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.
- 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	AARC Demo OIDC client to * +
	g. run VOMS demo to get a	🔦 🛈 🔒 https://rcdemo.nikhef.nl/demo.basii/oid/c_getproxy_demo_source.php 🛛 🖒 🔹 🗮
	proxy certificate with VOMS	Demo OIDC client to an EGI MasterPortal using the RCauth Delegation Server
	attributes	The demonstrator shows example portal integration code to do a full OpenID-connect handshake with a Master Portal plus the <u>/getproxy</u> request to obtain a (optionally VOMS) proxy
		The different steps are:
		1. Do an /authorize request at the Master Portal 2. Do a / token request using the received code
		3. Up a <u>restproxy</u> request using the received access_ower Steps 1. and 2. are standard ODC steps using the authorization flow, using the Master Portal as ODC Authorization Server. Step 3. acts as a request to a protected resource using the
		occess_token as bearer token. In step 1. the user is redirected from the Master Portal to the <u>RCauth eu</u> 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. RCauth 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.
		<pre><?php // // Smll depositation program showing how to obtain a prove via /gaturovy // Smll depositation</pre></pre>
		// and/commission of the second second and a prove via /geoproxy // endpoint on a MasterPortal. It is provided as is. //
		// Copyright (C) FOM-Winkhet 2015- // Licensed under the Apache License, Version 2.0 (the "License") // http://www.apache.org/licenses/LICENSE-2.0
		// // Authors: Nischa Salle (msalle (AT) nikhef.nl)
		<pre>imi_set("display_errors",1);</pre>
2	abaasa yayir bama IdP at tha	
2.	WAYF of the RCauth online CA	y seek you werkuy pro… × (+ (♦) ① A https://way/frauth.eu/way/fmodule.php/discopower/disco.php?entityID=https%34%2F%2Fway/frauth.eu%2Fway/%2E&return=https%34% C
		RCauth .eu The white-label Research and Collaboration Authentication CA Service for Europe
		English Nederlands Español Français Deutsch
		You have previously chosen to authenticate at EGLEngage AAI Pilot IdP Proxy Login at EGLEngage AAI Pilot IdP Proxy
		Research and e-Infrastructures InCommon Netherlands Sweden Switzerland Miscellaneous
		incrementa search
		Antoni van Leeuwenhoek - Netherlands Cancer Institute Koninkliike Bibliotheek
		Nikhef
		The D ^e with au MAVE is presided by D ^e with au Excrement places centret the help deal at usur num home acceptions
		na rusaura u vizi na proviesu gri rusaurazi na support, prese consectore replices o you con none organisatoris. Senice built on SimpleSAMLphp IdP Satware.
3.	login at your home IdP	
		C C Winter(NL) https://sso-niknet.nl/sso/module.php/core/loginuserpass.php/Autristate=_40b9daa88d9d9d5512U4lebduak08/a9e1ce88a./0%3Ahi C V Search T =
		NINTEFE National Institute for Subatomic Physics
		Bewae of phishing via the web - give your Nikhel 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.
		Usemane ppuk Login
		riceprison in termen in the finity password. We are some but both login and password are required for successful authentication. If you have lostyour password, please contact the Nikhef help desk (helpdesk at
		Inviterum of Lee exemption 2200 during once hours
		The Nikhel SSO service and IdP are provided by the CT group. For support, please contact the help desk (helpdesk@nikhel nl, or by phone on +31 20 592 2200). Service built on Simple/SAML.php IdP Software.

4.	give consent at the RCauth	RCAuth Online CA × +
	online CA for attribute release	🔄 🔿 🌢 https://pilot.ca1.rauth.eu/oauth2/authorize?scope=openid+email+profile+org.clogon.userinfo+edu.uiuc.ncsa.myproxy.getcert&response_ 🕜 👁 🔍 🧟 Search 🔒 🗮
		RCauth (egg The white-label Research and Collaboration Authentication CA Service for Europe
		RCautheu Online CA consent page The Master Portal below is requesting access to your personal information and to act on your behalt.
		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 PliotICA G1 CA privacy policy. For further information on the CA see the <u>RCauth eu homepage</u> .
