

# Identity and Certificates

Technical Evo

7/7/2017

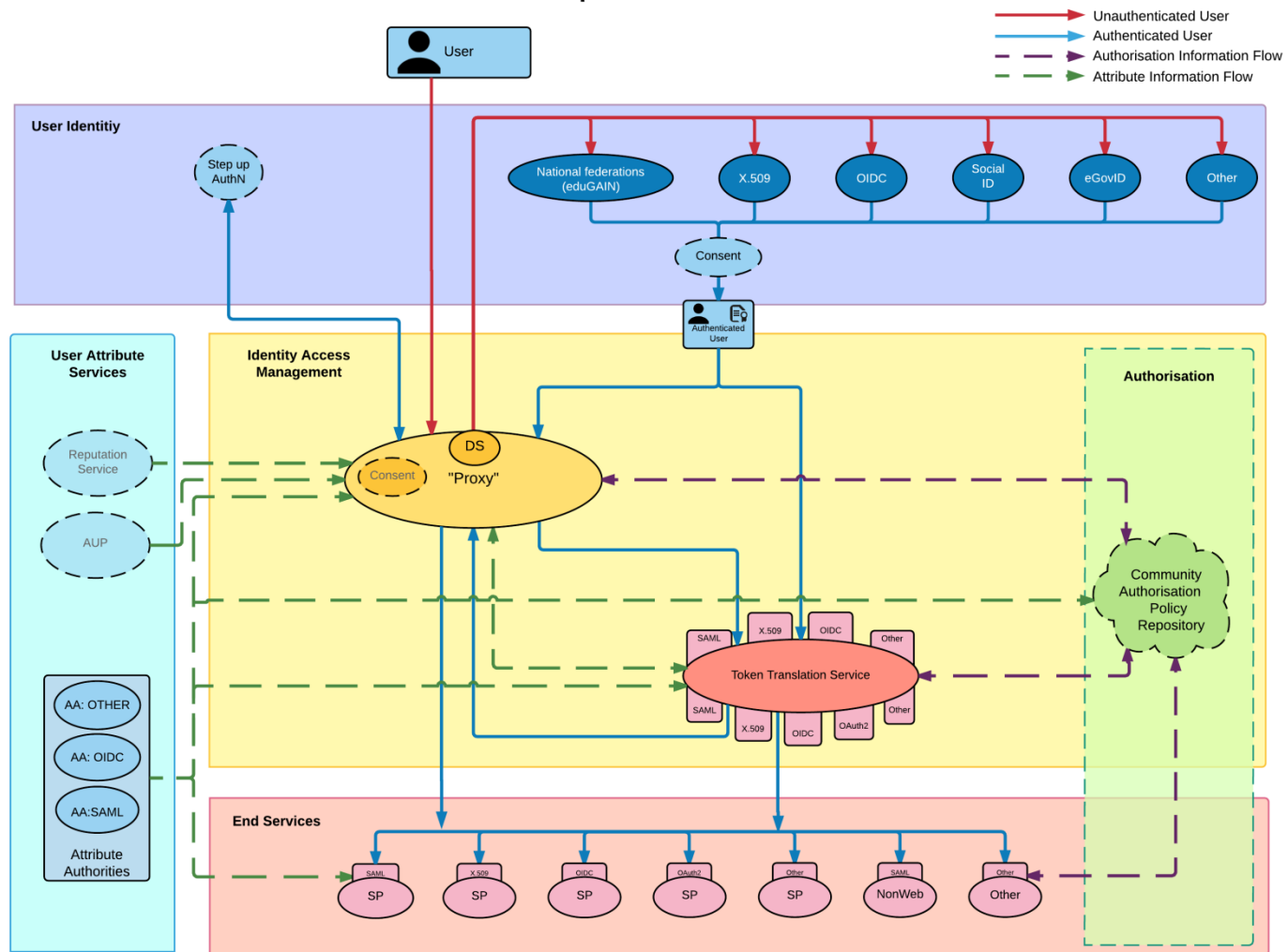
# Brief

- “Certificates behind the scenes”
  - OAUTH, OIDC, SAML (Shibboleth)
- AARC Project Pilots
  - Blueprint Arch., IdPs, Master Portals, Token Trans.
- Web-based (x.509) access to services
  - Non-web pilots coming (AARC2)

