v0.3

Nikhef

Maastricht University

How trust and identity enable
global infrastructures for distributing computing

In Infrastructures … we Trust!

ISGC 2025
David Groep, March 2025

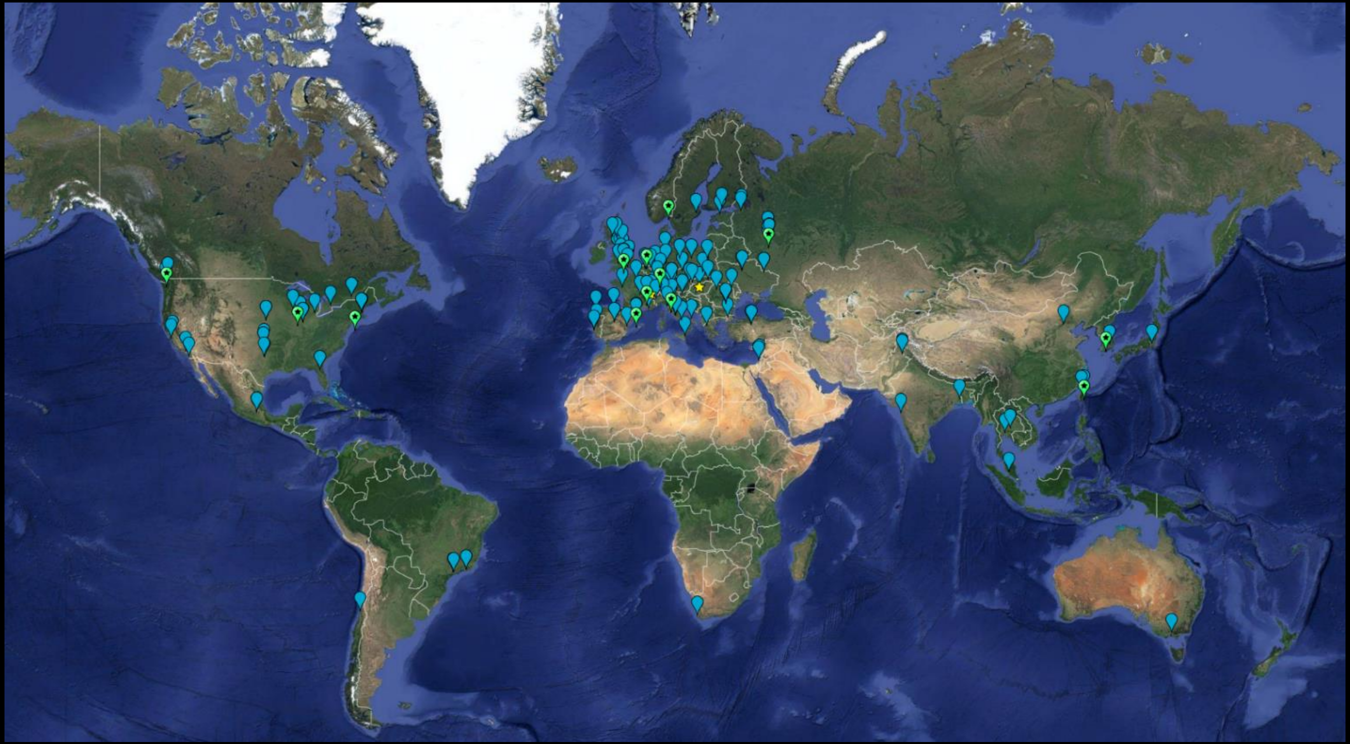
Collaborations: from small …

Nikhef user room H1.37 – terminal stations in the early 1990’s – image source: Nikhef

… to large collaborations (and shown here is a subset …)

a small part of the CMS collaboration in 2017, photo credit CERN on behalf the CMS collaboration, CMS-PHO-PUBLIC-2017-004-3

How many interactions? And just how many logins?



Worldwide LHC Computing Grid (~ 2024)
~ 1.4 million CPU cores
~ 1500 Petabyte
disk + archival

170+ institutes
42+ countries
13 'Tier-1 sites'
some multi-community:
NL-T1 @ SURF & Nikhef

Earth background: Google Earth; Data and compute animation: STFC RAL for WLCG and EGI.eu; Data: https://home.cern/science/computing/grid ;
LHC Computing Grid: wlcg.web.cern.ch, EGI: www.egi.eu; ACCESS CI: https://access-ci.org/, NL-T1 and FuSE: fuse-infra.nl, https://www.surf.nl/en/research-it

Do we ask for ~ 12 000 x 170+ passwords for everyone?

Image "trust fall" by Barret Anspach (https://www.flickr.com/photos/anspach/954545) used under CC-BY-2.0 license

Of course not!

But 12 000 people is still a lot,

and many more than you would trust with your bank PIN …

Yet we have found mechanisms to collaborate beyond the canonical ~150 people ("Dunbar's number")

but what we built, may both be unique for our 'high-trust' research community … and be an example for others

