



Authentication and Authorisation for Research and Collaboration

Sustainability for the AARC CILogin-like TTS Pilot

*Distribution and models for the CILogon-like TTS Pilot
for the European Open Science Cloud and
the Dutch National e-Infrastructure coordinated by SURF*

David Groep

NA3 coordinator

Nikhef PDP (Advanced Computing Research) group



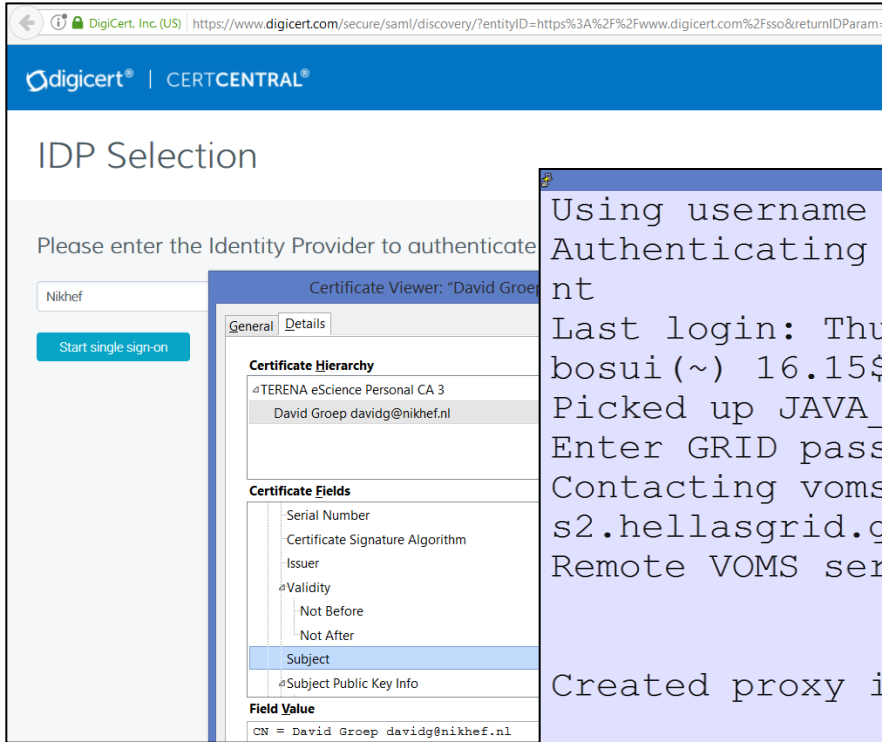
AARC I2GS session, EGI ENGAGE Conference

April, May 2017

Seamless (eduGAIN) Access to (non-Web) Resources using PKIX?



Traditional workflow – using a client-held credential



Works great *provided* the user understand the technology – and we may have found all users that know how to manage ☹️

```
Using username "davidg".
Authenticating with public key
nt
Last login: Thu Apr 13 17:43:46 2017 from 2a07:8500:120:e03b:
bosui(~) 16.15$ voms-proxy-init -voms dteam
Picked up JAVA_TOOL_OPTIONS: -Xmx512M
Enter GRID pass phrase for this identity:
Contacting voms2.hellasgrid.gr:15004 [/C=GR/O=HellasGrid/OU=h
s2.hellasgrid.gr] "dteam"...
Remote VOMS server contacted succesfully.

Created proxy in /tmp/x509up_u5917.

Your proxy is valid until Wed Apr 19 04:16:05 CEST 2017
bosui(~) 16.16$ █
```

```
bosui(/user/davidg (davidg.emin)
bosui(~) 16.25$ gsissh sgmlhcb@kot.nikhef.nl -p 1975 'id -a && hostname -f'
uid=991(sgmlhcb) gid=2015(lhcbsgm) groups=2015(lhcbsgm)
kot.nikhef.nl
bosui(~) 16.25$
```

