Science & Technology
Facilities Council

Federated A(A(A))I

Jens Jensen

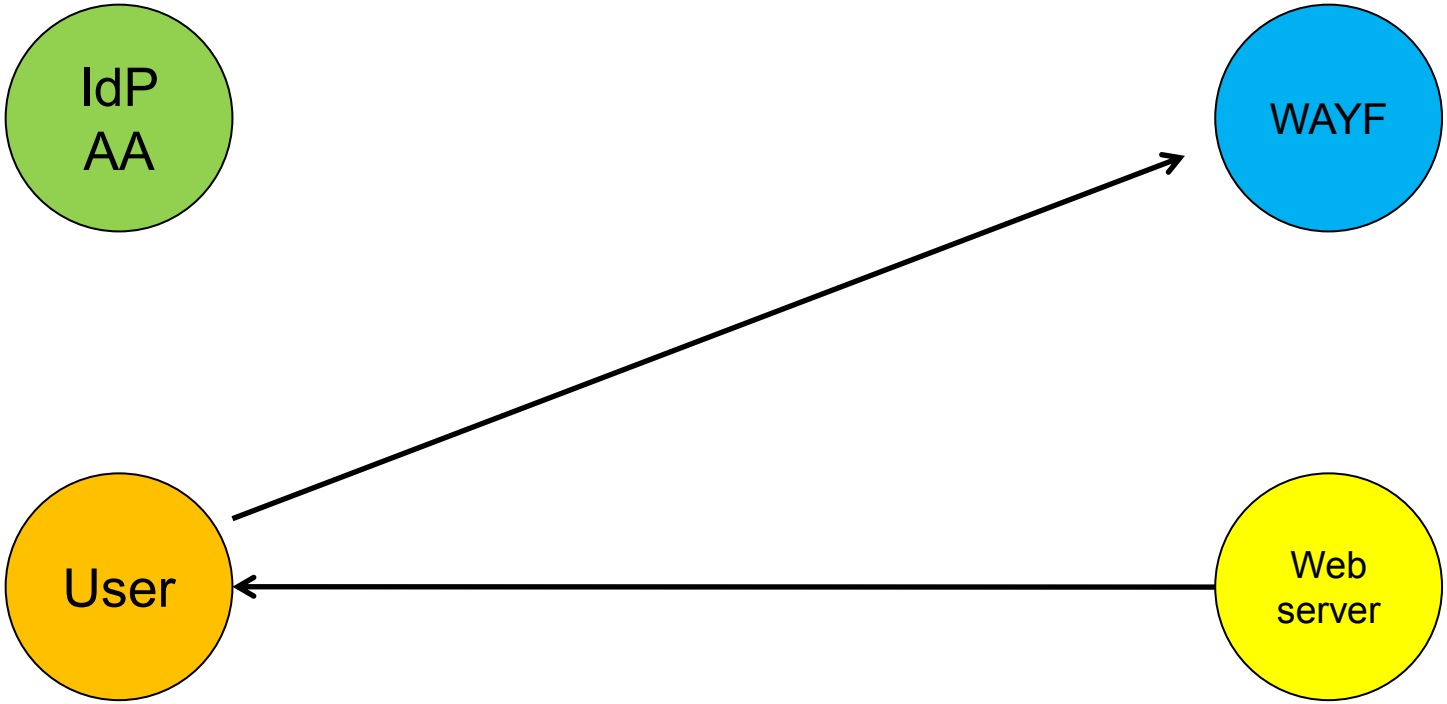
hepsysman, RAL, 20110701

Example: Shibboleth

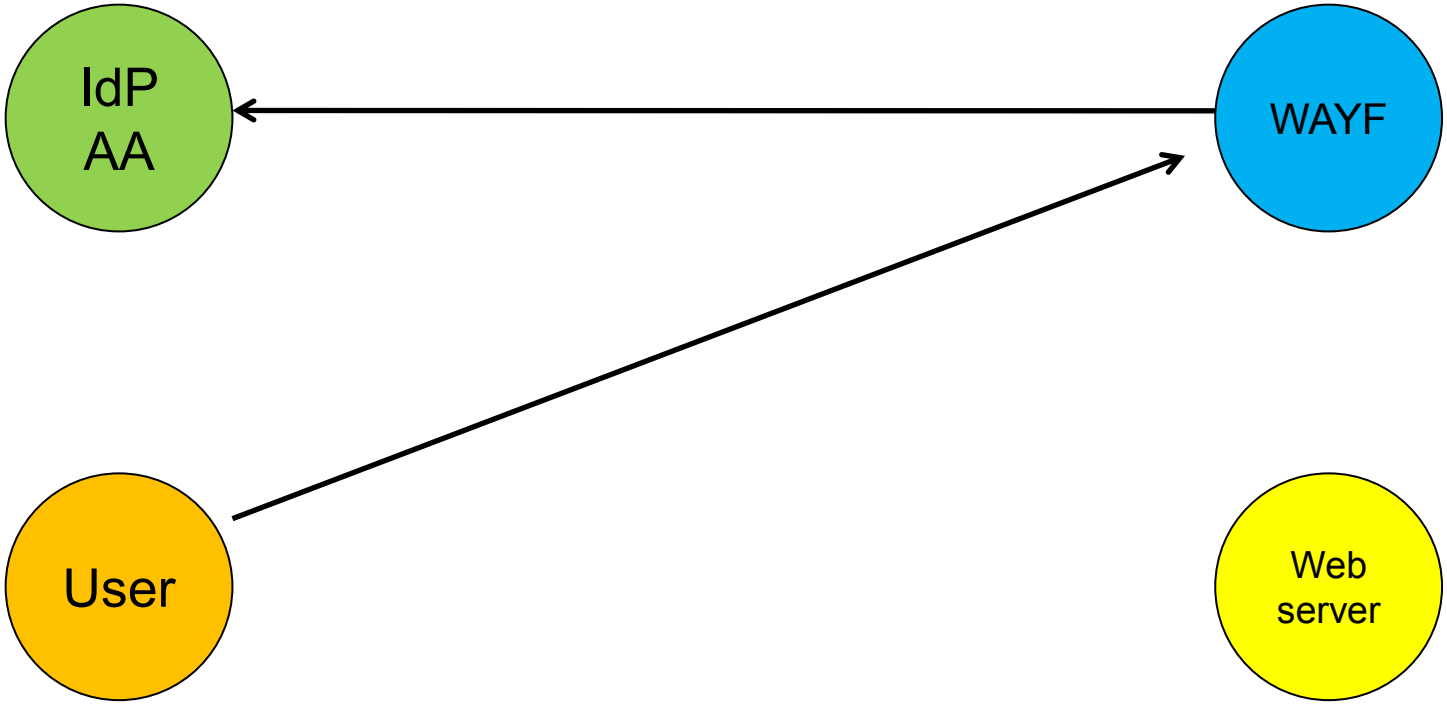
- Login with home id
  - Like Kerberos
- Issues SAML assertions
  - To work with web servers
- Based on HTTP redirects