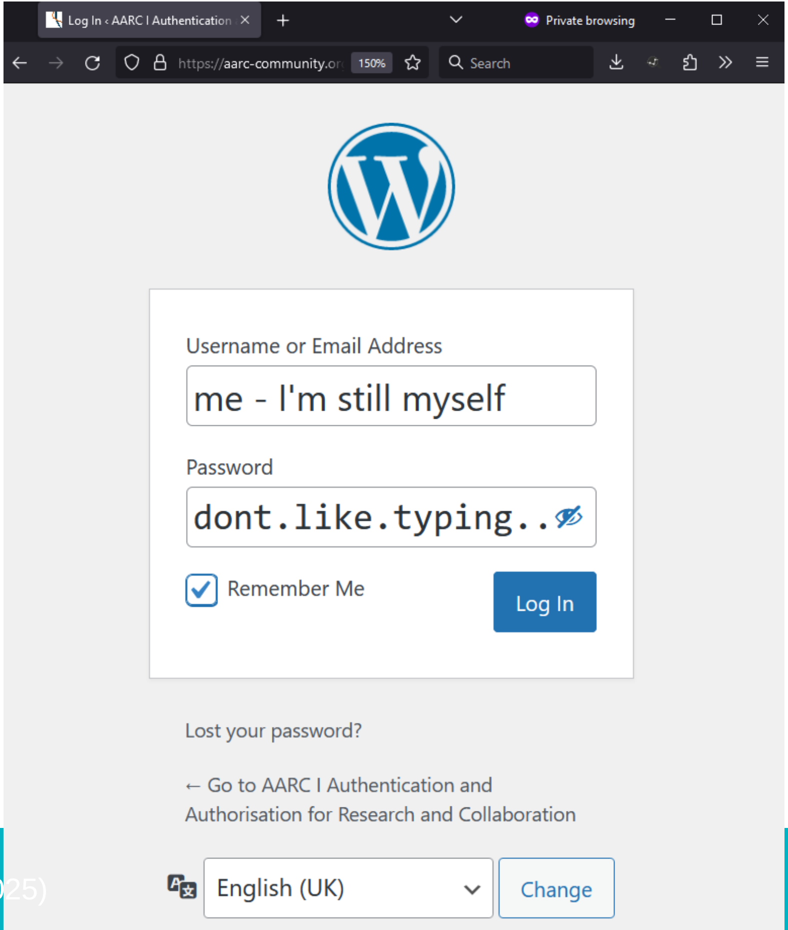
When you are asked to login again …

Authentication

demonstrating ‘you are you’

- ***authenticator***
  ‘you’ remains same ‘you’

- **vetted *identity***
  ‘you’ can be pseudonymous
  ‘you’ can be a vetted person



Username or Email Address
me - I'm still myself

Password
dont.like.typing..

☑ Remember Me

Log In

Lost your password?

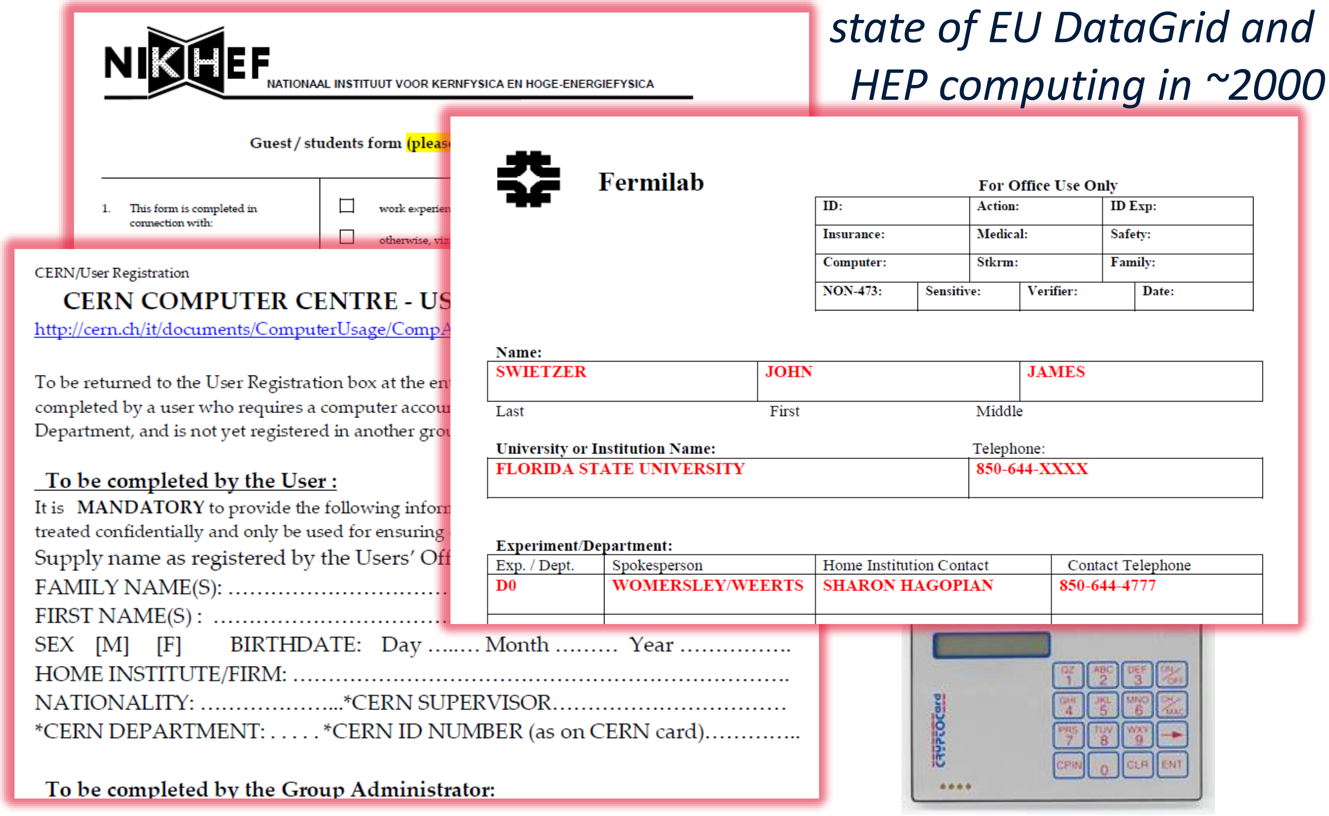
← Go to AARC I Authentication and Authorisation for Research and Collaboration

English (UK)

Change

Self-asserted or ‘pseudonymous’ often not enough

state of EU DataGrid and HEP 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, viz