Seamless (eduGAIN) Access via the CILogon-like TTS Pilot: aims

- **Ability to serve a large pan-European user base without national restrictions**
 - without having to rely on specific national participation exclusively for this service
 - serving the needs of cross-national user communities that have a large but sparsely distributed user base
- **Use existing resources and e-Infrastructure services**
 - without the needs for security model changes at the resource centre or national level
- **Allow integration of this system in science gateways and portals with minimal effort**
 - only light-weight industry-standard protocols, limit security expertise (and exposure)
- **Permit the use of the VOMS community membership service**
 - attributes for group and role management in attribute certificates
 - also for portals and science gateways access the e-Infrastructure
- **Concentrate service elements that require significant operational expertise**
 - not burden research communities with the need to care for security-sensitive service components
 - keep a secure credential management model
 - coordinate compliance and accreditation – and help meet EU privacy stuff in just one place to ease adoption
- *Optional elements: ability to obtain CLI tokens (via ssh agent or even U/P); implicit AuthZ*

Flow for RCauth-like scenarios

Community Science Portal

Permissions	User	Group	Size	Date	Filename
dr-x-----	davidg	davidg	512 Feb 7 06:00	lost+found	
dr-x-----	davidg	davidg	512 Feb 7 06:01	VOs	
dr-x-----	davidg	davidg	512 Feb 7 06:01	Users	
dr-x-----	davidg	davidg	512 Feb 7 06:02	UTF-8	
dr-x-----	davidg	davidg	512 Feb 7 06:03	Music	
dr-x-----	davidg	davidg	512 Feb 7 06:04	Video	
d--x-----	davidg	davidg	512 Feb 7 11:21	upload	

RCauth.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 and to act on your behalf. If you approve, please accept, otherwise, cancel.

Remember

Yes, continue No, cancel

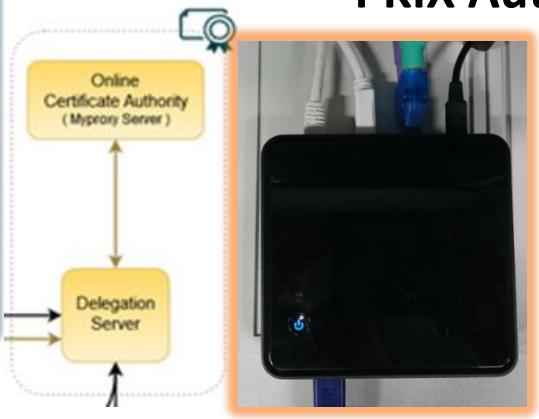
Master Portal Information:

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

Information that will be sent to the Master Portal:

sub : davidg@nikhef.nl
 idp : https://sso.nikhef.nl/sso/sem2/idp/metadata.php
 eduPersonTargetedID : https://sso.nikhef.nl/sso/sem2/idp/metadata.php/3960c9bec163785af515c33ab0a4346330639f
 idp_display_name : Nikhef
 cert_subject_dn : CN=David Griep QK-DH6ZHT1hoVTT16,OU=nikhef.nl,DC=rcauth-clients,DC=rcauth,DC=eu
 name : David Griep
 eduPersonPrincipalName : davidg@nikhef.nl
 given_name : David
 family_name : Griep
 email : davidg@nikhef.nl

Accredited PKIX Authority



Infrastructure Master Portal Credential Store

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 **Nikhef**

Logs at Nikhef

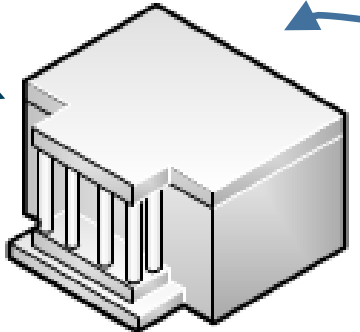
Research and e-Infrastructures | InCommon | UK | Netherlands | Sweden | Switzerland | Other countries | Miscellaneous

EGI ANI Check:
 ELIXIR research infrastructure ANI

Policy Filtering WAYF / eduGAIN

REFEDS R&S Sirtfi Trust

User Home Org or Infrastructure IdP



Built on CILogon and MyProxy!
www.cilogon.org

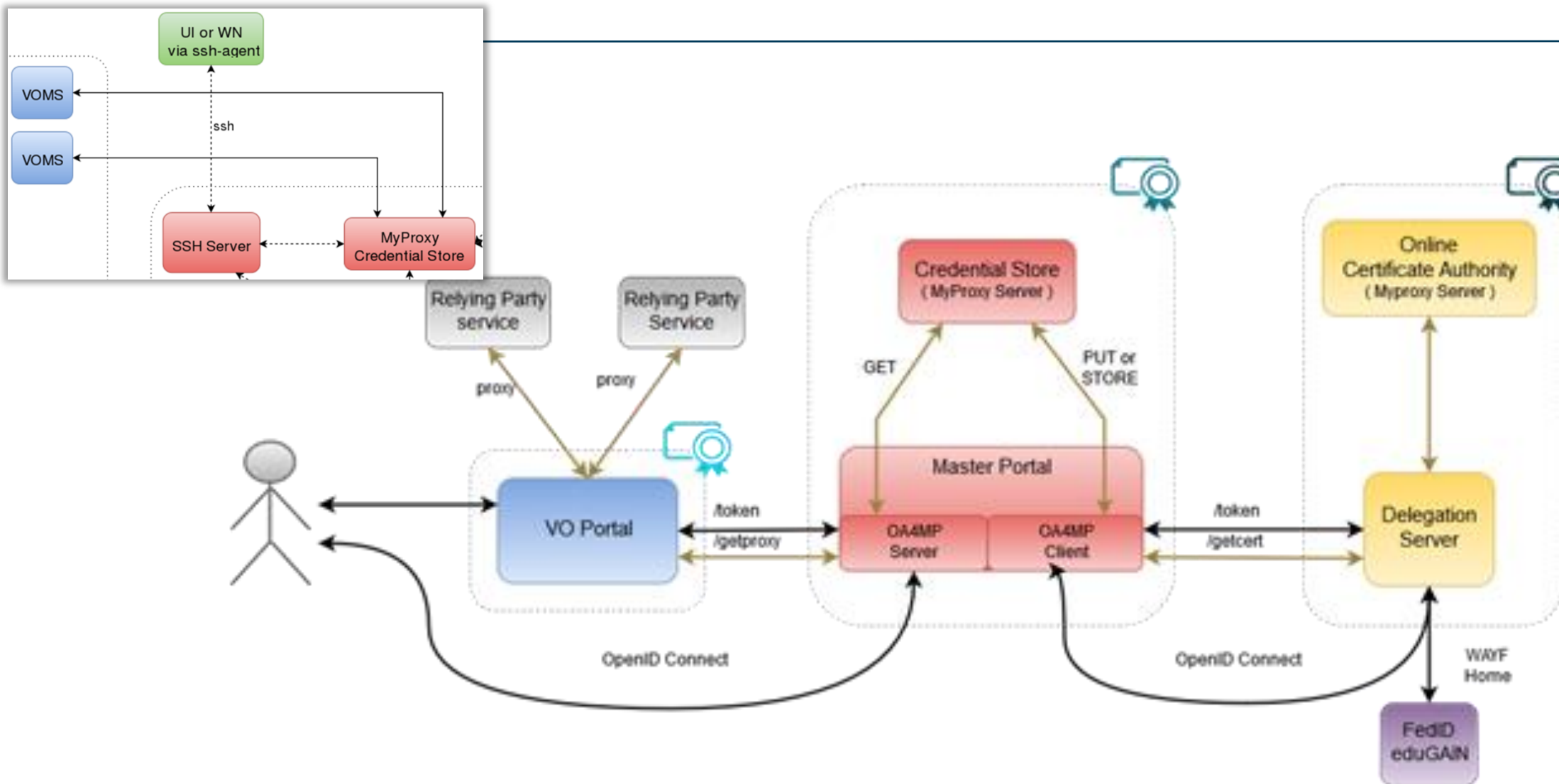
see also <https://rcdemo.nikhef.nl/>

DEMO

<https://rcdemo.nikhef.nl/>
<https://rcdemo.nikhef.nl/getproxy>

you can do most things except access the Prometheus dCache pool right now
that last elements needs your credential to be added to the permitted list

CILogon-like TTS Pilot - distributable elements



