Impact to Researchers of IdP Non-Compliance

Tom Barton

UChicago & Internet2

What non-compliance?

- Change ePTID or OIDC sub claim
  - Supposed to be persistent
- Change ePPN to opaque value
  - Supposed to be name-based, ie, usable by ordinary humans
- Change ePPN without also sending a persistent identifier
  - Best practice, but perhaps not incorporated into a standard

Impact when it happens: Globus example[1]

- Globus Auth is used to access many research services
  - Including Globus' own services: Transfer, Workflow, etc
- Affected researcher can't access their stuff
  - Asks Globus for help
  - Globus staff spend considerable time to see what happened, find and contact someone at the IdP, determine remediation at IdP
  - Globus most often is left with needing to update Auth with the researcher's new identifier so that their access can resume
  - This is risky – what if Globus is wrong?
  - For Globus High Assurance sites, they'll only notify, not change
  - Typically takes days
  - Hundreds of researchers have been impacted over the last year or so

1: httpd://TBD

Root causes

- IdP operator staff change
  - No idea of impact of operational choices to federated access
  - Predecessor left nothing written down
- IT leadership change at IdP org
  - “Go to the cloud!”
  - No idea of impact of operational choices to federated access
- Shibboleth IdP upgrade doesn’t follow recommended procedure
- Change to IdP software
  - No provision to persist old federated identifier values into new system

What might be done?

- Fed Ops
  - Do education and outreach
  - Keep IdP contacts fresh for effective education and outreach
  - Provide professional services, or pointers to them, in education and outreach
- Push IdPaaS, ie, make meshes more hub-like
  - Needn’t solve the problem per se, but provides opportunity to better manage it
- REFEDS
  - Produce education and outreach materials for Fed Ops to use
- Else??