Shibboleth Update
Fall 2012

Ch-ch-changes

- Chad moving on to new job opportunity, requires realigning product responsibilities and reviewing roadmap
- Tom Zeller coming on board as IdP lead
- Ian Young assuming responsibility for Metadata Aggregator
- Other roles largely the same

IdPv3

- Scope and schedule inevitably impacted
- Priority for project team is delivering a dev plan to the new Consortium Board this month
- Identify resource gaps, then adjust plan or find resources

Service Provider

- 2.5.0 release smooth apart from traditional packaging foibles
- Pending outcome of an issue under investigation, End of Life for V2.4.3 will be Nov 30th
- 2.5.1 patch update under development to address Apache 2.4 support, other bugs as time permits

SAML ECP + GSS-API/SASL + ISOC + NCSA =

SSH
IMAP
LDAP
XMPP
NFS
AFS
…

SAML ECP in GSS-API

- https://wiki.oasis-open.org/security/SAML2ChannelBindingExt
  - Authentication of TLS client/server session via SAML IdP
- https://wiki.oasis-open.org/security/SAML2EnhancedClientProfile
  - Backward-compatible profile adding channel binding, holder of key security, session key establishment
- http://tools.ietf.org/html/draft-ietf-kitten-sasl-saml-ec
  - GSS-API mechanism allowing use of IdP with ECP
  - Expose SAML identity via GSS-API Naming Extensions
  - SASL support via GS2 bridge mechanism

Takeaways

- Proof of concept stage, specs still evolving
- No browser for authentication, no implicit web-based flows alongside the real ones
- Strong complementary overlap with Project Moonshot:
  - client UI and IdP provisioning
  - GSS client and server changes
  - use of SAML-based identities, GSS naming extensions
  - likely to share code