

CILogon-like pilot

- [Introduction](#)
- [Detailed description](#)
- [Demonstration](#)
- [Demonstrator workflows](#)
 - [Basic demo:](#)
 - [GSIFTP demo:](#)
- [Components](#)

Introduction

The purpose of this pilot is to build a setup in which users can access X.509-based resources without the need for them to understand the intricacies of a PKI. The pilot requires an online CA, plus a scalable trust model applicable for the multi-infrastructure-multi-federation European research landscape.

A high-level introduction is given in the [this AARC blog post](#)

Detailed description

A detailed description can be found in these [wiki pages](#).

The setup consists of

- An online CA: [RCauth.eu](#)
- Several Master Portals, run by e.g. EGI, ELIXIR.
- Many VO-portal, also known as Science Gateways.

The online CA is a service provider which has entered eduGAIN, and has as CA been accredited by IGTF (as a so-called [IOTA CA](#)). In order to protect the service, a filtering WAYF has been implemented which only accepts Identity Providers that publish the [R&S set of attributes](#) and are conforming to the [Sirtfi](#). The combined service is running on a production level. The Master Portals run by EGI and ELIXIR are running as pilot services.

A [sustainability study](#) for the model has been produced by AARC-NA3.

Demonstration

We have created [two demonstrator Master Portal clients](#), which talk to a semi-production Master Portal (running for EGI), serviced by the production RCauth.eu online CA. We also have setup a test VOMS service with test VO, to test and showcase the integration with a VOMS attribute authority. The two demonstrators are:

1. a [simple PHP program](#) showing the basic API and handshake, with a possibility to execute the same demonstrator code. The code additionally shows how to integrate with VOMS or how to specify a specific IdP at the WAYF.
2. a [simple Science Gateway](#) allowing access to a gsiftp-enabled storage service (a test [dCache](#) instance, <https://prometheus.desy.de/>). This shows how X.509-based storage elements can be accessed using a science gateway, where authorization is based on VOMS attributes (group membership etc.).

Demonstrator workflows

Basic demo:

1. select one of the login pages, e.g. run VOMS demo to get a proxy certificate with VOMS attributes

AARC Demo OIDC client to ... x +
https://rcdemo.nikhef.nl/demobasic/oidc_getproxy_demo_source.php

Demo OIDC client to an EGI MasterPortal using the RCaution Delegation Server

The demonstrator shows example portal integration code to do a full OpenID-connect handshake with a Master Portal plus the [/getproxy](#) request to obtain a (optionally VOMS) proxy certificate.

The different steps are:

1. Do an [/authorize](#) request at the Master Portal
2. Do a [/token](#) request using the received code
3. Do a [/getproxy](#) request using the received `access_token`

Steps 1. and 2. are standard OIDC steps using the authorization flow, using the Master Portal as OIDC Authorization Server. Step 3. acts as a request to a protected resource using the `access_token` as bearer token. In step 1. the user is redirected from the Master Portal to the [RCaution.eu](#) Online CA for a second OIDC flow and ultimately doing a federated login at the home IdP. The consecutive services passed in step 1. are:

1. this 'VO portal'
2. EGI Master Portal
3. RCaution online CA and its filtering WAYF
4. home IdP or IdP proxy

Steps 2. and 3. are back-channel interactions between this 'VO portal' and the Master Portal. See [here](#) for a detailed description of the flow.

[download script](#) [run non-VOMS demo](#) [run demo using fixed IdP](#) [run VOMS demo](#)

```
<?php
//
// Small demonstration program showing how to obtain a proxy via /getproxy
// endpoint on a MasterPortal. It is provided as is.
//
// Copyright (C) FOM-Nikhef 2016-
// Licensed under the Apache License, Version 2.0 (the "License")
// http://www.apache.org/licenses/LICENSE-2.0
//
// Authors: Mischa Salla (msalle (AT) nikhef.nl)
//
ini_set("display_errors",1);
```

2. choose your home IdP at the WAYF of the RCaution online CA

Select your identity pro... x +
https://wayf.rcaution.eu/wayf/module.php/discopower/disco.php?entityID=https%3A%2F%2Fwayf.rcaution.eu%2Fwayf%2F6.return=https%3A%2F%2F...&return=https%3A%2F%2F...&return=https%3A%2F%2F...

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

English | Nederlands | Español | Français | Deutsch

You have previously chosen to authenticate at EGI-Engage AAI Pilot IdP Proxy
[Login at EGI-Engage AAI Pilot IdP Proxy](#)

Research and e-Infrastructures | InCommon | Netherlands | Sweden | Switzerland | Miscellaneous

Incremental search...
Nikh

Antoni van Leeuwenhoek - Netherlands Cancer Institute
Koninklijke Bibliotheek
Nikhef

The RCaution.eu WAYF is provided by RCaution.eu. For support, please contact the help desk of your own home organisations.
Service built on SimpleSAMLphp IdP Software.

3. login at your home IdP

Enter your username a... x +
Nikhef (NL) | https://sso.nikhef.nl/sso/module.php/core/loginuserpass.php?AuthState=_4bb9daa863f3d9f351204feb0ac087a9e1ce86a709e34ht

NIKHEF National Institute for Subatomic Physics

Nederlands

Beware of phishing via the web - give your Nikhef password to websites **only if they show a green address bar**. Like this:

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below. This is the Nikhef SSO username and password, i.e. the one used for your access to e.g. email.

Username:

Password:

Help! I don't remember my password.

We are sorry, but both login and password are required for successful authentication. If you have lost your password, please contact the Nikhef help desk (helpdesk@nikhef.nl) or call extension 2200 during office hours

The Nikhef SSO service and IdP are provided by the CT group. For support, please contact the help desk (helpdesk@nikhef.nl), or by phone on +31 20 592 2200.
Service built on SimpleSAMLphp IdP Software.

1. Read the information about the demonstrator and choose to log in either with or without VOMS attributes

2. choose your home IdP at the WAY of the RCauth online CA

3. login at your home IdP

4. give consent at the RCauth online CA for attribute release

RCauth.eu Online CA consent page

The Master Portal below is requesting access to your personal information and to act on your behalf.

If you approve, please accept, otherwise, cancel.

Details on which attributes are released, why, to whom, and how they are processed can be found in the RCauth Pilot ICA G1 CA privacy policy. For further information on the CA see the RCauth.eu homepage.

Yes, continue No, cancel

Remember

Master Portal Information:

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

Information that will be sent to the Master Portal:

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

5. choose to browse the remote dCache storage element (only works once you have access to the rcdemo VO, drop us a line to request access).

GSI FTP demo

Info Browse Proxy info User info Logged in as msalle@nikhef.nl VO: rcdemo.aarc-project.eu log out

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 a storage element. The user does not need to know anything about the underlying PKI infrastructure.

The different components integrated are:

- the new, IGTF accredited, IOTA CA [RCauth.eu](#)
- an EGI-run [Master Portal](#)
- a DESY-run test [dCache instance](#) ([Info / Details](#)) 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 'vomses' 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.

<https://rcdemo.nikhef.nl/demogisftp/browse.php?dir=/VOS/>

6 go to the VO home directory for rcdemo.

GSI FTP demo

Info Browse Proxy info User info Logged in as msalle@nikhef.nl VO: rcdemo.aarc-project.eu log out

gsiftp://prometheus.desy.de: / VOS/

dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	alice
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	lhb
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	stean
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	hitface
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	atlas
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	cms
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	Indigo
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	gss
drwxr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	rcdemo
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:16	Xesivo
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:19	lxxl
dr-xr-xr-x	1	rcdemo	rcdemo	512	Nov 28 11:19	desy

Delete selected entry Browse... No file selected. Upload file Create directory

<https://rcdemo.nikhef.nl/demogisftp/browse.php?dir=/VOS/rcdemo/>

Components

- RCauth.eu online CA is based on [CILogon-software](#) from the US-based [CILogon project](#). A few adaptations had to be made to conform to European privacy regulations. The backend CA is based on a myproxy-server with an eToken as simple HSM plus some extra software to run the CA on a separate network.

- The Master Portal is also based on the same software, implementing simultaneously an OA4MP client and server plus glue to connect the two. It has a backend myproxy-server for credential caching.

The adaptations of the code for this pilot can be found on the [RCauth.eu github repository](#).

Additionally:

- ansible scripts for setting up a [Delegation Server](#) (online CA) or a [Master Portal](#)
- SimpleSAMLPHP has been used to build a filtering WAYF.
- A [VOMS server](#) to run a test VO.
- some simple PHP clients to test the flow and make a demonstrator.