ESGF – IdEA:

Identity, Entitlement and Access Management

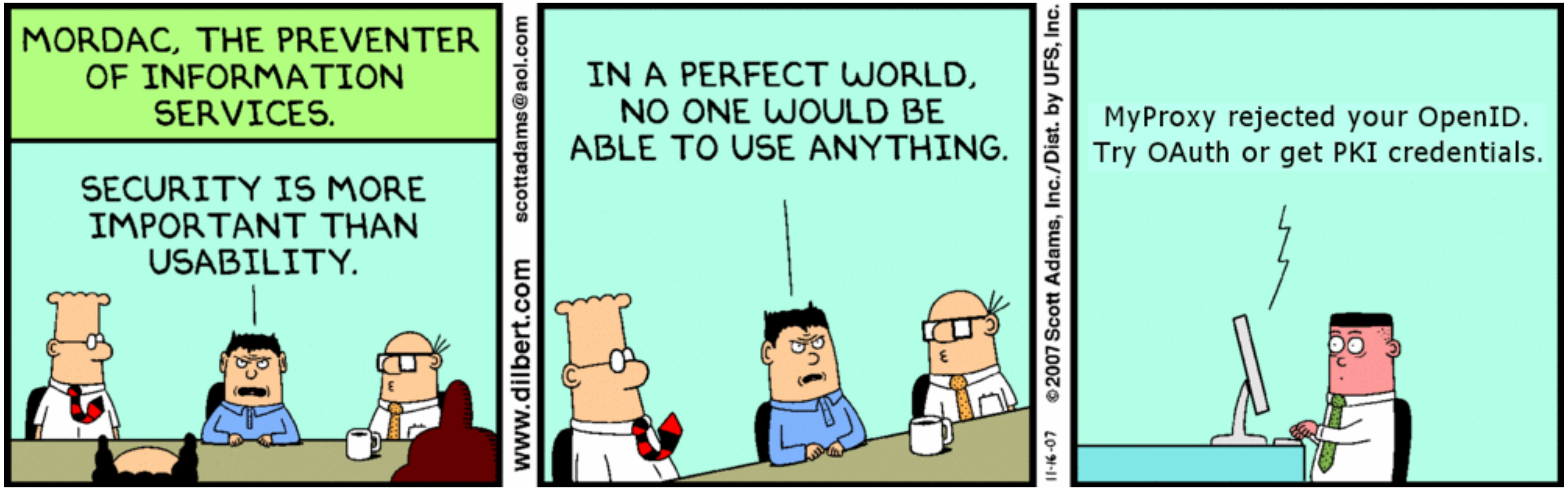
ESGF UV-CDAT Conference

09-11 December 2014

Philip Kershaw, Centre for Environmental Data Archival, RAL Space, STFC

Rachana Ananthakrishnan, Argonne National Laboratory

With Apologies to Scott Adams (credit Jennifer Adams)


MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
11-16-07
MyProxy rejected your OpenID. Try OAuth or get PKI credentials.

ESGF-IdEA Working Team

- https://acme-climate.atlassian.net/wiki/display/ESGF/Identity+Entitlement+Access+Working+Team+Members

- Luca Cinquini
- Aashish Chaudhary
- Antonio Cofino
- Katharina Berger
- Carsten Ehbrecht
- Georgi Kostov
- Kleanthis Tsaousis
- James McEnerney
- Mark Greenslade
- *Philip Kershaw*
- *Rachana Ananthakrishna*n
- Sandro Fiore
- Stephen Pascoe
- Dean N. Williams

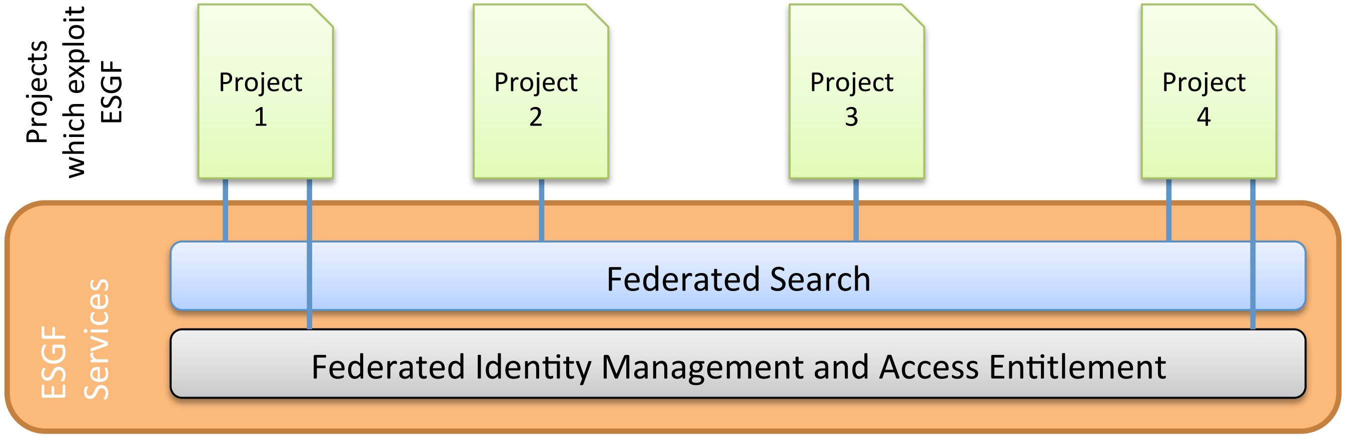
- We need more people
  a) non-security experts to give user feedback
  b) developers to get involved

Overview

- Requirements recap
- Operations
- Roadmap
- Implemented features of roadmap

Requirements Review

- Access control is an **optional** component which can be utilised or left out as fits the need of an *individual project* in the federation
- For projects using access control it should be straightforward to configure an access policy which makes some data restricted and some public as needed
- A low *Level of Assurance* (LoA) has been needed with projects to date. Some future projects may need higher LoA


Projects which exploit ESGF
Project 1
Project 2
Project 3
Project 4
ESGF Services
Federated Search
Federated Identity Management and Access Entitlement

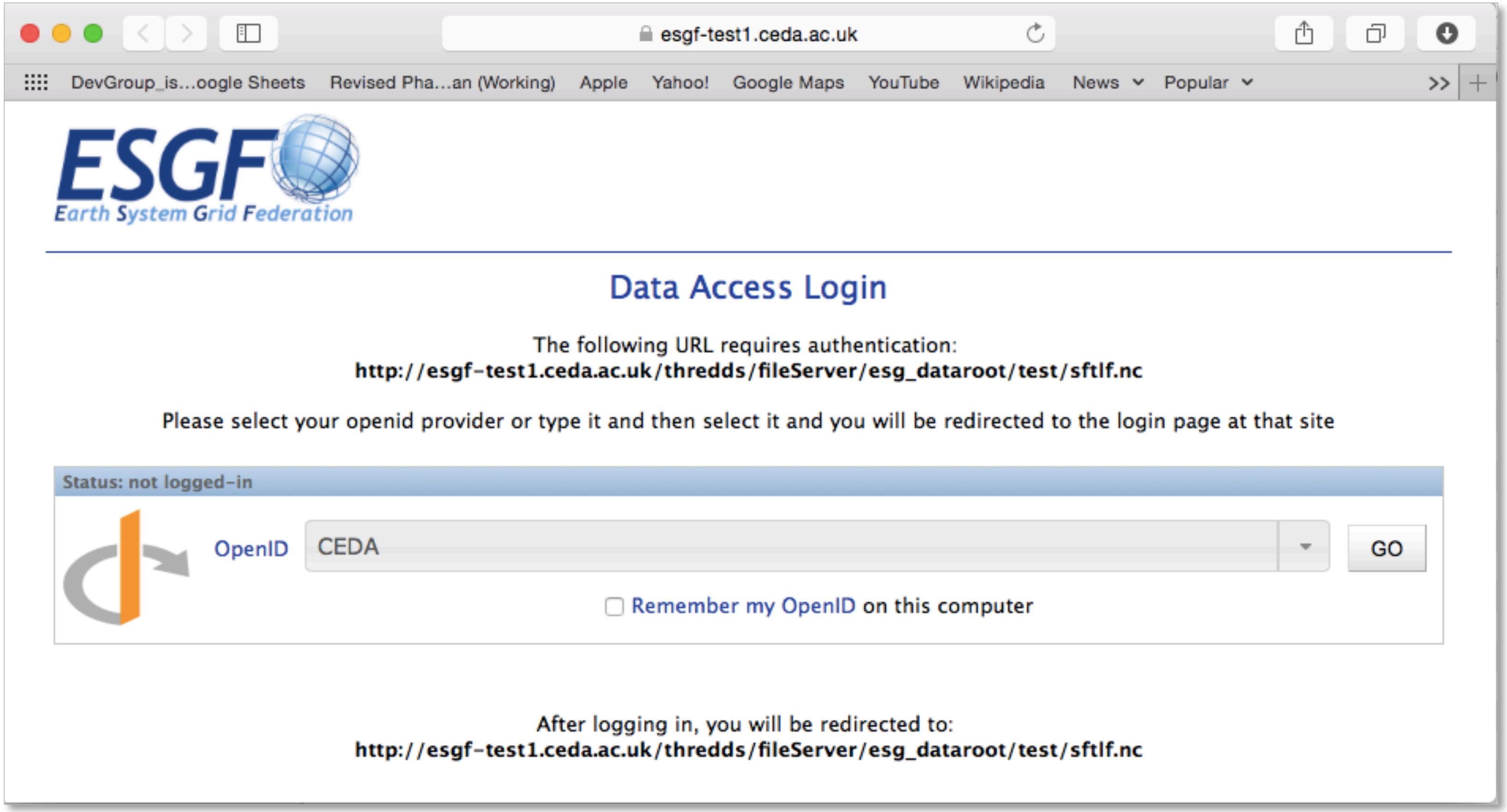
Operations

- Maintainability
  - Some of the code base has become brittle
  - Difficult to configure some elements
- Support
  - Security still figures large in help queries
- Security responses
  - Assessment of risk of vulnerability vs. upset to stability of the federation brought by change
- Up time + fixes – do we need SLAs?
  - A federation is inter-dependent on each institution's services
  - IdEA services are critical to the operation of the whole federation

Roadmap

- **Simplify trust roots**
- ✔ **Replace MyProxyCA and integrate *OAuth***
- Create an Attribute Registration web service interface
- ✔ **Improve usability for browser-based sign-in**
- ✔ **Simplify security for Wget**
- **Integrate *OpenID Connect* to simplify sign-in and user attribute release**
- Provide support for external IDs to the federation
- Review the use of central Virtual Organisation-wide attribute services
- Provide support for multiple Levels of Assurance (LoA)

OpenID Sign-in Enhancement


esgf-test1.ceda.ac.uk
DevGroup_is...oogle Sheets
Revised Pha...an (Working)
Apple
Yahoo!
Google Maps
YouTube
Wikipedia
News
Popular
ESGF
Earth System Grid Federation

Data Access Login

The following URL requires authentication:
http://esgf-test1.ceda.ac.uk/thredds/fileServer/esg_dataroot/test/sftlf.nc

Please select your openid provider or type it and then select it and you will be redirected to the login page at that site

Status: not logged-in

OpenID: CEDA

GO

□ Remember my OpenID on this computer

After logging in, you will be redirected to:
http://esgf-test1.ceda.ac.uk/thredds/fileServer/esg_dataroot/test/sftlf.nc

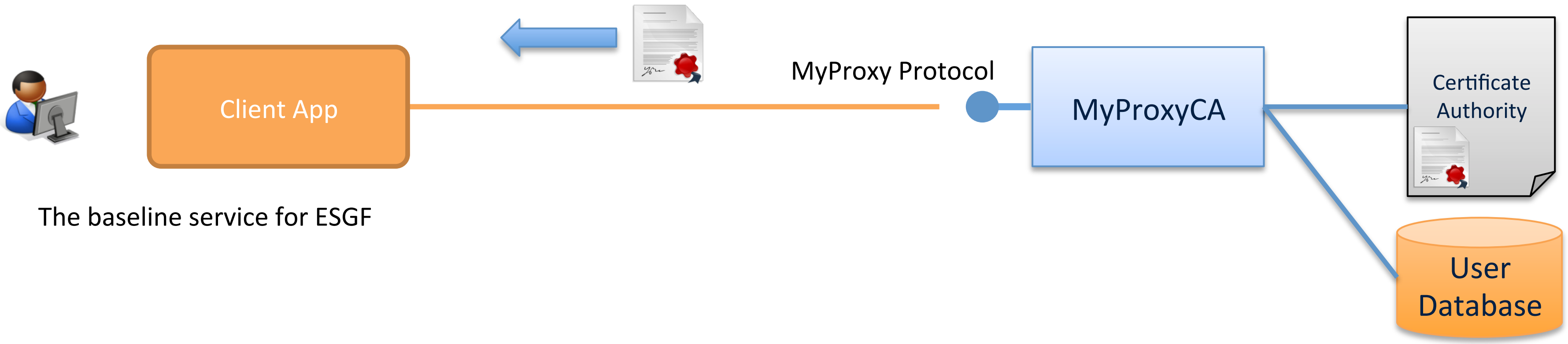
Wget Improvement

- **Wget scripts** provide a means for bulk data download for the web frontend
- Why was user certificate based authentication implemented in the first place?
  - United HTTP and GridFTP download services with one authentication method
- The problem: the certificate-based authentication process has been a major usability issue
  - Need for custom desktop software: Java plugin
  - SSL and PKI issues
- Solution: remove the need for user certificates
  - Wget scripts authenticate by means of HTTP redirects to user's IdP
  - IdP has a new HTTP Basic Auth interface for login suitable for scripts
  - Cookies maintain session state
- Demo: shown for data transfer talk Eric Blau, ANL

Future for Certificate-based Authentication + path for delegation support

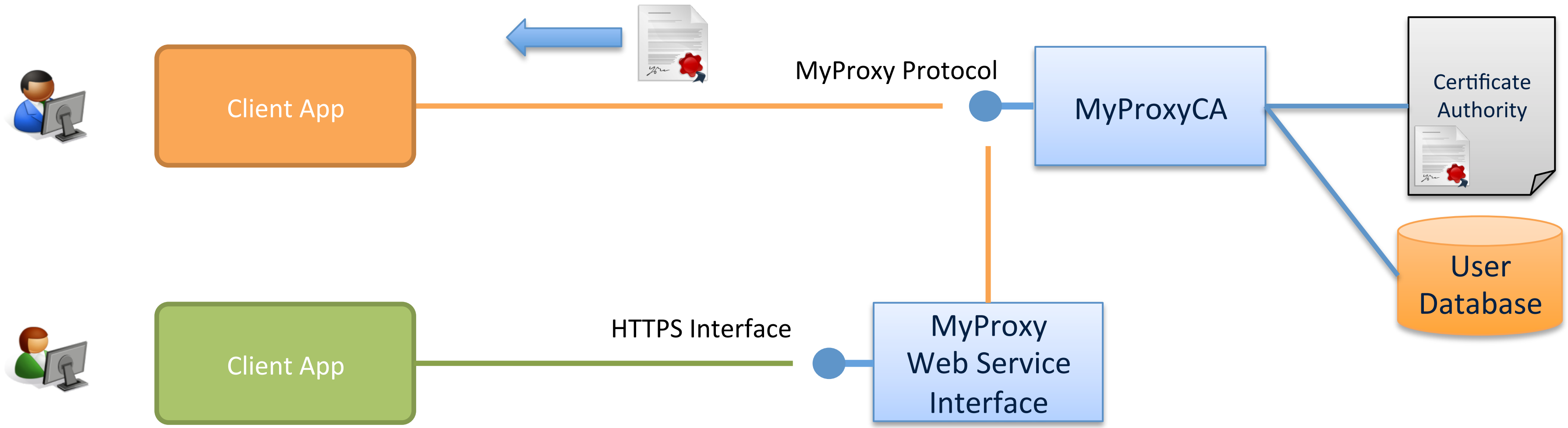
- It is important to retain certificate-based authentication capability for more advanced use cases:
  - advance scripted tools, power users
  - Inter-institution transfer
  - User delegation
- A section of the roadmap deals with this future:
  - Remove the dependency on MyProxy
  - Providing a new Short-Lived Credential Service
  - Which can be extended to support user delegation with OAuth 2.0
  - Provide a range of client tools: bash scripts, Python and Java clients
- This leads to delegation support and OpenID Connect.
  - This must align with efforts in the US and Europe (EUDAT) to standardise
- Next slides explain . . .

Evolution of Short-Lived Credential Services: 1) MyProxyCA



The baseline service for ESGF

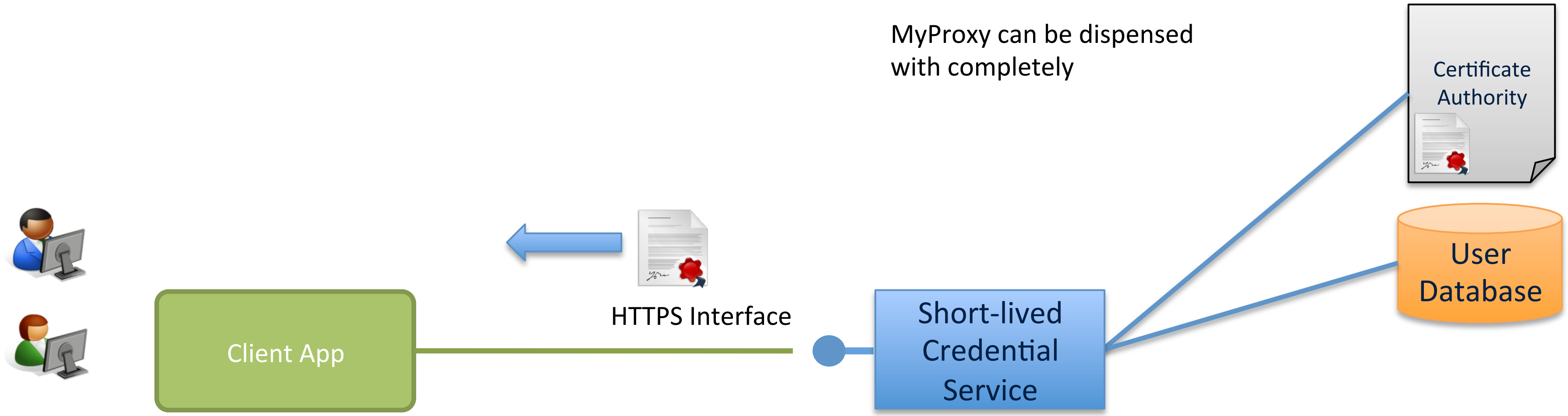
Evolution of Short-Lived Credential Services: 2) MyProxy Web Service Interface



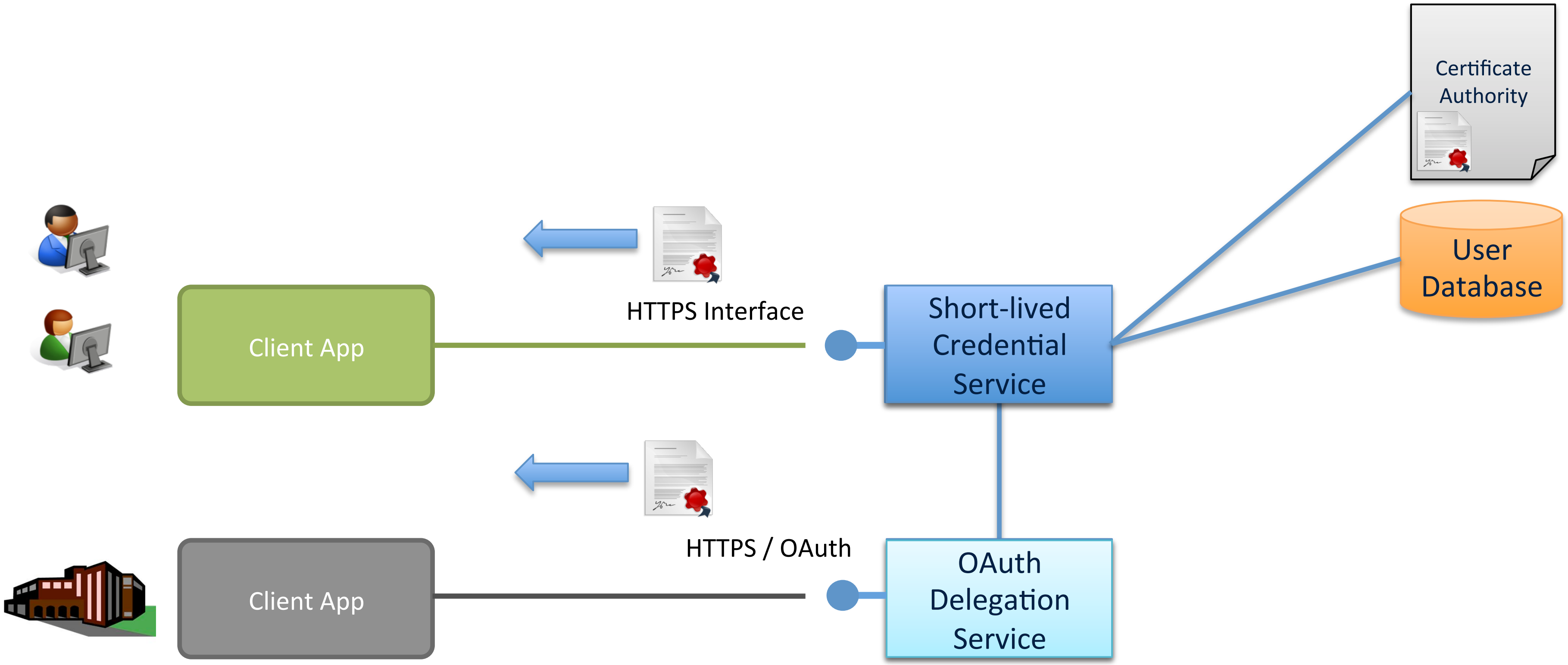
The MetOffice and some other users in the community used CEDA's MyProxy web service

Evolution of Short-Lived Credential Services: 3) Dispense with MyProxy altogether

MyProxy can be dispensed with completely



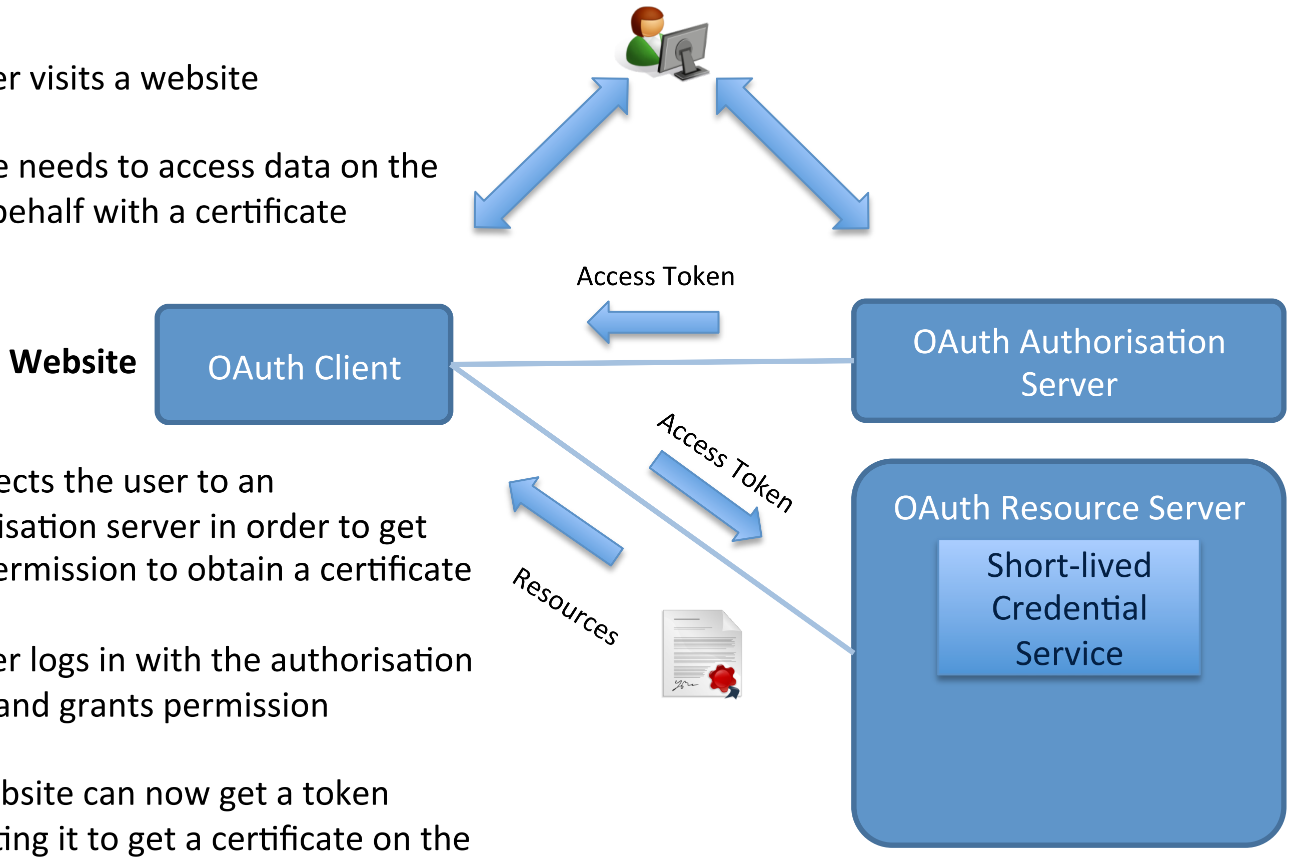
Evolution of Short-Lived Credential Services: 4) Add OAuth to provide delegation



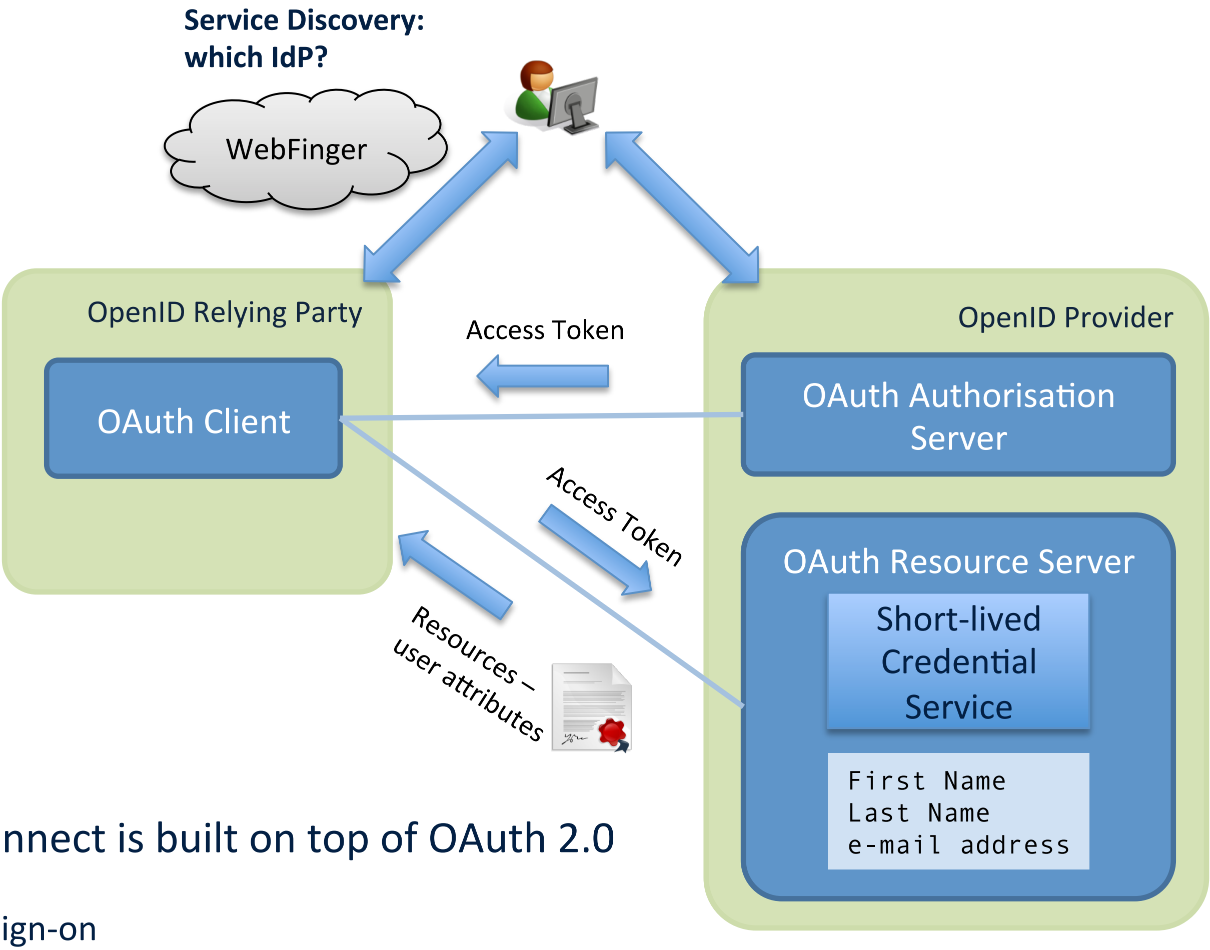
Client App such as a **portal** needing delegated credentials to access resources on behalf of the user

How does OAuth 2.0 work?

1. The user visits a website
2. The site needs to access data on the user's behalf with a certificate
3. It redirects the user to an Authorisation server in order to get their permission to obtain a certificate
4. The user logs in with the authorisation server and grants permission
5. The website can now get a token permitting it to get a certificate on the user's behalf



Overlaying OpenID Connect



```
First Name
Last Name
e-mail address
```

- OpenID Connect is built on top of OAuth 2.0 adding:
  - Single sign-on
  - Service discovery replacing Yadis with WebFinger