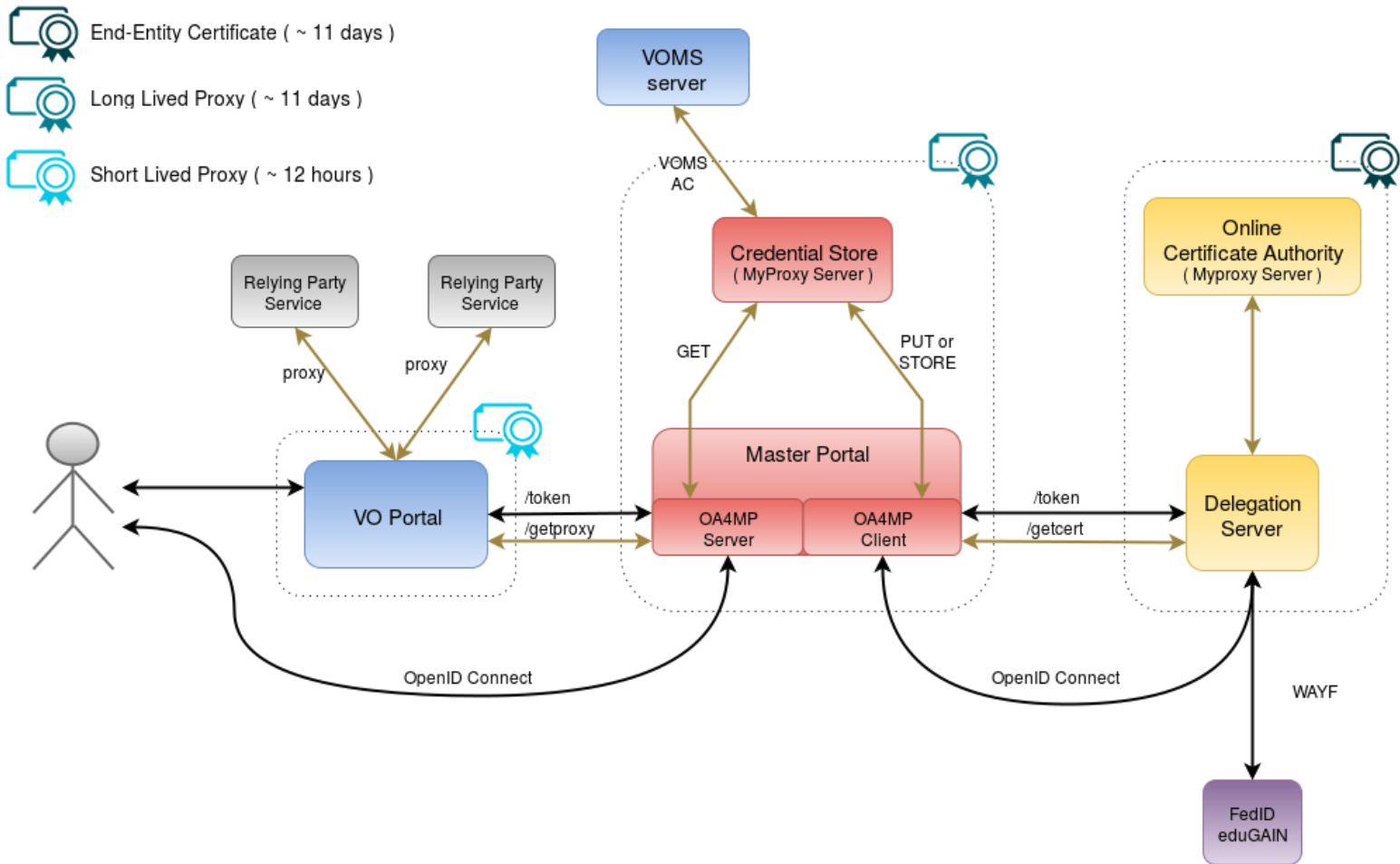
# AARC Blueprint

<https://aarc-project.eu/blueprint-architecture/>

## AARC Blueprint Architecture



# CILogon pilot - AARC



# 1. Web portal

*Imagine this is a VO web portal ...*

GSIFTP demo

[Info](#) [Browse](#) [Proxy info](#) [User info](#) [Log in](#) [Log in with VOMS](#)

Integration demo for a 'Science Gateway' with RCauth.eu

This 'VO portal' is showing a working demonstration of the [CILogon-based AARC pilot scenario](#). This is a 'portal delegation' scenario, where the user uses federated credentials to leave a personal (optionally VOMS) proxy on a Science Gateway, which can then be used for example to access user does not need to know anything about the underlying PKI infrastructure.

The different components integrated are:

- the new, IGF accredited, IOTA CA [RCauth.eu](#)
- an EGI-run [Master Portal](#)
- a DESY-run test [dCache instance \(/VOS/rcdemo\)](#) storage service.
- a test [VOMS server](#) providing optional VOMS attributes embedded in the proxy (VOMS proxy)
- some simple PHP scripts to do the OpenID Connect flow with its [getproxy](#) extension

Some notes:

- The EGI MasterPortal is completely agnostic concerning the VOMS server. The requested VO plus the corresponding necessary 'vomes' string is passed in via the client, and goes transparently through the Master Portal.
- The dCache test instance is completely wiped everyday, so do NOT rely on it for permanent storage (-;
- In order to access the storage element, the user needs to be authorized for accessing (either on identity or VOMS attributes). This provisioning is *not* part of the current demonstrator.
- Similarly the user needs to be enrolled in the VO. How to (semi-)automate this provisioning is currently under investigation within AARC.

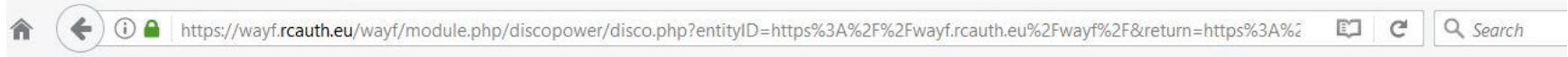
**How to start**

Start by clicking on either the [login](#) or [login with VOMS](#) tabs above to do a federated login and obtain a valid plain or VOMSified proxy.

Once successfully logged in, you can [browse](#) the storage element.

The [proxy info](#) and [user info](#) tabs show information about the underlying X.509 credential and the OpenID-Connect claims respectively.

# 2. Select Identity provider



English | Nederlands | Español | Français | Deutsch

eduGAIN | Research and e-Infrastructures | InCommon | Denmark | Germany | Greece | Italy | Netherlands | Sweden

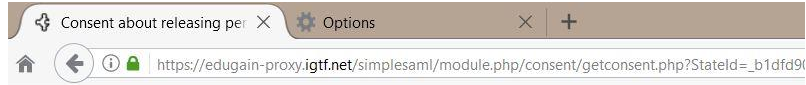
Switzerland | UK | Other countries | Miscellaneous

Incremental search...

AMOLF
Antoni van Leeuwenhoek - Netherlands Cancer Institute
Aristotle University of Thessaloniki
ArtEZ University of the Arts
HZ University of Applied Sciences
IFAE - Institute for High Energy Physics
<b>IGTF Certificate Proxy</b>
INFN - National Institute for Nuclear Physics
Inholland University of Applied Sciences

*...because STFC doesn't (yet) release all the required attributes ☹ ☹*

# 3.1 Personal data release



IGTF-to-eduGAIN Proxy | Consent about releasing personal information

English | Bokmål | Nynorsk | Sámeigiella | Dansk | Deutsch | Svenska | Suomi | Esperanto | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский

RCAuth Pilot Online CA requires that the information below is transferred.

Remember

Yes, continue No, cancel

Information that will be sent to RCAuth Pilot Online CA

Distinguished name (DN) of certificate subject /C=UK/O=eScience/OU=CLRC/L=RAL/CN=ian neilson
Display name ian neilson
Mail ian.neilson@stfc.ac.uk
Identity assurance profile <ul style="list-style-type: none"><li>1.3.6.1.4.1.11439.1.1.1.2.2.0</li><li>1.2.840.113612.5.2.2.1</li><li>1.2.840.113612.5.2.3.3.3</li></ul>
Long-lived, non re-assignable, omnidirectional identifier suitable for use as a unique external key by applications dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net
Person's principal name at home organization dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net

Copyright © 2017 IGTF | Powered by SimpleSAMLphp

*Identity provider asks permission to release personal data to the online Certificate Authority*

Information that will be sent to RCAuth Pilot Online CA

Distinguished name (DN) of certificate subject

/C=UK/O=eScience/OU=CLRC/L=RAL/CN=ian neilson

Display name

ian neilson

Mail

ian.neilson@stfc.ac.uk

Identity assurance profile

- 1.3.6.1.4.1.11439.1.1.1.2.2.0
- 1.2.840.113612.5.2.2.1
- 1.2.840.113612.5.2.3.3.3

Long-lived, non re-assignable, omnidirectional identifier suitable for use as a unique external key by applications

dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net

Person's principal name at home organization

dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net

*oid's from certificate - UK CA Policy with IGTF "classic" identity validation for a Natural Person*

# 3.2 Personal data release

*Certificate Authority asks permission to release personal data to the Master Portal*

**RCAuth.eu Online CA consent page**

The Master Portal will release your personal information to the following service for Europe:

If you approve, please accept, otherwise you will not be able to use the service.

Details on which attributes are released are available in the Master Portal.  
For further information on the CA see [https://aai.eui.eu/portal/](#)

Remember

**Master Portal Information:**

Name: EGI CheckIn Master Portal  
Description: EGI CheckIn Master Portal  
URL: <https://aai.eui.eu/portal/>

**Information that will be sent to the Master Portal:**

sub :	dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net
idp :	<a href="https://edugain-proxy.igtf.net/simplesaml/saml2/idp/metadata.php">https://edugain-proxy.igtf.net/simplesaml/saml2/idp/metadata.php</a>
eduPersonTargetedID :	<a href="https://edugain-proxy.igtf.net/simplesaml/saml2/idp/metadata.php!1adc91b6f9bfc05ce8c0">https://edugain-proxy.igtf.net/simplesaml/saml2/idp/metadata.php!1adc91b6f9bfc05ce8c0</a>
idp_display_name :	IGTF
cert_subject_dn :	CN=ian neilson 8a30nOHOe85TeN4Z,O=IGTF,DC=rcauth-clients,DC=rcauth,DC=eu
name :	ian neilson
eduPersonPrincipalName :	dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net
eduPersonUniqueId :	dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net
email :	ian.neilson@stfc.ac.uk



# 3.3 Personal data release

RAuth.eu Online CA

https://pilot-ca1.rcauth.eu/oauth2/authorize?scope=openid+email+profile+org.cilogon.userinfo+edu.uiuc.ncsa.myproxy.getcert&response\_

**RAuth.eu** The white-label Research and Collaboration Authentication CA Service for Europe

**RCAuth.eu Online CA consent page**

The Master Portal below is requesting access to your personal information. If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and how they will be used. For further information on the CA see the [RCAuth.eu homepage](#).

Remember

**Master Portal Information:**

<i>Name:</i>	EGI Master Portal
<i>Description:</i>	EGI Master Portal
<i>URL:</i>	https://masterportal-pilot.aai.egi.eu

**Information that will be sent to the Master Portal:**

<i>sub :</i>	msalle@nikhef.nl
<i>idp :</i>	https://sso.nikhef.nl/sso/saml2/idp/metadata.php

# 4 Delegated proxy

GSIFTP demo

Info Browse **Proxy info** User info Logged in as `dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtj.net` VO: `rcdemo.aarc-project.eu`

**Download**  
You can [download](#) your proxy

**Proxy information:**

```
subject : /DC=eu/DC=rcauth/DC=rcauth-clients/O=IGTF/CN=ian neilson 8a30nOHoe85TeN4Z/CN=889876458/CN=149746141
issuer  : /DC=eu/DC=rcauth/DC=rcauth-clients/O=IGTF/CN=ian neilson 8a30nOHoe85TeN4Z/CN=889876458
identity : /DC=eu/DC=rcauth/DC=rcauth-clients/O=IGTF/CN=ian neilson 8a30nOHoe85TeN4Z/CN=889876458
type    : RFC compliant proxy
strength : 2048 bits
path    : /tmp/x509up_upDN2rf
timeleft : 1:49:28
key usage : Digital Signature, Key Encipherment, Data Encipherment
=== VO rcdemo.aarc-project.eu extension information ===
vo      : rcdemo
subject : /DC=eu
issuer  : /DC=orc
attribute : /rcdemo
timeleft : 11:55:
uri     : rcvoms
Certificate:
  Data:
    Version: 3
    Serial Number:
    Signature Algorithm:
    Issuer: DC=
    Validity
      Not Before:
      Not After:
    Subject: D
    Subject Public Key Info:
      Public Key Algorithm:
      Public Key:
```

```
subject : /DC=eu/DC=rcauth/DC=rcauth-clients/O=IGTF/CN=ian neilson 8a30nOHoe85TeN4Z/CN=889876458/CN=149746141
issuer  : /DC=eu/DC=rcauth/DC=rcauth-clients/O=IGTF/CN=ian neilson 8a30nOHoe85TeN4Z/CN=889876458
identity : /DC=eu/DC=rcauth/DC=rcauth-clients/O=IGTF/CN=ian neilson 8a30nOHoe85TeN4Z/CN=889876458
type    : RFC compliant proxy
strength : 2048 bits
path    : /tmp/x509up_upDN2rf
timeleft : 11:49:28
key usage : Digital Signature, Key Encipherment, Data Encipherment
```

# Demo

## GSIFTP demo

[Info](#)[Browse](#)[Proxy info](#)[User info](#)Logged in as *dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net*

### Parsed ID Token:

Claim	Value
iss	https://aai.egi.eu/mp-aa2-server
sub	dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net
exp	1493220617
aud	myproxy:oa4mp.2012:/client_id/1eed11b966498967a3eea2f4c0141169
iat	1493219717
auth_time	1493219716
idp	https://edugain-proxy.igtf.net/simplesaml/saml2/idp/metadata.php
eduPersonTargetedID	https://edugain-proxy.igtf.net/simplesaml/saml2/idp/metadata.php/1adc91b6f9bfc05ce8c045c36ff6afa8881f74b6
idp_display_name	IGTF
cert_subject_dn	CN=ian neilson Sa30nOHOe85TeN4Z,O=IGTF,DC=rcauth-clients,DC=rcauth,DC=eu
name	ian neilson
eduPersonPrincipalName	dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net
eduPersonUniqueId	dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net
email	ian.neilson@stfc.ac.uk

# 6. Access the service

**GSIFTP demo**




<a href="#">Info</a>	<a href="#">Browse</a>	<a href="#">Proxy info</a>	<a href="#">User info</a>	Logged in as <i>dfcd8a6540e667712b30438b364a9472090da877d44fb22526055e0549b9a549@igtf.net</i>	VO: <i>rcdemo.aarc-project.eu</i>	<a href="#">log out</a>
----------------------	------------------------	----------------------------	---------------------------	---	-----------------------------------	-------------------------

gsiftp://prometheus.desy.de: /

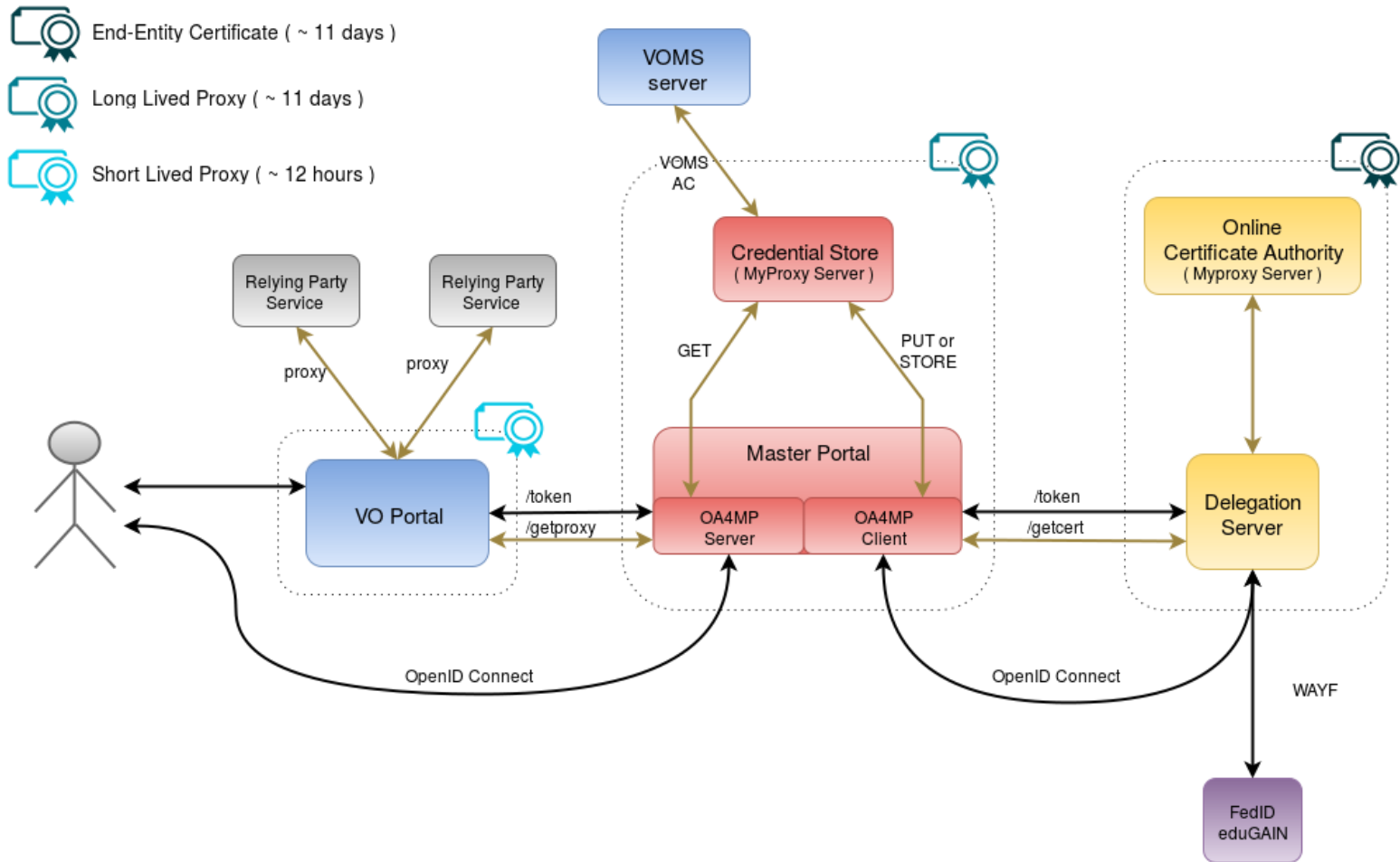
<input type="radio"/> d-----	1	rcdemo	rcdemo	512	Apr 26 06:00	<a href="#">lost+found</a>
<input type="radio"/> dr-x-----	1	rcdemo	rcdemo	512	Apr 26 06:01	<a href="#">VOs</a>
<input type="radio"/> dr-x-----	1	rcdemo	rcdemo	512	Apr 26 06:01	<a href="#">Users</a>
<input type="radio"/> dr-x-----	1	rcdemo	rcdemo	512	Apr 26 06:03	<a href="#">UTF-8</a>
<input type="radio"/> dr-x-----	1	rcdemo	rcdemo	512	Apr 26 06:03	<a href="#">Music</a>
<input type="radio"/> d--x-----	1	rcdemo	rcdemo	512	Apr 26 16:22	<a href="#">upload</a>
<input type="radio"/> dr-x-----	1	rcdemo	rcdemo	512	Apr 26 06:04	<a href="#">Video</a>

No file selected.

Remote name:



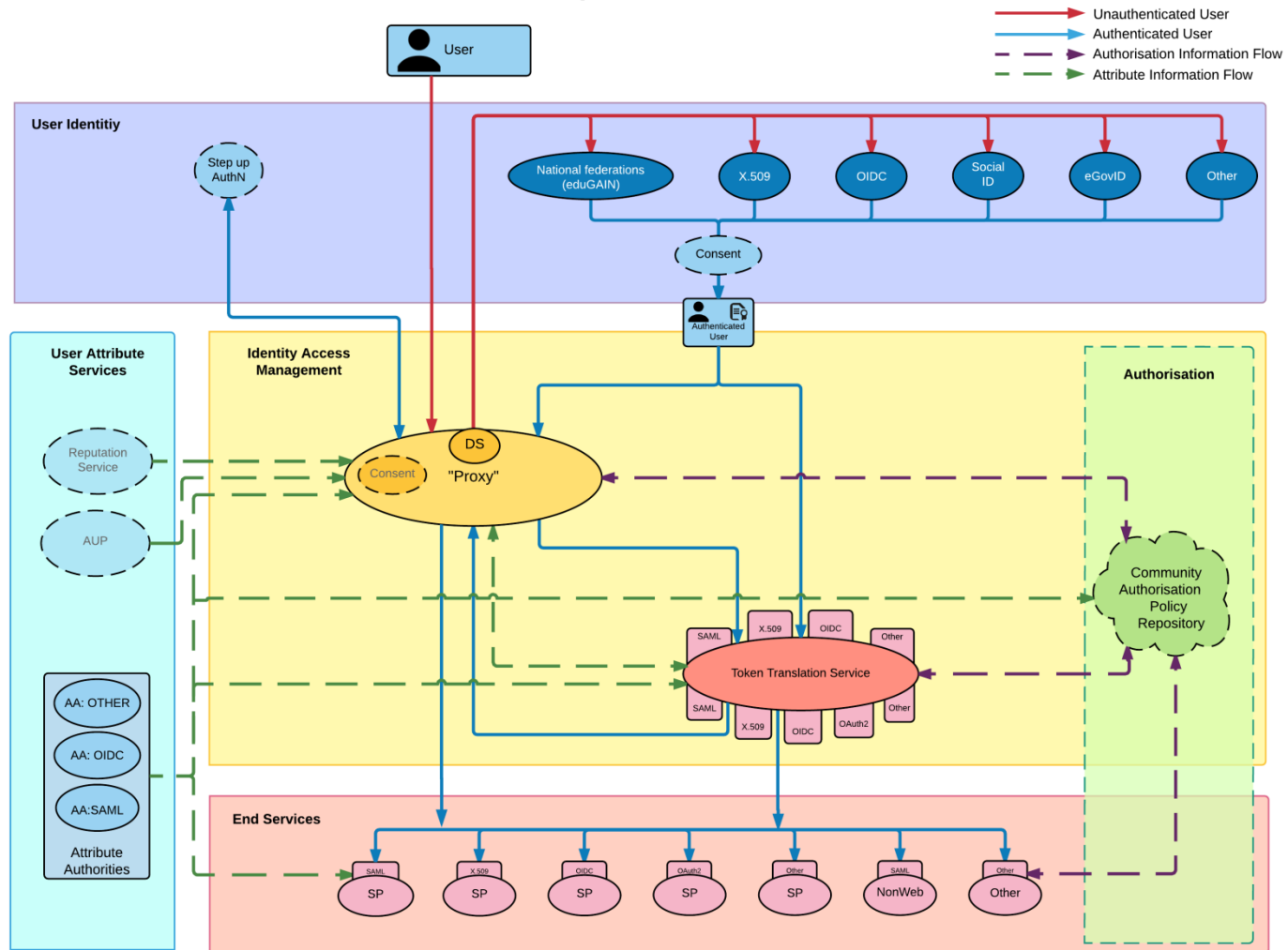
# CILogon pilot - AARC



# AARC Blueprint

<https://aarc-project.eu/blueprint-architecture/>

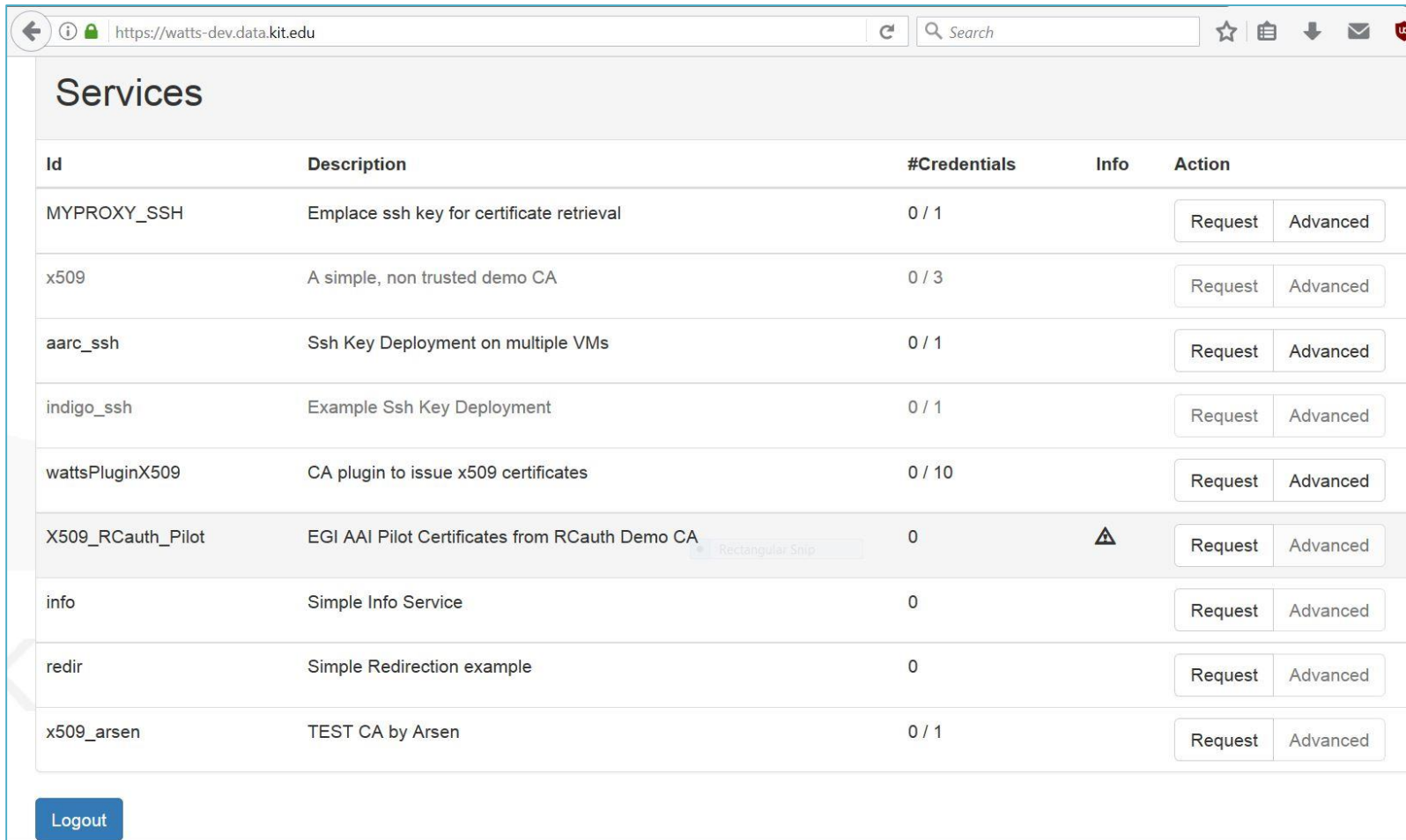
## AARC Blueprint Architecture




# Token Translation

The screenshot shows a web browser window with the URL <https://watts-dev.data.kit.edu>. The page title is "WaTTS - The INDIGO Token Translation Service". Below the title, there is a prompt: "Please select your OpenId Connect Provider". A search input field contains the text "INDIGO Datacloud Identity and Access Management (IAM)". A "Login" button is visible to the right of the search field. A dropdown menu is open, listing several providers: "INDIGO Datacloud Identity and Access Management (IAM)", "Human Brain Project (HBP)", "Unity Staging", "EUDAT (b2access)", "European Grid Infrastructure (EGI)", "Google, the well known search giant", and "Elixir". The "Elixir" option is highlighted with a blue background. A dashed blue line connects the "Elixir" option in the dropdown to a larger, magnified view of the same dropdown menu on the right side of the image. The magnified view shows the same list of providers, with "Elixir" highlighted. The background of the page features a faint "Karlsruh" logo and the text "This work was pa".

# Token Translation - WATTS



The screenshot shows a web browser window with the URL <https://watts-dev.data.kit.edu>. The page title is "Services". Below the title is a table with the following columns: "Id", "Description", "#Credentials", "Info", and "Action". The table contains ten rows of service entries. Each row has "Request" and "Advanced" buttons in the "Action" column. A "Logout" button is located at the bottom left of the page.

Id	Description	#Credentials	Info	Action
MYPROXY_SSH	Emplace ssh key for certificate retrieval	0 / 1		Request Advanced
x509	A simple, non trusted demo CA	0 / 3		Request Advanced
aarc_ssh	Ssh Key Deployment on multiple VMs	0 / 1		Request Advanced
indigo_ssh	Example Ssh Key Deployment	0 / 1		Request Advanced
wattsPluginX509	CA plugin to issue x509 certificates	0 / 10		Request Advanced
X509_RCauth_Pilot	EGI AAI Pilot Certificates from RCauth Demo CA	0		Request Advanced
info	Simple Info Service	0		Request Advanced
redir	Simple Redirection example	0		Request Advanced
x509_arsen	TEST CA by Arsen	0 / 1		Request Advanced

Logout



# Materials

- <https://rcdemo.nikhef.nl/>
  - <https://wiki.geant.org/display/AARC/CILogon-like+pilot>
  - <https://indico.cern.ch/event/569445/>
- <https://watts-dev.data.kit.edu/>
  - [https://aarc-project.eu/wp-content/uploads/2017/03/CI-demo-watts\\_new.pdf](https://aarc-project.eu/wp-content/uploads/2017/03/CI-demo-watts_new.pdf)
- <https://wiki.geant.org/display/AARC/Non-web+resources%3A+comparison+of+methods>

Thank You