CERN/User Registration

CERN COMPUTER CENTRE - US

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

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’ Of

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

Scaling credentials: per service per user

Many start with *credentials* dedicated
to each service where you need access

- In a multi-organizational system becomes

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

- usually creates a strong link to authorization:

  different accounts for different roles,
  multiplying the number of credentials per user

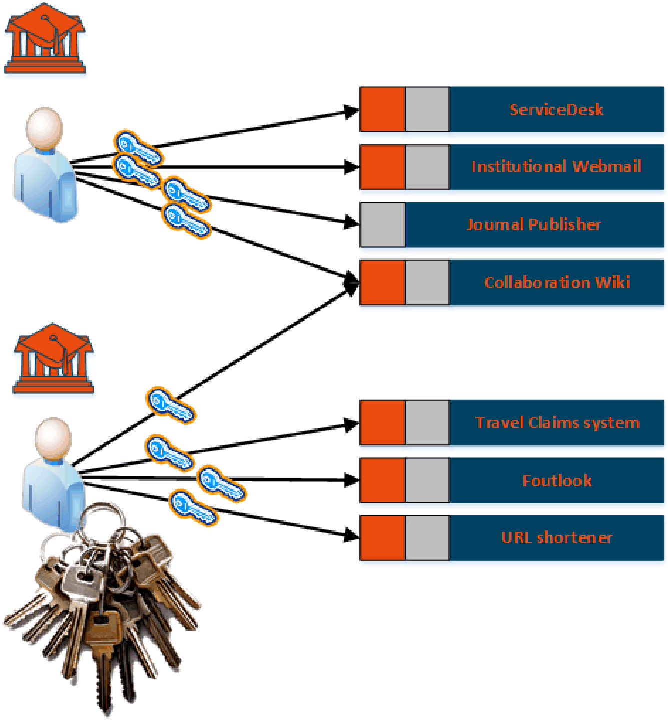


Image imspired by AARC NA2 training module “Authentication and Authorisation 101” – keychain image created by generative AI

bilateral ‘SSO’: a single service, or a single identity source

#credentials required?

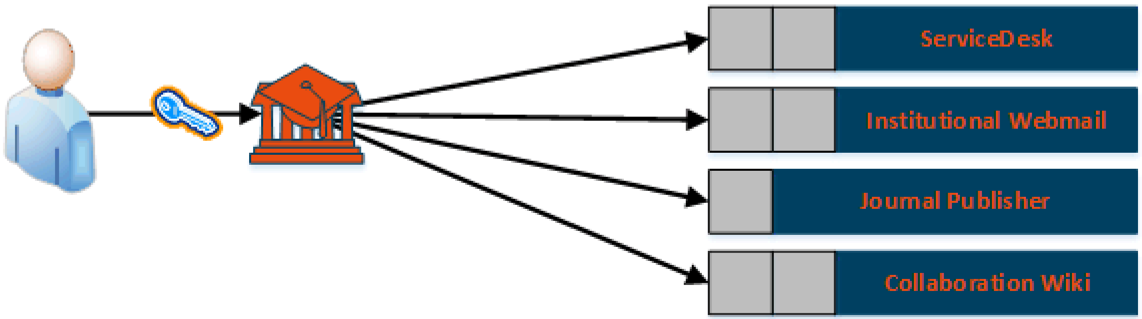
from previously

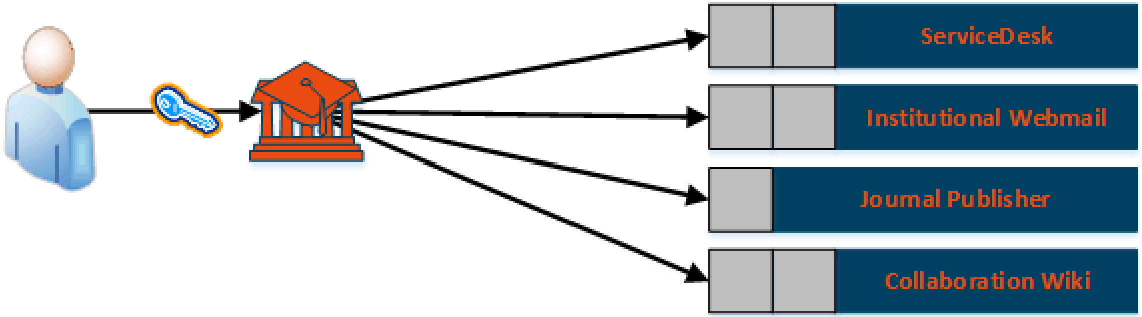
$\mathcal{O}(n_{services}) * \mathcal{O}(n_{users})$

