintains authorization data?
- Not every IdP is *in* Federation



Are there possibilities here for centralized authorization?

Fermilab

Identity and Access Management products



Typically

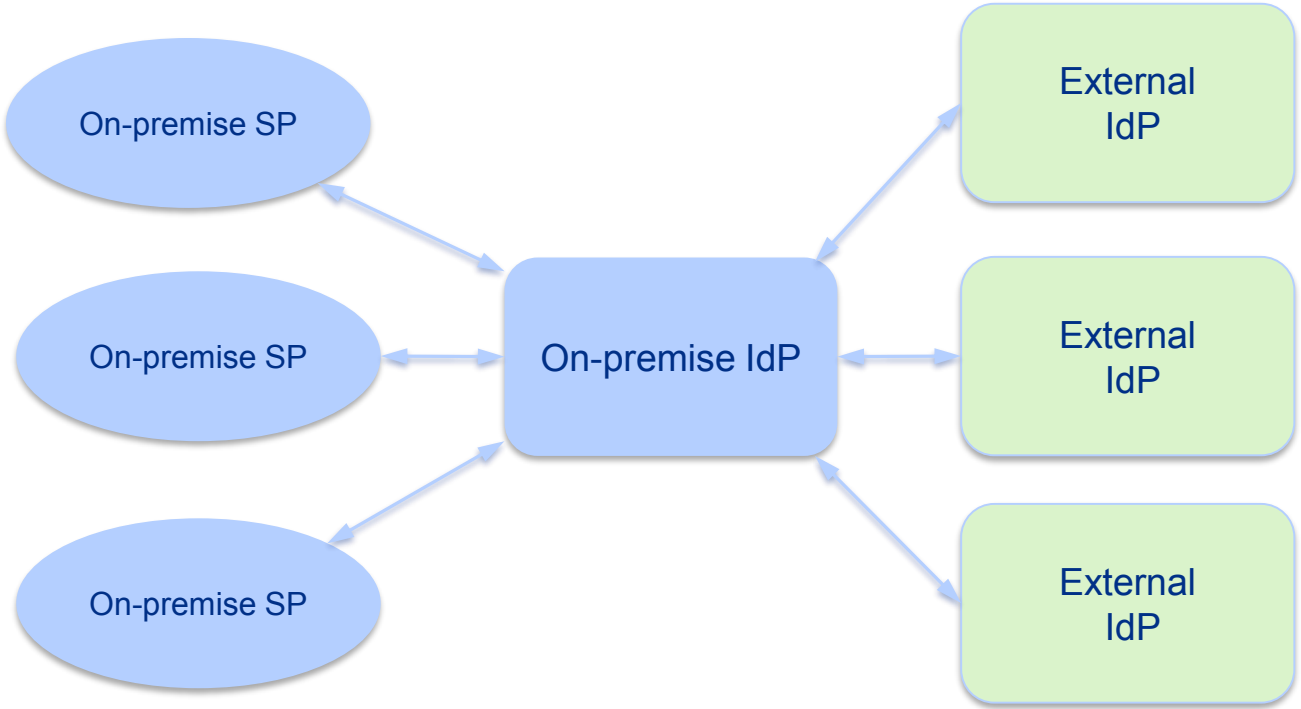
- Portal style
- Combine Authentication and Authorization
- More useful in self contained organizations

Some do integrate with federations

Fermilab

Federation Hub

This looks more centralized from Authentication point of view.



Are there possibilities here for centralized authorization?

Centralized Authorization in Non-Uniform Federation

Communities of Interest

What should we do?