CILogon-like pilot

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.

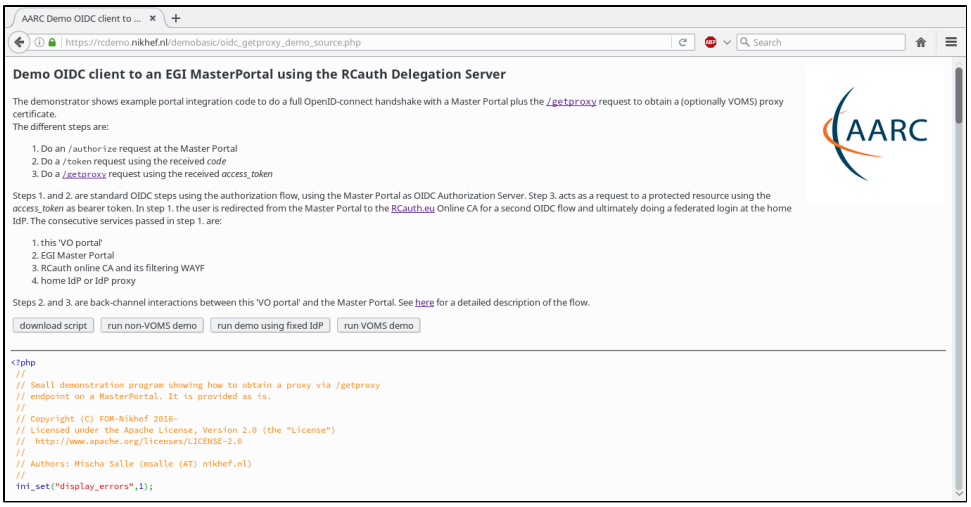
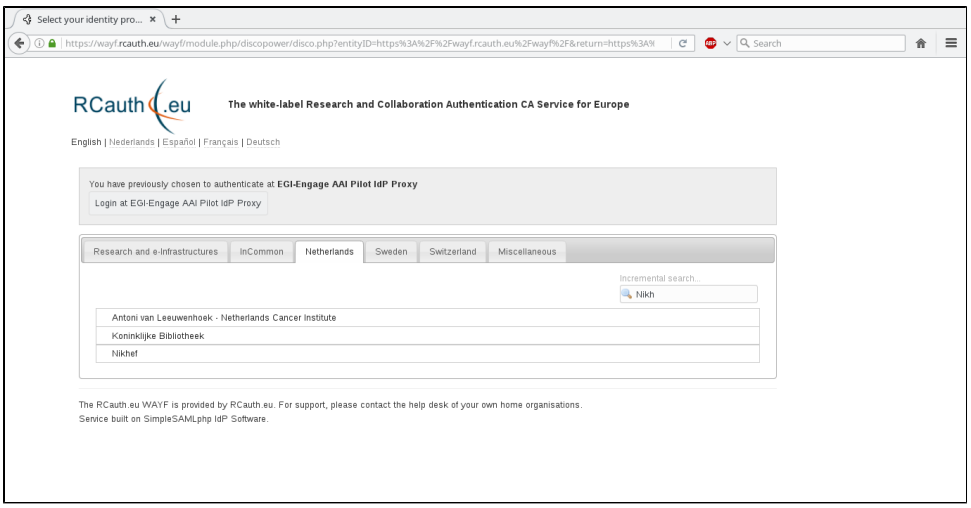
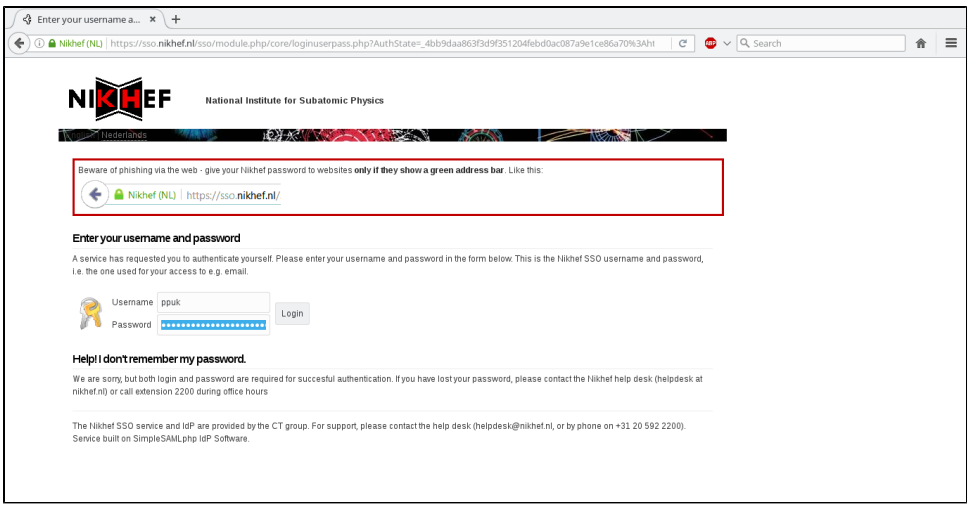
Demonstration