to

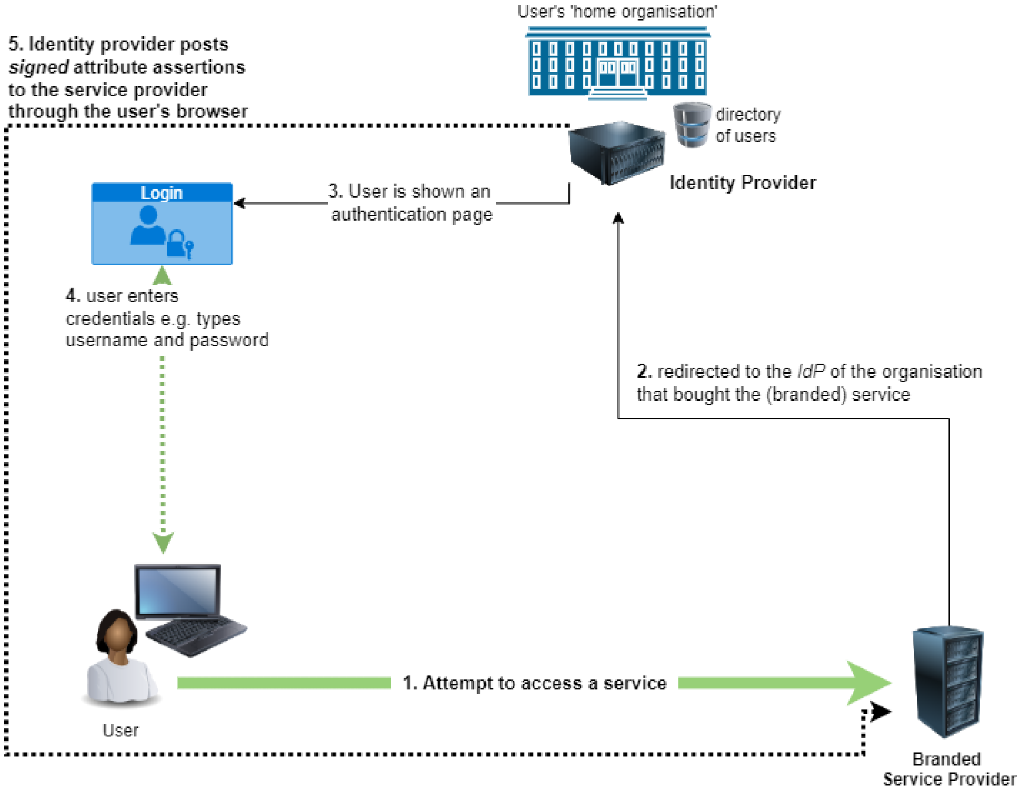
$\boldsymbol{\mathcal{O}(n_{users})}$
$+ \mathcal{O}(n_{services} * n_{home\text{-}orgs})$

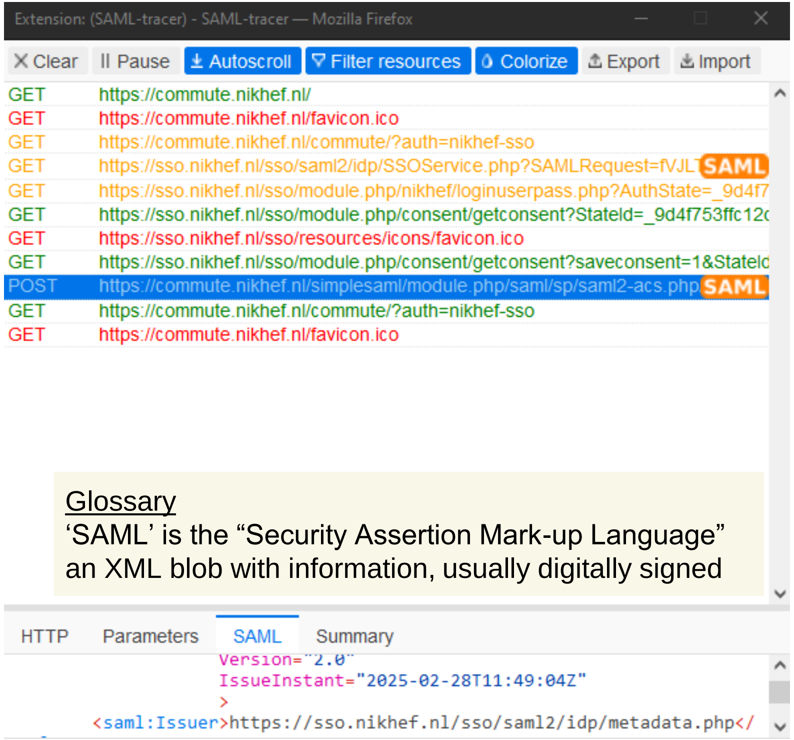
in first order at least





Single sign-on – why your browser keeps loading things


User's 'home organisation'
5. Identity provider posts *signed* attribute assertions to the service provider through the user's browser
directory of users
Identity Provider
Login
3. User is shown an authentication page
4. user enters credentials e.g. types username and password
2. redirected to the *IdP* of the organisation that bought the (branded) service
1. Attempt to access a service
User
Branded Service Provider



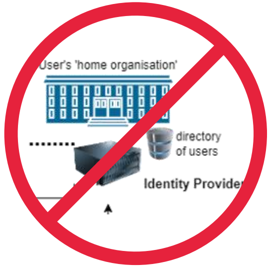
```
GET   https://commute.nikhef.nl/
GET   https://commute.nikhef.nl/favicon.ico
GET   https://commute.nikhef.nl/commute/?auth=nikhef-sso
GET   https://sso.nikhef.nl/sso/saml2/idp/SSOService.php?SAMLRequest=fVJLT SAML
GET   https://sso.nikhef.nl/sso/module.php/nikhef/loginuserpass.php?AuthState=_9d4f7
GET   https://sso.nikhef.nl/sso/module.php/consent/getconsent?StateId=_9d4f753ffc12c
GET   https://sso.nikhef.nl/sso/resources/icons/favicon.ico
GET   https://sso.nikhef.nl/sso/module.php/consent/getconsent?saveconsent=1&StateId
POST  https://commute.nikhef.nl/simplesaml/module.php/saml/sp/saml2-acs.php SAML
GET   https://commute.nikhef.nl/commute/?auth=nikhef-sso
GET   https://commute.nikhef.nl/favicon.ico
```

```
                 Version="2.0"
                 IssueInstant="2025-02-28T11:49:04Z"
                 >
    <saml:Issuer>https://sso.nikhef.nl/sso/saml2/idp/metadata.php</
```

<u>Glossary</u>
'SAML' is the "Security Assertion Mark-up Language"
an XML blob with information, usually digitally signed

SAML-tracer plugin by Tim van Dijen (SSC-ICT) *et al.*
https://github.com/simplesamlphp/SAML-tracer

User-centric identity: ‘I take my passport anywhere by myself’



Your ‘home organisation’ does not have to be in the loop …

user-centric trust: you yourself hold a credential from a trusted third party and can use it *without having to ask ‘home’ each time:*