		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 Portat: sub: msaile@nihtef.nl
		idp : https://sso.nik/tet.ni/sso/sami2/idp/metadata.php v
5	The demo shows the returned	https://rcde7c2d4zfa9eda × file///home/emo.php.html × +
a.	OpenID Connect information	 ♦ 0 c < q Search A =
	anu	First cURL response (/token request):
		Parsed response:
		Array (
		<pre>[access_token] >> https://msterportal-pilot.asi.gt.eu/mp-o2-server/sccessToken/12345678901234578901234578901234578901234578901234578901234578901234578901234578901234578012345789012345780123457890123457801234578012345789012345780123457801234578901234578012345780123457890123457801234578901234557890123455789012345578901234557890123455789012345578901234557890123455789012345578901234557890123455789012345578901234557890123455789012345789</pre>
		(token_type) => bearer (expires_in) => 900)
		Parsed ID Token:
		stdClass Object
		(a)(i) > one) stdClass Object
		<pre>{ (sub) => ppukgmikhef.nl [idp) => https://sso.nikhef.nl/sso/saml2/idp/metadata.php</pre>
		[eduPersonTargetedID] => https://sso.nikhef.nl/sso/saml2/idp/metadata.php11234567890987654321234567890987654321234 [idp_display_mame] >> Nikhef [cert_subject_dn] >> CMPPietj Puk 1234567890987654,0*nikhef.nl,DC*rcauth-Clients,DC*rcauth,DC*eu
		[name] >> Pietje Puk [eduPersonPrincipalNiame] => ppuk@mikhef.nl [given_name] -> Pietje
		[fantly_name] => Puk V
5	obtains a proxy, showing its	https://rcde7c2d42fa9eda × file///home/emo.php.html × +
b.	information	 (€) (0) (C) (0) < Q, Search (A) (A) (A) (A) (A) (A) (A) (A) (A) (A)
		abjeLLxer/om/gygsskashol (es/gm/kkash+htsan/kamkvAgrop-HgCLNzck/hMUCls//AcELnaT gs/mb/kzp355/ph/1 END CERTIFICATE
		Proxy information:
		subject :/DC=wu/DC=rcauth/DC=rcauth-Clients/D=mikhef.nl/CN=Pietje Puk 123456789987654/CN=863524387/CN=1978496446 issuer :/DC=wu/DC=rcauth/DC=rcauth-Clients/D=mikhef.nl/CN=Pietje Puk 123456789887654/CN=863524387
		identity : /DC=eu/Ox=cauth/DC=rcauth-Lients/O=nikhef.nl/CH=Pietje Puk 1234567899987654/CH=863524307 type : ERC compliant proxy strength : 2848 bits
		part : (rmp/savoug_usesanc timeleft : 655:565 key usage : Digital Signature, Key Encipherment, Data Encipherment ass Worden garcenciget ; usetparten information as
		Vi rusmo, alar cymolect. eu betens non immunatum
		tartitute: //ocom.goo.com/arc.as/a m/31 hood intender enacecommontener persimantenet attribute: //ocom.goo.com/arc.as/abc/ena/UL/Copability=WULL timeleft : 12:00:31 uri : :revom.siNeft.ch.115000
		Certificate: Data: Version: 3 (0x2)
		Serial Number: 1978496446 (BK75ed75be) Signature Algorithm: sha250HithAEAncryption Issuer: DC-eu, DC-euth, DC-exattr-Lints, O-mikhef.nl, CH-Pietje Puk 1234567890987654, CK-863524307
		Validity Not Before: Nov 28 09:56:51 2016 GMT Not After : Nov 28 16:56:57 2016 GMT
		Subject: DC+wu, DC+rcauth, DC+rcauth-Clients, O+nikhef.nl, CH+Pietje Puk 1234567809087654, CM+863524307, CH+1978496446 Subject Public Key Info: Public Key Info:
		Public-Key: (2848 bit) Modulus:

GSIFTP demo:

1.	Read the information about the	GSJF7P demo x +
	demonstrator and choose to log	🔄 🛈 🔒 https://rcdemo.nikhef.nl/demogsiltp/
	in either with or without VOMS	GSIFTP demo
	attributes	Info Browse Proxy info User info Log in Log in Log in the VOMS
		Integration demo for a 'Science Gateway' with RCauth.eu
		This VD portal is showing a working demonstration of the <u>CILogon-based AARC pilot scenario</u> . 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 <u>Reauth eu</u> an EGL-run <u>Moster Fortal</u>
		a des Youn (ess <u>examentation et your come</u>) storade service a test <u>YOMS server</u> providing optional VOMS attributes embedded in the proxy (VOMS proxy) some simple PHP kristis to the DeponDi Commet flow with its (instance) 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 VD. How to (semi-jautomate 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 pray info and user info tabs show information about the underlying X509 credential and the OpenID Connect claims respectively.
		https://rcdemo.nikhef.ni/demogsiftp/login.php?voms
2.	choose your home IdP at the	√ § Select your identity pro… × +
	WAYF of the RCauth online CA	🔄 🛈 🔒 https://wayf.rcauth.eu/wayf/module.php/disco.power/disco.php?entityID=https%34%2F%32Fwayf/rcauth.eu%2Fwayf%2F&return=https%34% C 💿 ∨ 🔍 Search 👔 🚍
		RCauth .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
		Antoni van Leeuwenhoek - Netherlands Cancer Institute
		Koninkijke Bibliotheek Nikhef
		The RCauth au WAYF is provided by RCauth au. For support, please contact the help desk of your own home organisations. Service built on SimpleSAMLphp IdP Software.
