# A Shibboleth Service Provider for OGC Web Map service

Shibboleth is a standards based open source package from Internet2 for web single sign-on across administrative boundaries. It allows informed authorisation decisions for individual access of protected resources in a privacy-preserving manner. The Open Geospatial Consortium (OGC) is a standards defining organisation working in the area of open geospatial interoperability. OGC standards are used globally across different sectors to exchange, store and process geographic information. This poster is reporting on a project that integrated Shibboleth with the OGC Web Map Service – the significance is the potential for establishing production strength access management federations that allow the sharing of a vast array of geospatial information using a standardised approach.

Shibboleth Interactions with Web Resources
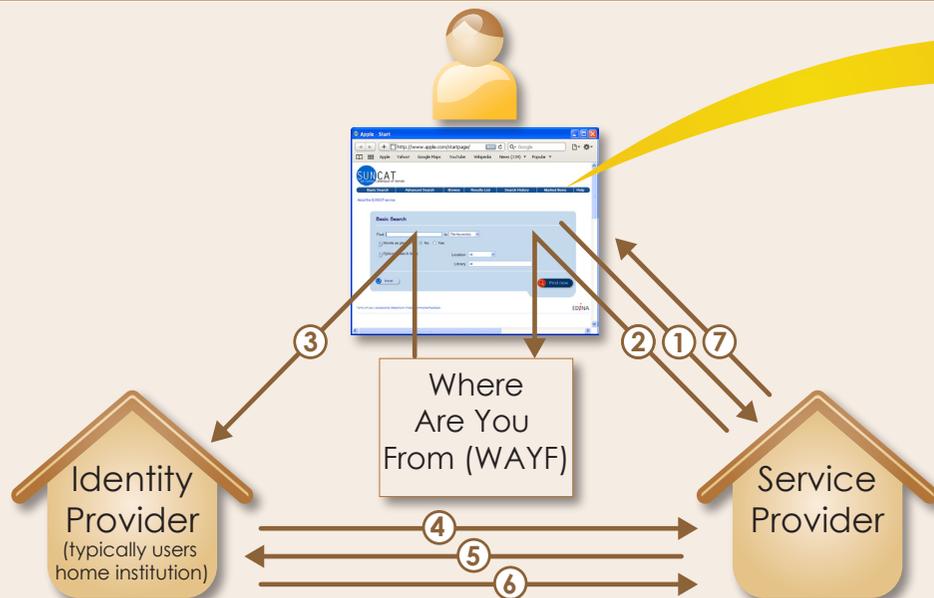
1. Application attempts to access a Shibboleth protected resource on service provider site
2. User redirected to WAYF in order to select home institution
3. User authenticates by whatever means Identity Provider deems appropriate
4. Handle generated for user and passed to service provider
5. Handle used to request attribute information for user
6. Identity Provider makes attributes available depending on their attribute release policy
7. Based on attributes, service provider decides whether the user is authorised to access the resource or not

Shibboleth Interactions with OGC Web Services
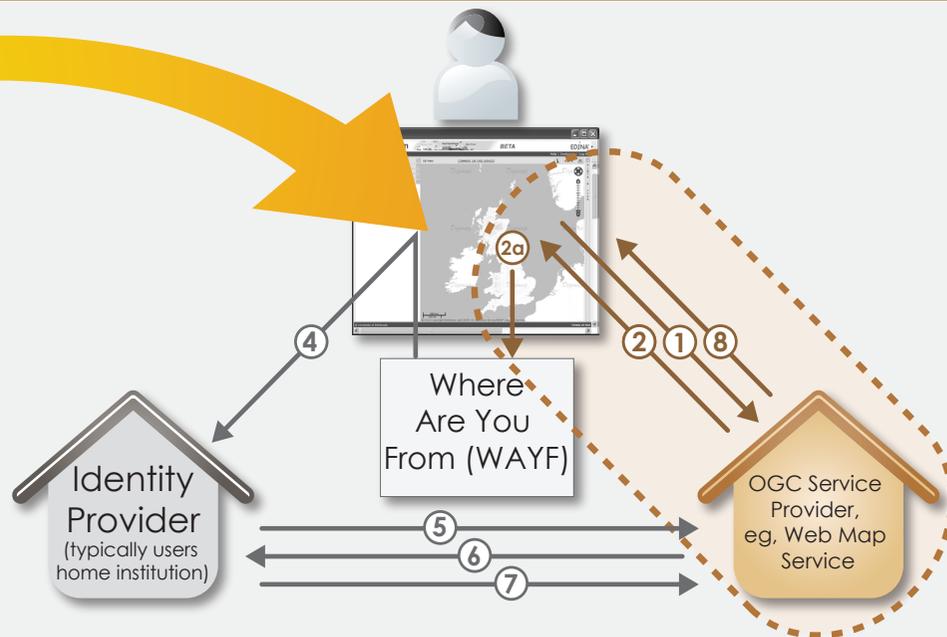
1. Application attempts to access a Shibboleth protected OGC Web Service (OWS)
2. Application receives an OWS exception informing that service is Shibboleth protected
2a. Application recognises exception and initiates typical Shibboleth interactions, ie, user redirected to WAYF in order to select home institution
3. User authenticates by whatever means Identity Provider deems appropriate
4. Handle generated for user and passed to service provider
5. Handle used to request attribute information for user
6. Identity Provider makes attributes available depending on their attribute release policy
7. Based on attributes, service provider decides whether the user is authorised to access the resource or not.
8. In this case, if the user is authorised; an OGC capabilities document containing a rewritten service URL with an embedded session ID is returned. This URL is used in all subsequent OWS interactions, eg, getMap. getFeatureID, etc.

Some key issues/points:

- **Demonstrated protection of OGC Web Map Server (WMS) using out-of-the-box Shibboleth without requiring any alteration to the WMS interface**
- **Requires installation of gatekeeper software around the OGC Web Service (OWS)**
- **Requires OWS clients capable of initiating the Shibboleth access management interactions**
- **Work underway investigating applicability to other OWS**

Supported by
JISC

EDINA

der Bundeswehr
Universität München

OGC®
Open Geospatial Consortium, Inc.