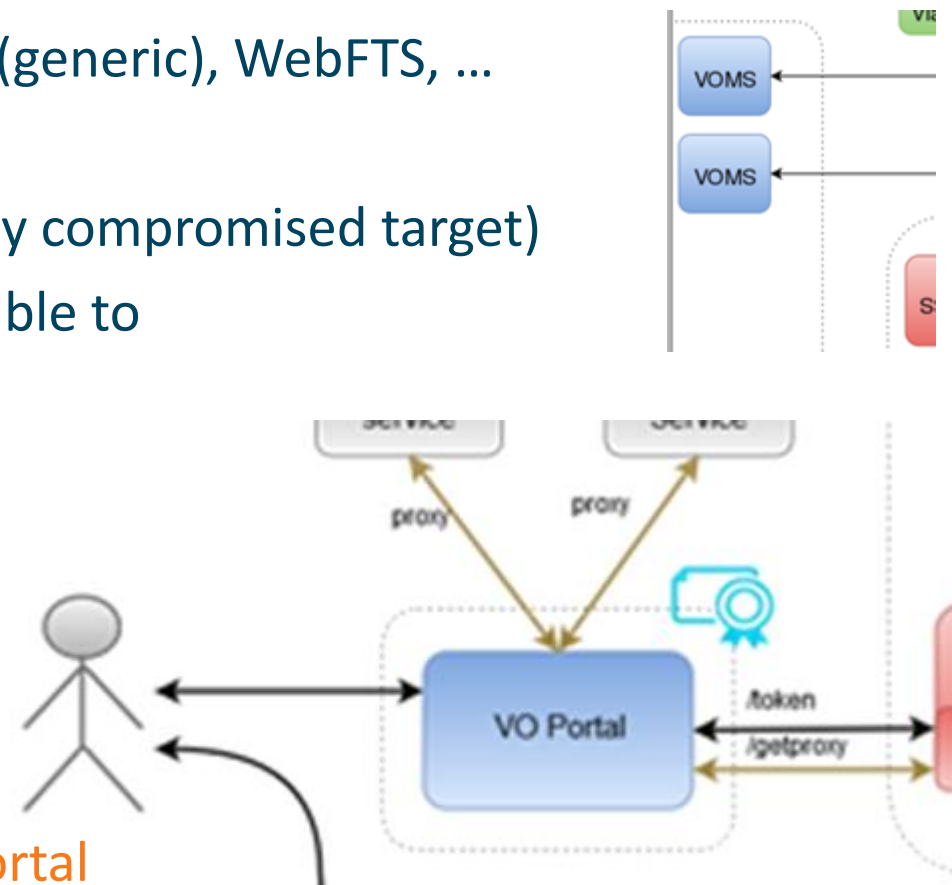
Blue: VO services and resources

- Are around today, either self-managed or hosted, in most communities
- Science gateways, portals, e.g. HADDOCK, Galaxy, LifeRay (generic), WebFTS, ...
- Omnipresent (and has unfortunately proven to be an easily compromised target)
- Will have to *get credentials* from the MPs, but should be able to do so *only for authenticated users*
- Downtime will impact its' own users, but there will be many of these (same service by different sites?)

Considerations:

Operated as today by the communities

Bound slightly stronger to the community via the Master Portal



Red: the Master Portal (MP) and Credential Repository

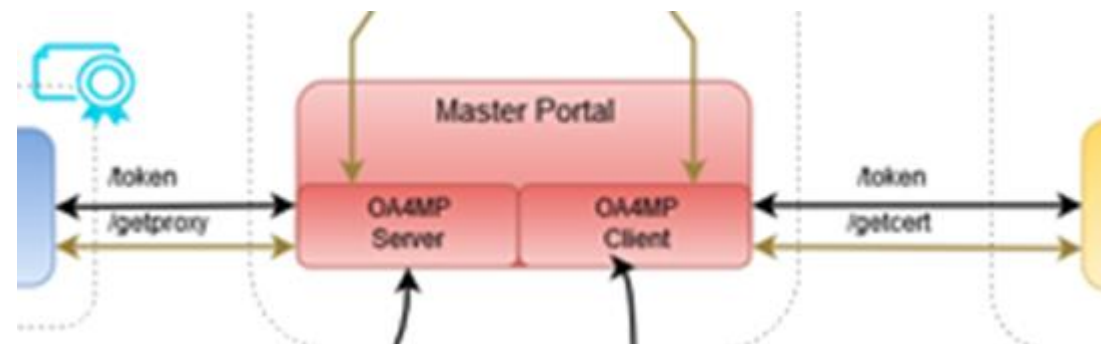
- Needs to be a trusted element (to permit credential storage by the TTS)
- Requires some operational and security expertise (managed data centre, locked racks, access controls, ability to designate infrastructure for security operations, trained staff)
- Connects to (many) workflow-specific VO portals
- Connects to a single Delegation Service/TTS – and can give *IdP hints*
- Downtime of an MP disables resource access for connected VO portals

Considerations:

One per Research or e-Infrastructure

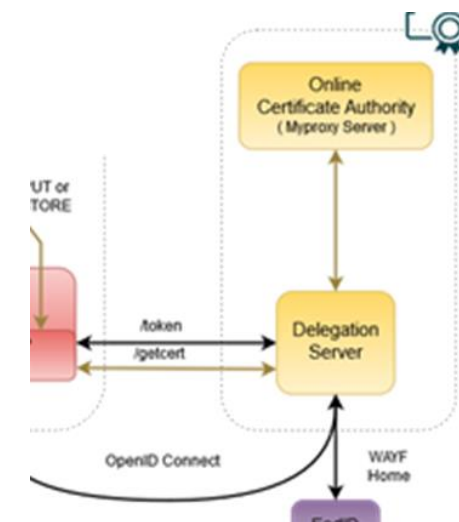
Should be highly available (database sync)

Infrastructures can also build their own (e.g. in WaTTS, Unity, ...)



Yellow: the Token Translator/OA4MP/CA service

- Needs security and policy expertise – and ability to maintain accreditation
- Needs operational and technical capabilities: hardware security modules, managed data centres, off-line and on-line secure areas, ROBAB-proof trained personnel, ability to designate infrastructure for security operations
- Connects to (a few, we hope) Master Portals (MPs) with explicit agreements *to take care of user credential protection and compliance*
- Connects (many, we hope scalably) federations, IdPs and (few) SP-IdP-Proxies
- *May have to present a WAYF, if the VO portal does not pass IdP entityID*



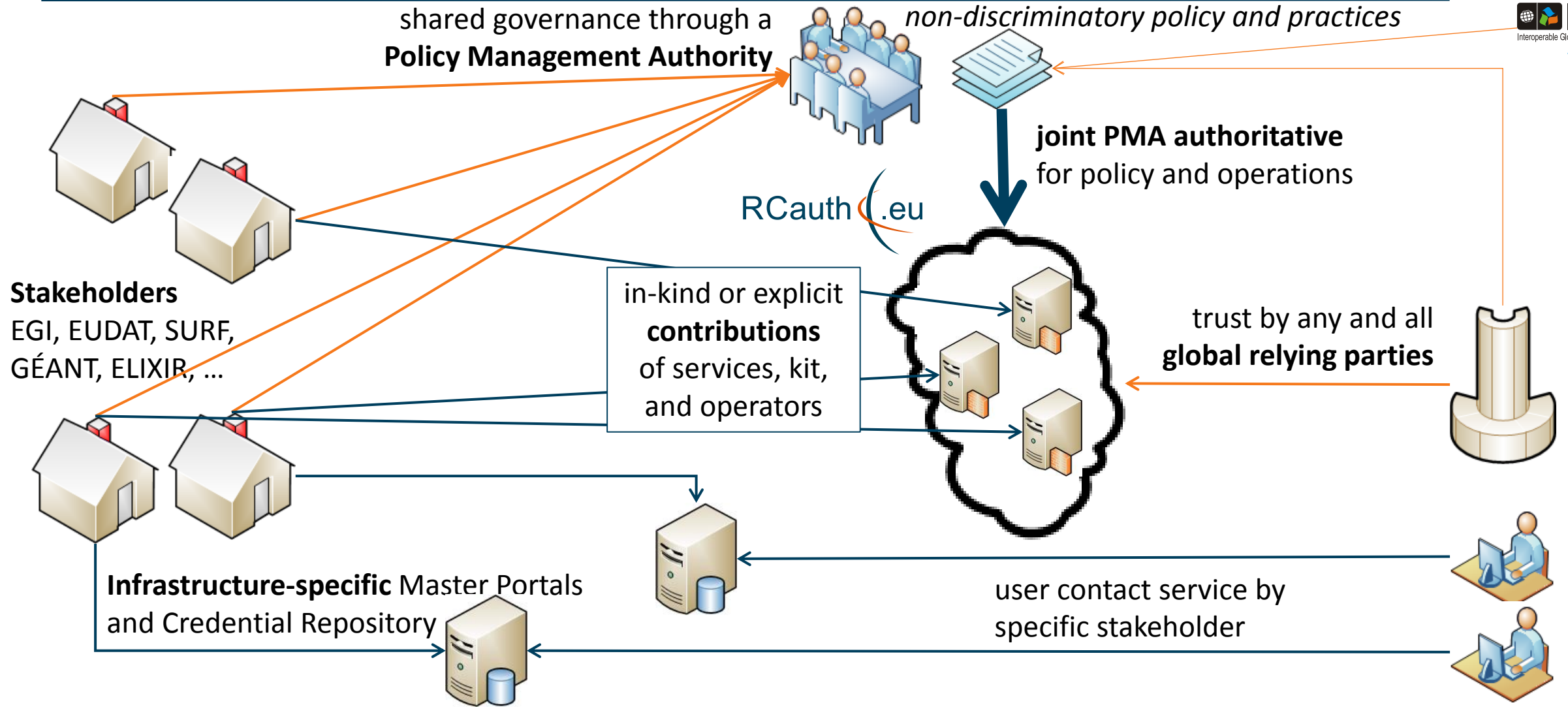
Considerations:

Trust and compliance, with IGTF accreditation

Single logical instance, with HA built in for production

Managed by a consortium: in Europe agreed by at least EGI, EUDAT, GÉANT, ELIXIR, and SURF

Potential RCauth.eu management model



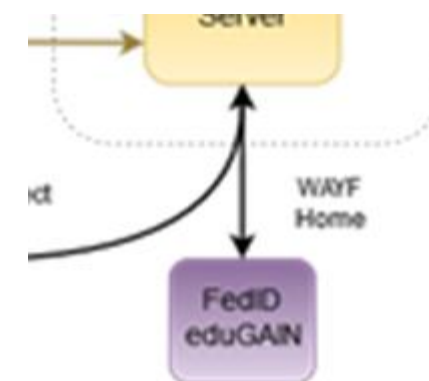
Purple: connected federations and IdPs (proxies)

