Technical considerations for participation in the UK federation

Josh Howlett, JANET(UK)
Introduction

• Strictly, the UK federation has no technology requirements.
• Operationally, the UK federation is SAML-based
  – Security Assertion Mark-up Language
  – Widely implemented and deployed OASIS standard
• Practically, the UK federation is Shibboleth-based
  – A SAML implementation with a focus on federating Research and Education communities
  – It’s what almost everyone in the UK federation uses.
• ‘Can I use something other than Shibboleth?’
  – Yes; but we wouldn’t recommend it!
  – This may become easier in the future, but not anytime soon
Introduction

• An Identity Provider (IdP) **issues** assertions:
  – **authentication** assertions
    • “I claim that I have authenticated this user”
  – **attribute** assertions
    • “I claim that this user has the following properties…”

• A Service Provider (SP) **consumes** assertions.
  – for “service access control or presentation”
  – for “generating anonymised aggregated usage statistics”
Introduction

• Issuing and consuming assertions requires **trust**
  – “Is this personal information secured from eavesdroppers?”
  – “Is the organisation who they claim to be?”
  – “Is this organisation a member of the UK federation?”
  – “Can I prove that an organisation issued a false assertion?”

• The UK federation provides a **trust fabric** that facilitates the exchange of assertions between participating members.
  – The lack of a trust fabric (e.g. OpenID) significantly reduces the benefits of federation.
Introduction

• What you need to consider
  – Shibboleth Identity Provider
    • issues assertions about your users to SPs.
  – Authentication service
    • authenticates your users, on behalf of the IdP.
  – Attribute store
    • stores information about your users, on behalf of the IdP.
  – Certificates
    • allows your IdP to prove to other UK federation members that it speaks for your organisation.
    • also useful for securing the authentication service.
  – Metadata
    • used by your IdP to establish that SPs are UK federation members.
Identity Provider

• Shibboleth IdP is a Java application
  – Runs on Linux, Unix, Windows, Mac.
• Installation is straightforward.
• Configuration complexity varies, depending on the other parts of your infrastructure that it uses.
Authentication service

- The authentication service informs the Identity Provider who the user is.
- This allows the use of different authentication methods.
- The Identity Provider is typically a client of an Institutional single sign-on service.
Authentication service

User browses to SP

User

Service Provider

Authentication service

Password or Certificate or Kerberos etc

Authentication request

FORM-based authentication protocol, or Certificate authentication protocol, or Windows Integrated Authentication protocol, or

Credential store

Shibboleth IdP

“User”

Generally LDAP or SQL
Authentication service

• **What to do next**
  – Which credential store are you going to use?
  – Do you already have an authentication service?
    • it will probably work, but check with the Vendor; if it won’t work, or…
  – If you don’t have an authentication service
    • A Tomcat-based authentication form is distributed with Shibboleth.
    • Consider using a Web SSO service
      – CAS, Pubcookie, WebAuth; or many commercial options.
    • For development and testing purposes, ‘Basic’ web server authentication can be useful.
Attributes

• Most service providers require one or more attributes describing each user.
  – may determine a user’s access privileges
  – allows a service to provide personalisation

• The IdP collects attributes corresponding to the authenticated user from an attribute store.
  – typically an LDAP directory or SQL database.

• Attributes can also be generated by scripts.
Attributes

• UK federation “core” attributes
  – eduPersonScopedAffiliation
    • controlled vocabulary (e.g. member@dev.ja.net)
  – eduPersonEntitlement
    • SP-specific values describing user privilege(s)
  – eduPersonPrincipalName
    • a global “persistent identifier” for the user (e.g. joshh@dev.ja.net)
  – eduPersonTargetedID
    • a pseudonymous identifier for the user, specific to the SP.

• Other attributes (e.g. from the eduPerson or other LDAP schema) may also be used if necessary.
Attributes

- Example attribute requirements

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Service</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elsevier</td>
<td>ScienceDirect</td>
<td>eduPersonTargetedID</td>
</tr>
<tr>
<td>Internet2</td>
<td>Shib Wiki</td>
<td>eduPersonPrincipalName</td>
</tr>
<tr>
<td>JISC</td>
<td>JISCmail</td>
<td>eduPersonTargetedID</td>
</tr>
<tr>
<td>MIMAS</td>
<td>Hairdressing</td>
<td>eduPersonScopedAffiliation</td>
</tr>
<tr>
<td></td>
<td>Training</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Landmap</td>
<td>eduPersonPrincipalName</td>
</tr>
</tbody>
</table>
Attributes

1. User does something
2. Attribute request
3. Attribute look-up
4. Attribute response

User

Service Provider

Shibboleth IdP

Attribute store(s)
Attributes

• What to do next
  – Do you have a single authoritative source of user information?
    • It’s not necessary, but highly desirable.
  – How are you going to manage user attribute release policies?
    • DPA 1998 requires “informed consent”
  – If you might be federating internal resources, consider the benefits of exposing a richer set of attributes to them.
Certificates

• Trust fabric certificates
  – Used by IdPs and SPs to authenticate each other, and protect assertions.
  – Must be issued by an accredited certificate authorities
    • JANET SCS, UK e-Science CA, GlobalSign, Thawte, VeriSign.

• Browser facing certificates
  – Out of scope of the UK federation, but useful to consider.
  – Allows users, if necessary, to authenticate the authentication service or Service Provider.
  – Use a certificate from any CA that meets your requirements.
Certificates

• What to do next
  – Determine where to acquire your trust fabric certificate(s) and browser-facing certificate(s).
  • JANET(UK) Server Certificate Service
    – http://www.ja.net/services/scs.html
Metadata

• What is federation metadata?
  • “In architecture, a keystone is the stone at the top of an arch. It is the supporting element for the entire arch — without it the arch would collapse.” – Wikipedia

– Functions
  • A directory of federation participants – where?
  • A description of their capabilities – what?
  • Establishment of technical trust – who?
Metadata

• **What to do next**
  – Understand the declarations that you will be asked to make when your entities are added to the UK federation metadata.
  – Ensure that your IdP is configured to regularly (at least once a day) refresh its UK federation metadata.
Other considerations

• Networking
  – IdP typically requires tcp/8443 from any.
  – Authentication service probably requires tcp/443 from any.

• Resilience
  – Two high availability options
    • HAShib
    • CryptoShibHandle
Conclusions

- Join the UK federation now, irrespective of technical readiness.
- Audit your existing infrastructure and identify and address any deficiencies.
- Acquire certificates & register entities.
- Implement your IdP.
- Test, and build confidence.
- Consider federating internal services.
Questions?

More info:  
www.ukfederation.org.uk

E-mail lists:  
Ukfederation-announce@jiscmail.ac.uk
Ukfederation-discuss@jiscmail.ac.uk