Alternative IdP Strategies and Assessment Criteria

Alternative IdP Strategies and Assessment Criteria

The following table outlines potential alternative IdP strategies to be considered by the work group, as well as potential assessment criteria.

IdP Strategy	Description	Fact Finder	Example Deployments (case studies)	Support for Recommended Technical Basics for IdPs (inc. ability to consume metadata)	Support for Attribute Release	Support for Entity Categories (R&S)	Support for Multiple AuthN Contexts for MFA and Assurance	Support for ECP	Support for User Consent	Expertise Required	Resources Required (amount of human resources)
Shibboleth IdP (local)	Integrated with the local IdMS and operated locally, the baseline for comparison	David /Janemarie		Yes	Yes	Yes	Yes, with the MCB add-on.	Yes	Yes, with uApprove or Privacy Lens add-on.	Expertise in the operation of Java-based services and XML, as well as general knowledge of federation.	Hardware resources are dependent on load, but are generally low.
ADFS IdP	Microsoft's SAML implementation for Active Directory, operated locally	Scott Koranda / Alex Chalmers	There are a number of organizations in InCommon and other higher ed federations using ADFS. Ball State is a concrete example of InCommon member using ADFS.	Partial, assuming use of pysfemma software.	Yes, assuming AD LDAP is the attribute store.	No (not without third-party scripts such as pysfemma).	No	No	No	PowerShell and Python scripting, vocabulary knowledge translating InCommon to ADFS speak	Standard Windows admin, fair amount of time starting from scratch without mentor. Finding information to make it work.
SimpleSAMLphp IdP	An open source IdP written in PHP, integrated with the local IdMS and operated locally	Ben Poliakoff	[https://simplesamlphp.org/users]Institutions listed using SimpleSAMLphp as an IdP: - Technischen Universität Wien - University of the Basque Country - University of Málaga - University of Zagreb	Yes, except for SAML V1.1 attribute queries.	Yes	No	No	Yes	Yes	PHP, knowledge of directory service underneath (AD, LDAP) since it's middleware;	
Insourced IdP with Vendor Support	An IdP run on a locally-supported platform with vendor support for the IdP itself, assume to be Shibboleth here.	David Walker		Yes	Yes	Yes	Yes, with the MCB add-on.	Yes	Yes, with uApprove or Privacy Lens add-on.	Expertise in the operation of the hardware and operating system are required	Hardware resources are dependent on load, but are generally low.
Outsourced Shibboleth IdP	Shibboleth, integrated with the local IdMS and operated by a third party	Mark Beadles	Fischer Identity; OARnet has schools doing this. Mark will check on them.	Yes	Yes	Yes	Yes, assuming configured by operator.	Yes, assuming configured by operator.	Yes, assuming configured by operator.		
Outsourced Vendor IdP • Cirrus Bridge	A non-Shibboleth SAML IdP, integrated with the local IdMS and operated by a third party, such as Ping Identity	Dedra Chamberlin	Dedra has permission to release use case.	Yes, except for ECP endpoints in metadata.	Yes	? (Not sure if it releases only to SPs with the R&S entity tag. - DHW)	Configured per SP.	No	On roadmap		
Hub and Spoke (or Trusted Third Party) IdP (Response assumes SimpleSAMLphp)	Likely used by systems such as community colleges, K-12, network providers, etc. where individual constituents don't want to run their own IdP. The IdP is located at the Hub and users enter local credentials for authentication. Attributes are passed on from the home institution to the Service Provider.	Mark Scheible	Some European Federations - WAYF, FEIDE, SURFnet	Yes, except for SAML V1.1 attribute queries.	Yes	No	Multiple authentication methods can be specified in one configuration.	Yes	Yes	Limited expertise required for Campuses (Hub Operator needs SimpleSAMLphp and IdP Proxy experience)	Minor resources at Campus
Assessment completed after the final report											

Azure AD											
Assessment not completed											
CAS (local) with Outsourced IdP	A SAML IdP, either Shibboleth or vendor, integrated with the local IdMS and operated by a third party, that uses a local CAS deployment for authentication										
CAS Gateway	A SAML-to-SAML gateway, often operated by a third party, for participants that use CAS for local authentication										
Google Apps Gateway	An OIDC-to-SAML gateway, often operated by a third party, for institutions that make use of Google Apps for Education	Shaun Abshere will investigate with respect to Cirrus Identity (vendor)									
Identity as-a-Service	An IDaaS option such as Google, Okta, or Stormpath where the institution uses identity data uploaded to the IDaaS which then functions as an outsourced IdMS.	David Walker (to explain why we decided it's out of scope)									