LInk to 2020 ACAMP wiki

Title: I have too many SSO's season 2/ Thoughts in integrating something like SATOSA fully in with Shibboleth for one complete container?
We run SAML, CAS, Azure (for oauth) and then we run a custom MFA plus Azure MFA. We are looking for one comprehensive solution and don't see ourselves moving away from Shibboleth, but rather trying to configure it to work with everything else...

Advance CAMP Wednesday Nov18,2020

1:20-2:10 pm ET

Room - Lodge

CONVENER: Keith W and Mike Mays

MAIN SCRIBE: Bruce Vincent

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 32

DISCUSSION:

- Keith Wessel gave a rundown of the origin of their institution (University of Illinois at Urbana-Champaign) having 3 different SSO infrastructures.

- Keith mentioning the challenge they have with multifactor support by the SSO tools. ADFS not supporting iframe from Duo
- Keith saying they will allow ADFS be authoritative for multiple SSO contexts (I believe?). Using ADFS for first factor and Shib for second to deal with second factor. Using forced reauthN built into Shib.
- Michael Mays mentioned SATOSA (Identity Python) and GLUU. Looking around. They (iUniversity of Delaware) are interested in Azure MFA more broadly.
- Bruce (Stanford) mentioned standardizing on Shib for both WebSSO and its IdP.
- Les LaCroix mentioning that they use Shib for WebSSO but also have ADFS for applications that “really want” to talk ADFS. Also, they are using Cirrus identity as ODIC bridge.
- ECP continues to be seen and a factor in IdP authentications.
- “Modern AuthN” has been causing Les’ institution a problem with ShibSSO clients.
- Azure AD connect is being used/coming at (UI?). Windows and non-Windows operations teams are together which helps coordinate the interactions of user authN flows.
- Question asked about which other institutions are using Shib form as a display layer of user authentication flow. Several are doing this in front of other auth contexts.
- Some are using cloud sourced user authN/IAM service e.g. Okta and AzureAD
- Discussions on merging backend IAM infrastructures (Kerb, LDAP)...as well as WebSSO
- Discussion on using Midpoint to merge convergence of backend these IAM subsystems.
- Discussion on the particular expression and taxonomy of claims for assertions. Sounds very particular to AD environments.
- Discussion on whether tightly serlinked services
- More practical to make multiple systems co-exist or abstract out their functionality than to hope for only one SSO solution