AAF Shibboleth Operational Requirements: Implications for enterprise identity management

James Dalziel
Professor of Learning Technology &
Director, Macquarie E-Learning Centre Of Excellence (MELCOE)
Macquarie University
james@melcoe.mq.edu.au

Presentation for Identity Management Workshop,
University of Queensland, 19th August, 2008

Overview

• AAF Shibboleth Overview
• Shibboleth Background
• AAF Shibboleth Operational Requirements & Recommendations
  – Principles
  – IdP Deployment Models
  – Floor of Trust
  – AAF Shibboleth for Local SSO
  – Other issues
• AAF Shibboleth System Screenshots
• Example Federation Applications Screenshots
AF Shibboleth Overview

- Deploying a production Shibboleth federation building on previous work by MAMS project
  - Each university would typically have one Identity Provider (IdP) based on enterprise directory, and a range of Service Providers across eResearch/eLearning/Libraries/Admin

- Core concept is home institution login for access to federated services (can also be used for local web SSO)

- MAMS Testbed Federation (Level 2) has 27 IdPs (approx 900,000 identities) & 28 SPs

- MAMS software to assist with deployment
  - Validated Shibboleth packages & ShARPE, Autograph, People Picker, IAMSuite, etc

Background

- Trust Federations are an alternative to the traditional approach of applications managing accounts

- Requires three components:
  - Identity Providers: (the part of) Organisations that can share who their users are and their attributes (eg, role)
  - Service Providers: Services (ie, applications) that are accessible by users from Identity Providers
  - Trust Federation: A trust framework (policy and technical) that connects Identity Providers and Services Providers

- A typical university contains one Identity Provider (the Directory) and may have many Service Providers
Background

Trust Federation Prior Requirements:
- Identity Provider establishes the identity and attributes of its members (users)
- Identity Provider joins trust federation, shares attributes
- Services Provider joins trust federation, uses attributes for access

Access Process:
1. A user logs in to their home organisation (Identity Provider)
2. The user attempts to access a service (Step 2 can come first)
3. The service requests/uses attributes about the user so as to make a decision about granting/denying access

Background

• Shibboleth is an open source implementation of the SAML open standard
  - Focus on trust federations for education and research
• Development led by Internet 2 in the US, with contributions from around the world
  - Including from Australia via the MAMS project
• Rollout of Shibboleth trust federations in the USA, UK, Australia, Switzerland, Finland, France, Germany, etc
Some AAF Shibboleth use cases

- Research data and facilities
- Institutional repositories
- Cross-institutional course delivery
- Collaboration tools and shared services
- Scholarly and information resource licensing
Typical Shibboleth Access Scenario

User wants to access SP

User is redirected and selects IdP: Where Are You From
Typical Shibboleth Access Scenario

User is redirected to IdP and logs in

IdP uses Attribute Release Policy for SAML assertion
Typical Shibboleth Access Scenario

User is redirected to SP with SAML handle

SP uses SAML handle to retrieve user attributes
AAF Shibboleth Federation

- Principles for AAF Shibboleth federation include:
  1. Unified Fabric for Authorisation
  2. Service Descriptions
  3. Customised Federation Metadata
  4. End-user management of release of Personal Information
  5. Prepared software packages or freedom to build own systems
     (Shib 1.3 baseline for interoperability; Shib 2/other systems ok if interoperable)
  6. Two Levels of Assurance (LoA)
  7. Core Attributes implementation detail (inc SharedToken)
  8. Federation Shared Services (inc People Picker)
  9. Assistance with liaison, support and logging

- From “AAF Shibboleth Operational Requirements and Recommendations” document - under sector consultation
  - See http://federation.org.au/requirements.doc

AAF Shibboleth Requirements

- AAF Shibboleth Operational Requirements and Recommendations describes the “rules of the road” for the AAF Shibboleth Federation
- 3 components:
  - Requirements (mandatory)
  - Recommendations (encouraged but not required)
  - Explanatory comments & advice
- Sector consultation just ended – currently preparing final draft
  - Keen for any feedback on showstoppers today
1 Common (IdP and SP) Requirements and Recommendations

1.1 Technical Infrastructure

1.1.1 Federation Software

**AAF Req14.** AAF Shibboleth Federation members must conform to technical standards and behaviours equivalent to Shibboleth version 1.3.3.

