

2016-09-26 Organizational Meeting at TechEx 2016

Attendees

- David Bantz, db@alaska.edu
- Russell Beall, beall@usc.edu
- Dedra Chamberlin, dedra@cirrusidentity.com
- Gary Chapman, gary.chapman@nyu.edu
- Greg Haverkamp, gahaverkamp@lbl.gov
- Roland Hedberg, roland@catalogix.se
- Ken Klingenstein, kjk@internet2.edu
- David Langenberg, DaveL@uchicago.edu
- Laura Paglione, l.paglione@orcid.org
- Glenn Ricart, glenn.ricart@us-ignite.org
- Nick Roy, nroy@internet2.edu
- Mark Scheible, mscheible@mailbox.mcn.org
- Mike Sullivan, msullivan@internet2.edu
- David Walker, dwalker@internet2.edu, flywheel/scribe
- Albert Wu, albertwu@ucla.edu, chair
- Yavor Yanakiev, yy27@nyu.edu
- Tom Zeller, tzeller@sphericalcowgroup.com

Meeting Summary

Highlights

- Communities we should survey
 - IAM
 - LTI
 - Health care
 - Kuai
 - Other developer communities?
- Questions for the survey
 - Is the ability to revoke permissions important?
 - Is user consent important?
 - Is the RP run by same organization as the OP?
 - Is there a business process for registering RPs?
 - What information is needed by the RP (e.g., location)?
 - Is the RP developed locally?
 - If so, what programming language? What IDE?
- Interesting observation: It may be that developer acceptance is a key success factor. For many developers, this means:
 - Everything they need is available in their favorite IDE.
 - NodeJS and other runtime environments, not Apache or other web servers.
 - JSON, not XML

Raw Notes

- Russ: Hasn't seen vendors asking for this.
 - Albert: UCLA is seeing this for APIs, not so much for user sign-on.
- Ken: Better support for consent (described in Consent session tomorrow)
- Ken: Should ask what parts of OIDC do we *not* care about?
 - E.g., dynamic client registration
 - user experiences like revocation of permissions
- Gary: How do we structure the survey so that people can understand this?
 - More esoteric issues may not come up.
 - Albert: who do we target? developers? IAM community?
- NYU has OIDC gateway so developers could use OIDC
- Ken: Need to distinguish between OAuth and OIDC. He expects much more OAuth.
 - Duke has a shim to produce OAuth from the (SAML) IdP
- UCLA has need for OAuth to support LTI.
- What communities should we survey?
 - IAM community
 - LTI?
 - Glen: I want whatever is in my IDE.
 - Developer communities
 - Health care
 - LTI
 - Kuai
 - Do developers want to run OP, as well as RP?
 - Probably not, but sometimes they're packaged together to provide everything needed.
- Things for the survey
 - Revocation of permissions
 - Consent

- How important to put OIDC/OAuth into Shib?
 - Is RP run by same organization as OP?
 - Is there a business process around registering RPs?
 - What information is needed (e.g., location)?
- Should OIDC be part of Shib?
 - It increases cost/effort for the Shibboleth project, but could increase cost to campuses for infrastructure, attribute release rules, interface with backend IAMS, *etc.*
 - Perhaps separate the common parts of Shib away from the protocol stuff.