Authentication and Authorisation for Research and Collaboration

“RaaS” – towards RCauth.eu as a Service

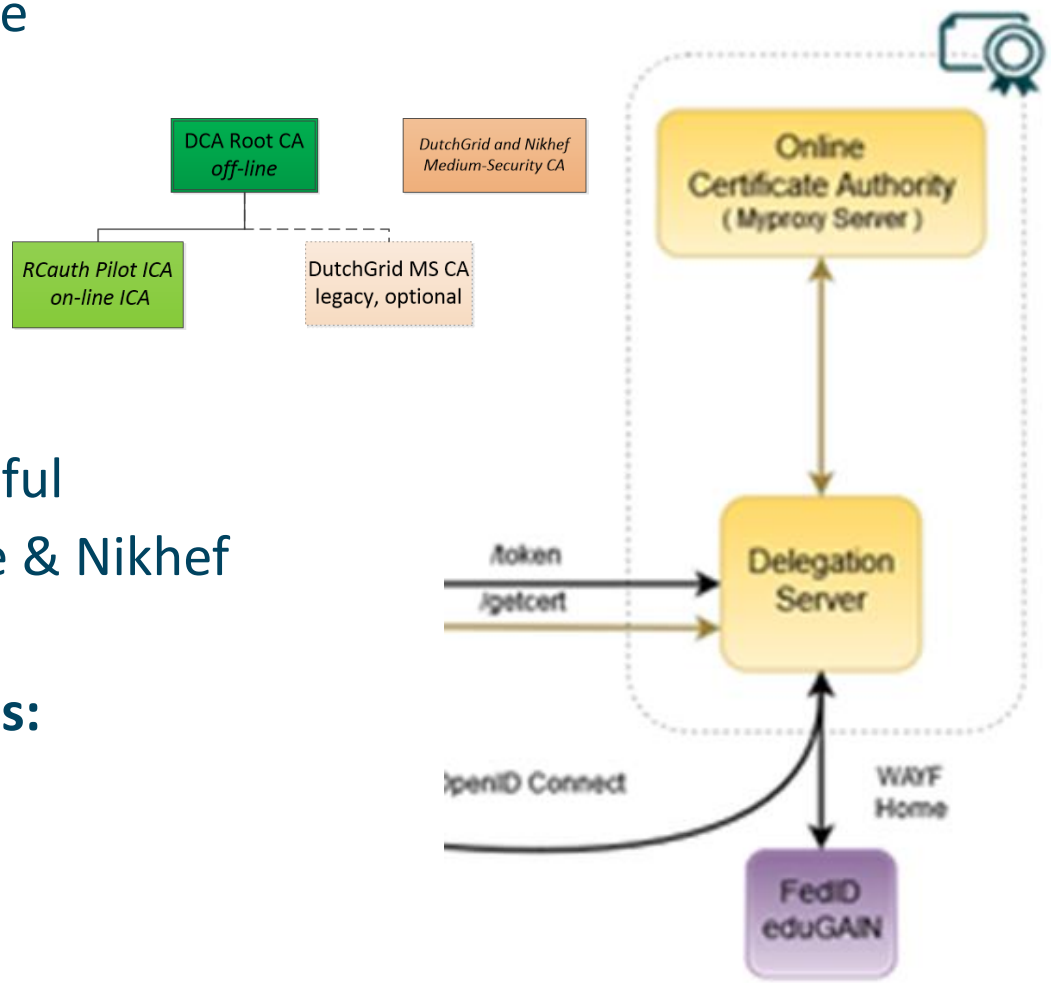
Changes in RCauth governance as a production service

David Groep
Policy and Best Practice Coordination, AARC
Nikhef PDP Advanced Computing Research

42nd EUGridPMA Plenary Meeting
January 2018

RCauth.eu – a white-label IOTA CA in Europe

- Cover as much as R&E Federated Europe as possible
- Scoped to research and collaborative use cases
- In a scalable and sustainable deployment model



Following the AARC pilot

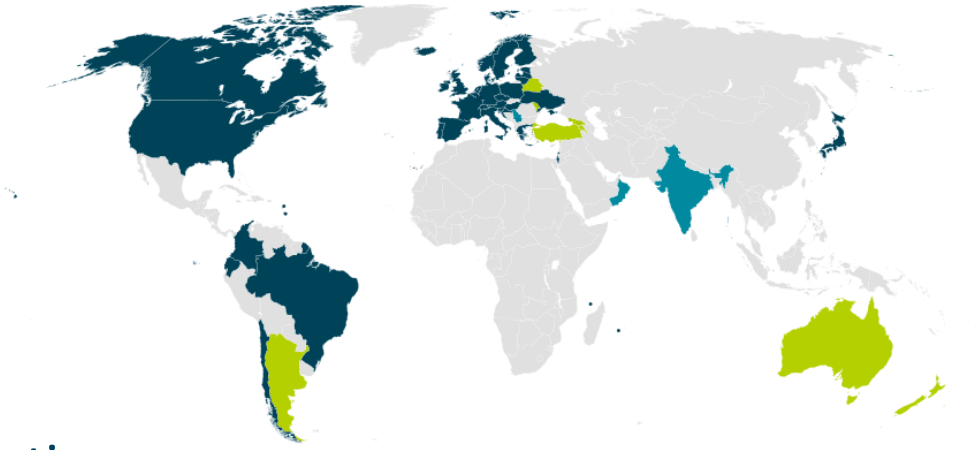
- operates as a 'production-compatible' pilot service
- which will operate for as long as necessary and useful
- is supported by the Dutch National e-Infrastructure & Nikhef

… to support multiple applications and communities:

- EGI CheckIn, B2ACCESS, and WaTTS instances
- Project MinE
- ELIXIR, and the Life Sciences AAI

Our Registration Authorities: the Federated IdPs [1.3.2]

- RAs are the eligible IdPs connected through a Federated Identity Management System (FIMS)
- primarily: ensemble of IdPs in eduGAIN that meet the policy requirements of this CA
- Eligible applicants are all affiliated to an RA



Three eligibility models

1. Direct relationship CA-IdP, with agreement declaration
2. Within the Netherlands: SURFconext Annex IX* compliance for all IdPs
3. Rest of eduGAIN: – "Sirtfi" security incident response and OpSec capabilities plus
   – REFEDS "R&S section 6" non-reassigned identifiers and applicant name

   are required, and tested via statement in 'meta-data' any by releasing the proper attributes

"IdPs within eduGAIN [#3] are deemed to have entered materially into an agreement with the CA"

RCauth.eu – values and principles

To guide management decisions, core principles (of scalable policy) were made explicit:

- RCauth.eu is a ‘white label’ service that can be integrated with as many services as useful

- target research and innovation capabilities of **global**, **cross-national**, and **national Research and e-Infrastructures**
- accessible to **any qualified person** that has a federated identity
- shall **meet assurance requirements** commonly agreed
- **leverages inter-federation** … Yet the service **shall allow for exceptions and explicit trust** relationships [to support] ubiquitous availability
- the service is **a collaborative effort** based on peer review and on appropriate assessments
- service **shall be open**, and its positions taken towards its peer and accreditation bodies be openly discussed

From what you accredited …

RCauth Today

Operated by the “DutchGrid CA” – a collaboration under the DNI operated by Nikhef

- for science and research
- for the purpose of cross-organisational distributed resource access,
- solely in the context of academic and research and similar, not-commercially competitive, applications.

“These services are

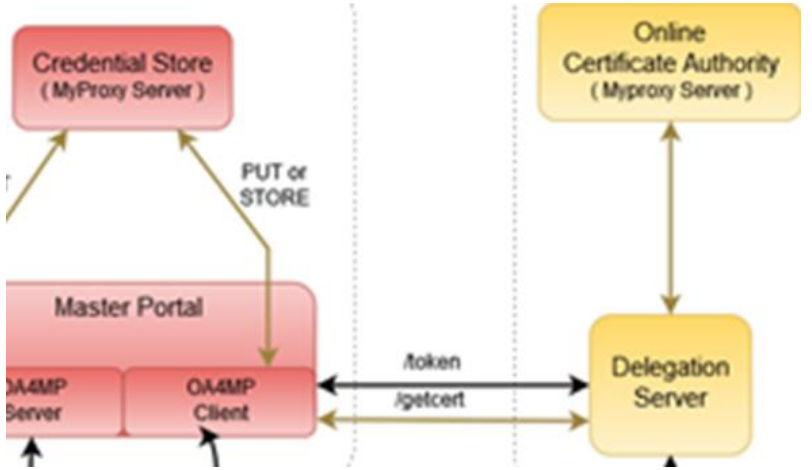
- primarily intended for the practitioners of scientific research in the Netherlands,
- appropriately taking into account the European and global nature of research and collaboration”

***read**: we will offer it to Europe and the world, but if the world diverges wildly from the aims of the Dutch National e-Infrastructure we might have to reconsider*

Other Participants

RCauth will seldom see individual users

- authentication requests come via the Master Portals
- we will (ourselves & directly!) authenticate the users, but …
- … then release the certificate to the intermediary



In the RCauth case:

- Explicit relationships required
- Encoded via a (shared) OIDC Client ID and Client Secret
- Contrary to e.g. Google, we will not accept ‘any’ OIDC client, but explicitly configure trust
- Assessment based on PKP Guidelines and Trusted Credential Repository guidelines
- *Along with other criteria (for scalability): constituency, community size, relevance, &c*

Operators and Administrators [1.5]

Three roles defined

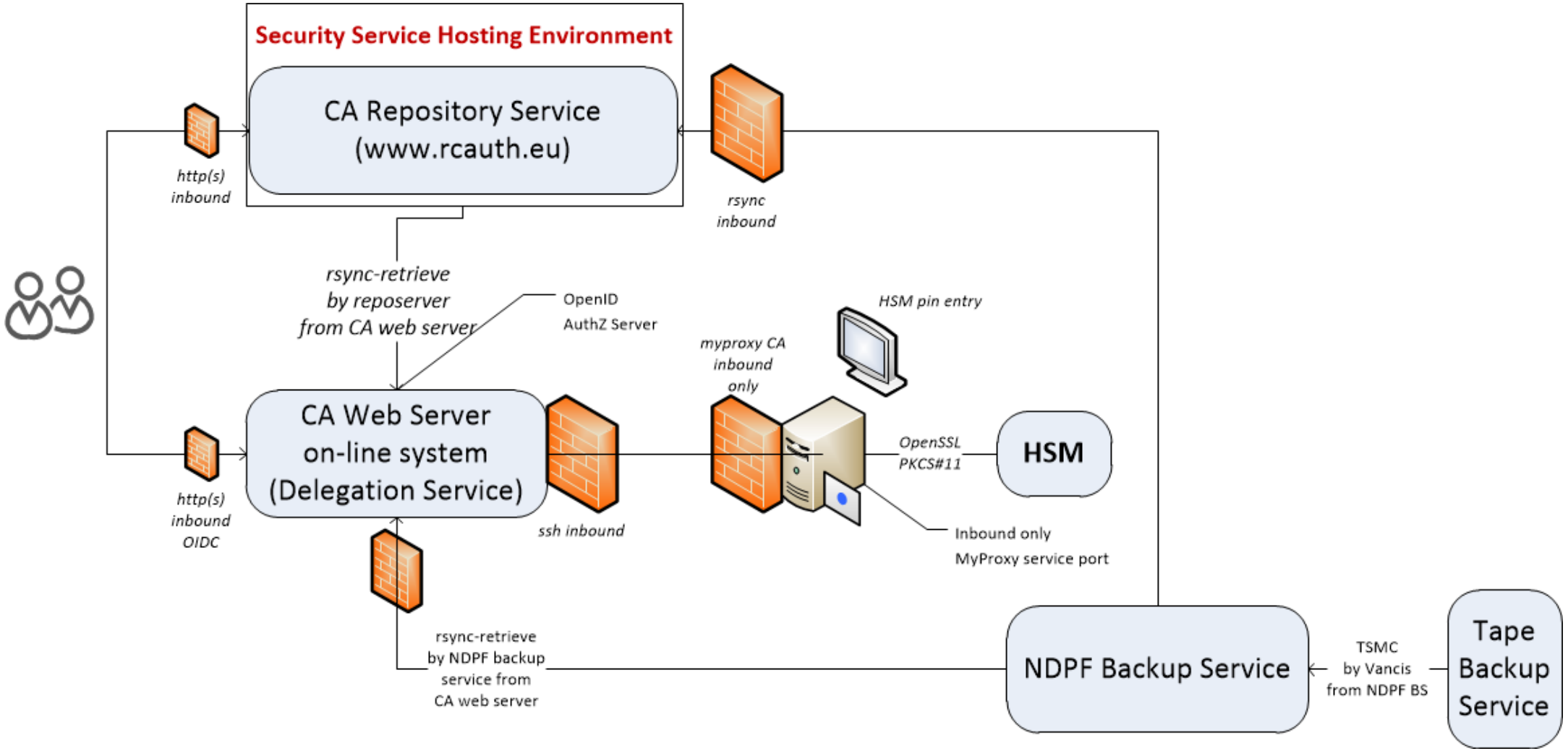
1. **Managers** of the DCA Service (by construction: joint with all other DCA CAs)
2. **Administrators** of the RCauth Pilot ICA (de facto joint with all other DCA CAs)
3. **Operators**, “individuals that can issue certificate and publish updated revocation information” (specific to the RCauth service)