The AAF Shibboleth Federation is based on Shibboleth 1.3.1. Shibboleth 1.3.3 technical specification documents are available from Internet2 (see https://spaces.internet2.edu/display/STC/WebHome).

While AAF Shibboleth Federation Members are not required to use Shibboleth 1.3.3 software, any alternative software (eg, Shibboleth 2; EZAsia, etc) must fully interoperate with Shibboleth 1.3.3 and the Requirements of the AAF Shibboleth Federation (ie, the requirements in this document). The AAF Shibboleth Federation Operator can provide advice to assist with conformance of IdPs and SP installations for Members not using Shibboleth 1.3.3 software.

In the future, the AAF Shibboleth Federation may be based on new standards or new versions of Shibboleth. Changes to new standards or versions of Shibboleth would require community consultation and approval by the AAF Steering Committee. This requirements document would be revised in the case of a future change.

**AAF Rec13.** It is recommended that AAF Shibboleth Federation members install only validated software packages made available from the AAF Shibboleth Federation Operator and obtain standard configurations where appropriate.

**The AAF Shibboleth Federation Operator will provide validated versions of Shibboleth IdPs and SPs.**

---

**IdP Deployment models**

- Shibboleth Operational Requirements document provides details for various “full deployment” models, but also allows for incremental models
- **AAF Req14**
  - AAF Shibboleth Federation IdPs must be able to deliver the core attributes defined in Attribute Recommendations for AAF Participants (ie, eduPersonTargetedID, eduPersonAffiliation, eduPersonScopedAffiliation, auEduPersonSharedToken, eduPersonEntitlement, mail, displayName) for any IdP staff end-user who needs to use the AAF Shibboleth Federation.
- **AAF Rec13**
  - Core attributes should be available for all potential end-users within an AAF Shibboleth Federation IdP.
IdP Deployment models

• Apart from full deployment, some incremental options include:
  – Minimal: Create a (separate) IdP just for federation users with core attributes, and add users as required
    • Downside – need to keep separate identity record current
  – Minimal (hosted): Hosted software (IdP) for above
  – Staff Only: Connect only staff directory to IdP with core attributes (and others if available)
    • Good for eResearch & Admin uses, less so for eLearning/Libraries
  – Full staff, partial student: Connect to directory with all core staff attributes; and include students but without all core attributes (and add more later)

IdP Deployment models

• Other deployment options:
  – Validated Shibboleth 1.3.3 or equivalent software
  – SharedToken: Federated or local service
  – End-user privacy management: Dynamic “per SP” approach or once off paper or digital process
  – Identity Level of Assurance “3”: Record in directory or combine with end-user Cert issuing process for Authentication Level of Assurance “3” (eg, only for those who need it)
  – People Picker: Name and email only or extra attributes (eg, Department, Phone, etc) for disambiguation
Floor of Trust

• Floor of Trust is the base level of assurance - AAF Req 11:
  – Institutional assertion of end-user identities and attributes (including maintenance of currency of user accounts and attributes);
  – IdP authentication using passwords with a minimum of six characters (with at least one letter & one number);
  – Disabling accounts if a breach is detected or if an end-user is no longer a member of the IdP

AAF Shibboleth for Local SSO

• AAF Shibboleth can be used for local institution Single-Sign-On (SSO) for web applications
• Federation Manager allows institutions to designate a SP as only viewed and accessed by one IdP (ie, themselves)
• Allows SSO for local web applications using the same technologies as the AAF for federated apps
  – However, local services are not viewed or accessed by rest of federation, restricting access to local users
Other Issues

