Towards FIM as a Service: Federated Identity Management for the Contrail Cloud Project

5th FIM4R Meeting, PSI Villigen
20 March 2013

Philip Kershaw, NCEO/Centre for Environmental Data Archival, STFC RAL
Jens Jensen, Scientific Computing Department, STFC RAL

Defining FIM as a Service

- Generic package for enabling federated identity management for an application, services or whole system
- Which would support multiple technologies for SSO
  - SAML
  - OpenID
  - WS-Federation
  - Moonshot
  - …
- Package as
  - Software packages
  - Certified VM image(s)
  - Or SaaS?! Delegating IdM to another party is implicit in this
- Contrail is offering *one* approach …

What is Contrail?

contrail

open computing
infrastructures
for elastic
services

- Building a system for federating multiple cloud providers
- Support for OpenNebula
- IaaS but also
- ConPaaS
  - Standard offerings like LAMP
  - Task scheduling
- Federated storage GAFS
- Virtual (secured!) networks
- SLA negotiation
- … and **FIM** (STFC-led)
- http://contrail-project.eu

COOPERATION

contrail is co-funded by the
EC 7th Framework Programme

Funded under: FP7 (Seventh Framework Programme)

Area: Internet of Services, Software & Virtualization (ICT-2009.1.2)

Project reference: FP7-IST-257438

Total cost: 11,29 million euro

EU contribution: 8,3 million euro

Execution: From 2010-10-01 till 2013-09-30

Duration: 36 months

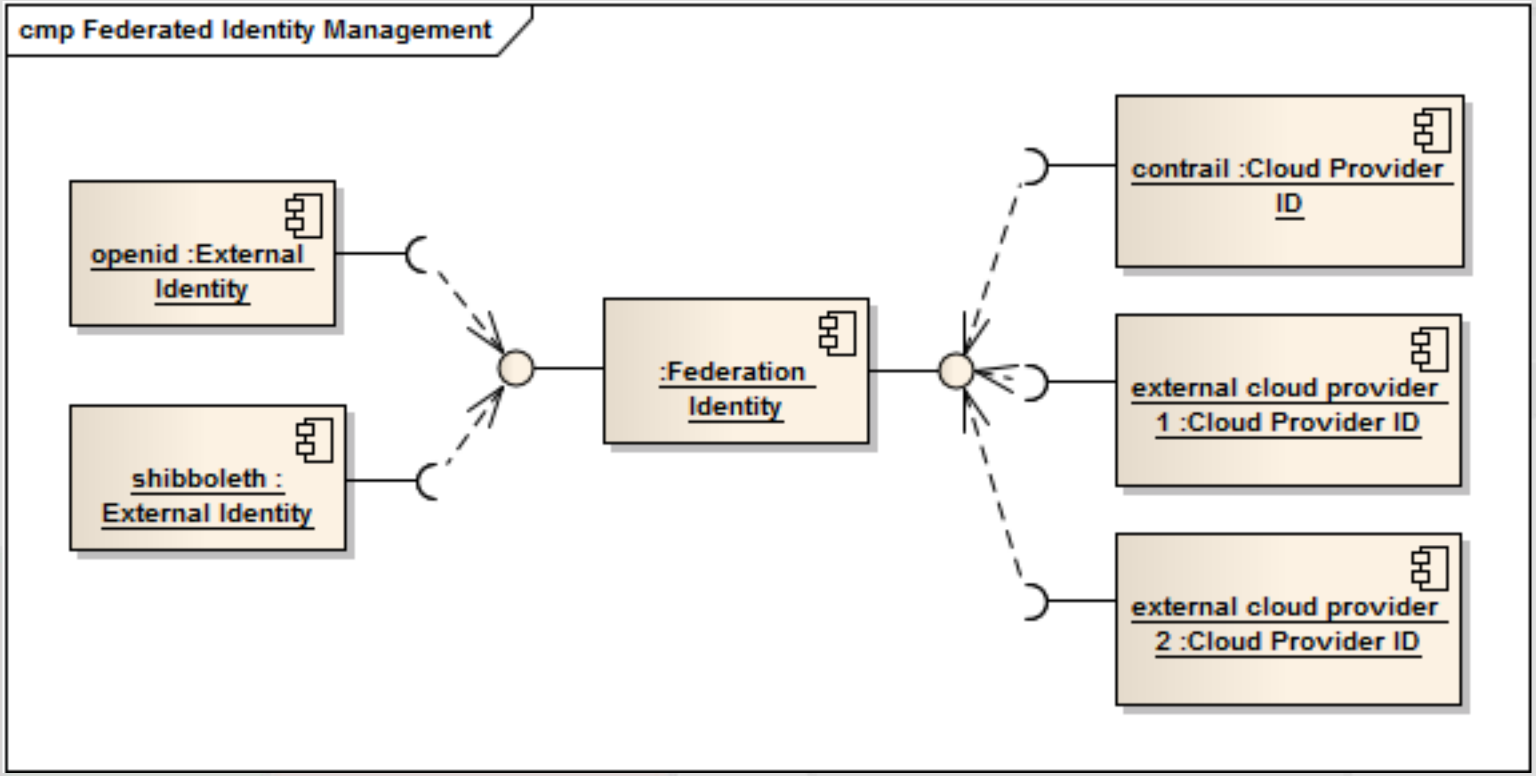
Contract type: Collaborative project (generic)

Contrail and FIM

- Provide *federated* access to *federated* clouds
  - Pragmatic: use (for the most part) existing components
  - Need for standards-based components which interoperate
  - Promote re-use by modularity and SOA
- Federated identity
  - Using external identity providers – OpenID
  - Using existing identity federations – Shibboleth
- Generate internal credential
  - Unified credential, independent of the choice of external credential
  - Using short-lived X.509, with attributes

FIM as a Service

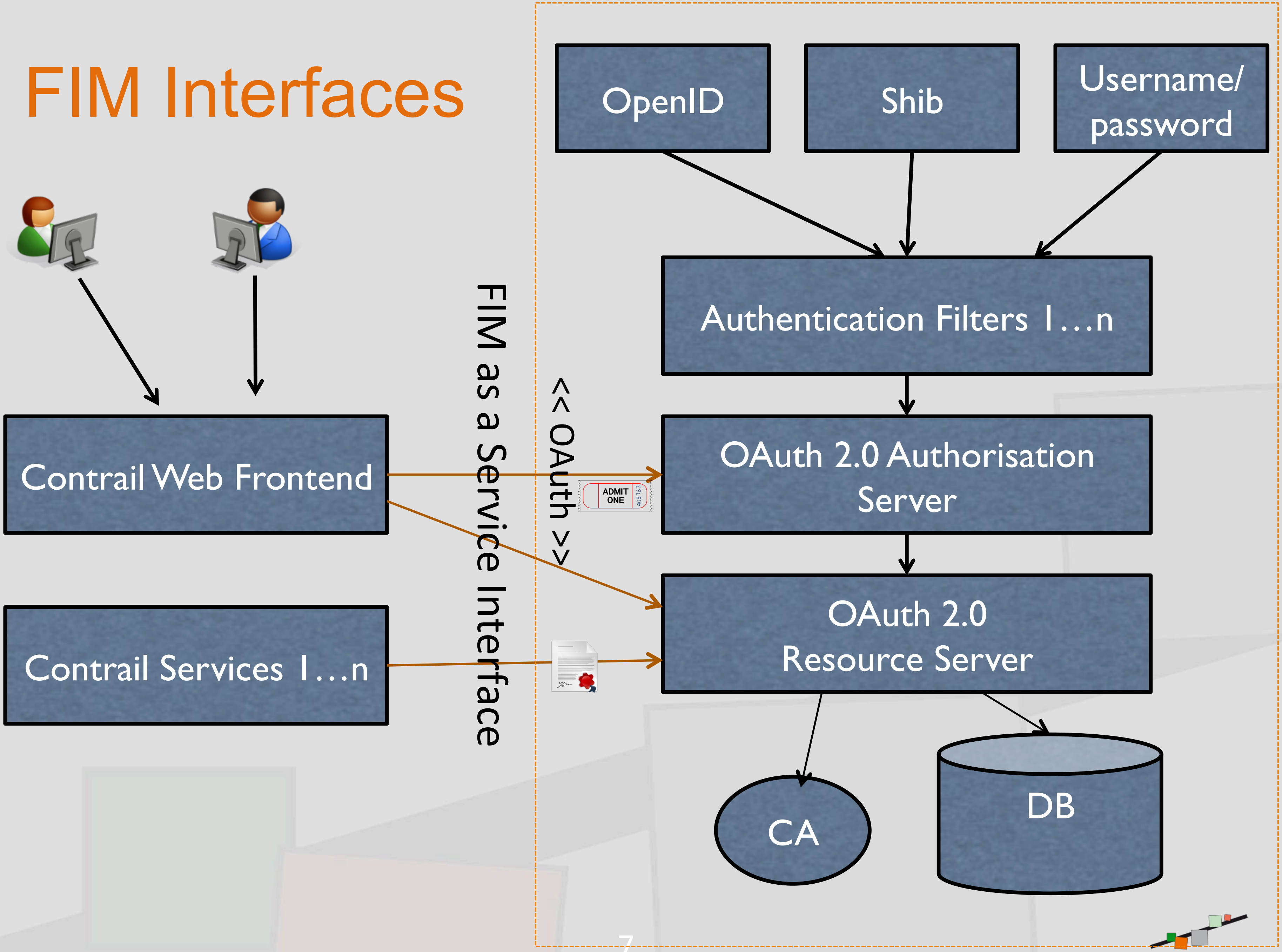
- Modular architecture and well-defined interfaces are essential to enable a standalone FIM as a Service component


cmp Federated Identity Management
openid :External Identity
shibboleth : External Identity
:Federation Identity
contrail :Cloud Provider ID
external cloud provider 1 :Cloud Provider ID
external cloud provider 2 :Cloud Provider ID

More about Contrail: Delegation

- Needed to enable various actors in the Contrail SOA to act on user's behalf
- "Delegation" of *identity* credentials *not* authorisation
  - A pragmatic approach
- Based on use of OAuth 2.0
  - Delegatee obtains permission for delegation (access token)
  - Can then obtain a credential (short-lived X.509 cert) from Resource server
  - Version 2.0 offered alternative flows such as *Client Credentials* which makes it more flexible
- Scope and permissions for delegated certificates
  - OAuth centrally controls release using OAuth client id and access token
  - Pro: prevent "unauthorised" delegation of credential (but not GSI deleg.)
  - Con: need for central online CA (which we needed anyway)
- Simple RESTful HTTP interface

FIM Interfaces



FIM as a Service Interface

<< OAuth >>

Contrail Web Frontend

Contrail Services 1…n

OpenID

Shib

Username/ password

Authentication Filters 1…n

OAuth 2.0 Authorisation Server

OAuth 2.0 Resource Server

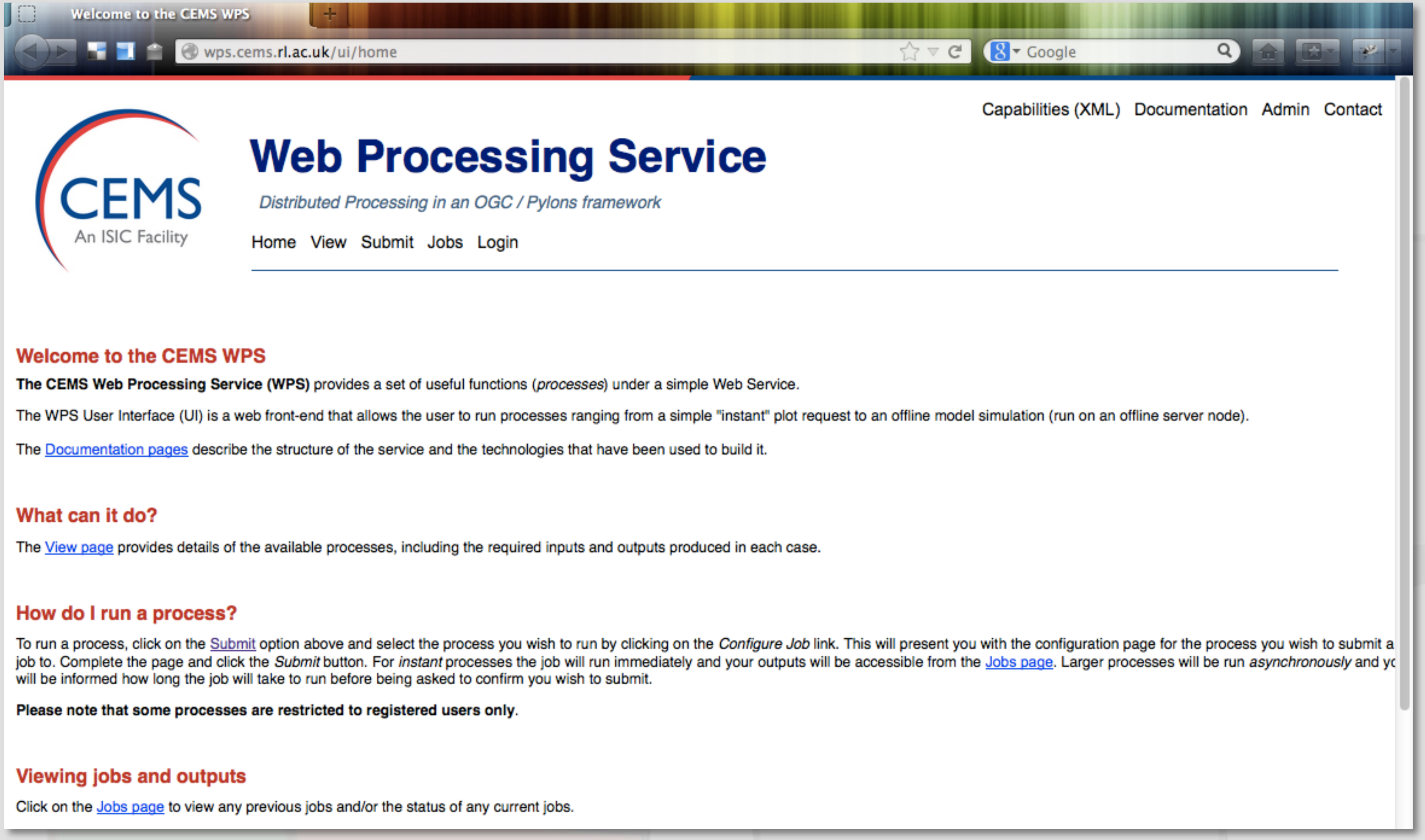
CA

DB

OAuth and FIM Deployments and Plans

- CEMS OGC Web Processing Service and Web Map Service
  - Web service wrapper to processing algorithm, delegation is essential
  - The original motivating work for development of *ndg_oauth*
  - CEMS (facility for Climate and Environmental Monitoring from Space), Harwell UK
  - Python implementation
- CLARIN project
  - At MPI the software is being used to integrate some tools in the CLARIN infrastructure
- EUDAT project
  - Re-using Contrail framework
  - Need to support both OpenID and Shibboleth
  - Also OAuth for ORCID support
  - Need for robust and resilient services
  - Need to support "long tail" researchers (who are not affiliated to an institution)

CEMS Deployment



Welcome to the CEMS WPS
wps.cems.rl.ac.uk/ui/home
Google
Capabilities (XML) Documentation Admin Contact
CEMS
An ISIC Facility

Web Processing Service

Distributed Processing in an OGC / Pylons framework

Home View Submit Jobs Login

Welcome to the CEMS WPS

The CEMS Web Processing Service (WPS) provides a set of useful functions (*processes*) under a simple Web Service.

The WPS User Interface (UI) is a web front-end that allows the user to run processes ranging from a simple "instant" plot request to an offline model simulation (run on an offline server node).

The Documentation pages describe the structure of the service and the technologies that have been used to build it.

What can it do?

The View page provides details of the available processes, including the required inputs and outputs produced in each case.

How do I run a process?

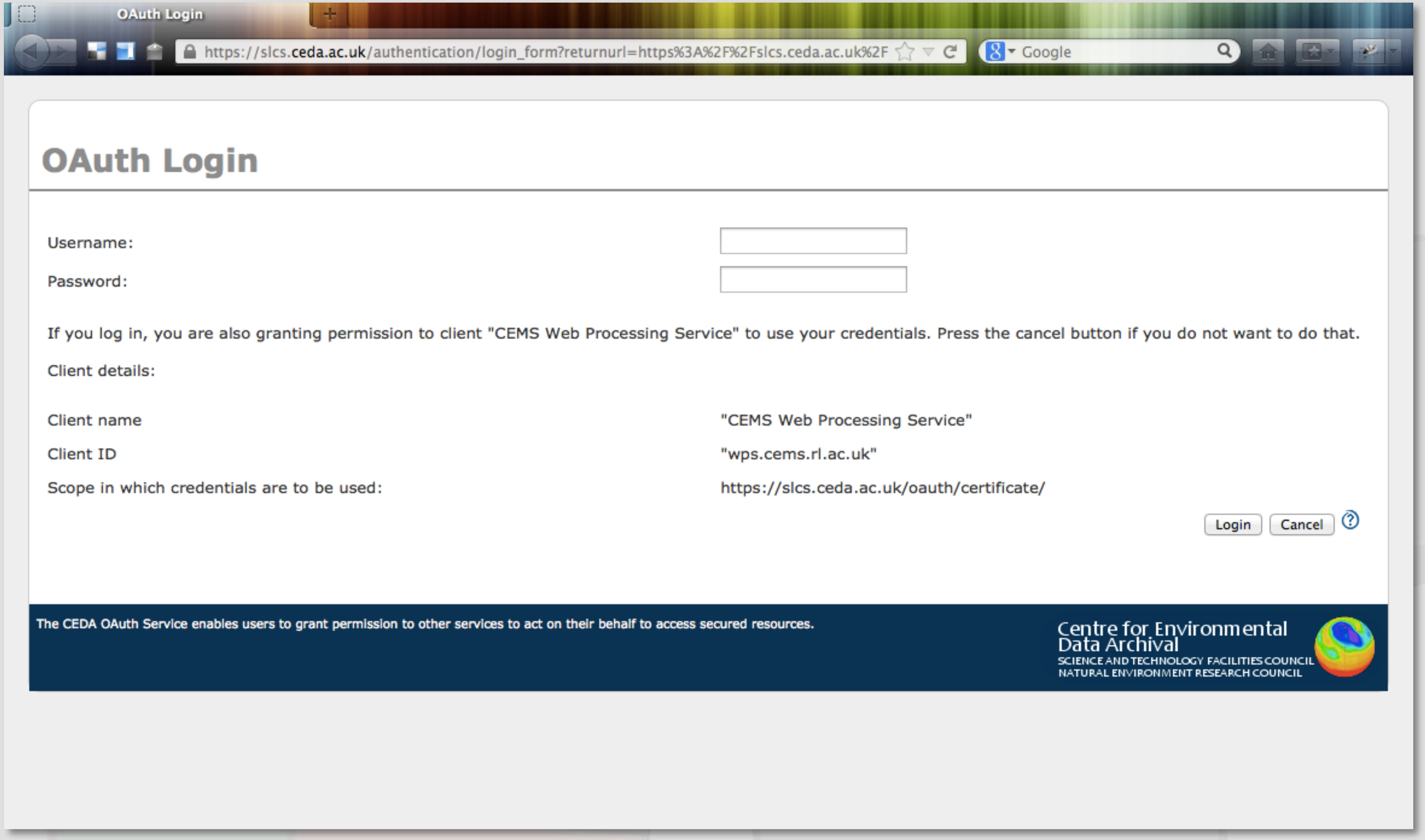
To run a process, click on the Submit option above and select the process you wish to run by clicking on the *Configure Job* link. This will present you with the configuration page for the process you wish to submit a job to. Complete the page and click the *Submit* button. For *instant* processes the job will run immediately and your outputs will be accessible from the Jobs page. Larger processes will be run *asynchronously* and yc will be informed how long the job will take to run before being asked to confirm you wish to submit.

Please note that some processes are restricted to registered users only.

Viewing jobs and outputs

Click on the Jobs page to view any previous jobs and/or the status of any current jobs.

CEMS Deployment



OAuth Login
https://slcs.ceda.ac.uk/authentication/login_form?returnurl=https%3A%2F%2Fslcs.ceda.ac.uk%2F
Google

OAuth Login

Username:

Password:

If you log in, you are also granting permission to client "CEMS Web Processing Service" to use your credentials. Press the cancel button if you do not want to do that.

