Return to Advance CAMP Wiki

Advance CAMP - Tuesday, Oct. 28, 2014, 3:30pm, White River Ballroom J

TOPIC: IdP of Last Resort (with priority on R&S applications)

CONVENER: Steve Olshansky

MAIN SCRIBE:

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 22

MAIN ISSUES DISCUSSED:

Charter of the InCommon Working Group: https://spaces.internet2.edu/display/IDPoLR/Home

The following list of requirements is preliminary. Please edit, comment and add content as appropriate.

- Support for self-registration
- Support for lost tokens, but valid account :)
- Registered as an R&S-supporting IdP with InCommon
- Ability to Assign/Assert ePPN; mandated for release to R&S SPs; values must not be reassigned
- Ability to Assign/Assert ePTIDs
- Must address the service longevity issue (even if for now the response is "TBD")
- Support for ECP
- Support for Multiple AuthN Contexts for MFA and Assurance
    - This is for their InCommon Bronze, as well as Silver and MFA, if supported.
-
- Support for Recommended Technical Basics for IdPs
- Support for attribute release
- Self-assertion of InCommon Bronze compliance
- No commercial interest in the use of user data
- ? Included in InC eduGAIN metadata submission ?

The following criteria are highly desirable, but not required.

- Support for user consent
- ? Support for Silver credentials and authN (to be combined with local identity vetting to achieve Silver LoA ?
- ? Low/no cost to SPs for use ?
- Available to users throughout the world (perhaps with invitation from "approved" projects)
- Language agnostic
- Support for some form of multi-factor authentication

Are Feide and other existing IdPs candidates? It would be good to have an entity category that marks IdPs as open to self-registration;

Branding, locale, are considerations;

Feide was an alternative for CA access federation, but there were issues with coherence and help desk.

EduID; open registration;
.
UnitedId.org: emphasis is on credential stthrength (2FA), no identity vetting. The product shall survive by living on donations, but will not ever sell personal information.

CirrusIdentity doesn't have such a service, but could spin one up if we could get to such a level of trust;

EduID plans to do a vetting service using microtransactions (credit card etc.)

If it's an account with an expected long life, then you may want to decorate the identity; Does the accuracy of the data drop;

Extending the identity lifecycle in both directions; if a higher ed institution, it ought to provide services like this for 'deserving parties'

Early on I2 evangelized IdPoLR: counter argument was it would discourage campuses from putting up their own IdPs; Social identity has shifted the debate.

Huge interfed problem; SP in InCommon won't solve the problem; But path forward is getting into eduGAIN; There are lots of cases where universal metadata distro is not essential to the solution;

Fed agencies are heartened by InCommon coverage, but there's a lot of work to onboard all these schools; I need all of higher ed; IdPoLR and/or IdMaaS;

Hub & mesh hybrid may be the path;

ACTIVITIES GOING FORWARD / NEXT STEPS:

your text here

If slides are used in the session, please ask presenters to convert their slides to PDF and email them to acamp-info@incommon.org