3	login at your home IdP	A Entervour username a. x +
0.		😧 🛈 🖨 Nikhef (NL) https://sso.mikhef.nl/sso/module.php/core/loginuserpass.php?AuthState=_4bbdaa863Bd9/351204febd0ac687a9e1ce86a70%3Ahn C 🕲 🗸 Q Search 🔒 🗮
		NICEF National Institute for Subatomic Physics
		Reware of phiching sig the web - noise your Nichel password to websites only if they show a green address bar Like this:
		Enter your usemame and password A service has requested you to authenticate yourself. Please enter your usemame and password in the form below. This is the Nikhel SSO usemame and password
		i.e. the one used for your access to e.g. email.
		Username ppuk Login
		p • Password
		HelpII don't remember my password. We are sony, but both login and password are required for succesful authentication. If you have lost your password, blease contact the Nikhef help desk thelpdesk at
		nikher (ni) or call extension 2200 during office hours
		The Nikhel SSO service and IdP are provided by the CT group. For support, please contact the help desk (helpdesk@nikhet.nl, or by phone on +31.20.592.2200). Service built on SimpleSAMLphp IdP Software.

4.	give consent at the RCauth	RCAuth Online CA X
	online CA for attribute release	🔄 🕐 🕼 https://pilot-ca1.rcauth.eu/oauth2/authorize?scope=openid+email+profile+org_cilogon.userinfo+edu.uiuc.ncsa.myproxy.getcert&response_ C 👁 v 🔍 Search 🔺 🚍
		RCauth Leu The white-label Research and Collaboration Authentication CA Service for Europe
		RGauth-eu Online CA consent page
		The Master Porta below is requesting access to your personal information and to act on your behalt.
		in you approve, prease a screep overeiment, sance. Details on which attributes are released, why to whom, and how they are processed can be found in the RCauth PilotICA GLCA privacy policy.
		For rumer information on the CA see the FC auth authomorphise.
		Remember
		Master Portal Information: Ilarne: EGI Master Portal
		Descriptor: EGI Master Portal URL: https://master.portal.edi.eu
		information that will be sent to the Master Portal:
		sub : msalle@nkhet.nl kdo : https://ss.on.khet.nl/ssofsaml2/ido/metadata.php
5.	choose to browse the remote	
	works once you have access to	GSIFTP demo
	the rcdemo VO, drop us a line to request access)	Info Browse Proxy info User info Logged in as msall@mikhef.nl VO: rademo.aarc-project.eu log.out
	to request docess).	Integration demo for a 'Science Gateway' with RCauth.eu
		This VD portal is showing a working demonstration of the <u>CLOgon-based AABC pilot scenario</u> . 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 <u>RCouth.eu</u>
		an EGF-run faster Entral a DESF-run test <u>decache instance (1/0); receiven</u>) storage service. a test <u>JOURS server</u> providing optional/VOMS attributes embedded in the proxy (VOMS proxy)
		some simple PHP scripts to do the OpenID Connect flow with its <u>/getproxy</u> 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 <i>not</i> 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 <i>kosh or login with</i> VOMS tabs above to do a federated login and obtain a valid plain or VOMS/fied 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/demogsiftp/browse.php?dir=/VOs/
6	go to the VO home directory for	GSIFTP demo x +
	rcdemo.	🔄 🕑 🔒 https://rcdemo.nikhef.nl/demogsiftp/browse.php?dir=%2FVOs%2F
		GSIFTP demo
		Info Browse Proxy.info User.info Logged in as msalle@nikhef.nl VO:rcdemo.aarc-project.eu log.out
		dr-x1 rcdemo 512 Nov 28 11:16 alice
		dr-x 1 rcdemo rcdemo 512 Nov 78 11:16 Lscb dr-x 1 rcdemo rcdemo 512 Nov 28 11:16 dtean dr-x 1 rcdemo rcdemo 512 Nov 28 11:16 dtean
		of -xerrer 1 receive receive of receive
		off-x 1 rcdemo fill Nov 28 11:16 indigo of-x 1 rcdemo rcdemo 512 Nov 28 11:16 optimized
		d rux 1 rcdemo rcdemo 512 Nov 28 11:16 rcdemo dr-x 1 rcdemo rcdemo 512 Nov 28 11:16 testro
		dr-x 1 rcdemo 512 Nov 28 11:19 jpr6 dr-x 1 rcdemo rcdemo 512 Nov 28 11:19 drxx
		BrowseNo file selected. Delete selected entry BrowseNo file selected. Create directory Create directory
		dCache
		https://rcdemo.nikhef.nl/demogsiftp/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.