- Public Key Infrastructure client certificates (“X.509”)
- Verifiable credentials in wallets
- *and who remembers CardSpace?*

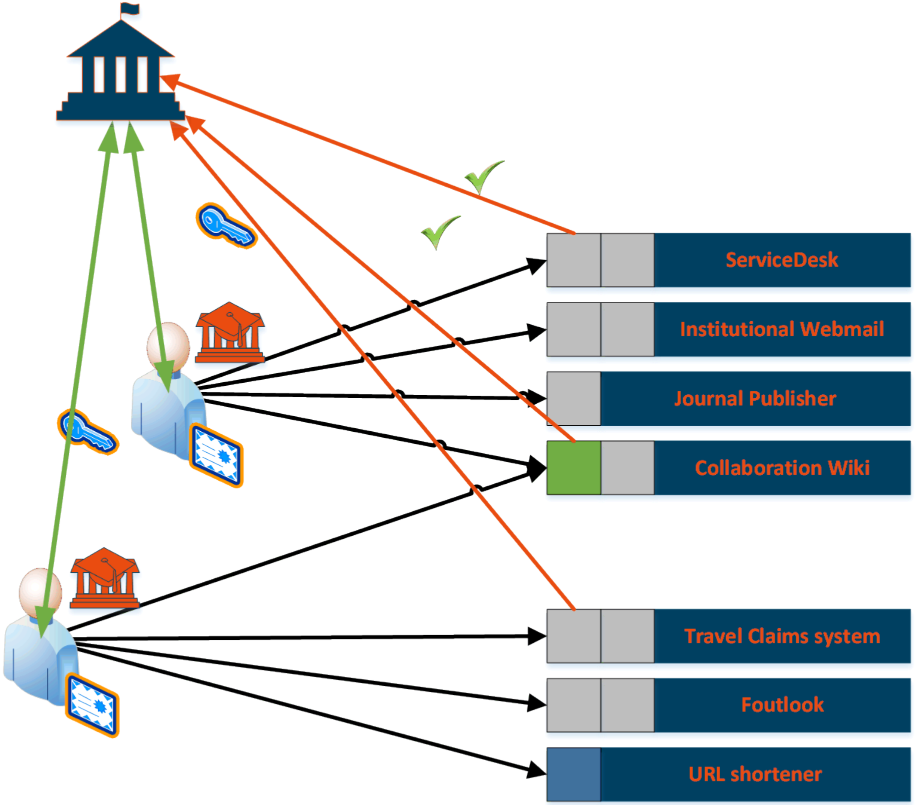
Passport image: cropped from original by Jon Tyson on Unsplash https://unsplash.com/photos/Hid-yhommOg

User-centric AAI

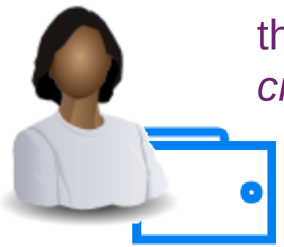
A **trusted authority** giving the user
a ‘self-managed’ credential, like a passport

- a personal authentication digital certificate
- a verifiable credential in a wallet
- …

verified (on-line and also offline)
at the original trusted issuer
or at an independent trusted verifier

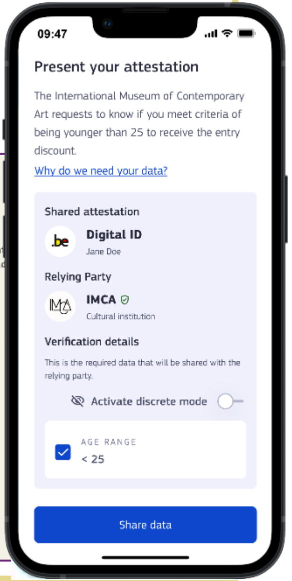


Identity wallets, held by the user, are another



the user as a
credential Holder

```
--------------- JWT header --------------
{
  "alg": "ES256",
  "typ": "JWT"
}
--------------- JWT payload --------------
// NOTE: The example below uses a valid VC-JWT serializat
//       that duplicates the iss, nbf, jti, and sub field
//       Verifiable Credential (vc) field.
{
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.w3.org/2018/credentials/examples/v1"
    ],
    "id": "http://example.edu/credentials/3732",
    "type": [
      "VerifiableCredential",
      "UniversityDegreeCredential"
    ],
    "issuer": "https://example.edu/issuers/565049",
    "issuanceDate": "2010-01-01T00:00:00Z",
    "credentialSubject": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "degree": {
        "type": "BachelorDegree",
        "name": "Bachelor of Science and Arts"
      }
```



09:47

Present your attestation

The International Museum of Contemporary Art requests to know if you meet criteria of being younger than 25 to receive the entry discount.

Why do we need your data?

Shared attestation

.be Digital ID
Jane Doe

Relying Party

IMCA
Cultural institution

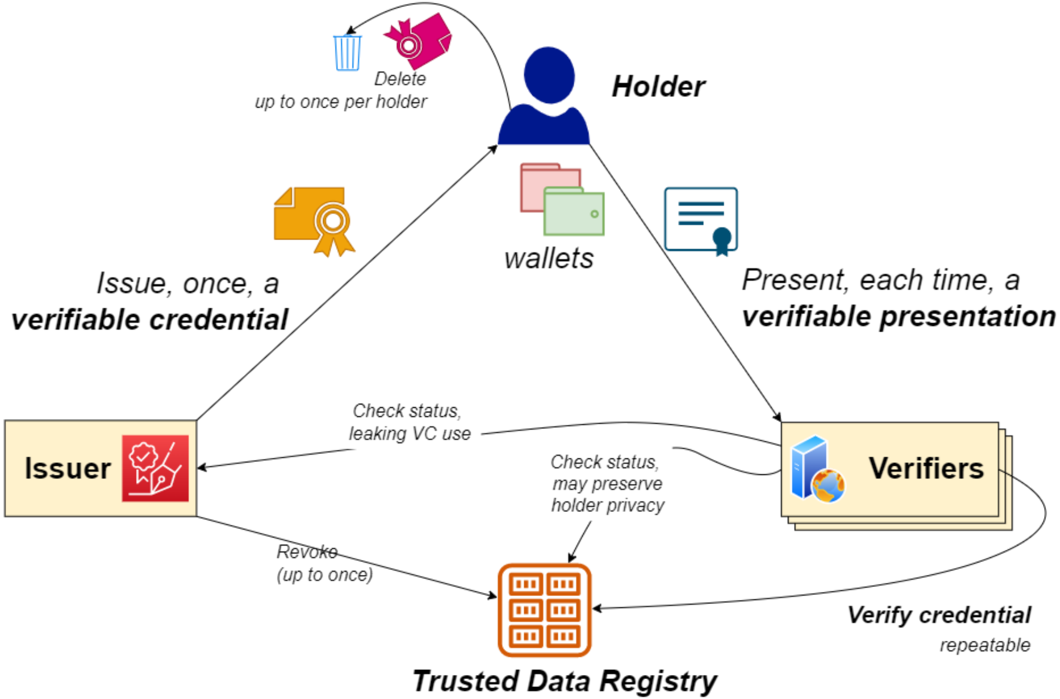
Verification details

This is the required data that will be shared with the relying party.

Activate discrete mode ○

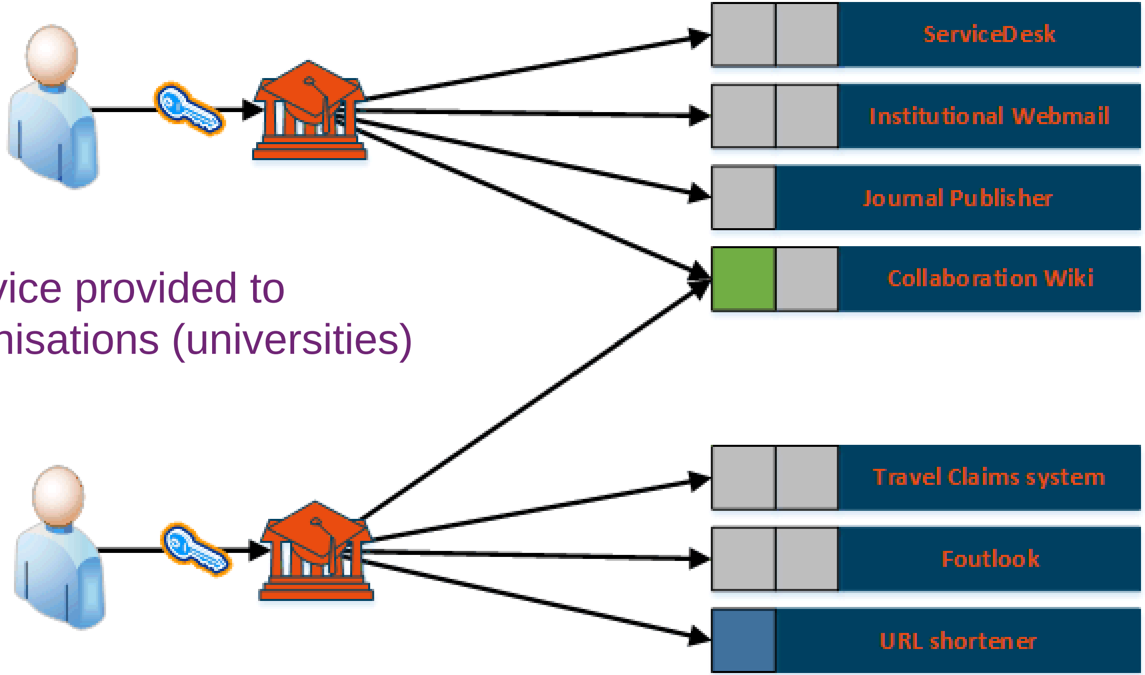
☑ AGE RANGE
< 25

Share data



Flow diagram inspired by: Lifecycle Details (5.1), Verifiable Credentials Data Model v1.1, W3C Recommendation 03 March 2022, https://www.w3.org/TR/vc-data-model/
EU eID Wallet from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
Annimage: European Commission, at https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Security+and+Privacy

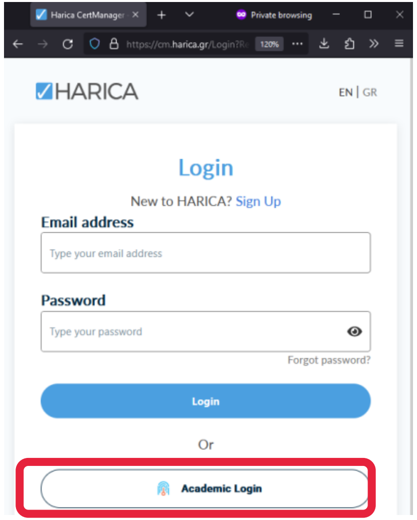
Can we scale better with an ‘federated’ Authentication and Authorisation Infrastructure (‘AAI’)



with one service provided to several organisations (universities)

we will get to authorisation in a bit …

Where are 'you' in the federated space – discovery!