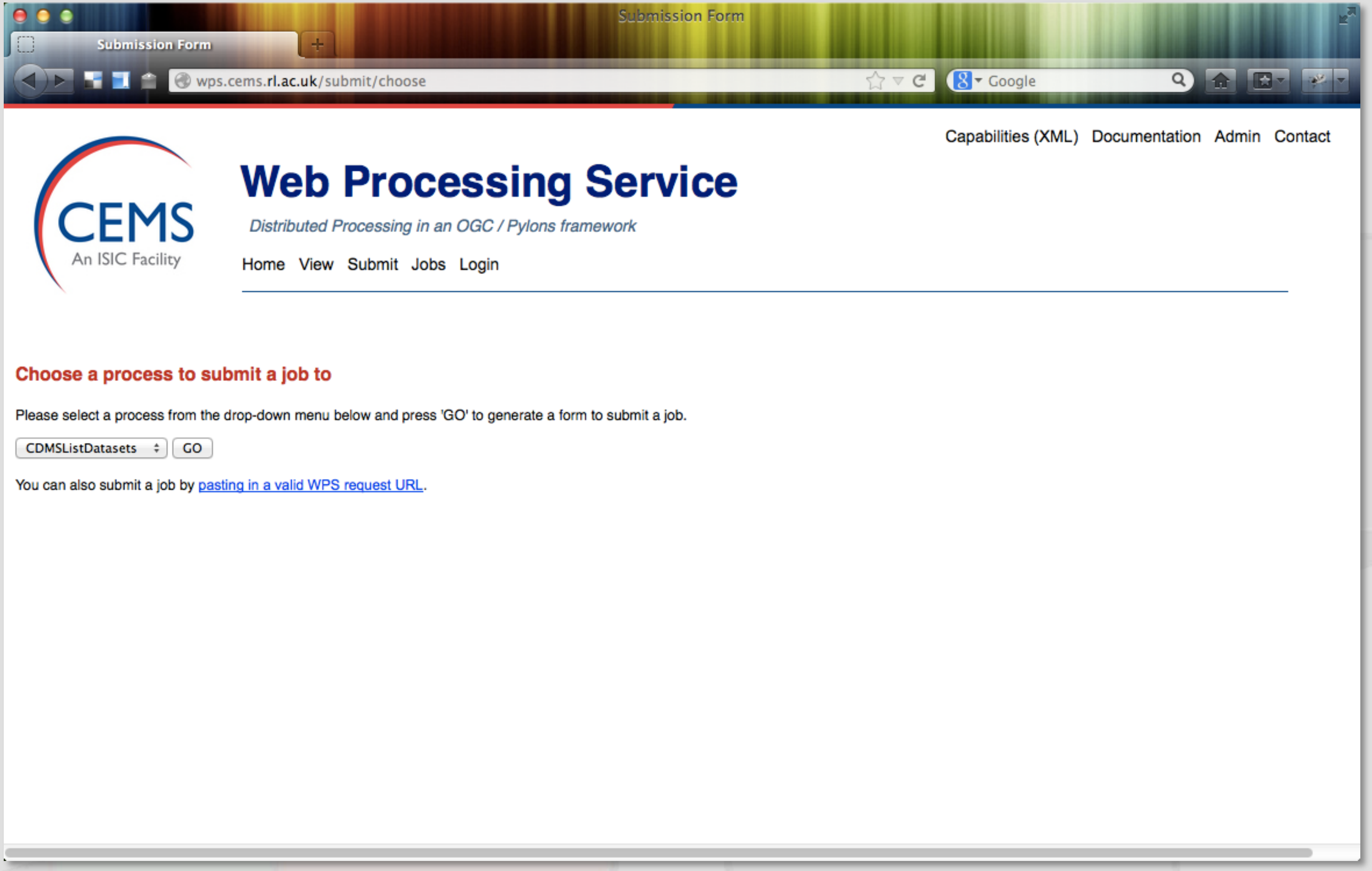
Client details:

Client name	"CEMS Web Processing Service"
Client ID	"wps.cems.rl.ac.uk"
Scope in which credentials are to be used:	https://slcs.ceda.ac.uk/oauth/certificate/

The CEDA OAuth Service enables users to grant permission to other services to act on their behalf to access secured resources.

Centre for Environmental Data Archival
SCIENCE AND TECHNOLOGY FACILITIES COUNCIL
NATURAL ENVIRONMENT RESEARCH COUNCIL

CEMS Deployment



Submission Form
Submission Form
wps.cems.rl.ac.uk/submit/choose
Google
Capabilities (XML) Documentation Admin Contact
CEMS
An ISIC Facility

Web Processing Service

Distributed Processing in an OGC / Pylons framework

Home View Submit Jobs Login

Choose a process to submit a job to

Please select a process from the drop-down menu below and press 'GO' to generate a form to submit a job.

You can also submit a job by pasting in a valid WPS request URL.

Contrail OAuth Demo

- Contrail partner XLab (SME based in Slovenia) have developed Java OAuth 2.0 and SAML 2.0 implementations
- (Also tested pySAML and SimpleSAMLphp)
- file:///Users/philipkershaw/Documents/Federated%20Identity%20Workshops/PSI/OAuthDemo.swf

Future directions

- Improve reuse/sharing of code as much as possible
- No single technology:
  - Mix of OAuth, OAuth2, SAML, OpenID, X.509, Moonshot
  - Maybe not all will survive but we will have more than one
  - Need to support “long tail” (eg individual researchers at home)
- Better understanding / use of LoA
- (Plea:) Improve attribute handling (negotiations), for authorisation
- Support individual data protection and control of data