Authentication issues in VO: Integrating Shibboleth with FAME and PERMIS
Authentication and authorisation in VO

In a VO environment:
- services are provided by dissimilar organisations from different administrative domains
- services are protected with dissimilar security policies and measures

We need a flexible authentication framework that supports:
- the use of various authentication tokens
- links the strength of the authentication token/method used with access control decision
## Level of Assurance

- Various authentication tokens/methods provide different Levels of Assurance (LoA)
- NIST recommendation: 4 LoAs based on strength of authentication token & protocol

<table>
<thead>
<tr>
<th></th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard token</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Soft token</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Zero knowledge password</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>One-time password</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Password</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
Examples

- IP-based authentication may be sufficient for library catalogue browsing from within campus
- Students viewing exam papers may use username/password pairs
- Lecturers updating exam papers may use certificates
- Medical doctors uploading private patient records may use smart cards
Shibboleth

- Infrastructure for enabling inter-institutional sharing of Web resources that are subject to authentication and access control
- User authentication is responsibility of origin organisation (identity provider)
- User authorisation is responsibility of target site (resource provider)
- Origin and target – members of the same trust federation
Shibboleth-FAME-PERMIS Integration

FAME

Authentication System

SHIBBOLETH ORIGIN

1. www.site.ac.uk/res

2. 

3. 

4. Handle

5. Handle

6. Attributes + LoA

SHIBBOLETH TARGET

Web Resource www.site.ac.uk/res

Target (resource provider)

Origin (identity provider)

PERMIS

Access Control Engine

7. 

8. 

www.site.ac.uk/res
Contact details

■ Dr. Ning Zhang
  – nzhang@cs.man.ac.uk
■ Dr. Alexandra Nenadic
  – anenadic@cs.man.ac.uk
■ Web: www.fame-pemis.org