Tues 3.15pm SalonsA-D

Scribing Template --Tues., Nov 12, 2013 at 3:15pm -- **Salons A-D**

TOPIC: Mobile SSO

CONVENER: Chris Phillips

SCRIBE: Eric Kool-Brown

# of ATTENDEES: 30 < a < 100

MAIN ISSUES DISCUSSED: Story around SSO for mobile WRT SAML

- Notion: it's not authN, rather it may be authZ for the mobile app's web API and hence not really SSO
  - OAuth 2.0 has token policy to limit token lifetime
  - It is possible to share (OAuth or other) session state between apps
- Questions about how to do mobile and/or OAuth authentication without a browser
  - Have the auth infrastructure isolated so that apps need only look at an auth cookie
  - OAuth specifies the use of a system browser for authN to enable MFA without app changes
- Michigan has an SSO applet that allows the sharing of auth session state (Scott)
- Android app store has implemented a solution
- Forums: CISOs, I2, TF/Mobility, InCommon TAC (via their IW CAMP session), campus librarians
- Need to succinctly scope the problem; mobile auth is too broad a topic (Steve)
- Get a profile outlined to see how much of OAuth must be implemented to address the use case (Scott)
- Folks are working on getting statements from NIST about API access because their current guidance docs do not address APIs (John)
- Scott asserts that it really is authN (plus authZ and rich attributes) so that users can access web APIs
- John discusses the subtle trust relationships between the parties (where does the IdP live in relation to the other components, etc.)
- Chris is concerned about IAM being leapfrogged by mobile app developers who roll their own auth (or lack thereof) because there is no simple, consumable recommendation/code/API from IAM
- Native app can use ECP; web SSO allows use of the central Shib IdP

ACTIVITIES GOING FORWARD / NEXT STEPS: