Nikhef

Maastricht University

Trust and Identity – the AARC way

Can I have eduGAIN without pain, please?

David Groep,
Nikhef Jamboree,
May 2024

Remember the times? …

Our state of DataGrid and the HEP LHC computing in ~ 2000

NIKHEF
NATIONAAL INSTITUUT VOOR KERNFYSICA EN HOGE-ENERGIEFYSICA

Guest / students form (pleas

1. This form is completed in connection with:
☐ work experien
☐ otherwise, via

CERN/User Registration

CERN COMPUTER CENTRE - US

http://cern.ch/it/documents/ComputerUsage/Comp

To be returned to the User Registration box at the en
completed by a user who requires a computer accou
Department, and is not yet registered in another grou

To be completed by the User :

It is MANDATORY to provide the following infor
treated confidentially and only be used for ensuring
Supply name as registered by the Users' Off
FAMILY NAME(S): ……
FIRST NAME(S) : ……
SEX [M] [F] BIRTHDATE: Day …..… Month …… Year ……
HOME INSTITUTE/FIRM: ……
NATIONALITY: ……..*CERN SUPERVISOR……
*CERN DEPARTMENT: . . . . . *CERN ID NUMBER (as on CERN card)……..

To be completed by the Group Administrator:

Fermilab

For Office Use Only

ID:	Action:	ID Exp:	
Insurance:	Medical:	Safety:	
Computer:	Stkrm:	Family:	
NON-473:	Sensitive:	Verifier:	Date:

Name:

SWIETZER	JOHN	JAMES
Last	First	Middle

University or Institution Name:	Telephone:
FLORIDA STATE UNIVERSITY	850-644-XXXX

Experiment/Department:

Exp. / Dept.	Spokesperson	Home Institution Contact	Contact Telephone
D0	WOMERSLEY/WEERTS	SHARON HAGOPIAN	850-644-4777

Authentication – who are you

Authenticating to a single service is relatively simple

- per-service username and secrets (e.g. password and/or one-time ‘6 digit’ code)
- server-side: list of valid users and (hashed and hopefully salted) secrets

```
[root@kwark ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

```
root:$6$s8ciAG5gLuv2bPQS$6EcskgtKvQ.rHbif
davidg:$6$nDYcIez2Uaufbtlg$RlhS/Qjn0qYQZk
marianne:$6$p3CeevG6jfNDqZj1$HKHqUTnt2fEqQfkA/m5J3oAOA0zSvgLCKOSQhPS
```

Passport image: cropped from original by Jon Tyson on Unsplash https://unsplash.com/photos/Hid-yhommOg

Access control in a single domain

Without **AAI,**
Authentication & Authorization Infrastructure
is dedicated to each service you want to access

- account linked directly to service authorization
- *sometimes even*
  different accounts for different roles

In a multi-organizational system becomes

$$\mathcal{O}(n_{sites} * n_{services}) * \mathcal{O}(n_{users})$$

Image: AARC NA2 training module “Authentication and Authorisation 101” - https://aarc-community.org/training/aai-101/

Authentication and Authorization Infrastructure

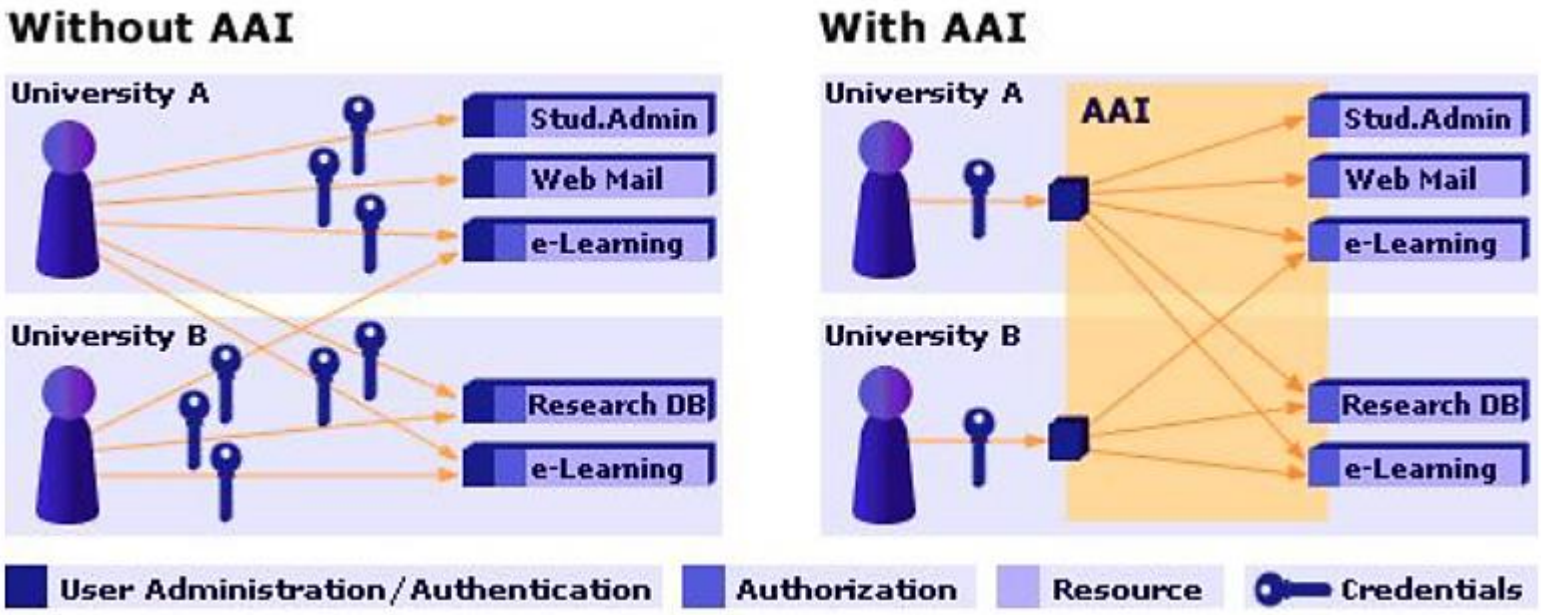
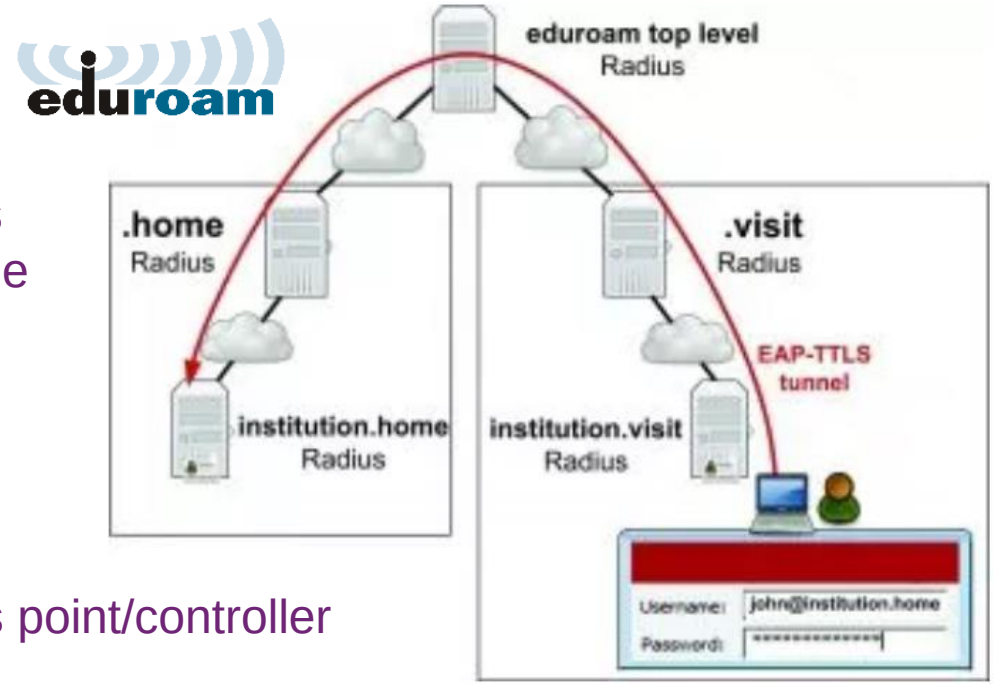


Image: AARC NA2 training module “Authentication and Authorisation 101” - https://aarc-community.org/training/aai-101/

One simple federation you know: eduroam

Service-specific “WiFi” trust
between organisations globally

- hierarchichy of authorization servers
- based on secure credential exchange
- tunneling your credentials
  back to your home institution



Local server then instructs WiFi access point/controller

eduroam: Klaas Wieringa et al., image from https://eduroam.org/how/, GEANT ; RADIUS: RC2865 https://www.rfc-editor.org/rfc/rfc2865; see also freeradius.org

But what can you do? How should a service decide?

Since you're (probably) not omnipotent … you need *authorization: a statement that the service recognises*

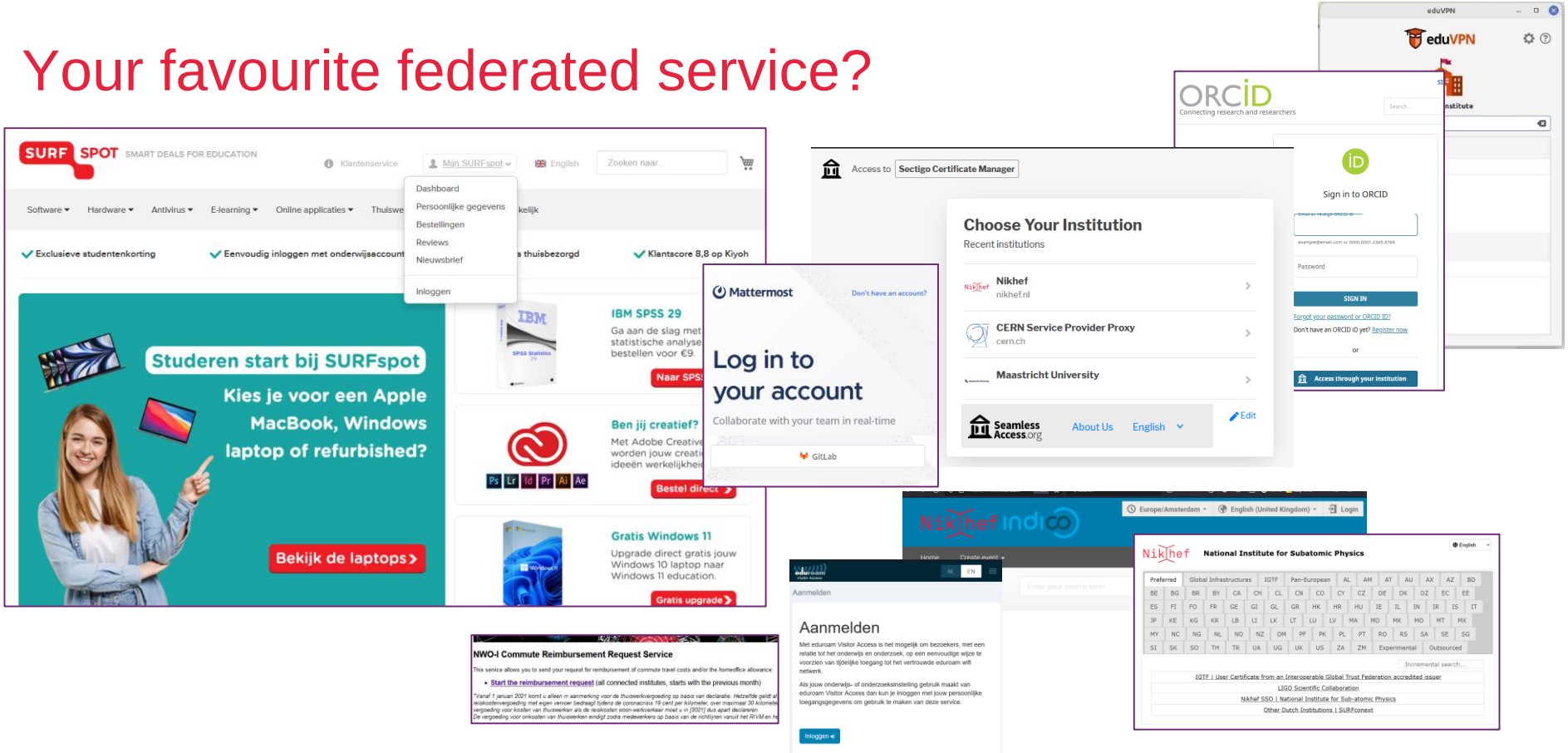
- bound to an verifiable identity statement
  e.g. visa are strongly linked to a specific entity, and asserted by a trusted party (by the service)

- be a bearer token
  scoped to a relying party, a service, or an action

- self-asserted
  quite useless unless backed by *verifiable evidence*, like in self-sovereign identity schemes

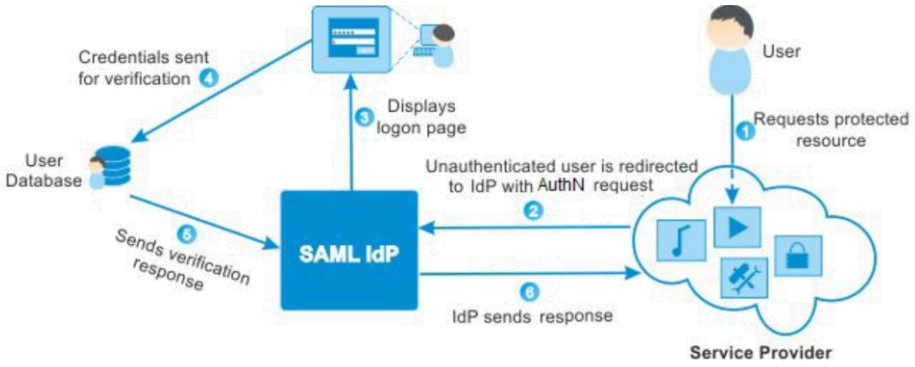
visa image source: dcgreer on flickr, CC-BY-NC-ND, https://www.flickr.com/photos/dcgreer/6562844777; RATP bearer token, issued for the Paris public transport system; self-managed identity image: Windows Cardspace , Kim Cameron, Mike Jones, et al. image from WikiMedia, Used with permission from Microsoft.(https://en.wikipedia.org/wiki/File:Cardspace_identity_selector.png)

Your favourite federated service?



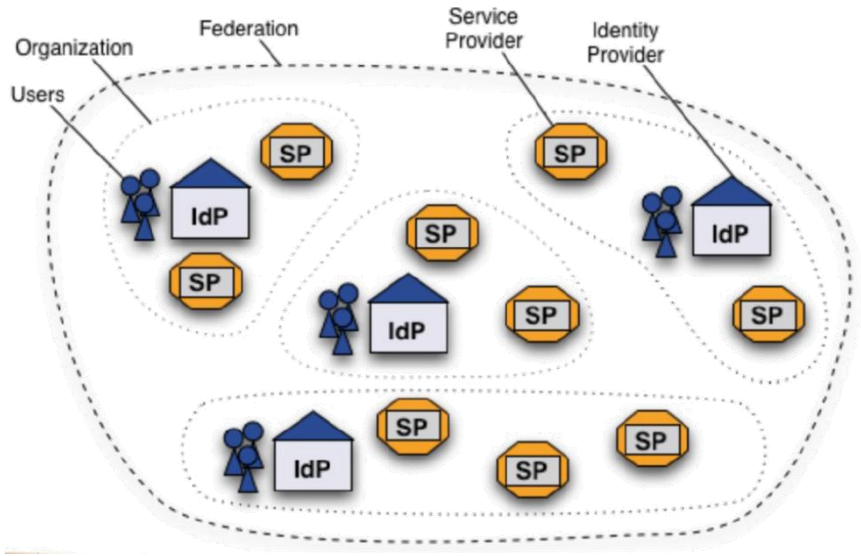
https://surfspot.nl/ - see also https://kb.nikhef.nl/ct for inspiration on more federated services available to you

Federation and the ‘SAML dance’ – web-based services



SAML2.0 auth flow

‘portability of identity across administrative domains’



Shibboleth IdP image and SAML2 auth flow by SWITCH (CH) – see also https://refeds.org/ on federation structure and (assurance and security) guidelines

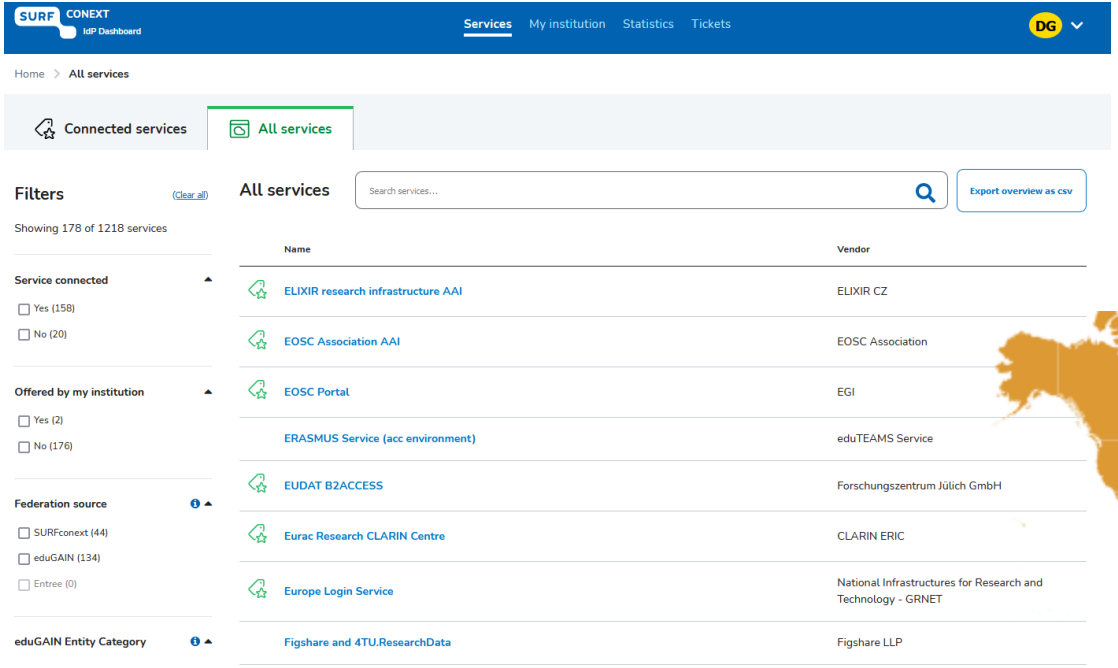
Under the hood, this is a (signed) XML document

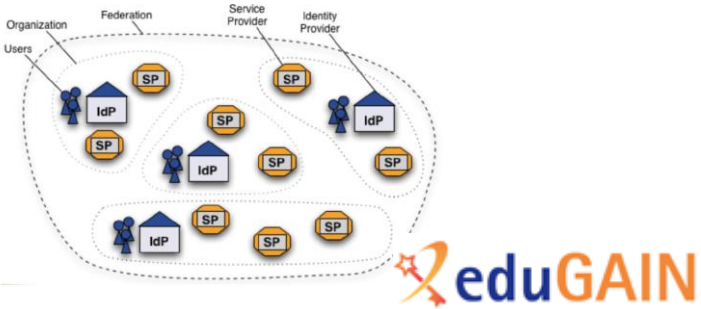
```
<saml:Subject>
     <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</saml:NameID>
     <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
       <saml:SubjectConfirmationData NotOnOrAfter="2022-10-21T18:16:40Z"
         Recipient="https://attribute-viewer.aai.switch.ch/Shibboleth.sso/SAML2/POST"
         InResponseTo="_64c10a60c382bdaeb328653d9d25951c" /></saml:SubjectConfirmation>
   </saml:Subject>
   <saml:Conditions NotBefore="2022-10-21T18:11:39Z"
                    NotOnOrAfter="2022-10-21T18:16:40Z">
     <saml:AudienceRestriction>
       <saml:Audience>https://attribute-viewer.aai.switch.
     </saml:AudienceRestriction>
   </saml:Conditions>
   <saml:AuthnStatement AuthnInstant="2022-10-21T17:33:29Z
                        SessionNotOnOrAfter="2022-10-22T02
                        SessionIndex="_90f745f18f712b6a567
    <saml:AuthnContext>
        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAMI
        <saml:AuthenticatingAuthority>https://sso.nikhef.r
    </saml:AuthnContext>
   </saml:AuthnStatement>
```

```
<saml:AttributeStatement>
      <saml:Attribute Name="urn:mace:dir:attribute-def:cn"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xsi:type="xs:string">David Groep</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="urn:oid:2.5.4.3"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xsi:type="xs:string">David Groep</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="urn:mace:dir:attribute-def:eduPersonAffiliation"
                      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xsi:type="xs:string">employee</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">member</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">faculty</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
      ...
```

Nikhef SSO
Try the **SAML-tracer for Firefox** by Jaime, Thijs and Jan:
https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/

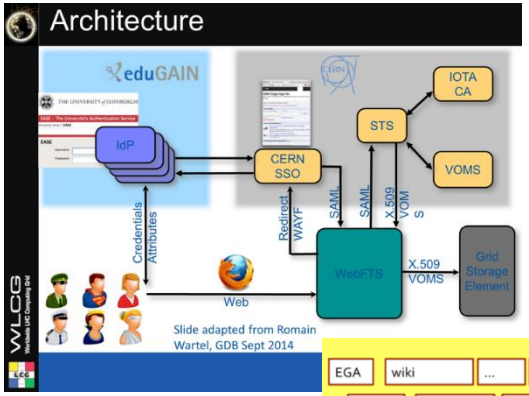
SURFconext & eduGAIN – we only solved half the issues …





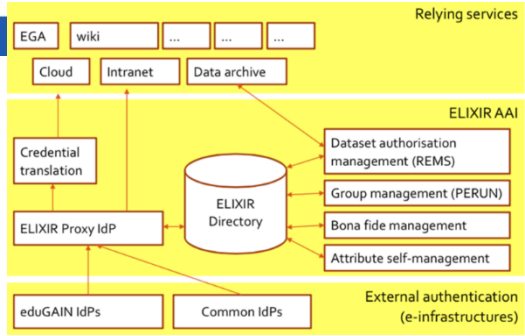
Images: SURFconext IdP dashboard by SURF, showing some services tagged with REFEDS R&S; eduGAIN map: GEANT, https://technical.edugain.org/status

AARC: managing complexities of federated communities

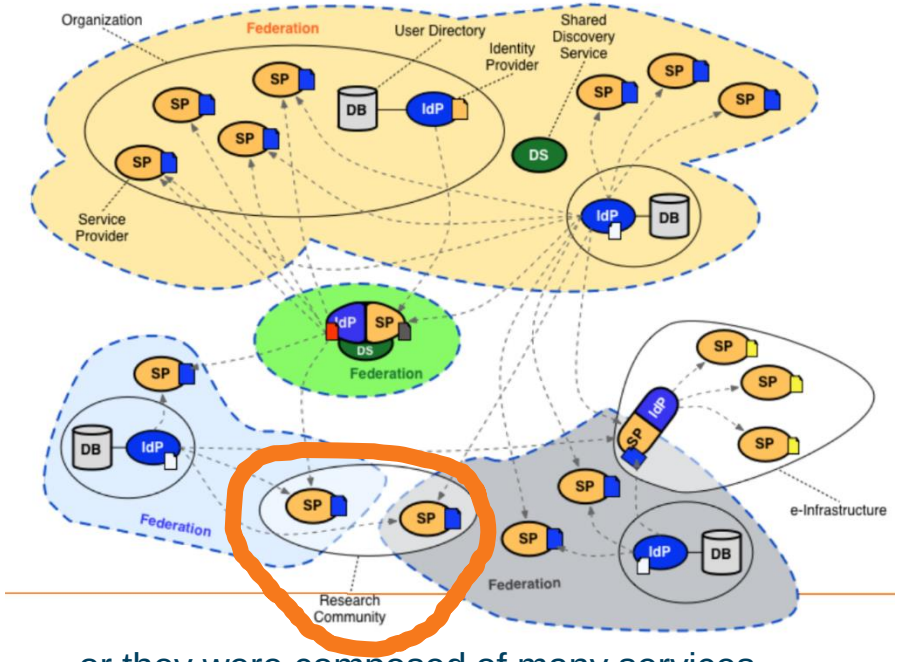


WebFTS prototype 'FIM4R' in wLCG Romain Wartel et al.

ELIXIR reference architecture 2016 Mikael Linden et al.



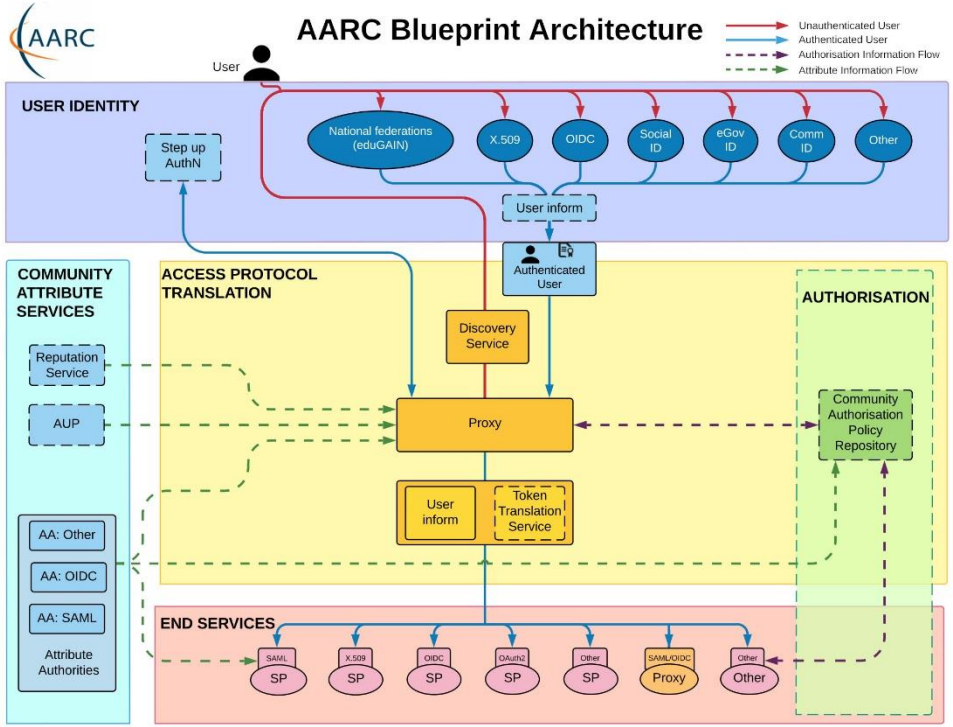
communities had either invented their own 'proxy' model to abstract complexity

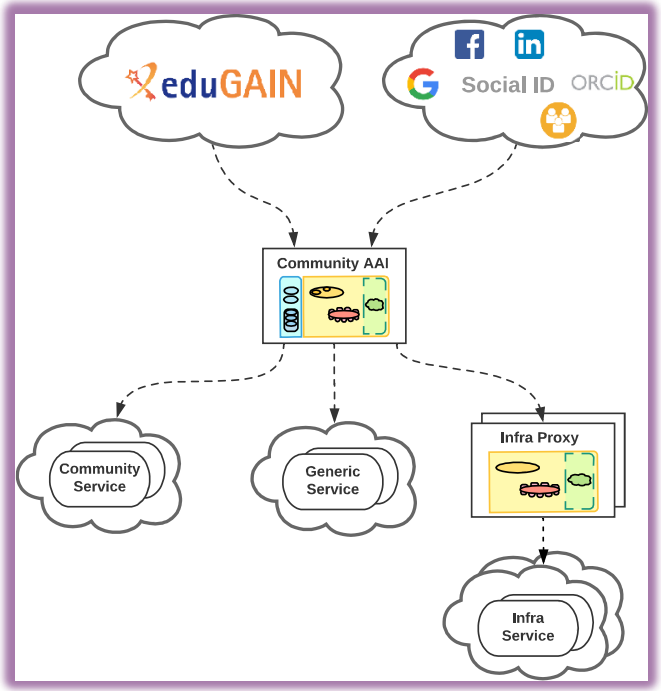


or they were composed of many services each of which had to manage federation complexity

Community images: Romain Wartel, CERN; Mikael Linden, CSC; Lukas Hammerle, SWITCH

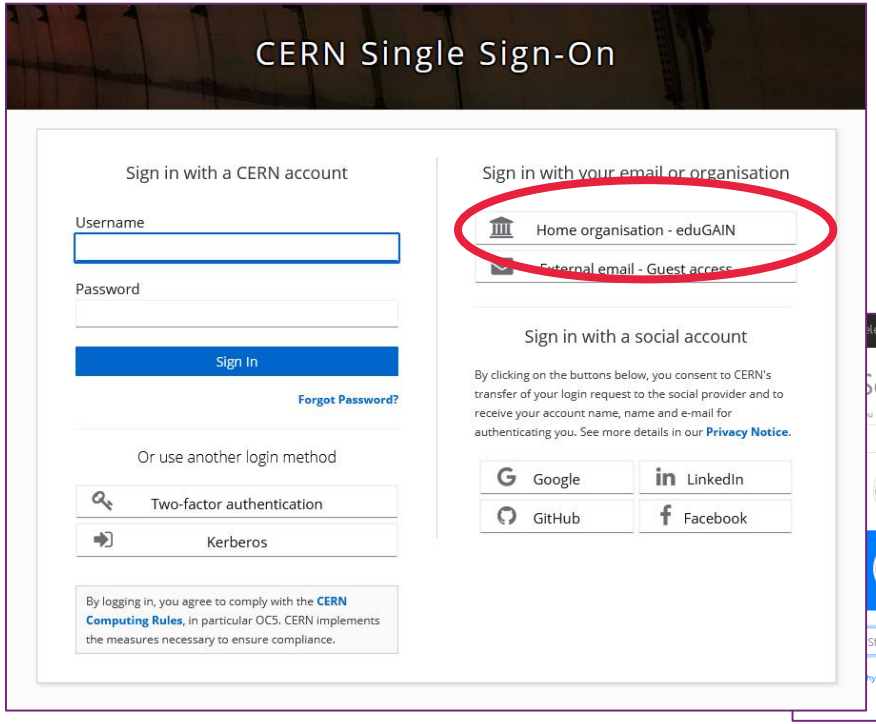
Most trust flows from the (research) community





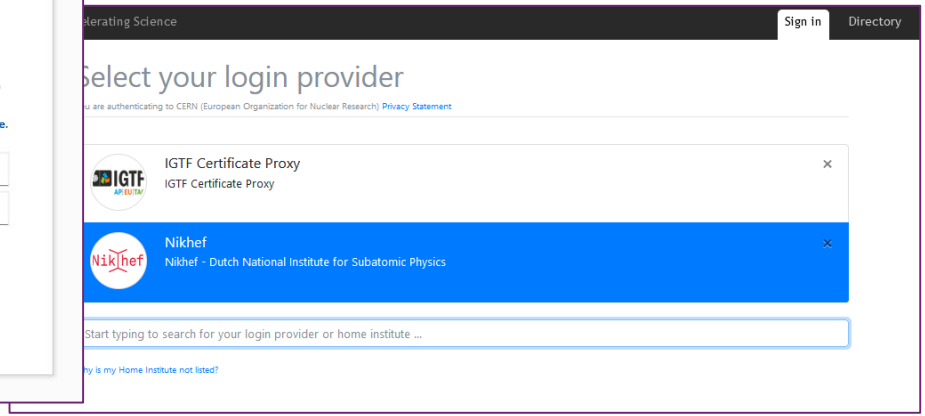
AARC Blueprint Architecture (2019) AARC-G045 https://aarc-community.org/guidelines/aarc-g045/;
stacked proxies: EOSC AAI Architecture: EOSC Authentication and Authorization Infrastructure (AAI), ISBN 978-92-76-28113-9, http://doi.org/10.2777/8702

New CERN single sign-on



Having done ***account linking*** at CERN, you can use your Nikhef or university home identity without having to login again.

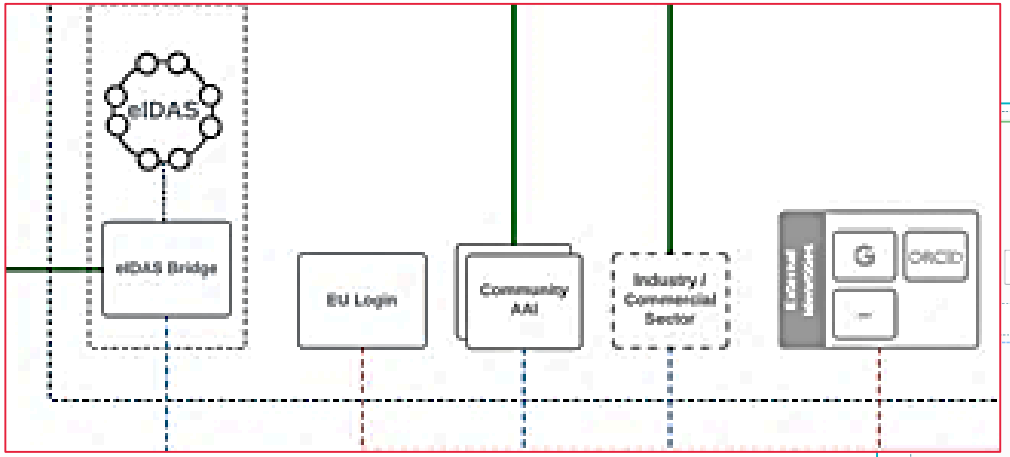
For up to ‘cappuccino’ (4/5) assurance level

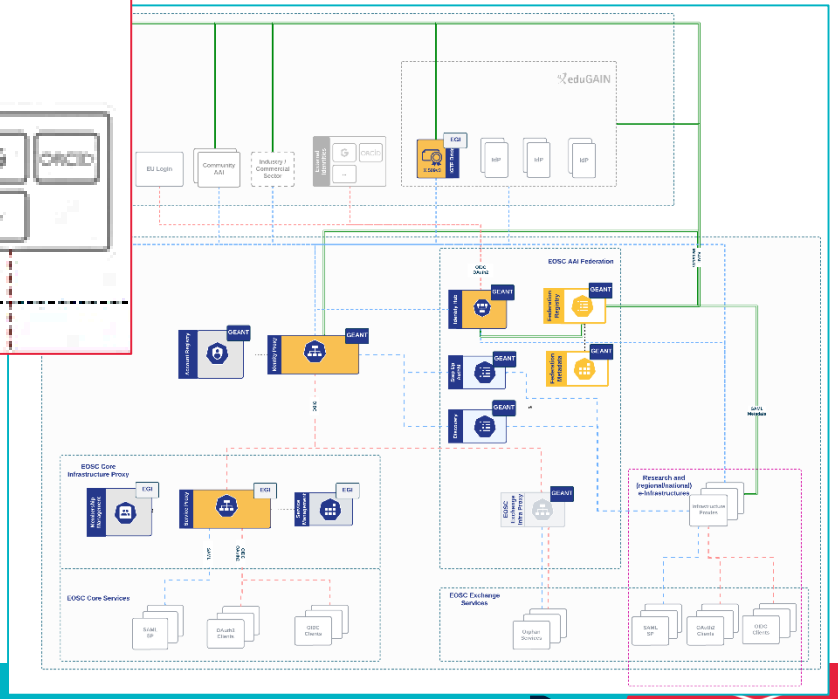


https://auth.cern.ch/auth/realms/cern/protocol/openid-connect/auth - CERN new SSO system design by Hannah Short *et al.*

EOSC AAI Federation, MyAccessID

***Identity assurance** brings the true value:*
authenticators are aplenty, and 'MFA'
far less interesting than vetted identities.
But education IdPs seem reluctant to provide it …

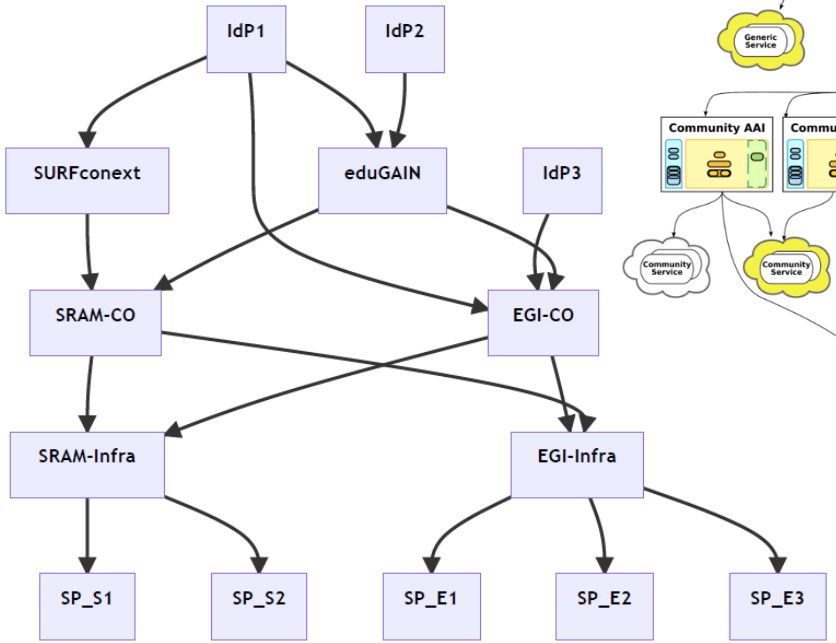


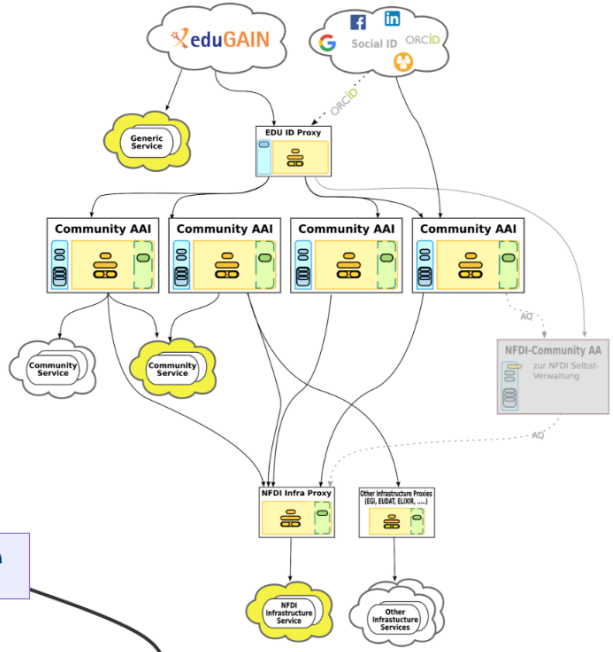


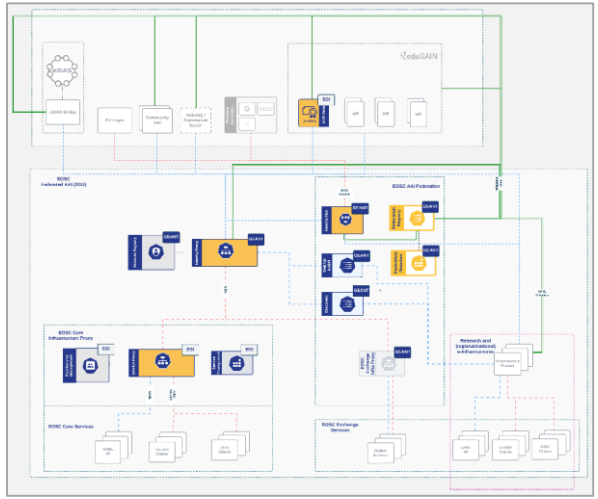
user identity comes 'with the user' from outside, mediated by the research community, ORCID, or from the home member state involved

Image: EOSC AAI for the EOSC Core and Exchange Federation for the EOSC European Node by Christos Kanellopoulos, Nicolas Liampotis, David Groep (June 2023)

And that is only the beginning!

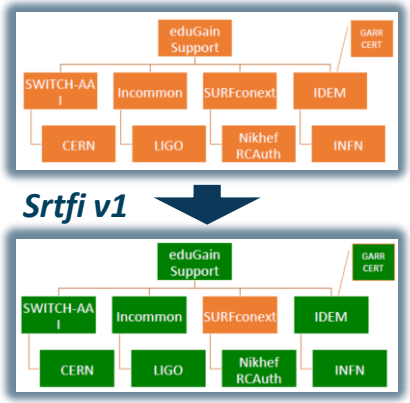


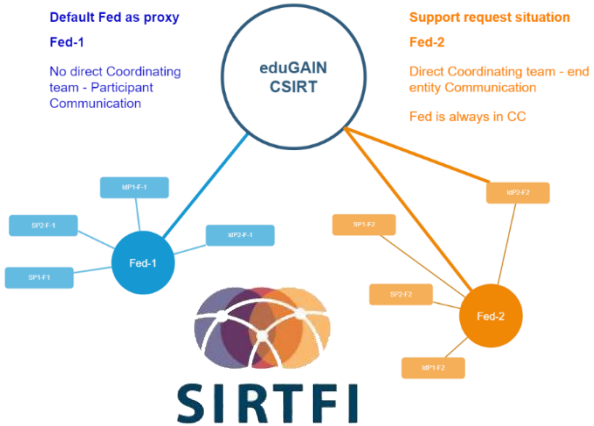


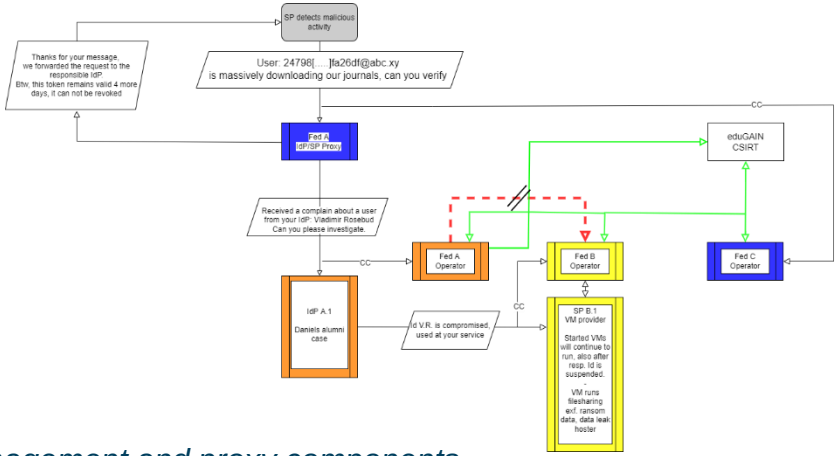


Images: SURF SSRAM and EGI by Maarten Kremers, NDFI AAI (Marcus Hardt),
EOSC AAI for the EOSC Core and Exchange Federation for the EOSC European Node by Christos Kanellopoulos, Nicolas Liampotis, David Groep (June 2023 version)

Response and traceability across IdP-SP Proxies and the limits of Sirtfi







*Guidelines for a joint **operational trust baseline** for membership management and proxy components, supplemented by policy guidance for sectoral federations with more specific policies where needed*

- *'How can we **convey the trust in what is in and behind the proxy**?'*
- *'How to provide **timely traceability** between services and identities through the proxy?'*

Based on requirements from FIM4R, WISE, and the proxy operators in AEGIS.

joint work with GN5-1 EnCo and eduGAIN CSIRT

images: AARC Sirtfi v1 exercise (Hannah Short), eduGAIN security TTX (Sven Gabriel, eduGAIN CSIRT)

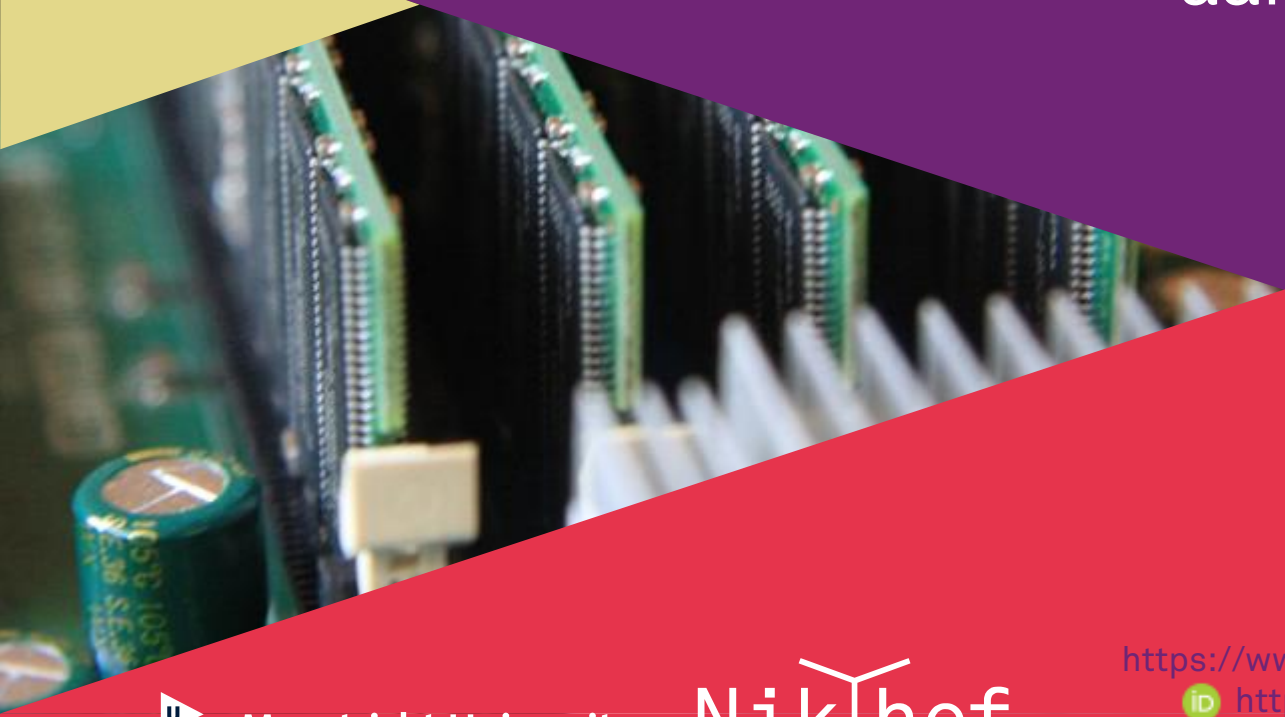
Co-funded by the European Union

AARC TREE and GEANT 5-1 are co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Thanks to the AARC Community, including folk from whom I re-used graphics and material in this overview. In random order: Licia Florio, Nicolas Liampotis, Christos Kanellopoulos, Marina Adomeit, Janos Mohacsi, Ilaria Fava, Slavek Licehammer, Dave Kelsey, Ian Neilson, Marcus Hardt, Mischa Salle, Hannah Short, and Maarten Kremers.

AARC

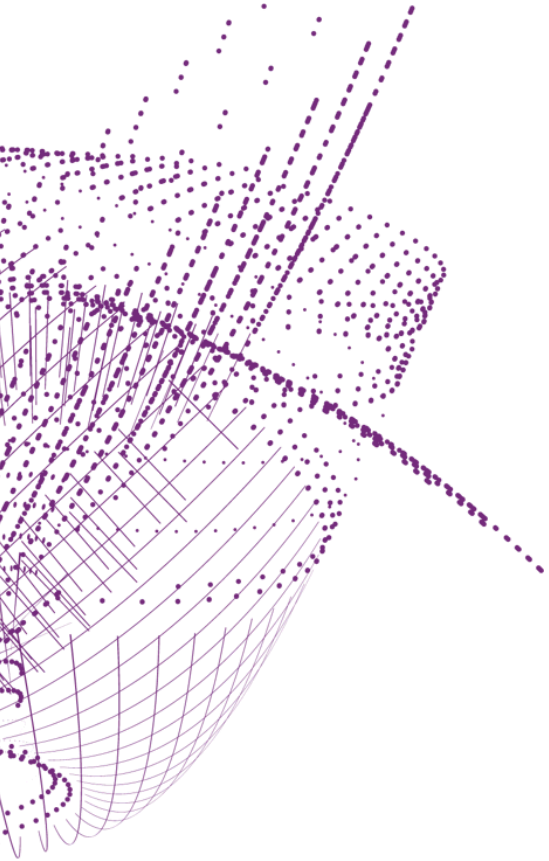
sso.nikhef.nl
aarc-community.org



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

Maastricht University

Nikhef



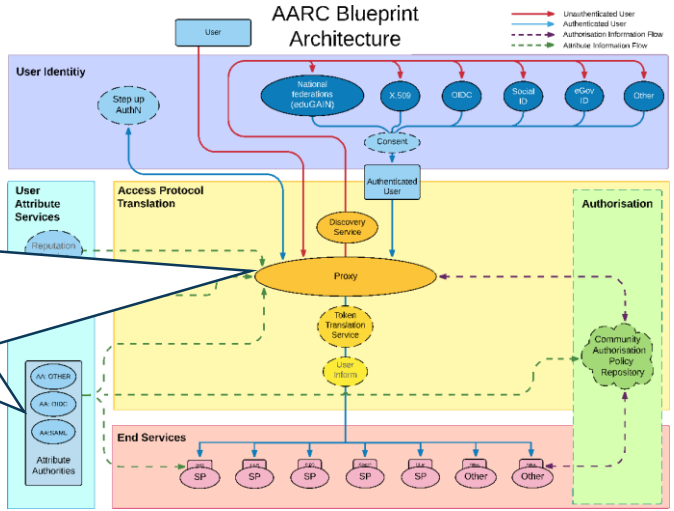
Background and supporting materials

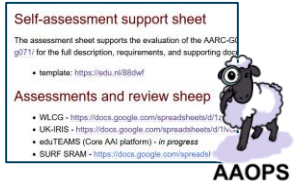
AARC G071 is there to help, but do we ‘get the trust across’?

Membership management service, attribute authorities, and proxy/token translator

- integrity of membership
- identification, traceability
- site and service security
- network protections
- assertion integrity

> Trust marks and expression





But when proxies are proxying proxies, can we proxy the trust?

Agree to a *common baseline*

… an approach that was successful previously!

See https://www.igtf.net/guidelines/aaops/ and https://aarc-community.org/guidelines/aarc-g071/

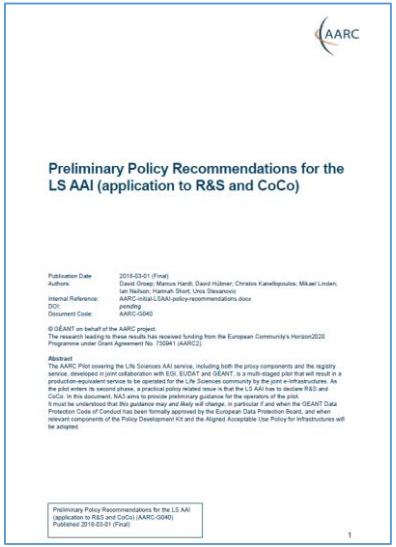
Proxies have their own challenges as well: AUPs, T&Cs, Privacy notices, …

For large 'multi-tenant' proxies

- some subset users in some communities use a set of services – how to present their Terms and Conditions and their privacy policies, so that users
  - only see the T&Cs and notices for services they will access
  - this does not to need to be manually configured for each community
  - is automatically updated when services join

For community and dedicated proxies

- when new (sensitive) services join, who needs to see the new T&Cs?
- can we communicate existing acceptance of T&Cs to downstream services?



AARC

Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo)

Publication Date: 2018-03-01 (Final)
Authors: David Groep, Marcus Hardt, David Hübner, Christos Kanellopoulos, Mikael Linden, Ian Neilson, Hannah Short, Uros Stevanovic
Internal Reference: AARC-initial-LSAAI-policy-recommendations.docx
DOI: *pending*
Document Code: AARC-G040

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
The AARC Pilot covering the Life Sciences AAI service, including both the proxy components and the registry service, developed in joint collaboration with EGI, EUDAT and GÉANT, is a multi-staged pilot that will result in a production-equivalent service to be operated for the Life Sciences community by the joint e-infrastructures. As the pilot enters its second phase, a practical policy related issue is that the LS AAI has to declare R&S and CoCo. In this document, NA3 aims to provide preliminary guidance for the operators of the pilot.
It must be understood that this guidance may and likely will change, in particular if and when the GÉANT Data Protection Code of Conduct has been formally approved by the European Data Protection Board, and when relevant components of the Policy Development Kit and the Aligned Acceptable Use Policy for Infrastructures will be adopted.

Preliminary Policy Recommendations for the LS AAI (application to R&S and CoCo) (AARC-G040)
Published 2018-03-01 (Final)

1

beyond AARC-G040

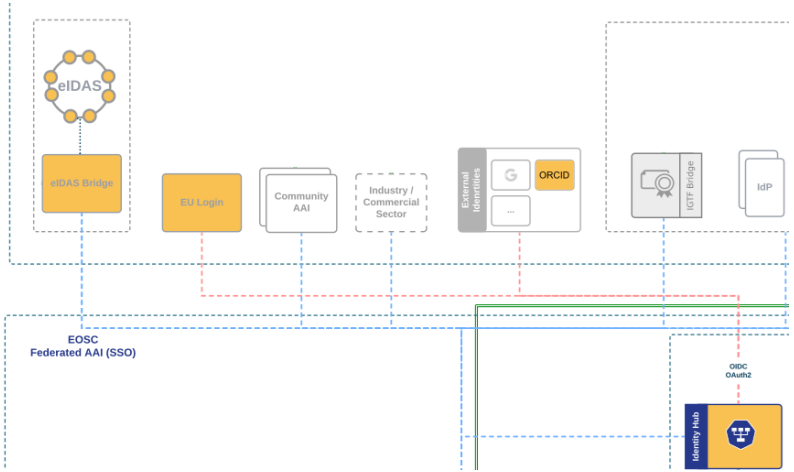
What is an acceptable user experience in clicking through agreements?
What is effective in exploiting the WISE Baseline AUP? What do researchers need?

'with fewer clicks to more resources'

And .. we'll be seeing more, and diverse, sources of identity assurance

An 'available' persistent source of assurance may be the (European) government-ID ecosystem

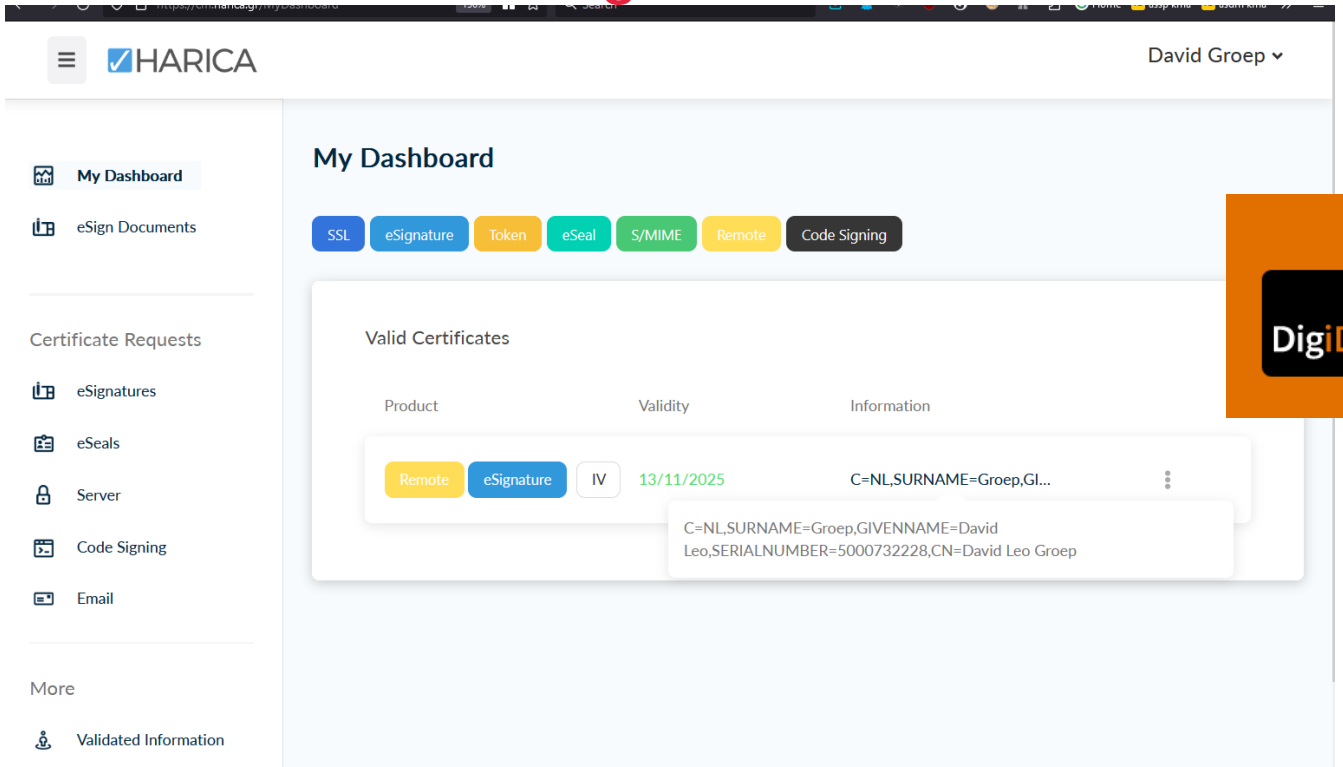
- step-up to at least *substantial* level can now readily be done 'at home' by many users through their national eID schemes
- Joint work on eIDAS, Erasmus Student Mobility, and more makes this more accessible
- step-up-as-a-service as a fall-back (like in .se)
- better attainable than relying on home institutions?



… but:

- what to do with non-European users?
- how to link the identities together

Better than a blue-ink signature, and assurance via DigID



images: screenshot of the HARICA remote signing interface, cm.harica.gr. Dutch eIDAS for citizens: DigID, excerpt from www.digid.nl screen shot
Thanks to Dimitris Zacharopoulos (HARICA) for getting the authentication working. eIDAS connected enabled through GRNET and Logius

RCauth.eu
by Mischa Sallé et al.

Example service translating to certificates

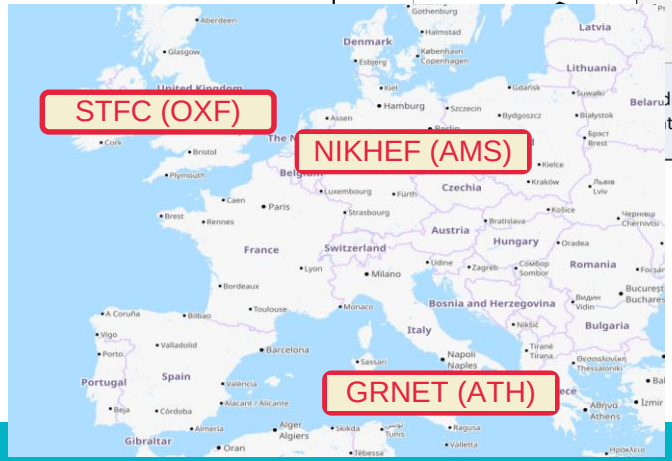
Token translation example: RCauth
from Heath Robinson to anycasted HA infrastructure

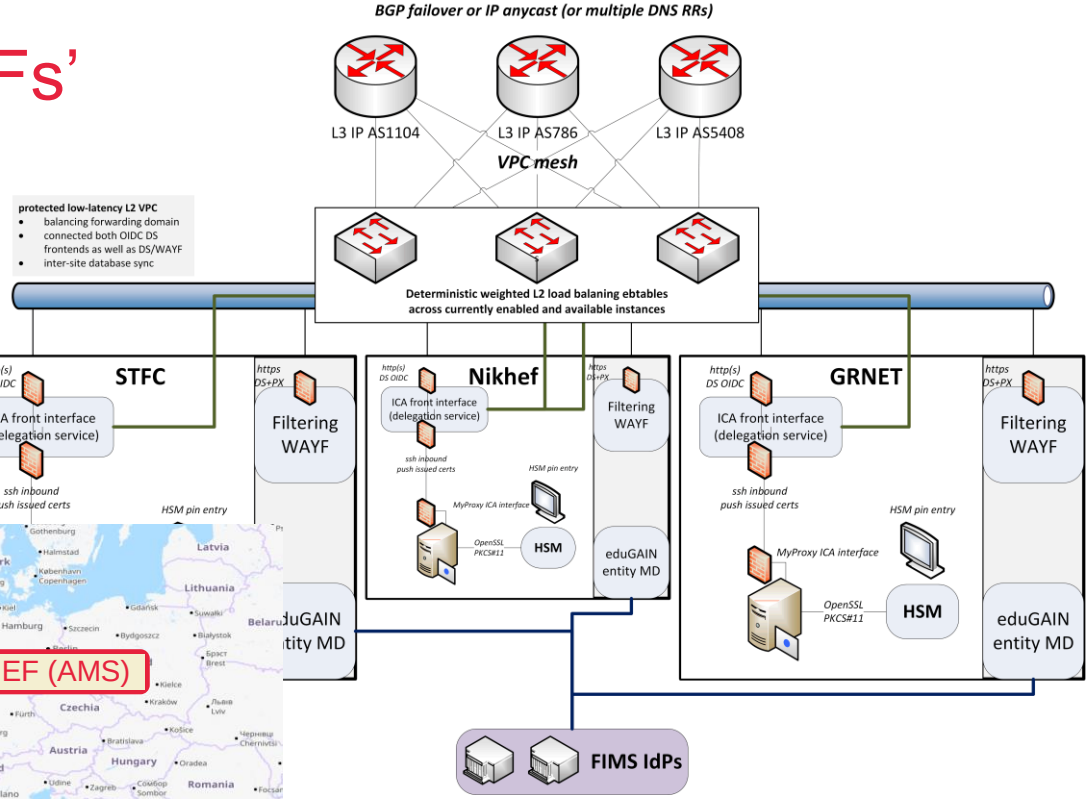
Nikhef RCauth prototype instance in 2019
Mischa Sallé

But we did not like ‘SPOFs’

Distributed High Availability setup
across the 3 sites
design for minimal effort
readily-available techniques

- L3 VPN (OpenVPN) or L2 VPC
- Linux HAProxy

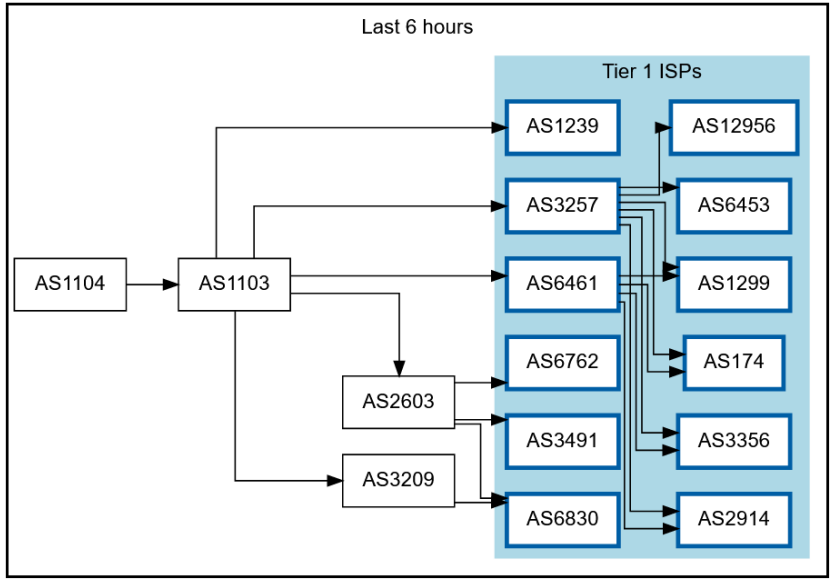


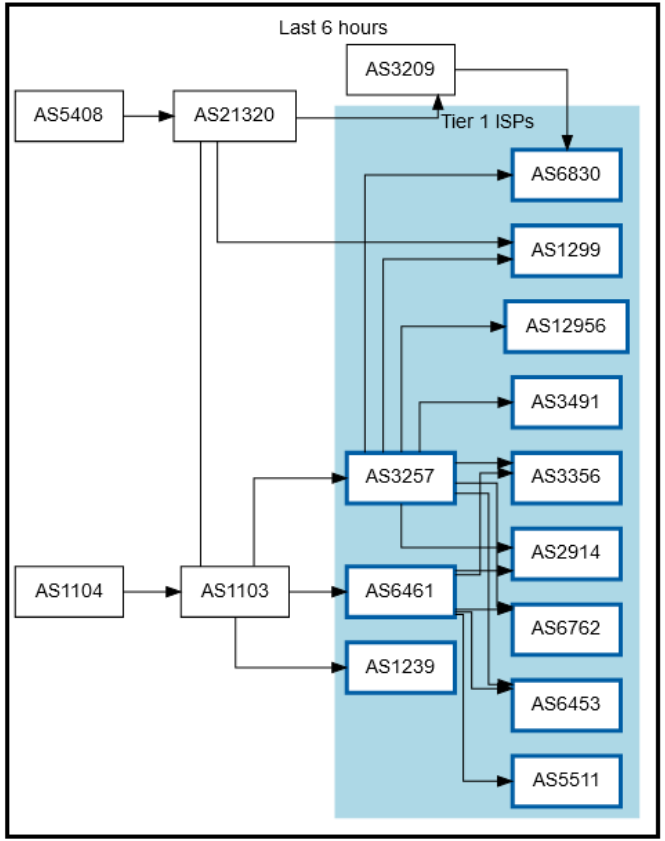


work supported by the EOSC Hub and EOSC Future projects
co-funded by the European Union

Design by Mischa Sallé, with Nicolas Liampotis and Kyriakos Gkynis

Getting 2a07:8504:1a0::/48 out there



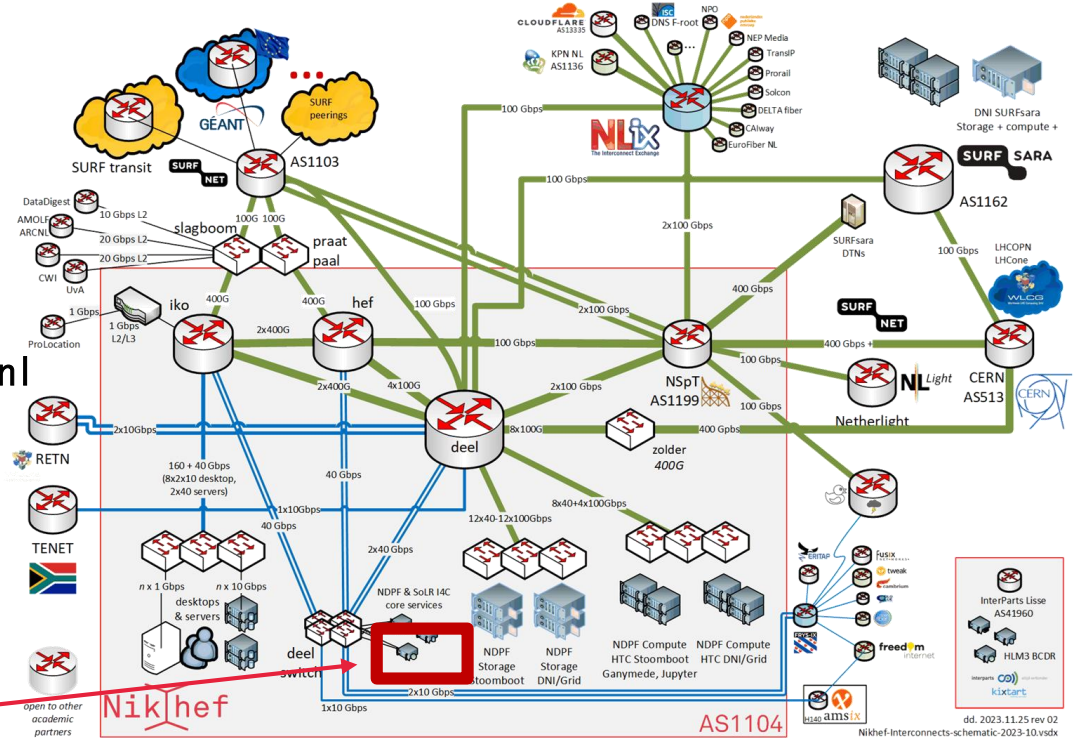


route maps: bgp.tools for 2a07:8504:1a0::/48 – IPv4 for 145.116.216.0/24 is similar – imagery from November 2022

Always the shortest path!

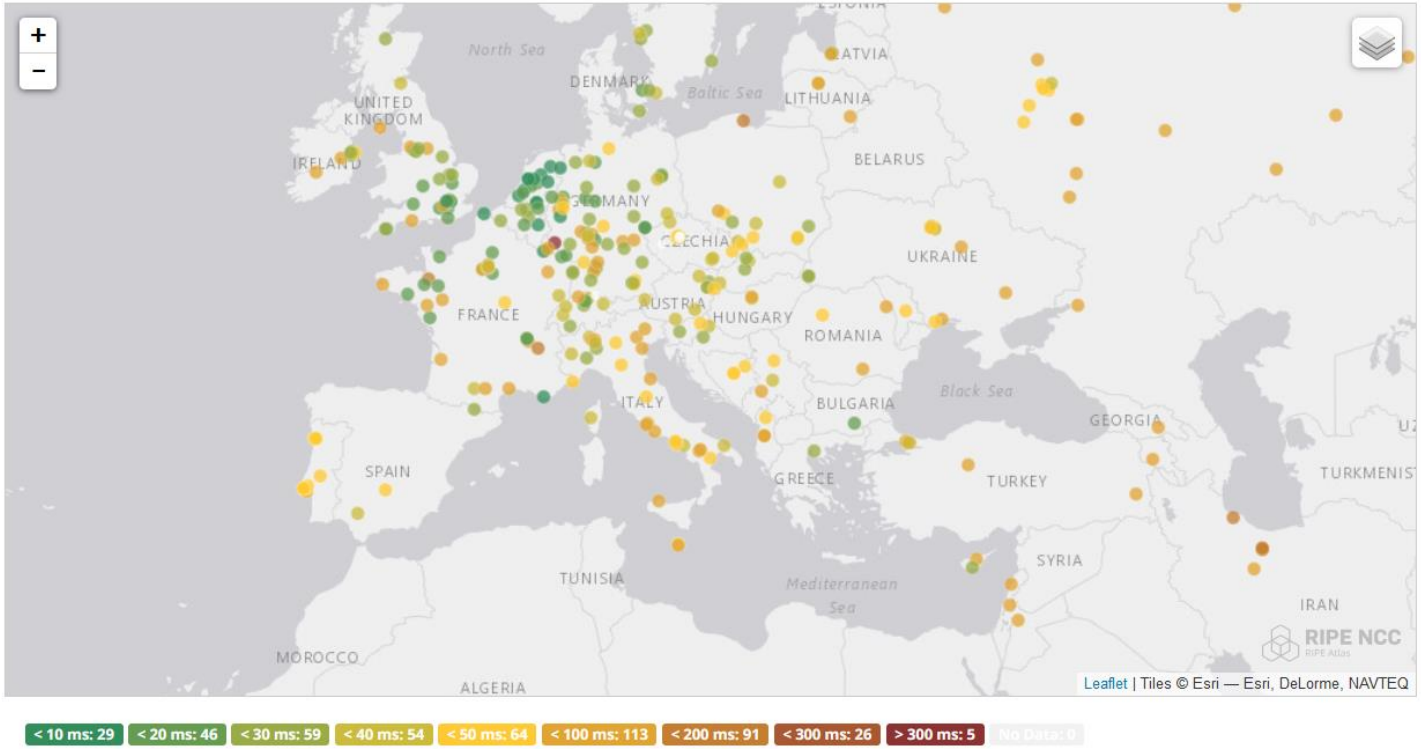
```
[root@kwark ~]# traceroute -IA 145.116.216.1
traceroute to 145.116.216.1 (145.116.216.1),
30 hops max, 60 byte packets
 1  cmbr.connected.by.freedominter.net
      (185.93.175.234) [AS206238]
 2  connected.by.freedom.nl
      (185.93.175.240) [AS206238]
 3  et-0-0-0-1002.core1.fi001.nl.freedomnet.nl
      (185.93.175.208) [AS206238]
 4  as1104.frys-ix.net (185.1.203.66) [*]
 5  parkwachter.nikhef.nl
      (192.16.186.141) [AS1104]
 6  gw-anyc-01.rcauth.eu
      (145.116.216.1) [AS786/AS5408/AS1104]
```

rcauth.eu HA proxy



Route from home to RCauth.eu, from my home ISP (Freedom Internet)

You get reasonable load balancing in Europe for free



< 10 ms: 29 | < 20 ms: 46 | < 30 ms: 59 | < 40 ms: 54 | < 50 ms: 64 | < 100 ms: 113 | < 200 ms: 91 | < 300 ms: 26 | > 300 ms: 5 | No Data: 0

map: RIPE NCC RIPE Atlas - 500 probes, distributed across Europe (https://atlas.ripe.net/measurements/50949024/)