• Mail (AAF Req19)
  – Where the “mail” attribute is implemented for relevant end-users (ie, for relevant staff it is required, for other end-users it is recommended), AAF Shibboleth Federation IdPs must provide only a single value for this attribute that represents (or is forwarded to) an active email account
    • (Should this be a recommendation rather than requirement? If so, harder for SPs to deal with multiple email addresses)

• Details for PKI in Shibboleth (AAF Req 2 & 3)
  – Yet to be resolved

• Attributes Usage & Attribute Mapping (AAF Req8)
  – AAF Shibboleth Federation Members are required to use the definitions (syntax, semantics, constraints) of AAF attributes specified by Attribute Recommendations for AAF Participants and this document.
    • Comment: IdPs are not required to implement AAF attributes in their directory – the requirement is only that when they conduct a Shibboleth transaction, that the attributes in that transaction conform to the Attribute specification and this document. There are various mechanisms available (eg, mappings in SHARPE) to construct AAF Attributes from other relevant and authoritative information held by the organization (eg, in the directory).
  – IE, you don’t have to change your Directory to use native AAF attributes, you can use mappings (eg, SHARPE mapping tool)
Other Issues

• SAML 1.x, SAML 2, Shibboleth 1.x, Shibboleth 2?
  – Focus on education sector interoperability and reliability
    • Standards: SAML 1.1 + some SAML 2.0
    • Systems: Shibboleth 1.3.3 as foundation, but Shibboleth 2, ESOE, etc are fine if they interoperate

• OpenID?
  – OpenID typically involves a weaker trust context than a production education sector federation
  – But AAF Shibboleth could easily add an OpenID option on top of Shibboleth if desired

Other Issues

• Does all staff now need 100 point check? (Authentication Level of Assurance “3”)
  – No, can handle on an “as needs” basis when (a small number of) staff try to access Services through Shibboleth, and get a message that they need strong authentication, then go get Cert

• AAF policy “Sunrise” clauses for desirable policies that not enough IdPs are ready for at the start of AAF, but could achieve over time
  – Eg, Audit: Could be self audit of identity management procedures for the first 2 years of AAF, then after that, potential for independent audit?
  – Other areas?
Additional Slides - screenshots

- The following slides were provided to accompany the AAF Shibboleth Operational Requirements and Recommendations consultation to provide annotated screenshots of how MAMS systems can support the requirements/recommendations
  - See http://federation.org.au/screenshots.pps
- Also include screenshots of other federation-enabled systems

AAF Shibboleth Systems

- The systems being developed by the MAMS team are:
  - Federation Manager (manages overall federation & members)
  - ShARPE (helps IdP Administrators manage attributes for services)
  - Autograph (helps end-users manage attributes & privacy)
  - People Picker (federated white pages services for finding users)
  - IAMSuite (web-based workspaces for virtual organisations)
  - NB: MAMS systems (except Federation Manager) will be available as validated software from the AAF Shibboleth support website

- The screenshots provided over are designed to illustrate the way these systems provide solutions to issues raised in the AAF Shibboleth Operational Requirements and Recommendations document
  - NB: Current screenshots may differ from final implementation
Federation Manager

• Federation Manager will be used to manage the overall AAF Shibboleth Federation, including:
  – Management of members, including contact details
  – Management of IdP details
  – Management of SP details
    • Including details of Service Offerings and attributes needed for these
    • Allows for limiting access of SPs to designated IdPs
  – Provision of custom federation metadata

  – NB: This system is run by the AAF for use by member institutions; members do not install this software

The AAF Federation Manager builds on the existing MAMS Level 2 Testbed Federation Manager, and adds features for managing IdPs, SPs, etc (demonstration screenshot shown)
Federation Manager provides forms for entering organisation details (IdP or SP). NB: Organisations are only added once AAF agreements are signed and organisations are validated.

Service Providers are added using forms similar to the example below. Configuration assistance for required fields will be provided.
Service Providers have the option of designating a Service as only available to certain members. This helps IdPs to manage only those SPs that are applicable to their organisation.