- In the generic case (conventional R&E federations) only limited control possible
- Infrastructure-managed IdPs will provide more specific capabilities, *e.g.*, uniqueness
- Connects to many services, of which the DS/TTS is just one
- Build on common technology (keep with SAML, no OIDC here)
- Shared policy compliance: REFEDS R&S, Sirtfi
- Negotiate only when needed (but a TTS must serve all users to prevent fragmentation!)
- Cope with heterogeneity (i.e.: use a ‘filtering WAYF/entity filter proxy’)

Considerations:

eduGAIN registration, Sirtfi adoption, REFEDS R&S, filtering capability

Needs a friendly registrar, but is otherwise ‘just another SP’



Sirtfi and R&S – policy needs for trust in identity providers and federations

- REFEDS and federation focused FAQ
- Definition of the global Security Contact meta-data profile for use in eduGAIN
- Namespace for Sirtfi Assurance at IANA
- Used in cyber ops roleplay exercises
- Promoted at I2TechX, FIM4R, Kantara, and TF-CSIRT
- Ingredient to the ‘CILogon pilot’
combination of
REFEDS “Research and Scholarship”
and
Sirfti v1.0

meets assurance requirements for RIs and EIs according to the IGTF “assured identifier trust”



The screenshot shows the SIRTFI website header with the URL <https://refeds.org/SIRTFI> and a breadcrumb trail 'REFEDS > SIRTFI'. The main content area includes an introductory paragraph about the Security Incident Response Trust Framework for Federated Identity (Sirtfi), a paragraph about the REFEDS' Sirtfi Working Group, and three navigation buttons: 'Benefits' (with a group of people icon), 'Sirtfi v 1.0' (with a document icon), and 'FAQs' (with a question mark icon). Below each button is a short description: 'Why should I join? What are the Benefits?', 'View the Sirtfi Framework', and 'Need help?'.



Mar 17th 137 IdPs in eduGAIN that support Sirtfi

Where are we now?

- Several pre-production instances deployed, for EGI and ELIXIR (all managed by Nikhef)
- A ‘production demonstrator’ instance of the TTS set up in conceptually the ‘right way’:
 - Dedicated servers, secure environment, FIPS 140 level 3 approved HSM, anchored in a stable way
 - Policy and practices accredited (under the ‘unique-identifier-only’ profile) at the IGTF – which is good enough for some infrastructures, and is expected to be good enough in EGI in combination with managed communities
 - Scalable negotiation model based on Sirtfi and REFEDS R&S section 6
 - Model requirements on attached MPs defined (for key protection)
 - Trust anchors in production (RCauth.eu and its “DCAROOT” HLCA)
- Last updates to the software ongoing: policy-filtering ‘proxy-WAYF’ to link to eduGAIN & more

RCauth (.eu)

But it’s a production demonstrator, *not* production, *without* an SLA, and with limited capacity

- ... and it’s a bit a ‘Heath Robinson’ service, using mostly pre-available hardware

Costing the services

Highly depends!

- What is 'the service'? Delegation Service & WAYF? Master Portals?
- Technical elements only, or operational service implementation?
- Desired service level (support & availability)
- Extent of the service (number of users, communities, ...)

Can be anywhere between a few kEur to well over 100+kEur cost per year 😊

Recuperation model appears to converge

- Master Portals (Credential Management) on a per-Infrastructure basis, from own funding
- Delegation Service/RCauth.eu: free at point of use
- Funded via in-kind contributions by the major e-Infrastructures
- Distributed H/A setup, leveraging existing capabilities and some additional person effort

References

<https://wiki.geant.org/display/AARC/Models+for+the+CILogon-like+TTS+Pilot>

Thank you

Any Questions?

davidg@nikhef.nl



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).