Status of ExtID Deliverables

Deliverables from the External IDs Charter

#	Description	Status	References	Next Steps	Comments
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 1. Social account linked to a campus-issued account 2. Social identity used by a non-community member	Complete	Use Cases for External Identities	N/A	
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.	Complete	Evaluating External Identity Providers, and included in final report drafts	N/A	
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 1. how the account is managed for authentication purposes, and 2. attributes asserted by the account provider.	Complete	Evaluating External Identity Providers and included in final report drafts	N/A	Combined with #2.
4	Define and document how a gateway would represent the properties of an external account to an application.	Not Done		Recommend as future work.	The group did not focus on the specifics of how attributes would be represented. The work group did discuss approaches for implementing integration, which is included in the report.
5	Contrast a central gateway with a local gateway. List the advantages and disadvantages of each deployment model.	Complete	Account Linking Approaches with Risks and incorporated in final document.	N/A	In the final report, the information from the document listed here was split some across multiple sections, but the contrast between the approaches was discussed.
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.	Complete	External Identities Workgroup Meeting at ACAMP - 2014-10-27 and incoporated and expanded upon in final document.	N/A	This was done more as stating the risks and calling out use cases that affect assessment of risk than defining formal risk profiles.
7	Document various approaches to account linking: 1. Accounts can be linked either centrally (in a campus Person Registry, and visible via the campus IDP), or at a specific SP (application). 2. 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. 3. Identify the properties that an external account must/should possess that would affect its use. 4. Using an external authentication provider to authenticate to a campus-based service. 5. Identify ways that campus-owned attributes could be asserted following authentication with an external account (e.g., group memberships)	Complete	Account Linking Approaches with Risks External Identities Workgroup Meeting at ACAMP - 2014-10-27 and in final document	N/A	These topics were all addressed, with the possible exception of #3, where the concept of an "identifier" is defined, but requirements of external identity properties were not elaborated upon.
8	Produce a set of longer-lived recommendations for practitioners, roughly comparable to the NMI-DIR documents (e.g., papers, not just wiki pages).	Complete?	The final document is intended to meet this role. Out for comment to see how well it holds up to the desire.		

Potential Deliverables Considered to be Out of Scope for this Phase

#	Description	Status	References	Comments
A	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.			
B	Technical requirements for Interop/deployment profile for OpenID Connect (OIDC)			
C	Recommendations on approaches for elevating an external account authentication event to LoA 2.			
D	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.			