The Operators know how to activate the HSM and access the off-line machine, but have no access to the private key outside the HSM*

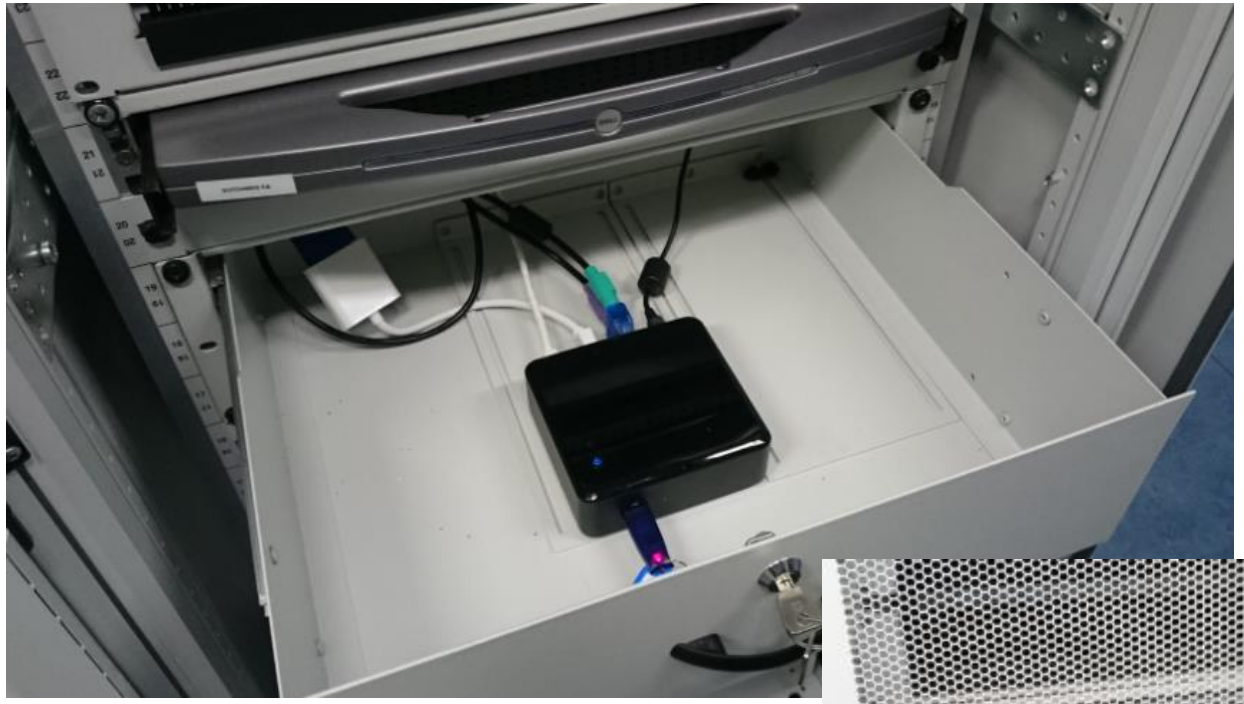
There are more people that have selected access to some physical systems (Housing, ICT operators staff), but they don’t know any activation data and controls are in place to make physical interventions complicated (padlocks, protected cabinets, nested safe boxes)