Shibboleth

Shibboleth

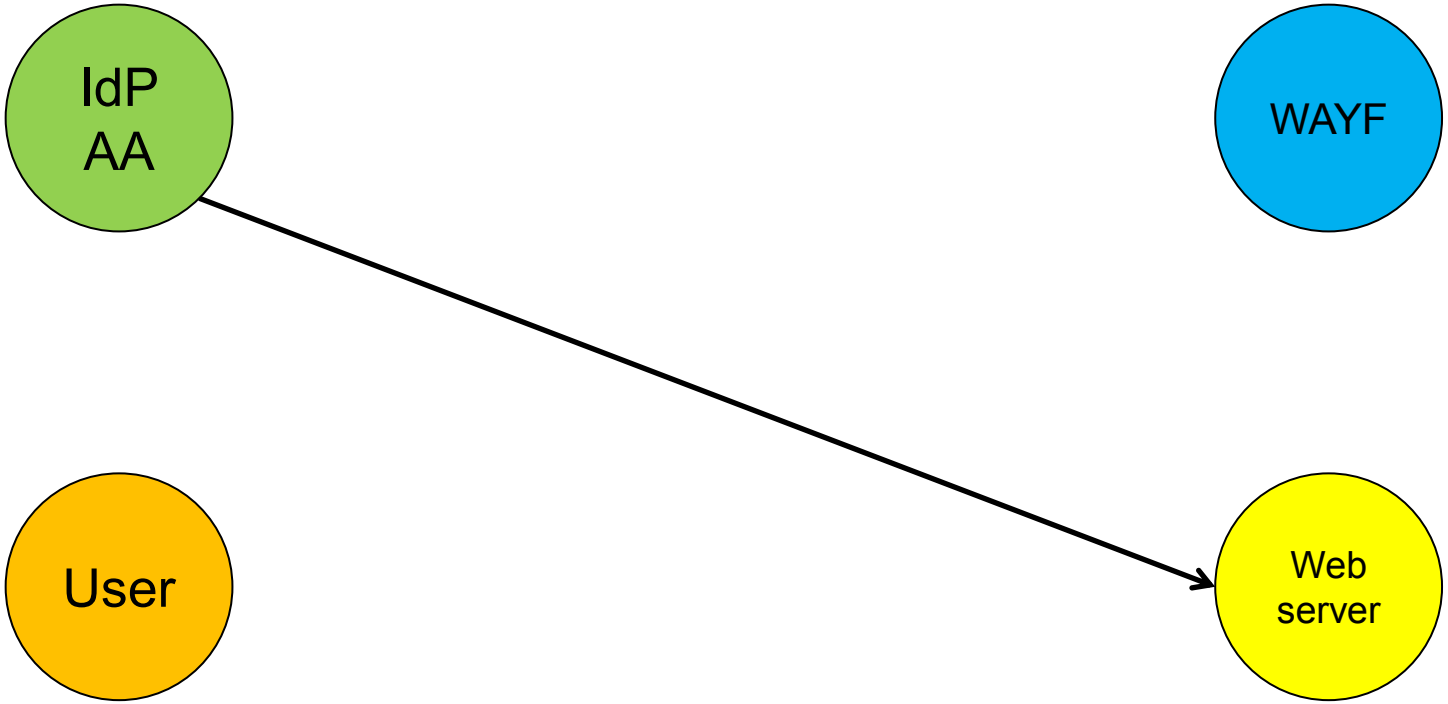


Shibboleth



Shibboleth

Shibboleth



What's good?

- Implementation of **federated identity**
  - Needs federation **policies**
- Gives SSO to (web) resources
  - Scales authentication
  - Solves the NxM problem
- Based on standards (SAML, HTTP)
- Wide national uptake across EU, AU, US, …
- Can be superfederated

Science & Technology Facilities Council

Issues

- Attributes
  - Q: Who can set the attributes? (A: IdP)
  - Who defines the ARP?
  - Scaling attribute management?
  - What can be released (policy-wise)?
- Implementation
  - Actual infrastructure stability? (e.g. against upgrades)
  - Webby

Making Use of Existing Infra

- Using existing credentials
  - E.g. SAML assertions, or RFC3281 ACs
  - Standards based...
- Convert credentials to something else
  - Example: grid needs certificates
  - Example: “export” K5

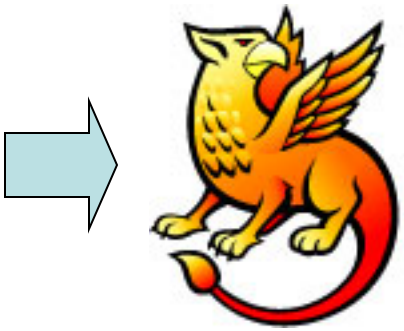
Making use of existing infrastructures:

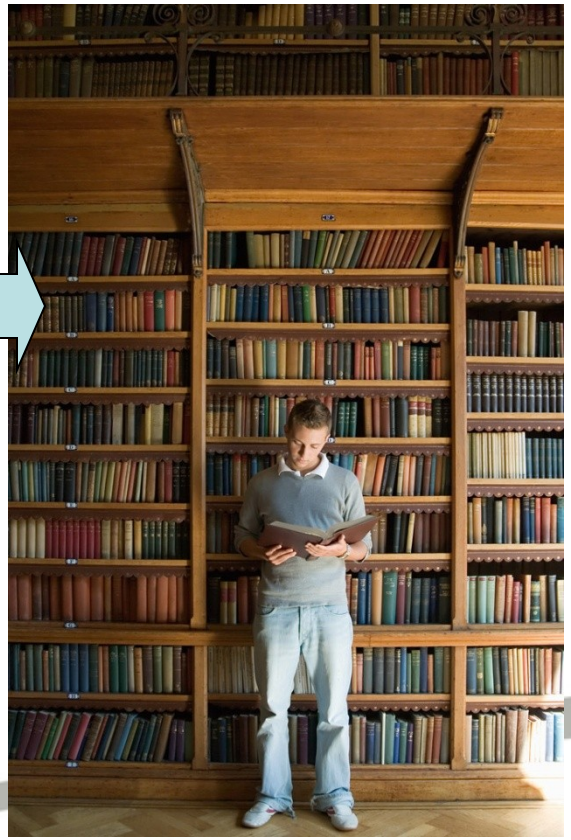
Credential Conversion

Science & Technology Facilities Council

Shib for CC

Resource access





Password

Shibboleth

Create certificates instead (portal)

Science & Technology Facilities Council

Convert a Credential

- Example, based on MyProxy from NCSA
- Shibboleth login
- “Silently” creates a certificate (and keys)
- Adds VO attributes

MyProxy for CC

http://grid.ncsa.uiuc.edu/myproxy/

Kerberos
or
Active Directory

NCSA

Grids (NGS, gLite/GridPP, SRB)

Science & Technology Facilities Council

And now for something completely the same – back to

Federations

Science & Technology Facilities Council

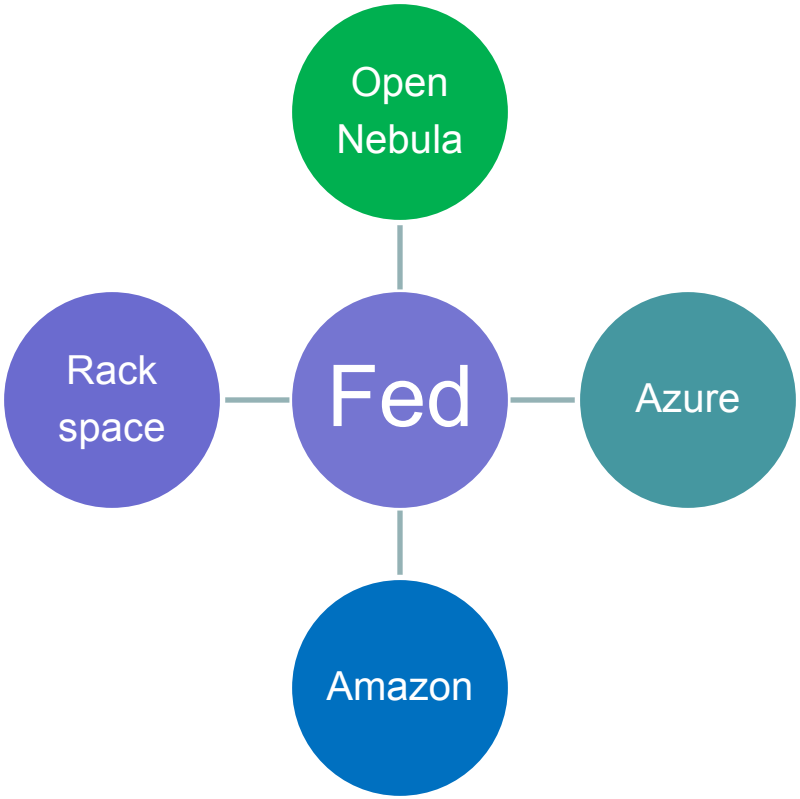
Other Federation Tech

- OpenID
- Certificates – IGTF, bridge/hierarchies
- WS-Federation
- Kerberos – cross domain trust
- eduRoam
- Moonshot

Features (or Not)

- Authentication
  - Credentials: named or anonymised
  - Traceability: can trace orig user
  - Supports delegation
  - LoA and LoWF
- Security
- Policies & trust
- Accounting

Cloud Federations



Contrail: http://contrail-project.eu/

Role of Federation

- Make use of existing identity management
- Provide harmonised accounting
- Built-in AA, also make use of ext'l;

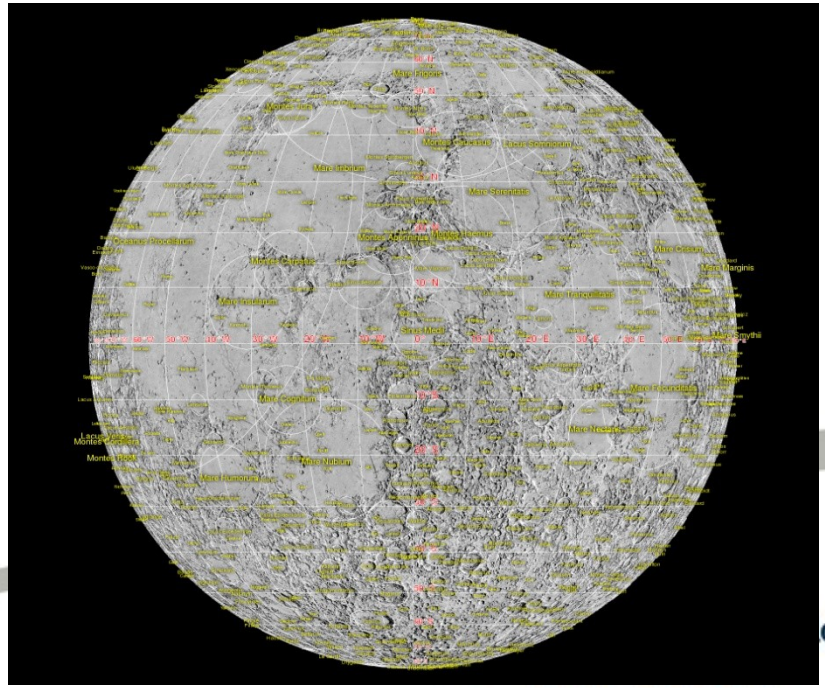
Science & Technology Facilities Council

Delegation

- Of identity (“impersonation”)
  - Cf. GSI proxies
- Of authority
  - More like roles
  - Or other attributes
  - Or specific actions on objects

Authorisation

- Access control – granting access to *some resource* to do *some thing* at *some time*
- According to *some policy*
- Based on
  - *Identity*
  - *Roles (RBAC)*
  - *Group memberships*
  - *Phase of moon* ☺
  - Etc



Federations in HEP?

- Grids: already federated (eg IGTF, NGIs)
- Universities: local SSO
  - Integrated into UK AMF (= Shib)
  - eduRoam
  - Moonshot (in progress)
- Outside universities
  - Er…

Implications for HEP?

- Users:
  - Convenience – single login
  - And inconvenience – single login
- Sites
  - SEP

Final Words...

- Fed = Tech + Policies + Support (sort of)
- Give techies time to play with tech
  - Need to *evaluate* and *interoperate*
- Watch Moonshot
- ... and Contrail of course ☺
- OGF: delegation, federations, cloudsec

Science & Technology Facilities Council