# Identity and Access Management Renewal

Introducing SAML to the Campus Infrastructure

April 16th, 2015

Sean Mason : sean.mason@uwaterloo.ca : x42511

# Where are we now?

- Batch Identity Data Processing
- LDAP (Active Directory) Authentication
- CAS Web Application Single Sign-on

# Why use SAML?

- The Cloud
  - Many vendors support the SAML protocol
  - Avoid provisioning identity data in the cloud
- Identity Data Transfer
  - Communicate identity data in real-time, rather than batch transfer
  - Active directory cannot store sensitive user attributes
  - Active directory should not store users that are not part of the campus community

# Why start with an identity provider?

- Identity lifecycle changes are coming to address:
  - Current lifecycle problems.  For example, instructors
  - Improved student applicant handling
  - Graduate student applications – OUAC
  - Prospective student handling
- Introduce services that will help mitigate these changes before they are introduced to give systems time to adapt

# What do I need to migrate?

- A SAML service provider
  - A trusted component of the authentication infrastructure for the university
  - Service provider metadata
- An understanding of the SAML authentication protocol
- A list of required attributes

# When?

- A pilot identity provider is deployed and being used by:
  - Concur
  - Lynda.com
- Production ready instance to be launched this summer
- Migration planning discussions with ISS may begin at any time

# Definitions

- Identity Provider (IdP): A service that maintains a data store of users to which known authentication mechanisms are offered.  Constructs assertions for requesting service providers
- Service Provider (SP): Represents a target web application.  Consumes assertions from the IdP
- SAML Assertion (Token):  An XML response from the IdP constructed for the requesting SP which contains the configured identity information about the authenticated user
- Metadata: XML that describes an SP or an IdP that is exchanged between the two in order to configure their integration

# Resources

- How a SAML authentication environment fits together: https://wiki.shibboleth.net/confluence/display/CONCEPT/FlowsAndConfig
- Getting started with the Shibboleth service provider: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPGettingStarted
- “Shibbolize” an application: https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPEnableApplication