Authentication and Authorisation for Research and Collaboration

RCauth.eu CILogon-like service in EGI and the EOSC

Deployment and Sustainability Models
for the AARC CILogon-like TTS Pilot

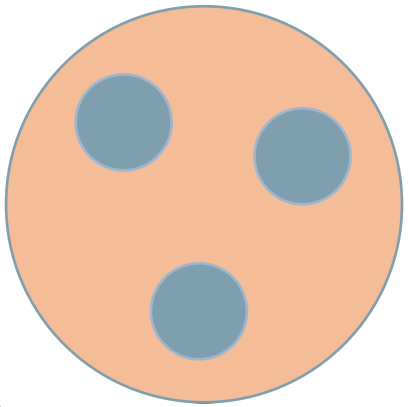
David Groep
AARC NA3 coordinator, EGI AAI-TCB
Nikhef PDP group

EGI TCB-AAI
May 2017

RCauth.eu is operated by Nikhef as part of the
Dutch National e-Infrastructure for Research coordinated by SURF
for the benefit of the collective European Research and e-Infrastructures

Aim: seamless access to existing services with eduGAIN for all

Pan-European Access
not country-opt-in based
standards-based assurance



Dispersed User Base
critical mass is beyond
any single institution

Concentrate Sensitive Components
no long-term token needs in the VO portal
credential management by the Infrastructures

No Changes to the Model
for infrastructures and
their service providers

Command-line and VOMS
with delegation and brokering

Minimal Coding
for the VO portals

CILogon-like TTS Pilot, the User's work flow

user login flow: VO portal → Community Infrastructure → RCauth service → federated AAI

credential flow: authentication, SAML federation, Policy Filter, OpenID Connect, PKIX+OIDC, (VOMS), proxy-on-portal

voms admin

MyProxy Credential Management Service

RCauth.eu

SIRTFI

R&S

science gateways

AARC Master Portal or Infrastructure Solution

delegation

server

CILogon

filtering WAYF

SURF SARA MinE project Make it yours

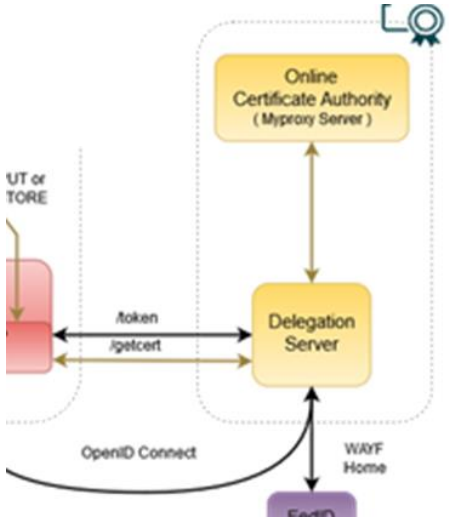
eduGAIN

egi

elixir Data for Life

Token Translator RCauth.eu service component

- Needs **security and policy expertise** (people) – and ability to maintain accreditation
- Needs **operational and technical capabilities (**hardware):
  hardware security modules, managed data centres, off-line and on-line secure areas, trained personnel, designate infrastructure to security operations
- Connects to – a handful of – 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
- Serves many communities, some of which we don't yet know, and beyond just the European e-Infrastructures



Considerations:

Trust and compliance, with IGTF accreditation

Single logical instance, with HA built in for production

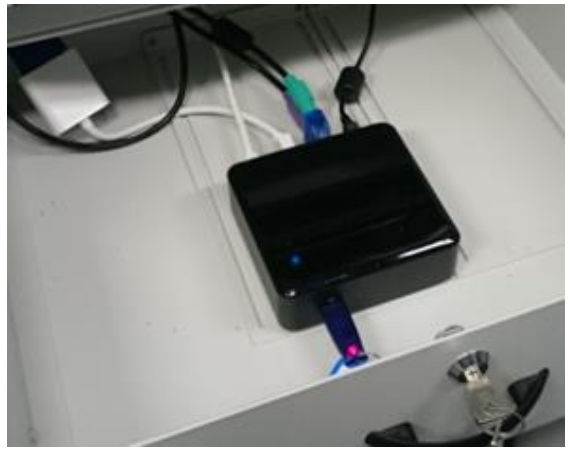
Managed by a consortium: in Europe agreed by at least EGI, EUDAT, GÉANT, ELIXIR, and SURF

Where are we today?

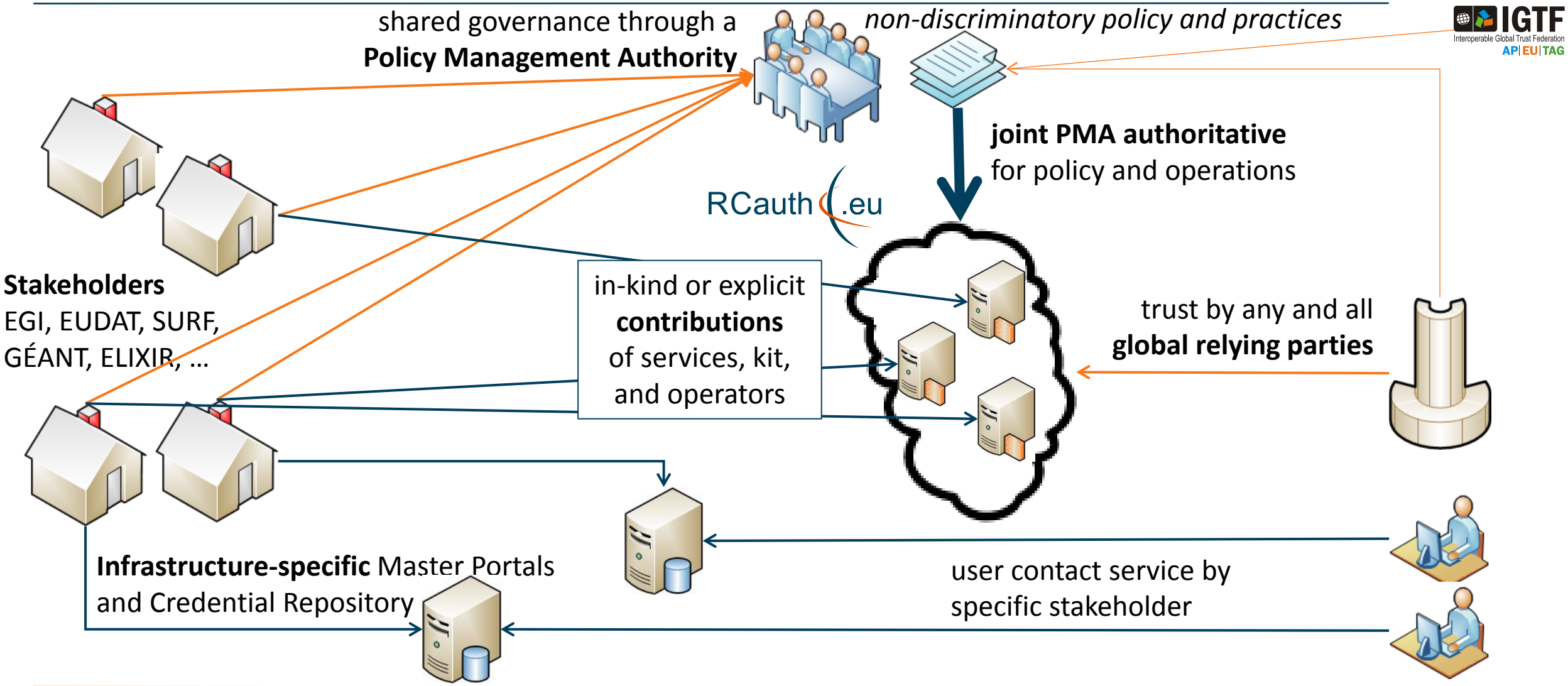
- In ‘pre-production’ since May 2016, now several connections deployed to EGI, ELIXIR, DNI/SURF, …
- ‘production demonstrator’ instance of *Rcauth.eu* set up in the ‘right way’ at Nikhef (only for now):
  - Dedicated secure environment, FIPS 140 level 3 approved HSM, anchored in a stable way
  - Policy and practices accredited under ‘unique-identifier’ profile at the IGTF
    – good enough for some infrastuctures, and within EGI *in combination with* vetted & managed communities
  - Scalable negotiation model based on Sirtfi and REFEDS R&S section 6
  - Requirements on attached credential stores defined (for key protection)
  - Trust anchors in production (RCauth.eu is part of the ‘EGI-CAM’ package)

But it’s a **production demonstrator**, *not* true production,
without an SLA, and with limited capacity (~2k users)

- … and it’s a bit a ‘Heath Robinson’ service, using mostly pre-available hardware
- … intended availability is high, but no on-site 24x365, nor redundancy



Planned RCauth.eu management model



Service distribution and support plans

Beyond just the ‘Nikhef Best Effort’ service

- what is ‘the service’ in this context: Delegation Service & WAYF
- can be anywhere between a few kEur to well over 100+kEur cost per year …

Recuperation model

- Master Portals (Credential Management) from other (non-RCauth) 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

EOSC Hub Consortium picked middle ground

- contribute effort and some hardware resources to the joint pan-European pool
- help steer the development through joint, independent, management body (PMA)
- partners with existing security operations expertise: GRNET, STFC, FZJ + SURF/Nikhef

References

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

https://www.rcauth.eu/

DIY demo – for users from Sirtfi'ed R&S Institutions, or through the IGTF eduGAIN bridge:
https://rcdemo.nikhef.nl/

Parts of this work have also been performed as part of the work programme of EGI-ENGAGE
EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Thank you

Any Questions?

davidg@nikhef.nl

Thanks to all collaborators on this joint enterprise:
EGI, EUDAT, GEANT, SURF;
Nikhef, GRNET, Christos Kanellopoulos and to Jim Basney of
NCSA, CTSC and CILogon

https://aarc-project.eu

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).