Harica CertManager × | Private browsing

https://cm.harica.gr/Login?R | 120%

HARICA | EN | GR

Login

New to HARICA? Sign Up

Email address

Type your email address

Password

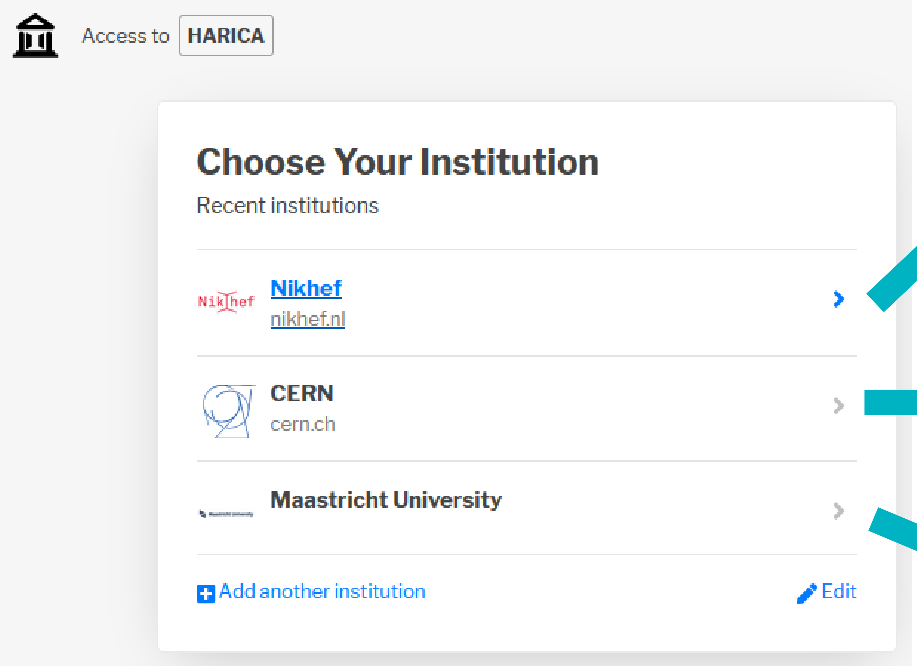
Type your password

Forgot password?

Login

Or

Academic Login



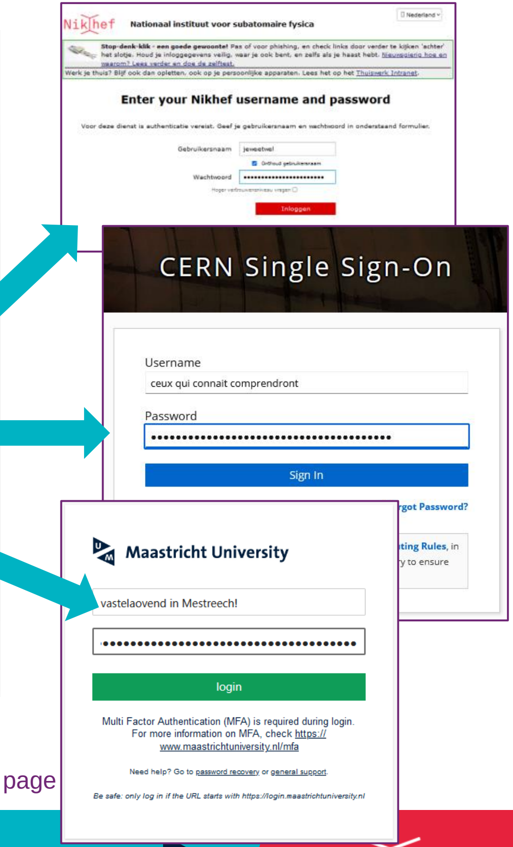
Access to **HARICA**

Choose Your Institution

Recent institutions

- **Nikhef** – nikhef.nl
- **CERN** – cern.ch
- **Maastricht University**

Add another institution | Edit



Nikhef Nationaal instituut voor subatomaire fysica | Nederland

Stop-denk-klik - een goede gewoonte! Pas of voor phishing, en check links door verder te kijken 'achter' het slotje. Houd je inloggegevens veilig, waar je ook bent, en zelfs als je haast hebt. Nieuwsgierig hoe en waarom? Lees verder en doe de zelftest.

Werk je thuis? Blijf ook dan opletten, ook op je persoonlijke apparaten. Lees het op het Thuiswerk Intranet.

Enter your Nikhef username and password

Voor deze dienst is authenticatie vereist. Geef je gebruikersnaam en wachtwoord in onderstaand formulier.

Gebruikersnaam: jeweetwel

☑ Onthoud gebruikersnaam

Wachtwoord: ••••••••••••••••••••••

Hoger vertrouwensniveau vragen □

Inloggen

CERN Single Sign-On

Username: ceux qui connait comprendront

Password: ••

Sign In

rgot Password?

ting Rules, in

y to ensure

Maastricht University

vastelaovend in Mestreech!

••••••••••••••••••••••••••••••••••••

login

Multi Factor Authentication (MFA) is required during login. For more information on MFA, check https://www.maastrichtuniversity.nl/mfa

Need help? Go to password recovery or general support.

Be safe: only log in if the URL starts with https://login.maastrichtuniversity.nl

An example cross-institutional service by HARICA, the GEANT TCS G5 provider, presenting a SeamlessAccess.org discovery page

