Issues in federated identity management

Sandy Shaw
EDINA

IASSIST 24-27 May 2005, Edinburgh
Contents

- Federated identity management overview
- Open issues for federations
Introduction

• Federated identity management a live topic
• Both commercial and academic interest:
  – Liberty Alliance
  – Shibboleth (Internet2 – MACE)
• Both make use of SAML, which specifies rules for encoding security assertions
The familiar problem

- Users required to present different name/pass pairs for each service they use
- Addressed by the introduction of single-signon for local institutional services
- But distinct name/pass pairs are still often required for access to external services
Federated identity solution

- Use **locally-managed** credentials to enable access to **remote services**
- Extends the scope of single-signon to external services
Shibboleth

- Does neither authentication nor authorisation itself
- Conveys security assertions from Identity Provider (IdP) to Service Provider (SP)
- Security assertions (SAML) about:
  - user authentication
  - user attributes
- Privacy preserving
How does it work?

1. User requests access to a resource.
2. Resource Owner authenticates the user.
3. WAYF forwards the user's credentials.
4. HS checks the user's handle.
5. SHAR checks the user's handle.
6. AA checks the user's attributes.
7. Resource Manager grants access.

SWITCH
Benefits to users

SSO to local services
SSO to remote services (JISC IE)

Enables proliferation of secure services

once-only login screen
Management devolved to the institution

• Institution has control over choice of:
  – Authentication method (passwords, certs, …)
  – SSO system (pubcookie, CoSign, …)
  – Attribute store (LDAP, SQL, …)
  – Attribute disclosure policy

• The main cost is the integration effort required
Benefits to Service Providers

Hide N\times M users behind N IdPs

Federation metadata provides authoritative information on IdPs

ed.ac.uk  ncl.ac.uk

medium term
~50 UK sites
Working definition of federation

• A register of identity providers and service providers interworking in a common trust network

• Basis of trust:
  – reasonable expectation of behaviour
  – common understanding of obligations and rights

• …rather than technical assurance
What does a federation do?

- Acts as trusted third party to vet new members:
  - are they who they say they are?
  - do they speak for their organisation?
  - do they agree to federation policies?
- Maintains a list of members (metadata)
- Sets policies, such as acceptable CAs
UK activity

- JISC Core Middleware Programme
  - significant support for technical development projects and infrastructure

- SDSS project at EDINA
  - Shibboleth Development and Support Services
  - investigating federation development issues
Current Shibboleth status

- Shibboleth version 1.3 expected soon
  - use of (new) SAML 2.0 standard
- The federation model is still fluid
- Might develop in a variety of directions
Contents

- Federated identity management overview
- Open issues for federations
How many federations?

• Early view: one per country
• One federation implies:
  – single administrative framework
  – everyone on same development path
• Already three UK Education Federations
• So multiple federations (and multiple membership) already a reality
Federation interworking

• Required for international use:
  – InCommon
  – SWITCH
  – HAKA
• … and nationally (SDSS, Becta, Eduserv)
• Need more operational experience!
Virtual organisation support

• Examples of VOs:
  – Institutions sharing L&T responsibilities
  – Disparate groups of collaborating researchers
• Sub-federation / spanning federations
• Must be easy to create
• Relevance of GRID VO model?
Multiple identity assurance levels

• To cover a wider range of requirements:
  – cross-institutional access to e-Learning resources
  – access to high value e-Science resources
• Factors include:
  – value of resources protected
  – rigour of institutional identity management process
• Accommodate a range of levels in one federation?
• Or simply create distinct federations?
Metadata distribution methods

- Federation signs aggregated metadata (IdP and SP member details) in a single file
- Could separately sign each member's metadata as a discrete packet (SAML 2.0)
- Fetch on-the-fly
  - does this avoid revocation checking?
Next steps

• Deployment for live service
• Launch of UK production federation
• Further investigation of the technology
• Strive for commonality in approach (to enable future interworking):
  – attributes, certification, policy, assurance rules
• Many issues will be resolved over the next year
Further information

- Shibboleth: http://shibboleth.internet2.edu
- JISC Core Middleware Programme: http://www.jisc.ac.uk/index.cfm?name=programme Middleware
- SDSS project: http://sdss.ac.uk