Draft Charter for External Identities Working Group

Proposed Charter: External Identities Working Group

Name

External Identities Working Group

Sponsor

TBD

Group Leader (Chair)

Paul Caskey (UT System) <pcaskey@utsystem.edu>

Mission/Goals

The mission of the External Identities Working Group is to move the community of knowledge towards the goal of making external identities useful and sufficiently trusted in a variety of campus-based use cases. This group is focused on the use of external identities by individuals, rather than an enterprise using an external identity provider as their enterprise IdP.

Specific goals for the External Identities Working Group include:

- Exploring/developing deployment models for using external identities in a variety of risk profiles
- Identifying and examining the technical components that are needed to make external identities useful across a broad array of services
- Exploring the notion of account linking between a campus-issued account and an external account
- Understanding the differences between external identities and local identities

Membership

Membership in the Working Group is open to all interested parties. Members join the Working Group by subscribing to the mailing list, participating in the phone calls, and otherwise actively engaging in the work of the group.

The chair of the Working Group is appointed by the InCommon TAC and is responsible for keeping the TAC informed regarding Working Group status.

Deliverables

1. Update (i.e., make current) the set of use cases previously developed by the Social Identities Working Group. This should include use cases for the following situations:
    a. Social account linked to a campus-issued account
    b. Social identity used by a non-community member
2. Develop a set of criteria for selecting external providers in a variety of usage scenarios. Ensure that both social providers (e.g., Google, Facebook, Twitter) and non-social providers (e.g., Microsoft, PayPal, VeriSign) are included.
3. Identify and document properties of external accounts that would be of interest to web application owners and other relying parties. This should include both a) how the account is managed for authentication purposes, and b) attributes asserted by the account provider.
4. Define and document how a gateway would represent the properties of an external account to an application.
5. Contrast a central gateway with a local gateway. List the advantages and disadvantages of each deployment model.
6. Provide application owners with recommendations regarding risk profiles when using external identities. (These profiles need not be based on the traditional 800-63 categories.) Describe various approaches to risk management.
7. Document various approaches to account linking:
    a. Accounts can be linked either centrally (in a campus Person Registry, and visible via the campus IDP), or at a specific SP (application).
    b. Linking a campus account to a known external account, and linking an external account to an existing campus-issued account, where both accounts are used by the same person.
    c. Identify the properties that an external account must/should possess that would affect its use.
    d. Using an external authentication provider to authenticate to a campus-based service.
    e. Identify ways that campus-owned attributes could be asserted following authentication with an external account (e.g., group memberships)
8. Produce a set of longer-lived recommendations for practitioners, roughly comparable to the NMI-DIR documents (e.g., papers, not just wiki pages).

Potential Deliverables Considered to be Out of Scope for this Phase

1. This WG will be looking at the use of personal external accounts; it will NOT be looking at situations where an enterprise is using a social provider as their IDP, for access to enterprise apps outside of google.
2. Technical requirements for Interop/deployment profile for OpenID Connect (OIDC)
3. Recommendations on approaches for elevating an external account authentication event to LoA 2.
4. Identify and document pro's and con's of having students continue to use their social account to access campus business systems during their student days. Identify an interim step toward this milestone.

Expected End Date

The working group is expected to complete all deliverables by Dec 31, 2014.

Required Resources

- wiki space
- phone line for conference calls: usual Internet2 conference call line
- incommon.org group email list socialidentity@internet2.edu

Teleconferences

Reference Material

- FICAM Relying Party Guidance for External Credentials
- OASIS WOrking Group on Trust Elevation