Service Providers also describe the specific “Service Offerings” they provide, and the attributes needed for these. Service Offerings can also be limited to designated IdPs.
This summary page shows the details for a particular organisation (in this case, a SP). It shows contact people, basic host information and specific SP (or IdP) information.

ShARPE

- ShARPE (Shibboleth Attribute Release Policy Editor) is a system for IdP administrators to assist with the management of services available to users

- ShARPE administrators can receive notification of new services as they become available, and can then choose to enable these automatically for end-users, or configure access for particular groups of end-users
  - ShARPE allows administrators to see the different “service offerings” of SPs to choose which of these are made available to different users
ShARPE provides a list of all Service Providers (based on information from Federation Manager) to allow the IdP Admin to configure end-user access to SPs according to attributes and desired Service Offerings.

This page shows an example Service Provider with three Service Offerings (Bronze, Silver and Gold), with the IdP Admin choosing to enable Bronze access for all users (Bronze access requires the "Affiliation" attribute).
ShARPE includes features for Attribute Mapping, which allows IdPs to map existing LDAP attributes (which may not match AAF attribute formats) to AAF formats.

**Autograph**

- Autograph is an optional system for end-user management of attribute release and privacy

- Autograph can be configured so all end-users see which attributes (either personal information only, or all attributes) about them are to be released on their first visit to a SP
  - Users can then approve this for all future access, approve for this session only, or choose not to access the SP

- Autograph can also allow end-users to view Service Offerings, and choose which attributes they will release (and hence show which Service Offerings are available)
Example showing Autograph “pop-up” page which appears after Shibboleth login, but before access to a service, showing personal information to be released (Shared Token in this case) for the relevant Service Offering.

This is the more detailed Autograph page showing all information about the user being released, as well as all potential Service Offerings which can be enabled; and the Attributes required for these.
Autograph can also present a “Terms and Conditions” page for users to agree to. This page can be presented prior to any use of the Shibboleth Federation & Autograph. Another use of this Terms and Conditions page is as an alternative to the Autograph functions shown in the previous two screenshots – IdPs may have users agree once to the release of their details to all relevant SPs (i.e., once agreed, no use of Autograph popup screens).

People Picker

- People Picker is a federated white pages service. It allows authenticated AAF end-users to search for other users (name and email address)
  - NB: This is a protected service only available to logged in AAF end-users (it is not available publicly on the web)
  - Usually only applies to staff members

- People Picker can also be used by AAF-approved Service Providers to designate individuals for access to services
  - This greatly reduces the burden on IdP administrators for managing individual access to Services via Entitlements
    - See IAMSuite example at end of slides
Example of People Picker search for "Williams", showing name, email address and (test example) IdPs.

Configure option allows for limiting search to specific IdPs.

NB: The AAF People Picker will have a (low) enforced result limit.
IAMSuite

- IAMSuite (Identity and Access Management Suite) is a toolkit for managing secure web workspaces for virtual organisations
  - IAMSuite can be provided as a Federation service or run locally

- IAMSuite provides tools for managing a set of SPs that are only relevant to particular VO workspaces, rather than the entire AAF Shibboleth Federation

- IAMSuite provides tools for delegating the management of particular workspaces to research team leaders or their sysadmins

IAMSuite login via existing Shibboleth login, or if relevant via a local OpenIdP login (applicable just to IAMSuite).
IAMSuite secure workspace, showing IAMSuite Shibboleth-enabled services (in this case DSpace repository); content folders; and workspace users and roles.

Example of integration of People Picker with approved Service Provider (IAMSuite) to allow workspace managers to find and select users to access to workspace.
Example Federation Applications

- **Muradora**: Secure Shibboleth-enabled repository
  - Uses XACML for access control policies

- **Online Librarian**: Live library reference desk enquiries

- **RAMS**: Online collaborative workflow system
  - (& LAMS: shared classes for elearning)

- **IAMSuite**: Secure online workspace management (see above)
  - Also includes Grid certificate integration
Shibboleth-based Online Librarian chat service

RAMS workflow authoring: Example of online research group meeting
IAMSuite integration with Grid Portlet for Certificates