** they may have physically touched encrypted key material, but don’t know the activation data*

Logical set-up



More pretty pictures



Slightly more ugly pictures …

… to what it could become: Tiered Governance

Multiple stakeholders – uniform governance

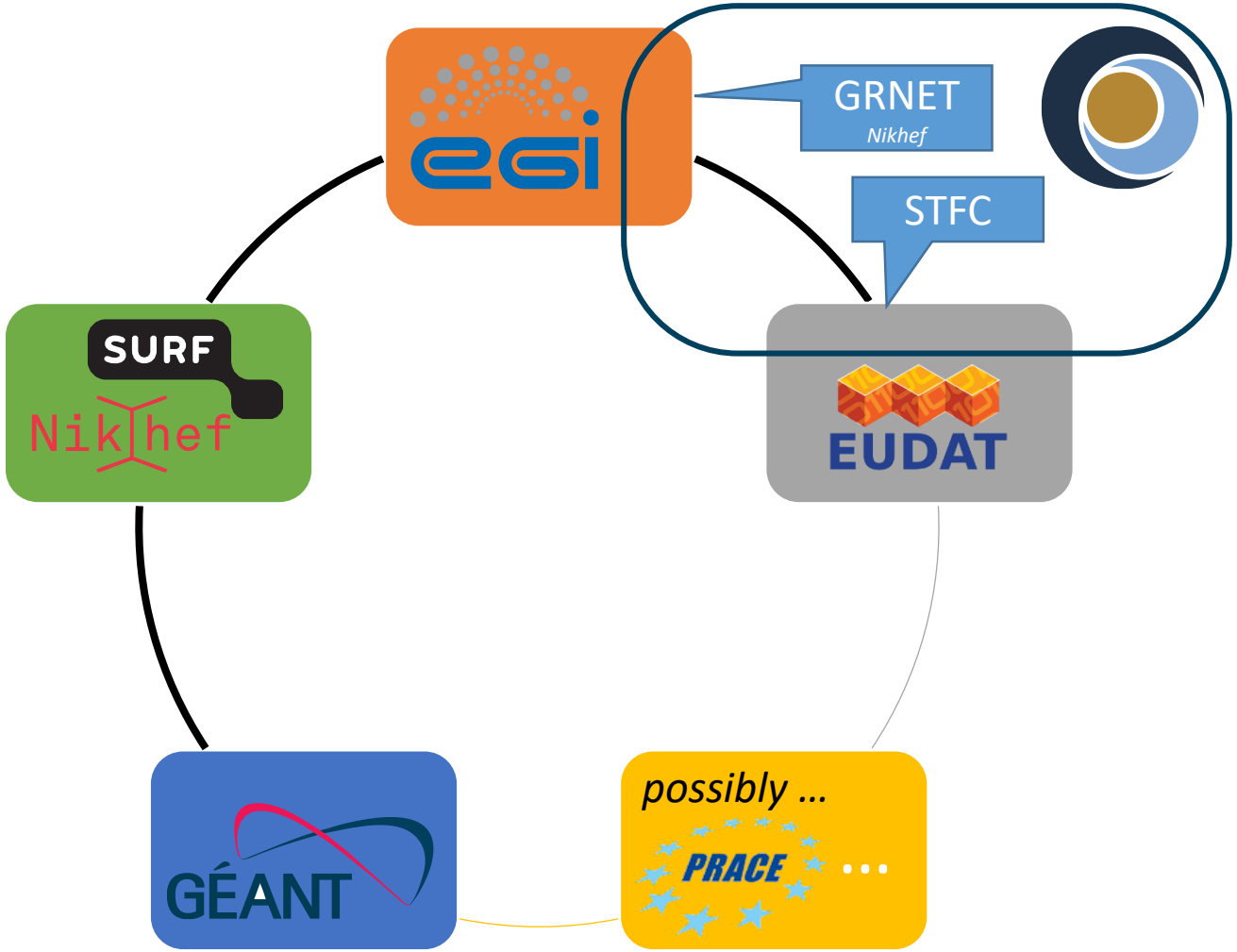
Qualified Stakeholders

- Research Infrastructures
- User Communities
- Users
- Generic e-Infrastructures
- those actively relying on RCauth.eu credentials

and that contribute (in any way) to the service

Materially Contributing Qualified Stakeholders

- are qualified stakeholders
- that contribute materially to the service
- with effort, money, hardware, or services



Considerations

Part of the operations will be funded

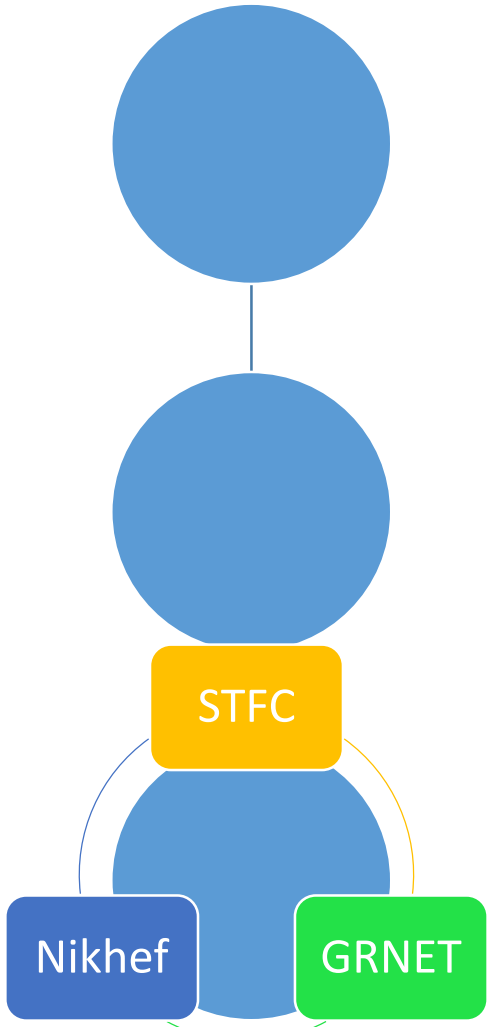
- by EOSC-HUB through its partners for the technical ops
- by SURF DNI for both support and operations
- in-kind for trusted network connectivity by GÉANT

and those who put in resources have a rightful say in where the resources go … up to a point

