AST Federation Strategy

Ken Runyon, SUNY OAS
Program Manager
Identity Management and Common Enterprise Architecture
Federation Strategy

Agenda

• Goals
• Strategy
• Way Forward
• Where We Stand
• Project Strategy
• Questions
Federation Background

Federation Goals

• Information Sharing and maintenance across all SUNY entities.

• Establish common mechanisms by which information is accessed

• Permit university-wide and campus-based systems to provide a richer user experience
Federation Plans/Goals

Federation Strategy

- Improve Information Exchange
- Provide Industry Standard Solution
- Ensure Extensibility and Supportability
- Establish Common Mechanisms
- Enrich user experience with U-wide and campus-based systems
AST Way Forward

Federation Strategy

2010 +
- Finalize Federation Governance
- SWIFT (SUNY Wide Identity Federation Technologies)

2011
- Federation Phase II
  - OIF/Shib IdP Cookbook
  - OIF SP Cookbook
- Campus Implementations & Support

SUNY Federation
Federation

Where We Stand

• EduPerson Attributes
  – Attribute Harvesting code complete
  – Initial POC w/ Geneseo successful
  – Capability now exists in Production System
  – Awaiting campus population of attributes

• Oracle Identity Federation (OIF)
  – OAS OIF Identity and Service Providers running in Production
  – Federation established between OAS & NYS Office for Technology
  – NYS Learn training now accessible via SUNY Portal link
AST Federation Project Strategy

SUNY Federation

- SUNY Federation
- 5/21/10: Integrate w/ OIF 11g
- 6/1/10: Initial EduPerson Attribute Utilization
- 7/1/10: Integration w/ OIF/OAM 11G
- Continued Support

EduPerson

- 12/3/10: Banner Sync. Kickoff
- 1/1/10: Already Populated
- 3/1/10: Existing Attributes
- 5/1/10: Inferable Attributes
- 8/1/10: Difficult Attributes
- 9/1/10: Fully Populated

Oracle Federation 11G

- 11/15/10: Inception
- 12/1/10: Initial OAM Use Case
- 1/1/10: Use Case Validated
- 4/1/10: OIF 11G Deployed
- 7/1/10: OAM 11G GA?
- 9/1/10: IdP/SP Available
- 9/15/10: Cookbooks
- 1/1/11: Full Federation

Revised: 06/14/2010
Federation Strategy
(version 1.1.2)
May – Integrate SUNY Federation with OIF 11G
Jun – Code complete for full EduPerson Attribute Harvesting via existing security infrastructure
Jul – Begin Integrating SUNY Federation into OIF/OAM 11G Federation infrastructure

Note: Existing SUNY Federation capability continues to be supported until no longer required and is expected to coexist with and be accounted for in the new Identity Federation design until no longer required.
EduPerson Strategy

• Banner Kickoff – Develop scripts or other standard methods to sync AD/LDAP with Banner info
  • Existing – Attributes that may already be populated within your LDAP
    – mail
    – displayName
    – telephoneNumber
    – postalAddress
  • Easy – Attributes that most likely map to existing LDAP fields
    – eduPersonPrincipalName [userPrincipalName]
    – eduPersonNickName [nickname/displayName]
• Inferable - Attributes you may be able to infer from other systems
  – eduPersonAffiliation
  – eduPersonPrimaryAffiliation
  – eduPersonScopedAffiliation
• Difficult - Attributes are either difficult to understand or populate.
  – eduPersonOrgDN
  – eduPersonOrgUnitDN
  – eduPersonPrimaryOrgUnitDN
  – eduPersonEntitlement
• We can help you with these attributes
  – sunyPersonSunyID
  – sunyStudentID

Banner Sync. Kickoff
Already Populated
Existing Attributes
Inferable Attributes
Difficult Attributes
Fully Populated

SUNY Federation

Federation Phase I
Federation Phase II

Revised: 06/14/2010

Federation Strategy (version 1.1.2)
Oracle Federation Strategy

Oracle Federation 11G
- 11/15/10: Inception
- 12/1/10: Initial OAM Use Case
- 1/1/10: Use Case Validated
- 4/1/10: OIF 11G Deployed
- 7/1/10: OAM 11G GA?
- 9/1/10: IdP/SP Available
- 9/15/10: Cookbooks
- 1/1/11: Full Federation

• Dec – Initial OAM use cases sent to Oracle. Dependency on participation in OAM 11G Beta.
• Apr - Leveraging experience from EC2 POC with Oracle OIF team. Project goal is to validate and document OIF 11G SP and Shibboleth v2.x IdP capabilities and configurations.
• July - Expect initial non-beta release of OAM in July/Aug time frame. Begin integration with OAM R1 GA leveraging experience from OAM beta.
• Sept - Expect initial IdP/SP availability for integration testing with select campuses (TBD).
• Sept – IdP/SP Cookbooks OIF and IdP Cookbook for Shibboleth IdP.
• Jan 2011 - Fully integrated Federation capable of supporting all SAML2 compliant IdPs. SUNY Security integrated with OAM. Oracle Federation with attribute passing via artifact.

NOTE: Existing SUNY Federation is expected to continue in use and be integrated where appropriate.
Q&A