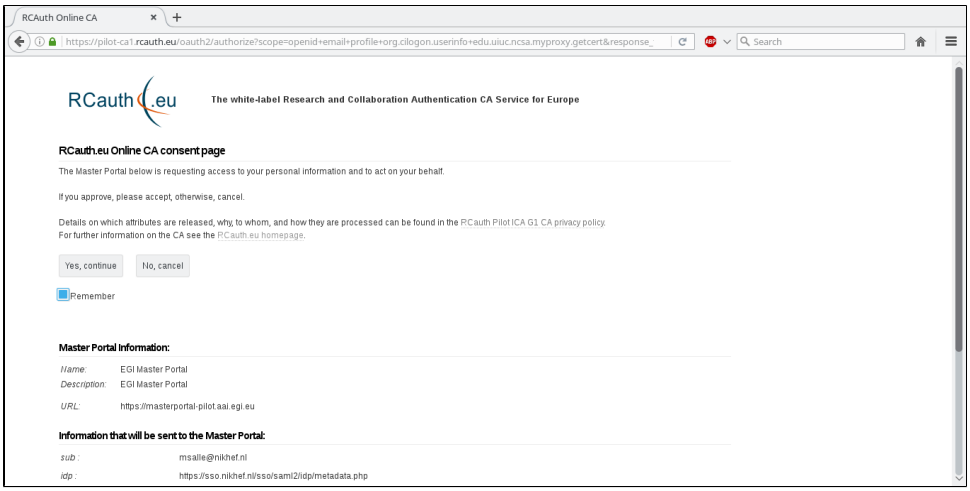
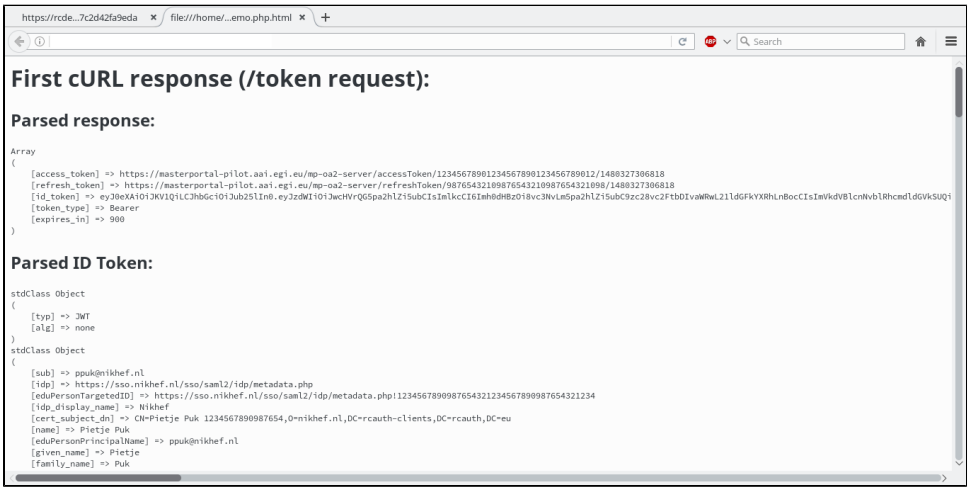
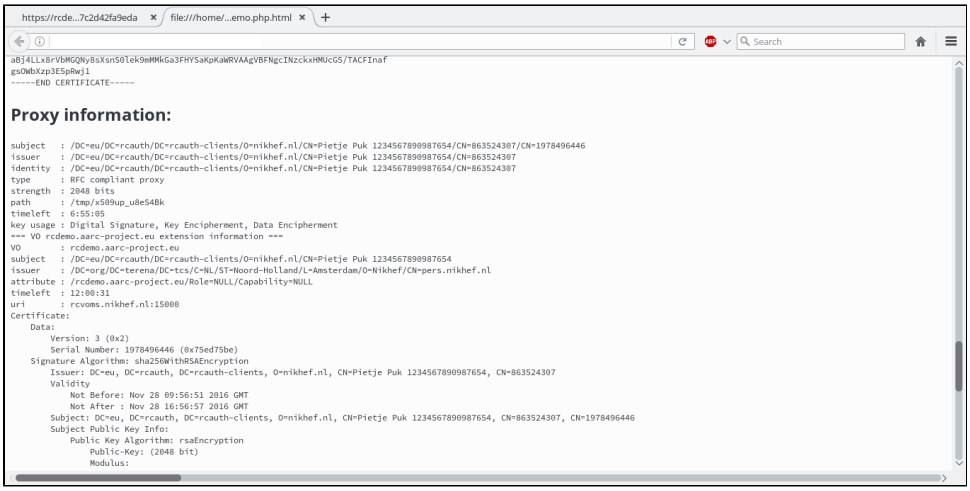
We have created two demonstrator Master Portal clients, which talk to a semi-production Master Portal (running for EGI), serviced by the production RCauth.eu online CA. We also have setup a test VOMS service with test VO, to test and showcase the integration with a VOMS attribute authority. The two demonstrators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

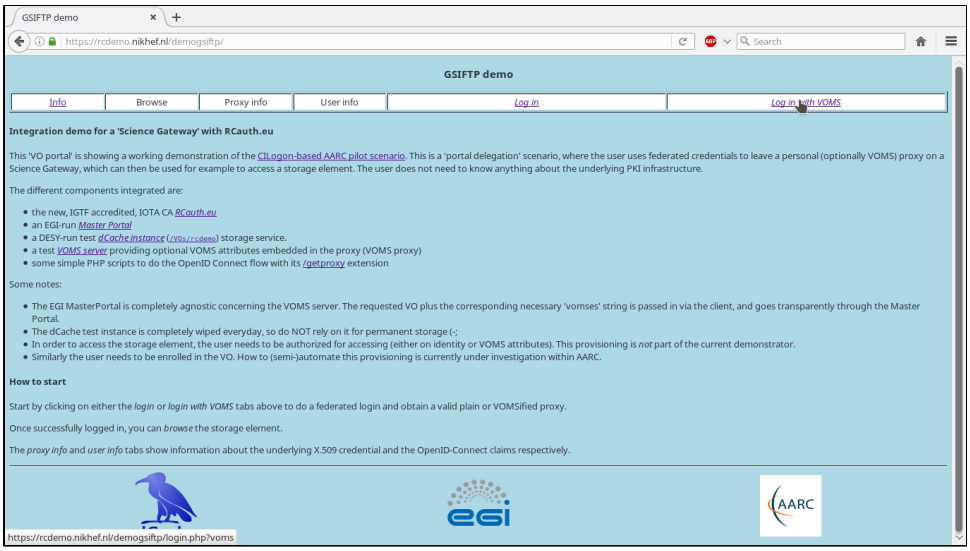
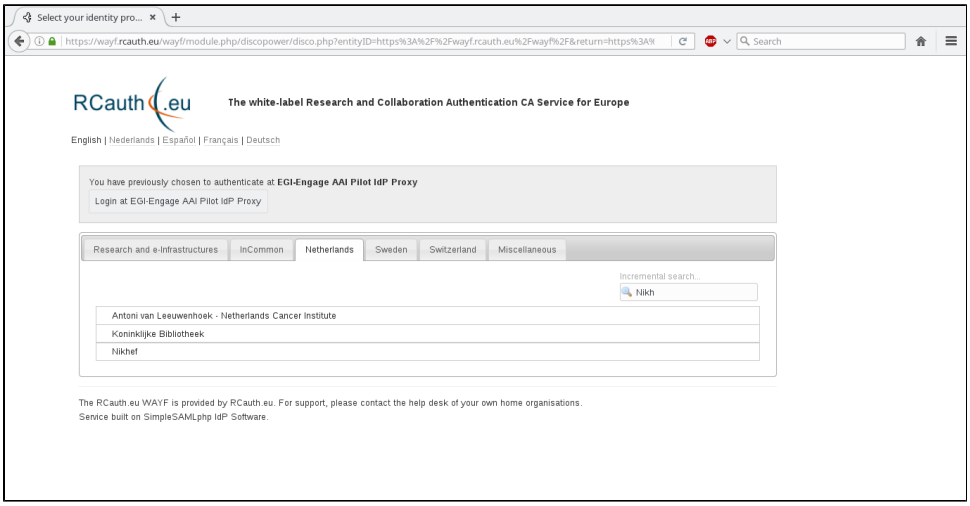
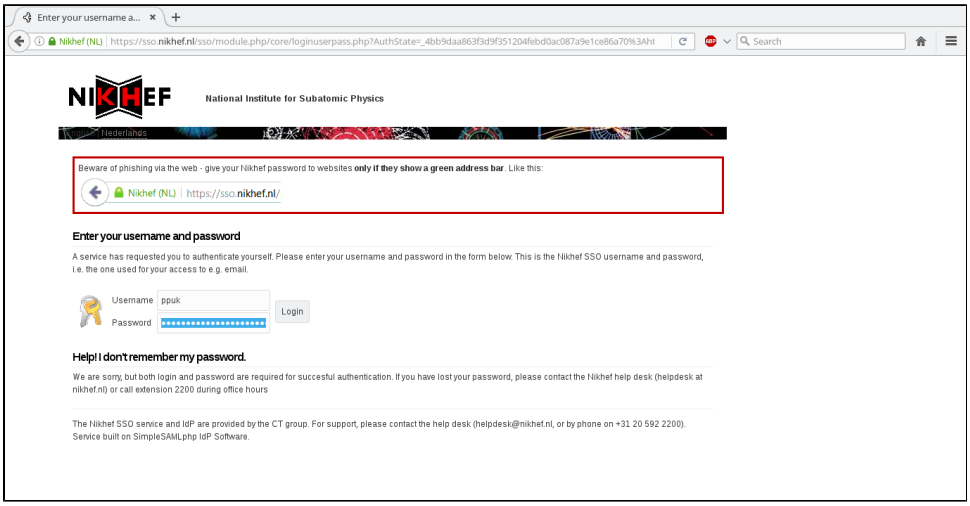
Demonstrator workflows

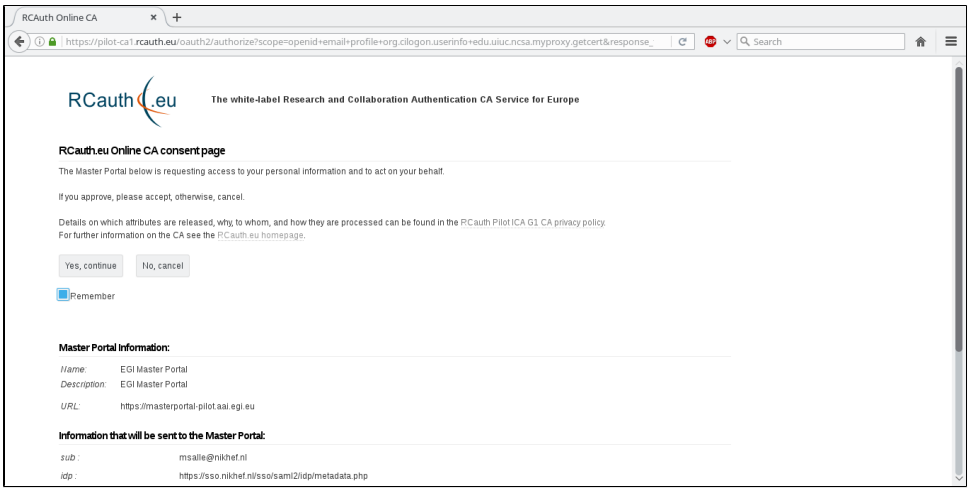
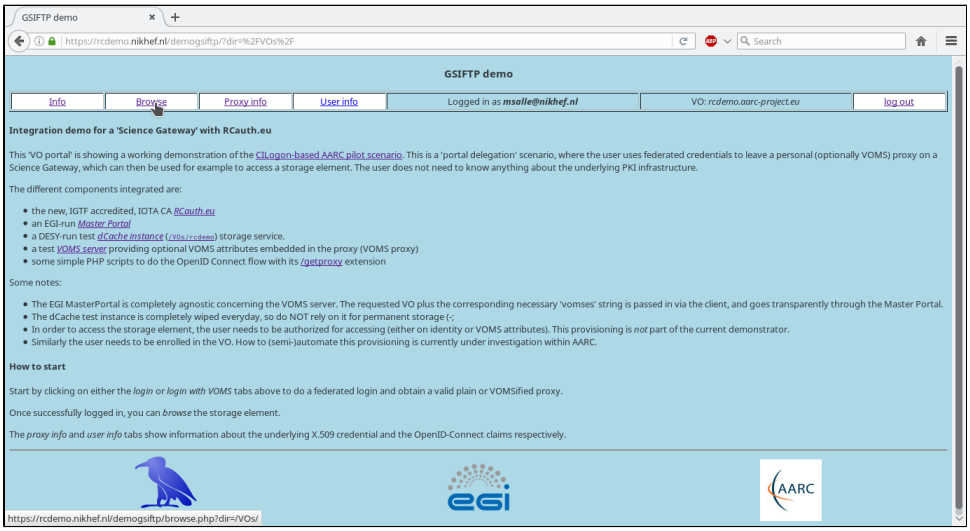
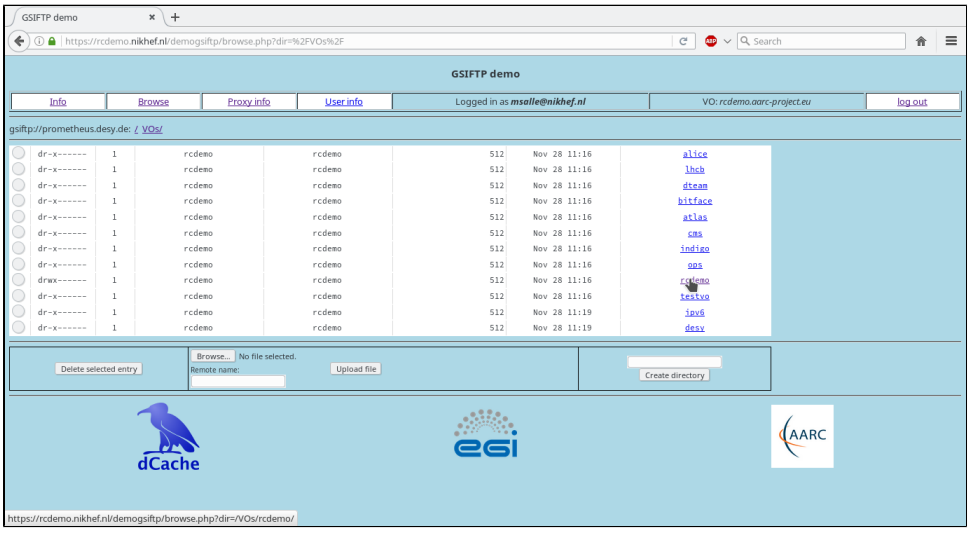
Basic demo:

1.	select one of the login pages, e. g. run VOMS demo to get a proxy certificate with VOMS attributes	
2.	choose your home IdP at the WAYF of the RCauth online CA	
3.	login at your home IdP	

4.	give consent at the RCauth online CA for attribute release	
5 a.	The demo shows the returned OpenID Connect information and ...	
5 b.	... obtains a proxy, showing its information	

GSIFTP demo:

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 WAYF of the RCauth online CA	
3.	login at your home IdP	

4.	give consent at the RCauth online CA for attribute release	
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).	
6	go to the VO home directory for 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.