Core values and principles of RCauth.eu are beyond those contributing stakeholders

- must be open to anyone for any acceptable work – we don't want a fragmented community
- nobody to be 'left out of the rain' (unlike to TCS which depends on NREN policy and sign-up)
- usefulness to research and collaboration is paramount and must be the deciding factor

RCauth.eu Governance



Governance Board

Representatives (and one alternate) from each Materially Contributing Stakeholder
EGI.eu, EUDAT (ETFC), GÉANT, Nikhef (SURF)

RCauth PMA

Individuals drawn from the wide community […] experts in the field of identity management for research and collaboration, PKI technology and identity bridging

Ops Coordination Team

Operations people from each of the **hosting partners** with a (copy of) the RCauth.eu signing key, and those partners otherwise involved in OPS

What do they manage? Two options!

1. Most consistent external view – closest internal coordination and trust
   - Single RCauth.eu signing key
   - Securely distributed to each operational partner
   - Fully owned and managed by the PMA
   - Requires partners to accept stringent controls by the PMA to ensure trust
   - Fully transparent to users and external RPs

2. Most distributed and resilient view – with global user and RP impact on usability
   - Each partner gets a different RCauth.eu signing key
   - These will show up as independent ICAs in the IGTF distribution
   - Same Subject DN namespace, but different issuer names in parallel and simultaneously
   - Partners can join and leave, validity of ICA controlled through the CRL of upstream root
   - Allows PMA to control a leaving party without such party's co-operation and without special measures
   - Floods IGTF distribution with multiple ICAs, and persistently exposes CA internal to VOMS and RPs

Governance board

- ensuring continued and adequate material support for the service
- ensuring the service fulfils its mission and adheres to its principles and values
- appointing and dismissing Policy Management Authority members based on the recommendations and nominations of the Policy Management Authority
- designate and support the operational management and the operational coordination team
- liaising with Qualified Stakeholders to ensure the service meets needs of its target audience
- rule on all aspects that are not otherwise covered in the mission statement, the principle and values, this Governing Model, the CP and CPS, and that cannot be resolved by the Policy Management Authority

[It may] decide to terminate the service only by unanimous vote following a one-year consultation period with all Qualified Stakeholders, and then only in accordance with the CP and CPS policies.

PMA

- implementing the Management Guidance
- monitoring the operations of the service by the operational team(s) with respect to the Mission and the CP and CPS policies and practices
- ensuring continued accreditation of RCauth.eu to the IGTF and other relevant accreditation bodies
- informing the Governance Board about requisite changes to the CP and CPS policies and practices
- liaising with standardisation and technology groups to improve and evolve the service to further the fulfilment of its mission
- proposing new PMA members to the Governance Board

The PMA shall have at least 3 members. The members of the PMA shall exercise their duty independently and on a personal basis.

The PMA members shall be appointed or dismissed by the Governance Board, based on nomination by the current PMA membership. PMA members may step down on their own accord.

Operations Coordination Team maintains

- records of all places where trust anchor key material is maintained
- a registry of directly-connected federated identity providers, including such documentation submitted by them to assert compliance with the CP and CPS
- a registry of connected credential repository and management systems that are connected as clients to the RCauth.eu delegation service instances,
  including such documentation submitted by them to assert compliance with the CP and CPS
- any audit records maintained or prepared for assessment by the RCauth PMA
- a list of Qualified Stakeholders and contact information to the extent to which these have registered themselves to receive information from the RCauth.eu service

This team shall be responsible for the day-to-day provisioning of the service, implementing the decisions of and reporting to the Policy Management Authority, resolving issues of availability, reliability, and access to the service, and for the maintenance of any registries so-designated by the Policy Management Authority.

The most important element of trust

… I cannot yet write on a slide …

www.rcauth.eu/policy

Thank you

Any Questions?

davidg@nikhef.nl

ca@rcauth.eu

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).