



# Security Mash-up with the MashMyData Project: Delegation and Workflows with OPeNDAP and OGC Based Services

Philip Kershaw [[philip.kershaw@stfc.ac.uk](mailto:philip.kershaw@stfc.ac.uk)] (CEDA)

Stephen Pascoe (CEDA)

Ag Stephens (CEDA)

Jon Blower (Reading e-Science Centre)

Alastair Gemmell (Reading e-Science Centre)



British Atmospheric  
Data Centre

NATIONAL CENTRE FOR ATMOSPHERIC SCIENCE  
NATURAL ENVIRONMENT RESEARCH COUNCIL



Reading  
e-Science  
Centre

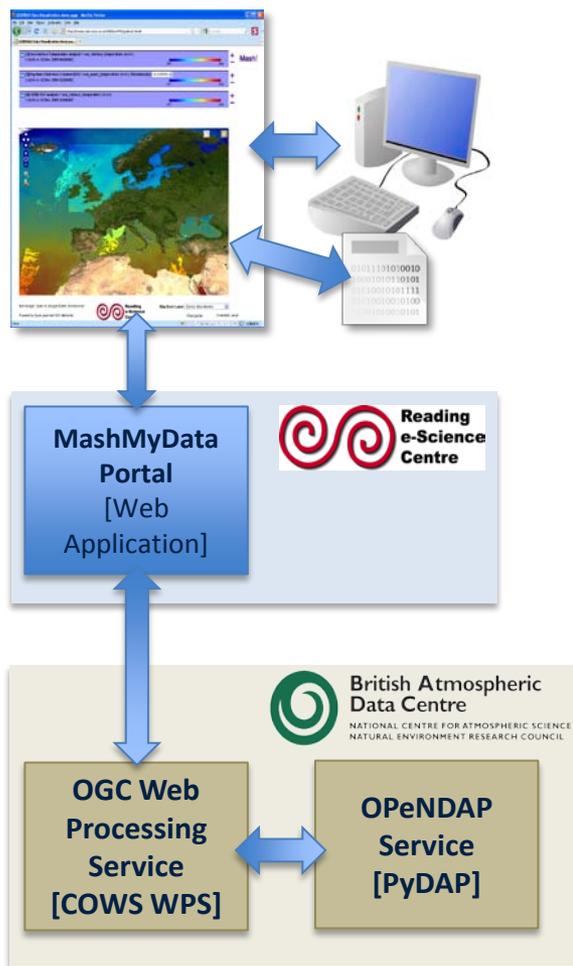
Centre for Environmental  
Data Archival

SCIENCE AND TECHNOLOGY FACILITIES COUNCIL  
NATURAL ENVIRONMENT RESEARCH COUNCIL





# Background and Aims



- **NERC** (Natural Environment Research Council) funded *Technology Proof of Concept* project
- Aim: enable environmental scientists to combine and overlay geospatial data quickly and easily
- Mash-up: Users can upload *their own data* and compare it with data pulled from other sources.
- MashMyData explores a use case of multiple services working together to perform retrievals and intercomparison of datasets.
- Sprint style development approach
- CEDA OGC Web Processing Service (WPS) performs calculations on data in situ as a means to avoid large data transfers
- BIG challenges for access control and security...



# Mash-My-Security

*Mash!*

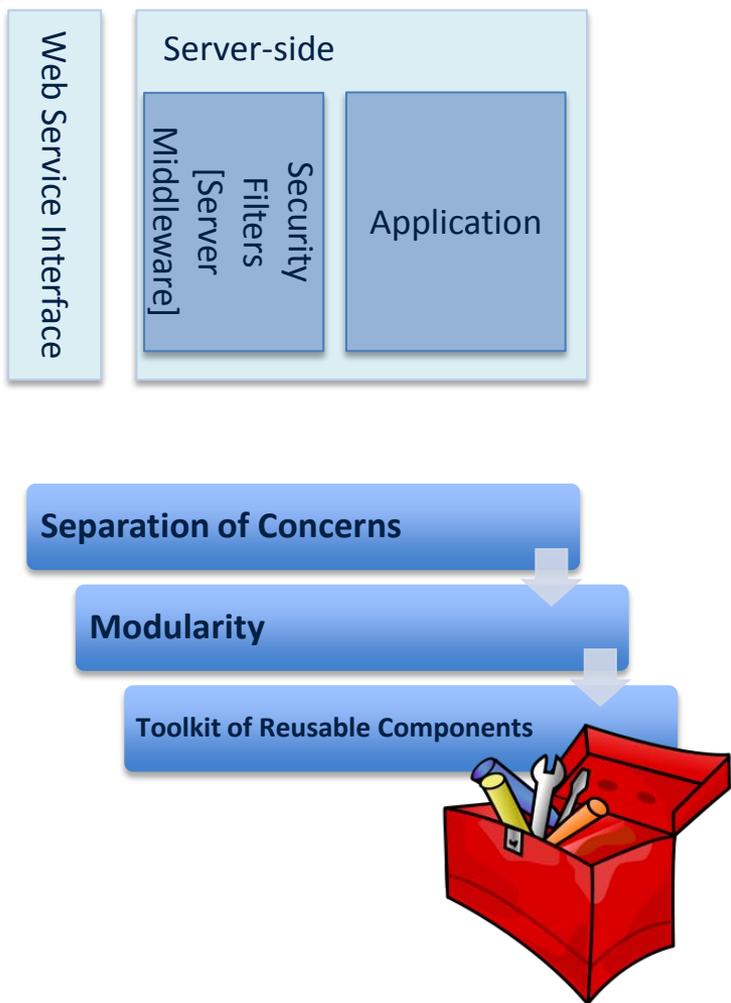


- MashMyData: a **short** technology proof of concept project
  - What could we mash-up quickly?
  - Sprint approach where practicality valued over beauty
- The security mash-up implementing and exploiting these ingredients ...
  - **Federation, Delegation, Translation**
- **Federation:**
  - large distributed datasets, international collaborations are drivers for security solutions which can cross organisational domains
- **Delegation:**
  - a service needs to access some secured resource on a user's behalf
- **Translation:**
  - credentials may need to be translated from one domain to another





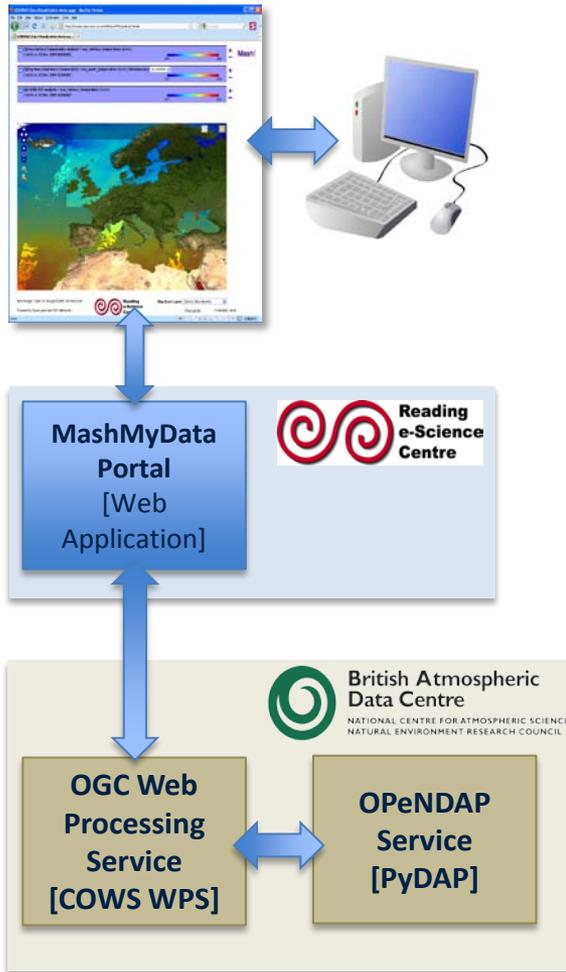
# Federation: using ESGF



- Interfaces across **organisational boundaries**:
  - Defined interfaces with web services OpenID, SAML
- Slicing up the server side functionality:
  - Maintain a separation of concerns between **access control functionality** and **application** to be protected
  - Modular Security filters
  - Dual authentication mechanisms: OpenID and PKI
- Client Side:
  - Security hooks integrated into NetCDF client libraries
- Use ESGF authorisation infrastructure



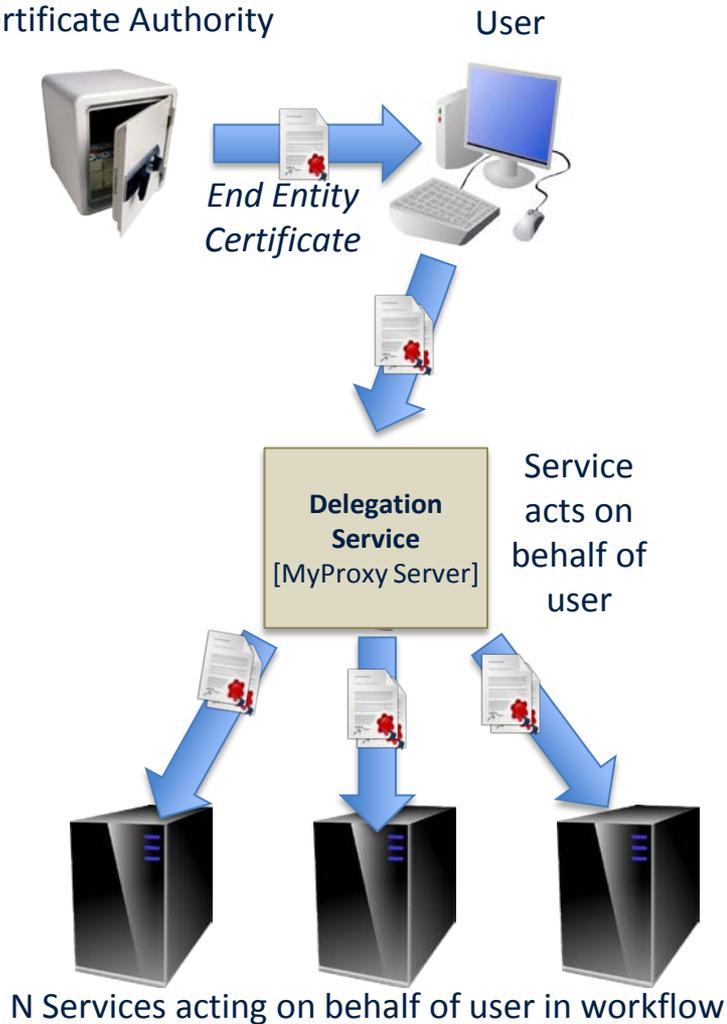
# Delegation



- Only an *authorised* user may access the WPS
- The Portal wishes to access it on *behalf* of the user
- Therefore the Portal needs some credential which gives it the same access rights as the user
- Solutions
  - OAuth: security filters could be added but ...
  - Proxy certificates: easier to add ESGF
- For the purposes of this talk, we focus on solution based on proxy certificates



# Delegation with Proxy Certificates



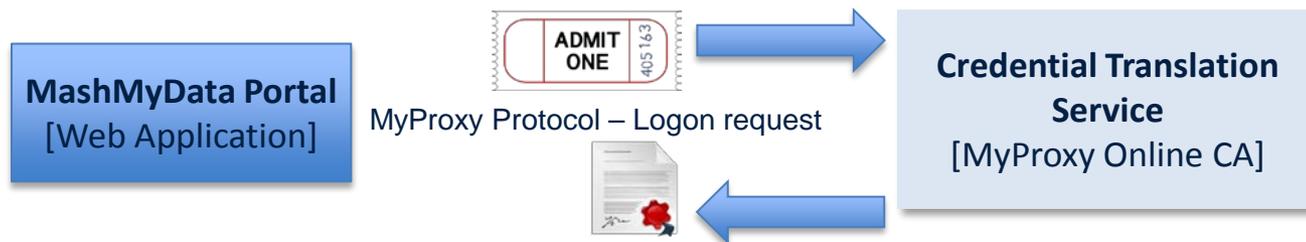
- Certificate Authority signs user **End Entity Certificate**
- **Proxy certificate** signed by user's certificate delegates authority to service to act on its behalf
- MyProxy acts as a repository
- Hold proxy certificates issued by user certificate
- Any number of services can obtain further proxy certificates from MyProxy



# Translation

- ESGF supports two authentication technologies – **Why?!**
  - OpenID is browser-centric with implicit user interaction
  - But we need non-interactive, non-browser based access for scripts and rich clients: SSL / certificate-based solution
- Users authenticate at the MashMyData Portal *interactively* via a *browser* with OpenID
- The Portal needs to authenticate with WPS *non-interactively* without a *browser*
- We need to *translate* from OpenID to a certificate

*I, the Portal assert that this user with this OpenID authenticated*



*New User End Entity Certificate*



# Bringing it Together

1) A user accesses the **MashMyData Portal**

2) They select some datasets for an intercomparison operation requiring a process run by the WPS.

5) translate user's OpenID to a user certificate using the **Credential Translation Service**. The Portal uses this to authenticate with the WPS.

7) The portal also provisions a **Delegation Service** with a **proxy certificate** configuring it to enable the WPS to get a proxy certificate

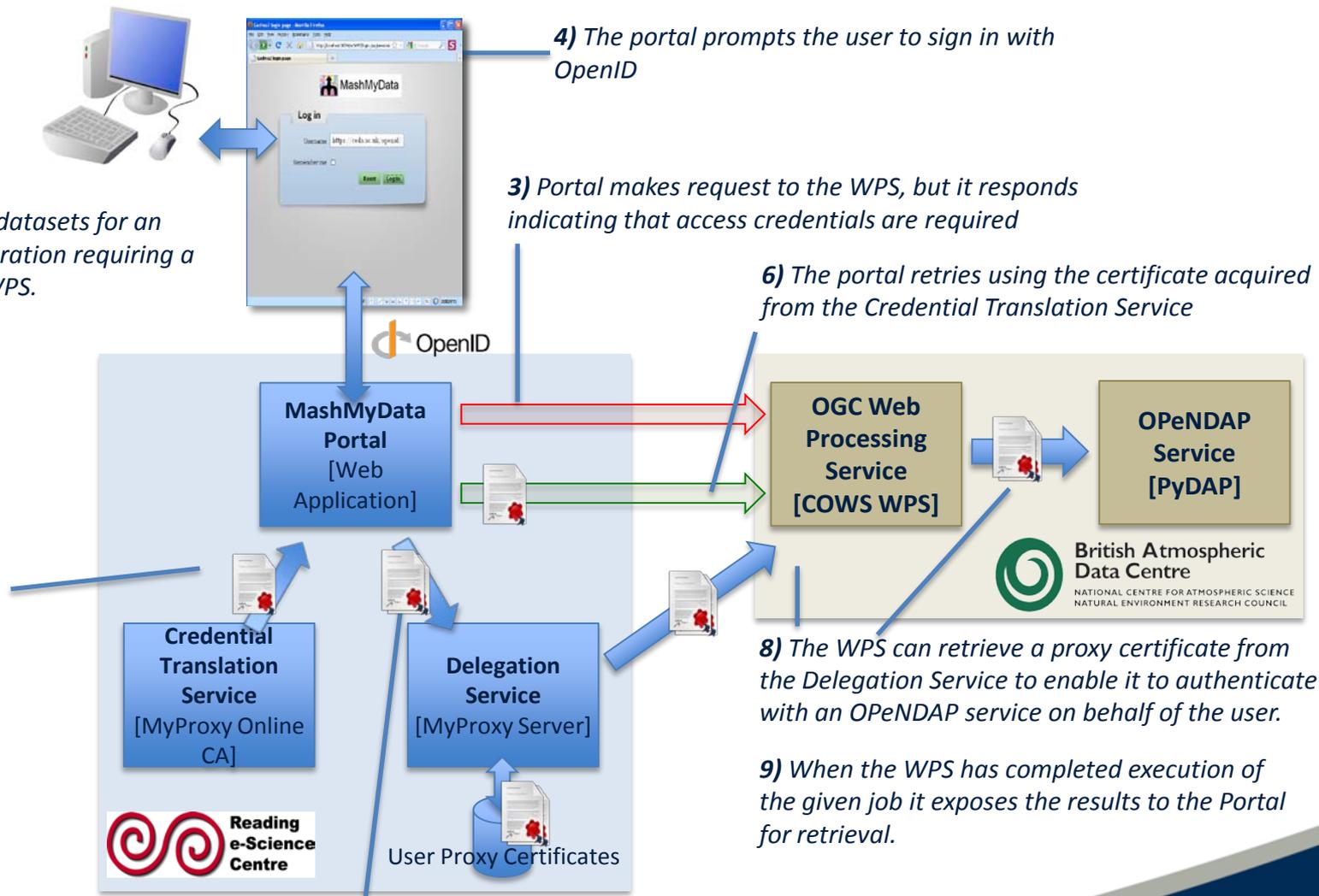
4) The portal prompts the user to sign in with OpenID

3) Portal makes request to the WPS, but it responds indicating that access credentials are required

6) The portal retries using the certificate acquired from the **Credential Translation Service**

8) The WPS can retrieve a proxy certificate from the **Delegation Service** to enable it to authenticate with an **OPeNDAP** service on behalf of the user.

9) When the WPS has completed execution of the given job it exposes the results to the Portal for retrieval.



# Summary and Future Work

- Federation
  - Mediating access across independent organisational domains
  - MashMyData builds on all the ground work with ESGF
- Delegation
  - ESGF doesn't support this
    - But we can easily add support for proxy certificates
    - Modification to server-side SSL set-up
  - Breaking new ground in this domain, new to OPeNDAP over HTTP
- Proxy certificates won as solution vs. OAuth?
  - A twist in this tale: OAuth supports delegated *authorisation* ...
  - Whereas proxy certificates are delegation by 'impersonation'!
  - Further work with OAuth over the remainder of the project
- Credential Translation – why is this important?
  - Extending ESGF to interoperate with systems using other security technologies
  - Translation of credentials to be compatible with them
  - European Grid Initiative, Shibboleth ...

