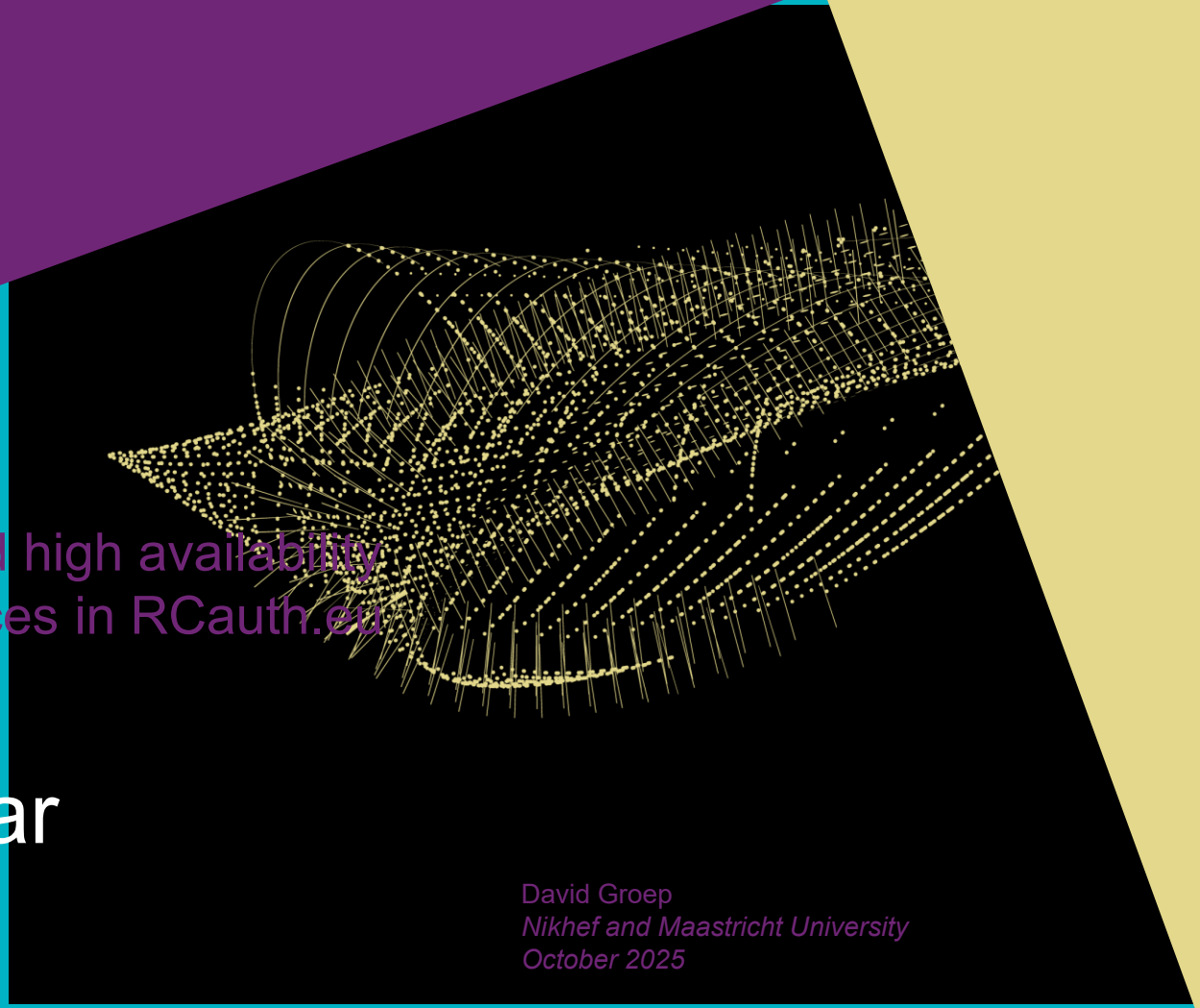
Nikhef

Maastricht University



a multi-domain anycasted high availability solution for stateful services in RCauth.eu

RCauth 10th year birthday party

David Groep
Nikhef and Maastricht University
October 2025

Remember the days … ?

AARC

Authentication and Authorisation for Research and Collaboration

RCauth.eu – a white-label IOTA CA for

On-line CA for the AARC CILogon-like TTS Pilot S

David Groep
NA3 Policy and Best Practice Coordination, AARC
Nikhef PDP Advanced Computing Research

Logo (optional)

37th EUGridPMA Plenary Meeting
May 2016

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

AARC

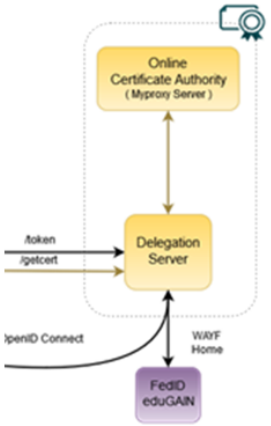
- Cover as much as R&E Federated Europe as possible
- Scoped to research and collaborative use cases
- In a scalable and sustainable deployment model

In today's AARC Pilot we

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

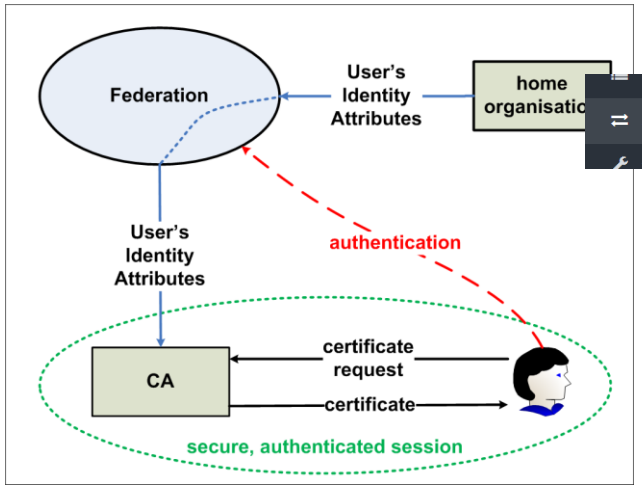
… and that can, in the subsequent phase, be:

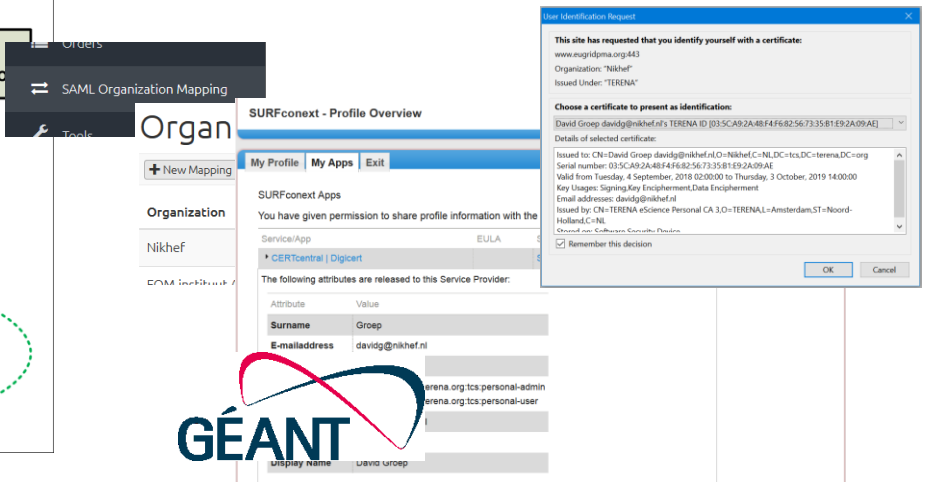
- taken up by sustained infrastructures (RIs or e-Infra's)
- replicated by the same if so preferred
- co-branded and migrated to a new managing entity



The first ‘Token Translation Service’?

GEANT Trusted Certificate Service





grnet

And the reverse: IGTF eduGAIN Bridge by GRNET

IGTF AP|EU|TAG

IGTF-to-eduGAIN Proxy

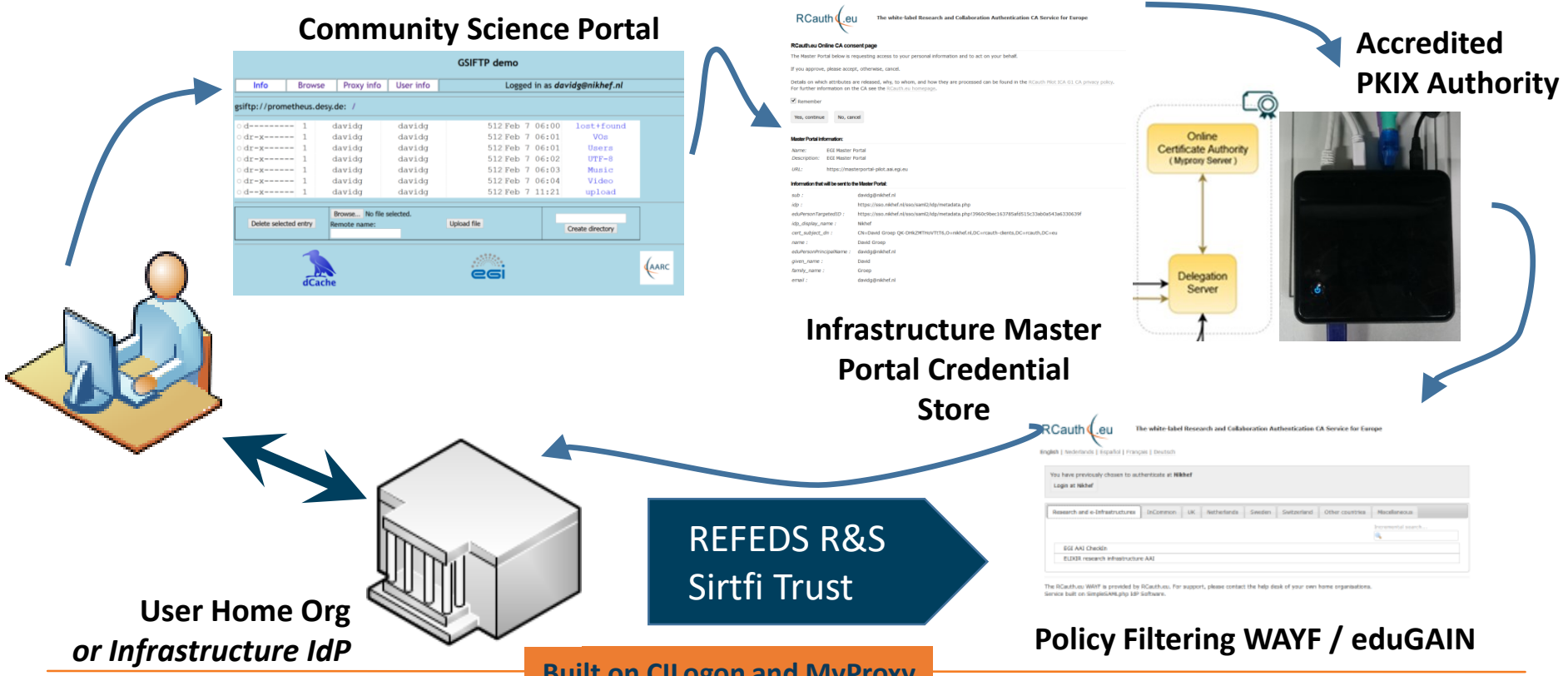
Afrikaans | Català | Čeština | Dans
Lëtzebuergesch | Lietuvių kalba |

GEANT TCS acts as SAML Service provider to eduGAIN: eligible authenticated users can obtain client certificate for access and delegation to services

https://ca.dutchgrid.nl/tcs/
https://cert-manager.com/customer/surfnet/idp/clientgeant
https://www.geant.org/Services/Trust_identity_and_security/Pages/TCS.aspx

Nikhef

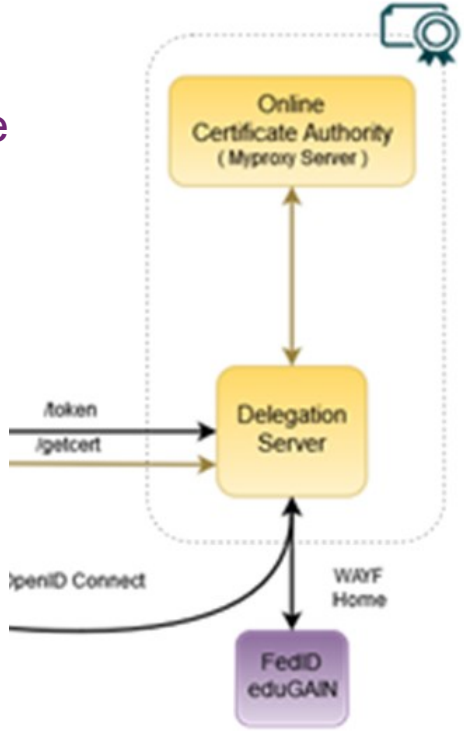
Flow for RCauth-like scenarios



Built on CILogon and MyProxy
www.cilogon.org

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



CILogon Service

Service inspired by and using components (such as the DS) from
Jim Basney's CILogon, see https://www.cilogon.org/docs/20141030-basney-cilogon.pdf

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 declaratic..
2. 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
3. within the Netherlands, SURFconext Annex IX* already ensures compliance for all IdPs

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

6. Attribute Release

Identity Providers are strongly encouraged to release the following bundle of attributes to R&S category Service Providers:

- personal identifiers: email address, person name, eduPersonPrincipalName.
- pseudonymous identifier: eduPersonTargetedID.
- affiliation: eduPersonScopedAffiliation.

Where email address refers to the mail attribute and person name refers to displayName and optionally givenName and sn (i.e., surname).

https://refeds.org/category/research-and-scholarship

REFEDS R&S section 6 – the non-reassigned identifier

The following attributes constitute a minimal subset of the R&S attribute bundle:

- eduPersonPrincipalName
- mail
- displayName OR (givenName AND sn)

For the purposes of access control, a non-reassigned persistent identifier is required. If your deployment of eduPersonPrincipalName is non-reassigned, it will suffice. Otherwise you MUST release eduPersonTargetedID (which is non-reassigned by definition) in addition to eduPersonPrincipalName. In any case, release of both identifiers is RECOMMENDED.

Sirtfi – Security Incident Response Trust framework for Federated Identity

A means by which to enable a **coordinated response to a security incident in a federated context** that does not depend on a centralised authority or governance structure to assign roles and responsibilities for doing so, but entity **organisations self-asserts**. The Sirtfi trust framework posits that organisations asserting conformance with these will coordinate their response to security incidents.

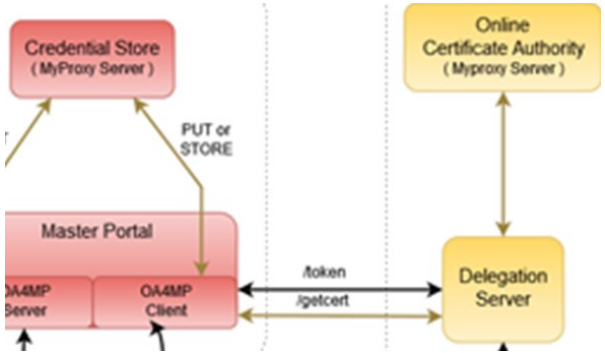
Derived from the first four elements of the SCI Framework

- **Operational Security**: patch and vulnerability management; IDS and threat mitigation; service ownership management; user suspension and termination; CSIRT capability
- **Incident Response**: CSIRT contact in meta-data; timely response; **collaborate** in IR; defined processes; privacy respect; TLP information sharing
- **Traceability**: timestamped accurate logs are available; log retention process in place
- **Participant Responsibilities**: users agree to an AUP; awareness and acceptance of the AUP

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*

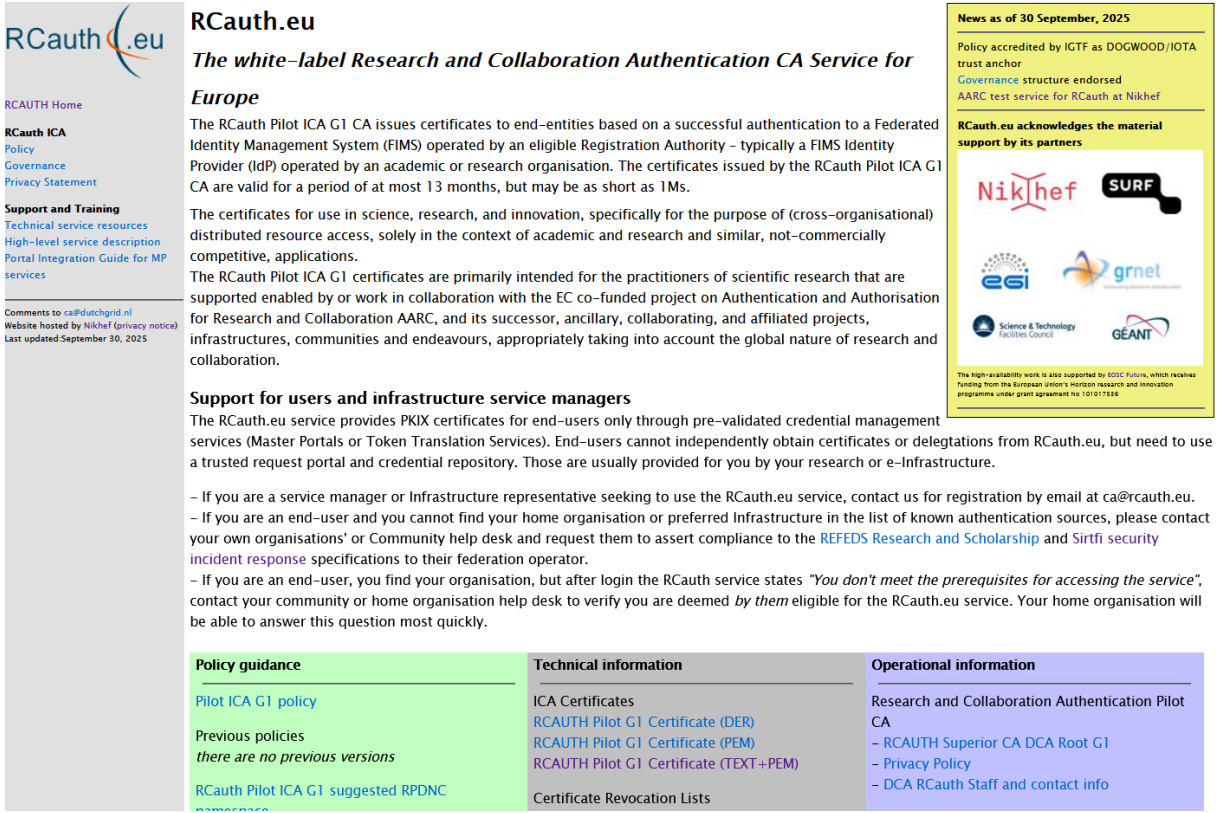
The basics for any Certification Authority: Policy and Practice Statement in RFC 3647 format

https://www.rcauth.eu/

- CP/CPS document
- CA certs, link to superior (“DCA Root”) CA
- CRL – issued daily for a period of 30 days (and after each revocation)

- Supplementary policy documents (links to SURFnet contract Annex IX, eduGAIN, R&S, Sirtfi)

- Sign-up form (unilateral) for explicit IdPs
  – but the fact that you can sign up does not mean you’ll be accepted…



RCauth.eu

RCAUTH Home

RCauth ICA
Policy
Governance
Privacy Statement

Support and Training
Technical service resources
High-level service description
Portal Integration Guide for MP services

Comments to ca@dutchgrid.nl
Website hosted by Nikhef (privacy notice)
Last updated:September 30, 2025

RCauth.eu

The white-label Research and Collaboration Authentication CA Service for Europe

The RCauth Pilot ICA G1 CA issues certificates to end-entities based on a successful authentication to a Federated Identity Management System (FIMS) operated by an eligible Registration Authority - typically a FIMS Identity Provider (IdP) operated by an academic or research organisation. The certificates issued by the RCauth Pilot ICA G1 CA are valid for a period of at most 13 months, but may be as short as 1Ms.

The certificates for use in science, research, and innovation, specifically for the purpose of (cross-organisational) distributed resource access, solely in the context of academic and research and similar, not-commercially competitive, applications.
The RCauth Pilot ICA G1 certificates are primarily intended for the practitioners of scientific research that are supported enabled by or work in collaboration with the EC co-funded project on Authentication and Authorisation for Research and Collaboration AARC, and its successor, ancillary, collaborating, and affiliated projects, infrastructures, communities and endeavours, appropriately taking into account the global nature of research and collaboration.

News as of 30 September, 2025

Policy accredited by IGTF as DOGWOOD/IOTA trust anchor
Governance structure endorsed
AARC test service for RCauth at Nikhef

RCauth.eu acknowledges the material support by its partners

The high-availability work is also supported by EOSC Future, which receives funding from the European Union's Horizon research and innovation programme under grant agreement No 101017536

Support for users and infrastructure service managers

The RCauth.eu service provides PKIX certificates for end-users only through pre-validated credential management services (Master Portals or Token Translation Services). End-users cannot independently obtain certificates or delegtations from RCauth.eu, but need to use a trusted request portal and credential repository. Those are usually provided for you by your research or e-Infrastructure.

- If you are a service manager or Infrastructure representative seeking to use the RCauth.eu service, contact us for registration by email at ca@rcauth.eu.
- If you are an end-user and you cannot find your home organisation or preferred Infrastructure in the list of known authentication sources, please contact your own organisations' or Community help desk and request them to assert compliance to the REFEDS Research and Scholarship and Sirtfi security incident response specifications to their federation operator.
- If you are an end-user, you find your organisation, but after login the RCauth service states *"You don't meet the prerequisites for accessing the service"*, contact your community or home organisation help desk to verify you are deemed *by them* eligible for the RCauth.eu service. Your home organisation will be able to answer this question most quickly.

Policy guidance	Technical information	Operational information
Pilot ICA G1 policy	ICA Certificates	Research and Collaboration Authentication Pilot CA
Previous policies *there are no previous versions*	RCAUTH Pilot G1 Certificate (DER) RCAUTH Pilot G1 Certificate (PEM) RCAUTH Pilot G1 Certificate (TEXT+PEM)	- RCAUTH Superior CA DCA Root G1 - Privacy Policy - DCA RCauth Staff and contact info
RCauth Pilot ICA G1 suggested RPDNC namespace	Certificate Revocation Lists	

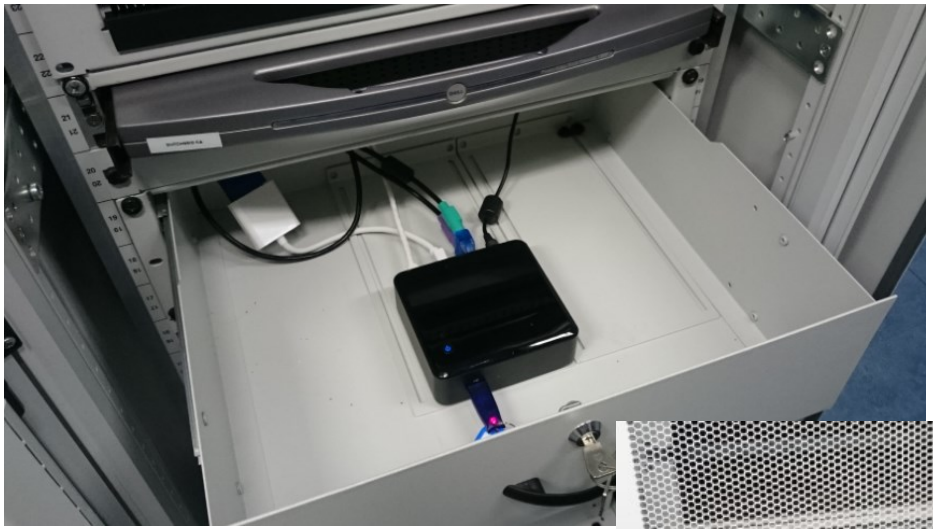
The AARC Pilot started on Feb 1st, 2016 …

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            09:f5:d7:56:8e:89:e8:87:d8:16:53:fe:ab:c7:84:e2
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=nl, DC=dutchgrid, O=Certification Authorities,
            CN=DCA Root G1 CA
        Validity
            Not Before: Feb  1 00:00:00 2016 GMT
            Not After : Jan 31 23:59:59 2026 GMT
        Subject: DC=eu, DC=rcauth, O=Certification Authorities,
            CN=Research and Collaboration Authentication Pilot G1 CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

Physical controls

- Located at Nikhef, Amsterdam, NL
- Nikhef-specific part of the DC Housing Facilities
- Room capacity 400kW, total ~ 2MW, 2N+ no-break
- ID based access control, 24hr guard on-site, 2nd floor (above see-level)
- CA and security systems in locked dedicated cabinet.
  On-line CA signing system in locked drawer

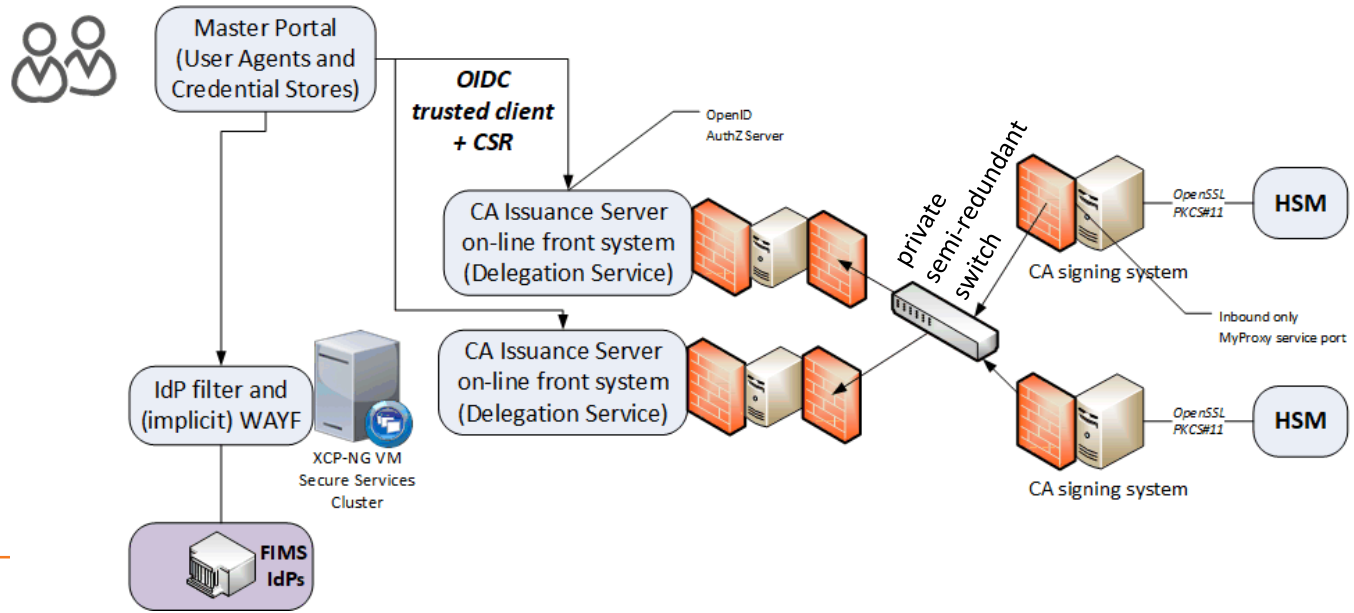
More pretty pictures



Slightly more ugly pictures …

A local highly-available setup at Nikhef Amsterdam

- Most ‘fault-prone’ components are
  - Intel NUC (single power supply)
  - HSM (can lock itself down, and the USB connection is prone to oxidation)
  - DS front-end servers (they are physical hardware, albeit with redundant disks and powersupplies)
- Eliminated first using ‘local HA’



Meeting the world: from naming to addressing …

Name uniqueness [3.1]

- Federations, with their distributed responsibility model, always face a consistency challenge
  - Release of any identifier associated with a individual person (‘privacy concerns’)
  - Guaranteeing non-reassignment of an identifier - has not played a major role *inside* any single org till now
  - Agreeing on how to name the name (attribute) of the authenticated user is different

- We have to rely on the RAs (institutions) to provide an identifier that we can use - **even if** the institution itself does not consider RCauth.eu *on its own* worthy of specific attention

We can leverage grander schemes and agreements

- eduPerson schema – almost all federations use this, and most require specs compliance
- REFEDS Research and Scholarship (“R&S”) specification – aligns attribute release (and federation registrars check for minimal compliance
- Sirtfi – new standard to harmonize incident response and opsec capabilities and processes

But straightforward translation is not always good

So the (for now) best combination seems to be the ordered transformation:

```
Transliterator.getInstance( "Russian-Latin/BGN;"+
        "Serbian-Latin/BGN;"+
        "Greek-Latin/UNGEGN;"+
        "[:Nonspacing Mark:] remove;"+
        "Any-Latin/BGN;“ +
        "Any-Latin;“ +
        "Latin-Ascii“
);
result.replaceAll("[^\\p{Lower}\\p{Upper}\\p{Digit} '()+,-.?@]",  "X");
```

⟸ *ordering to retain “ɯ” → “sh”*

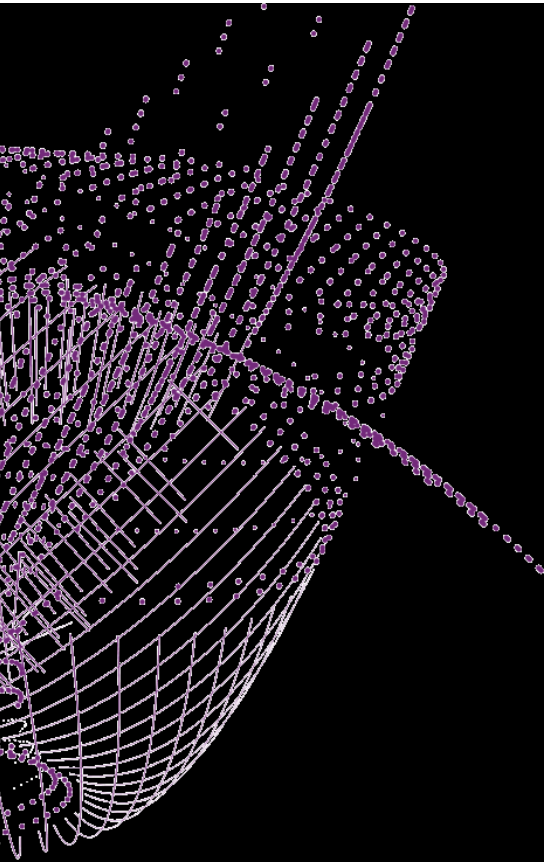
⟸ *Fixes greek Λ adding a useless space*

⟸ *Retain proper “sh” when coming from Armenian or Hebrew by /BGN first*

What will we get?

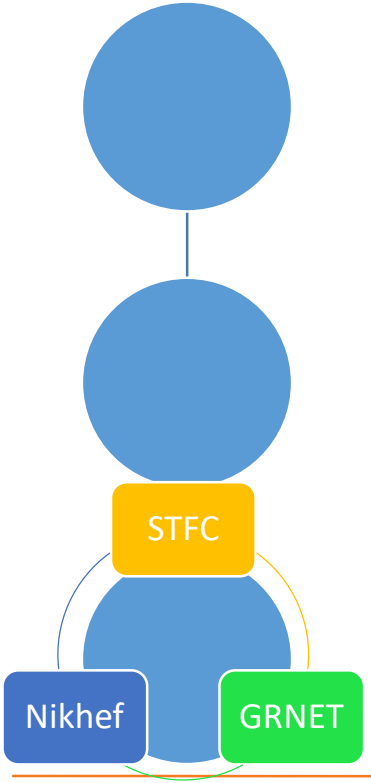

```
$ java -cp icu4j-59_1.jar:. transliterate2 [...]
 "Jőzsi Bácsi" "Guðrún Ósvífursdóttir" \
 "Χρηστος Κανελλοπουλος" "簡禎儀"
```

```
Input:   Jőzsi Bácsi
Output:  Jozsi Bacsi
Input:   Guðrún Ósvífursdóttir
Output:  Gudrun Osvifursdottir
Input:   Χρηστος Κανελλοπουλος
Output:  Christos Kanellopoulos
Input:   簡禎儀
Output:  jian zhen yi
```



The RCauth pan-European distributed service

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

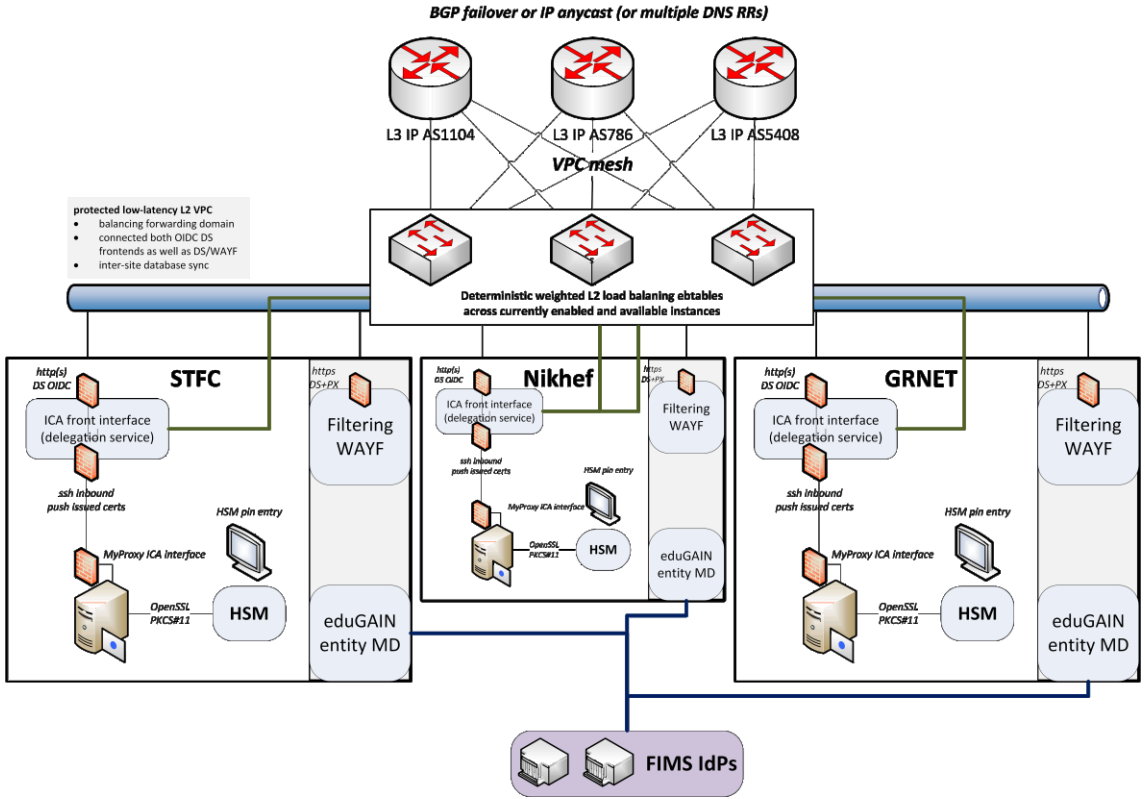
Ops Coordination Team

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

Since we do not like SPOFs

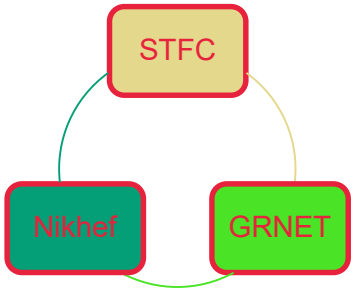
Implement a High Availability setup

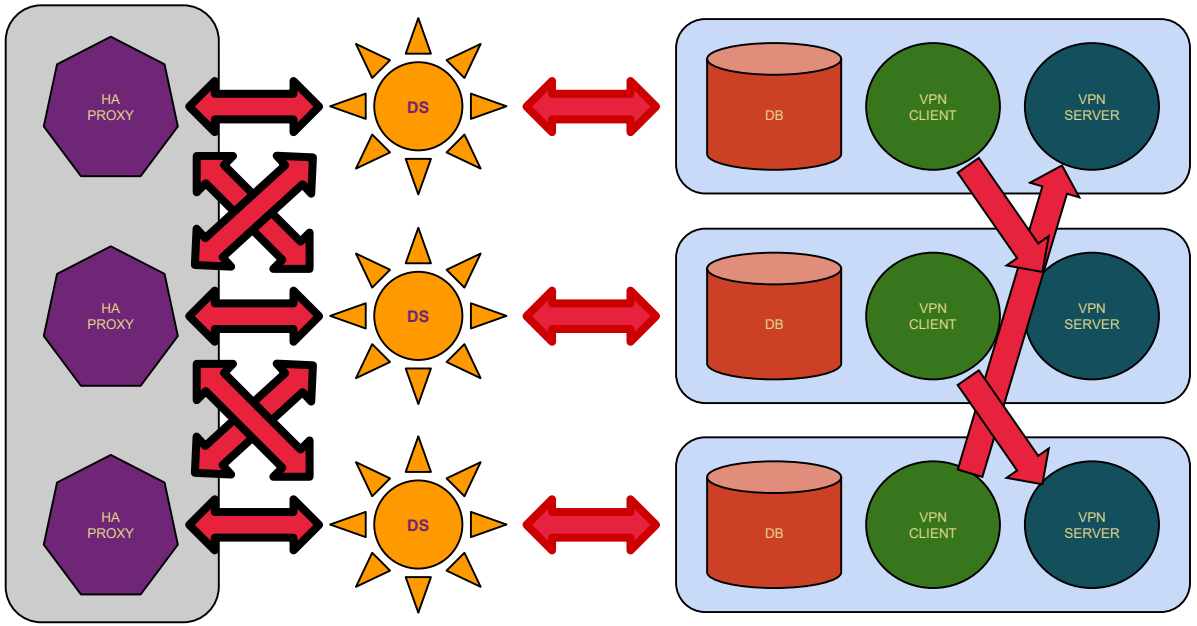
- across the 3 sites
- using IP anycast
- L3 VPN or L2 VPC
- with minimal effort



work supported by EOSC Hub and EOSC Future

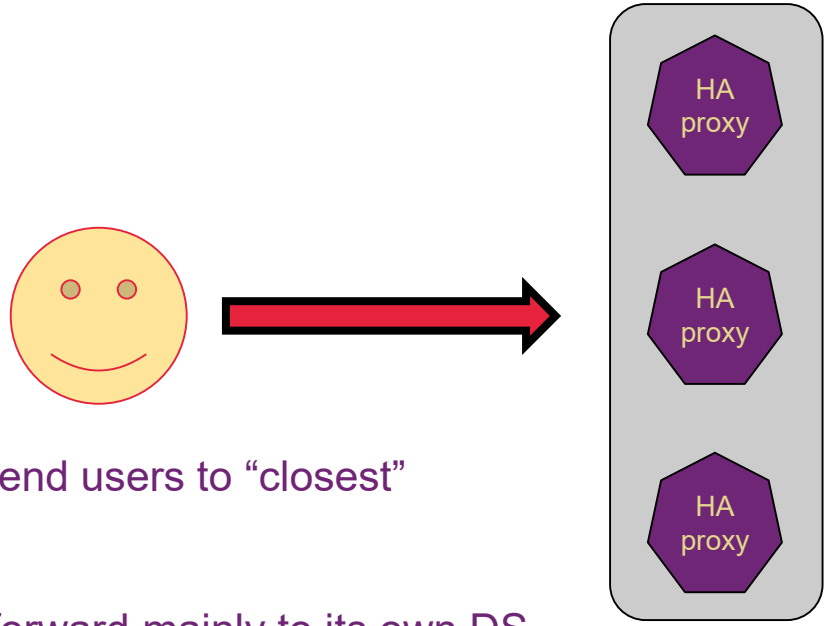
Distributed RCauth service





selected imagery: Mischa Sallé, Jens Jensen, Nicolas Liampotis

A transparent multi-site setup



Need a way to send users to “closest” working service

Each HA proxy forward mainly to its own DS

If a HA loses its backend DS, it can still route to the other DS’es

selected imagery: Mischa Sallé, Jens Jensen, Nicolas Liampotis

CERN Looking Glass Results - ee1

Date: Wed Oct 12 13:41:55 2022 CEST

Query:
Argument(s): 2a07:8504:1a0::/48

```
inet6.0: 155476 destinations, 303862 routes (155437 active, 0 holddown, 234 hidden)
+ = Active Route, - = Last Active, * = Both

2a07:8504:1a0::/48 *[BGP/170] 01:08:50, MED 20, localpref 10500
                     AS path: 20965 5408 I, validation-state: unverified
                   >  to 2001:798:99:1::39 via irb.200
                   [BGP/170] 4d 23:13:16, MED 20, localpref 10500, from 2001:1458:0:5::1
                     AS path: 1103 1104 I, validation-state: unverified
                   >  to fe80::1a2a:d300:140f:bdb0 via irb.20
                   [BGP/170] 6d 23:17:01, MED 20, localpref 10500
                     AS path: 2603 1103 1104 I, validation-state: unverified
                   >  to 2001:1458:0:9::2 via irb.2903
                   [BGP/170] 01:08:26, MED 25, localpref 10500
                     AS path: 559 20965 5408 I, validation-state: unverified
                   >  to 2001:1458:0:2c::2 via irb.2902
                   [BGP/170] 01:08:49, MED 10, localpref 10200
                     AS path: 174 174 21320 5408 I, validation-state: unverified
                   >  to 2001:978:2:2::2a:1 via irb.3811
```

2a07:8504:1a0::/48

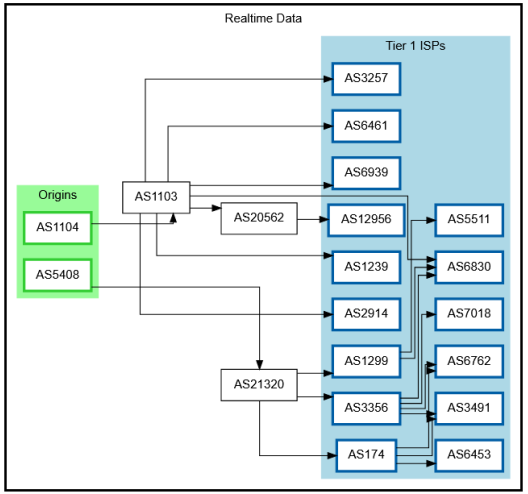
Announced by **AS1104, and 1 other**

Overview | Connectivity | Whois | DNS | Validation

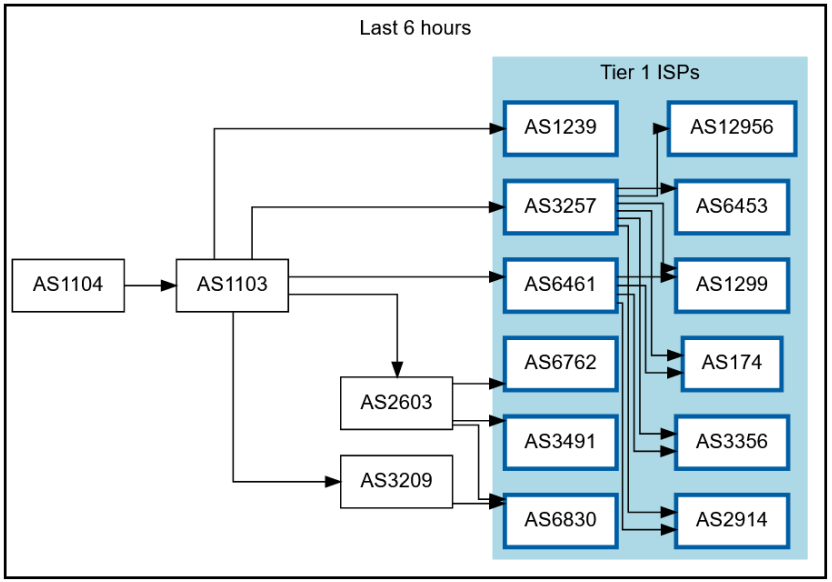
Originators

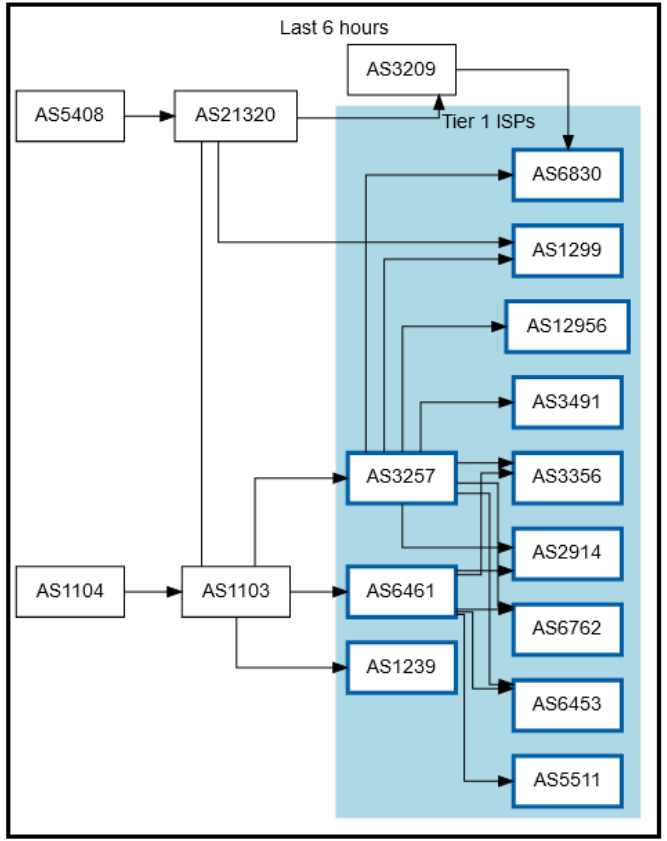
	ASN	Description
	AS1104	Nikhef - Dutch National Institute for Sub-atomic Physics
	AS5408	National Infrastructures for Research and Technology S.A.

How can a prefix have multiple ASNs?



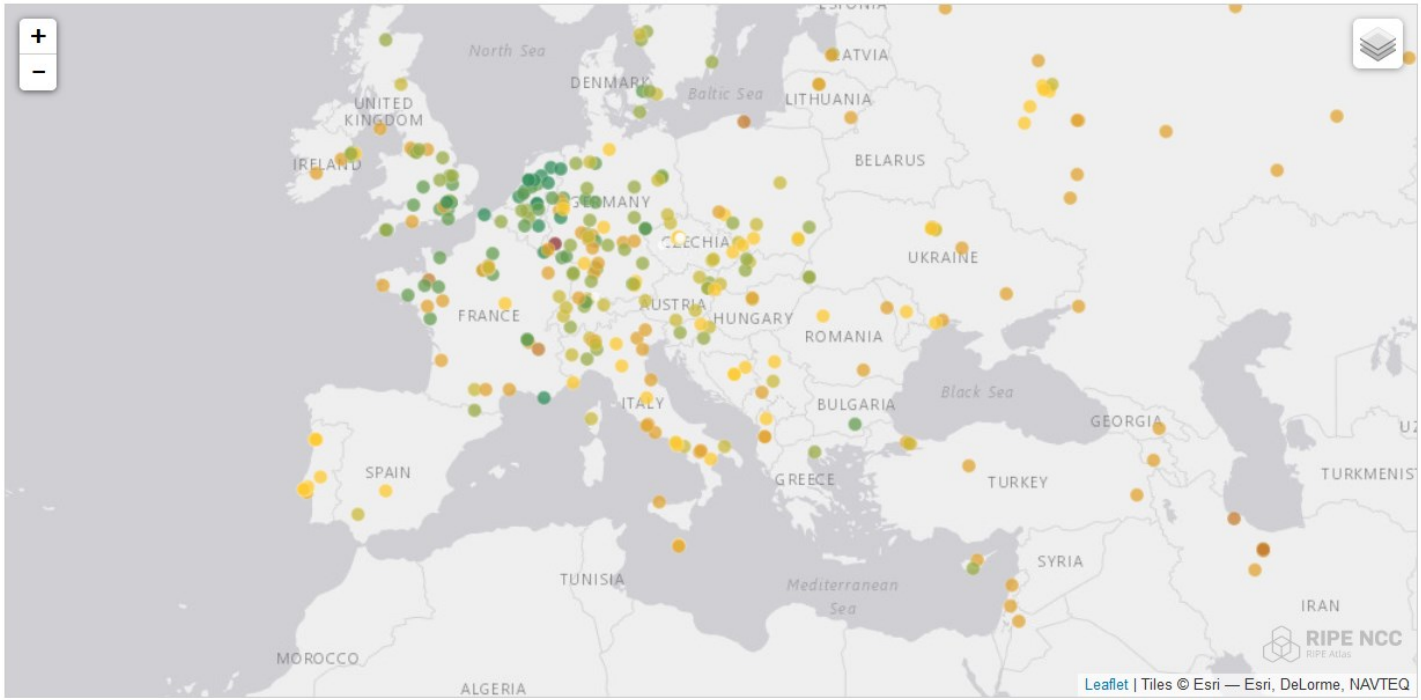
Getting 145.116.216.0/24 out there





route maps: bgp.tools for 145.116.216.0/24 – IPv6 would be similar

And you get reasonable load balancing



map: RIPE NCC RIPE Atlas- 500 probes, zoomed in on Europe

Current status

- All sites can sign production certificates
- DS databases cross-site replication using Galera over OpenVPN
- HA CRL cross site synchronisation and issuance
- WAYF servers (GRNET and Nikhef)

Reusing the RCauth experience!

HA distributed web service with HA database backend

- HA database
  - 3x node peer-peer redundant VPN: automatic failover
  - In principle extensible to >3 but what topology?
  - Galera cluster well known, MySQL/MariaDB has both advantages and drawbacks
- Web service
  - 3x HAproxy: stability and flexibility
- HAHAP | BGP Anycast: ‘bog-standard’ if service admins, cloud admins, and network people can collaborate and investigate incidents together

Credential issuance and moving shared secrets is still cumbersome in practice

- The difference between theory and practice is that, in theory, there is no difference

The journey is not over jus ye

- While RCauth use today is limited, technology and experience lives on
  - anycasted stateful services,
  - token translation and assurance alignment

- and still used, also for teaching, so it makes sense to keep it around

```
** CA RCauth-Pilot-ICA-G1 v1.137 (RCauth-Pilot-ICA-G1 in ..//EUGridPMA/NIKHEF)
WARNING: ..//EUGridPMA/NIKHEF/RCauth-Pilot-ICA-G1.0:
         certificate for RCauth-Pilot-ICA-G1 will expire within 180 days
         on: Jan 31 23:59:59 2026 GMT
```

Re-issuance based on same key, new serial

```
Data:
    Serial Number:
        05:77:6b:ba:ff:bf:1e:86:a4:6a:ca:a5:d9:60:8b:98
Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC=nl, DC=dutchgrid, O=Certification Authorities,
        CN=DCA Root G1 CA
    Validity
        Not Before: Feb  1 00:00:00 2016 GMT
        Not After : Jan 31 23:59:59 2036 GMT
    Subject: DC=eu, DC=rcauth, O=Certification Authorities,
        CN=Research and Collaboration Authentication Pilot G1 CA
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:b7:a3:91:cb:e3:2a:19:c5:f7:8f:0f:a0:e2:44:
```

Plan

- Update the certificate in the validator and master portals
- distribute in 1.138 release (November 2025)
- Keep the service and technology running, and
  … re-use expertise for new services!

This work has also been co-supported by projects that have received funding from the European Union's Horizon research and innovation programmes under Grant Agreement No. 856726 (GN4-3), 101017536 (EOSC Future), 777536 (EOSC-hub), 730941 (AARC2).

Still here? Thanks!

RCauth.eu distributed setup in collaboration with Mischa Sallé and Tristan Suerink (Nikhef), Nicolas Liampotis and Kyriakos Gkinis (GRNET), and Jens Jensen (STFC RAL)

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606

Maastricht University

Nikhef