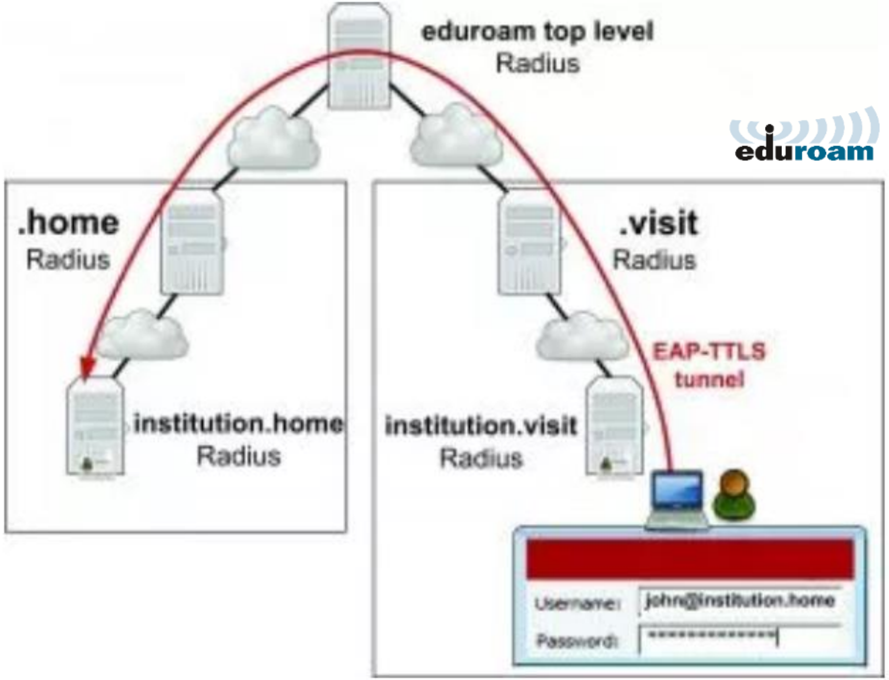
The federation you most likely know …

service-specific trust
between organisations

hierarchical server path, based on
a network-specific secure exchange

sending your credentials back
to *only* your home institution

found via <anon**@domain.name**>

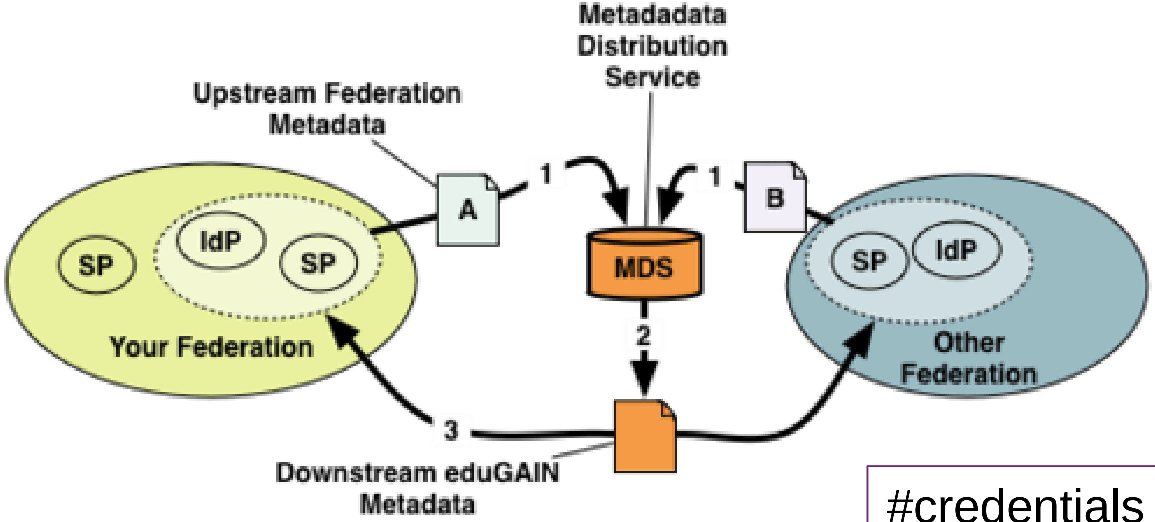


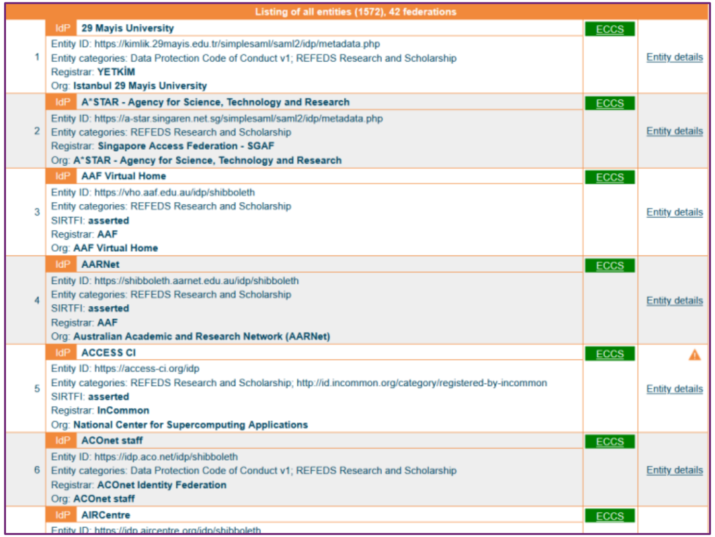
eduroam image from https://eduroam.org/how/, GEANT ; RADIUS: RC2865 https://www.rfc-editor.org/rfc/rfc2865; see also freeradius.org

We live in a federated world!

aconet
AUSTRALIAN ACCESS FEDERATION
The UK Access Management Federation FOR EDUCATION AND RESEARCH
eduID.cz
DFN-AAI
Edugate Gaining Access to Education
SURF CONEXT
RCTSaai REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE
RENATER CONNECTEUR DE SAVOIRS
cafe
SIR
haka
GakuNin
SWITCHaai
grnet
MiNGA
idem garr aai
SIFULAN
Carsi
Belnet R&E Federation
Colfire Colombian Federation of Identity for Research and Education
GakuNin
FEIDE
AFIRE
InCommon
COFRe Comunidad Federada REUNA
CILogon
TAAT
Tuakiri NEW ZEALAND ACCESS FEDERATION
AAI @EduHr
eduID
IGTF Interoperable Global Trust Federation AP | EU | TAG
TAIFE
arnes
WAYF Where are you from

Meta-data and trust in IdP-SP ‘multi-lateral’ federations


Metadadata Distribution Service
Upstream Federation Metadata
1
1
A
B
SP
IdP
SP
Your Federation
MDS
2
SP
IdP
Other Federation
3
Downstream eduGAIN Metadata



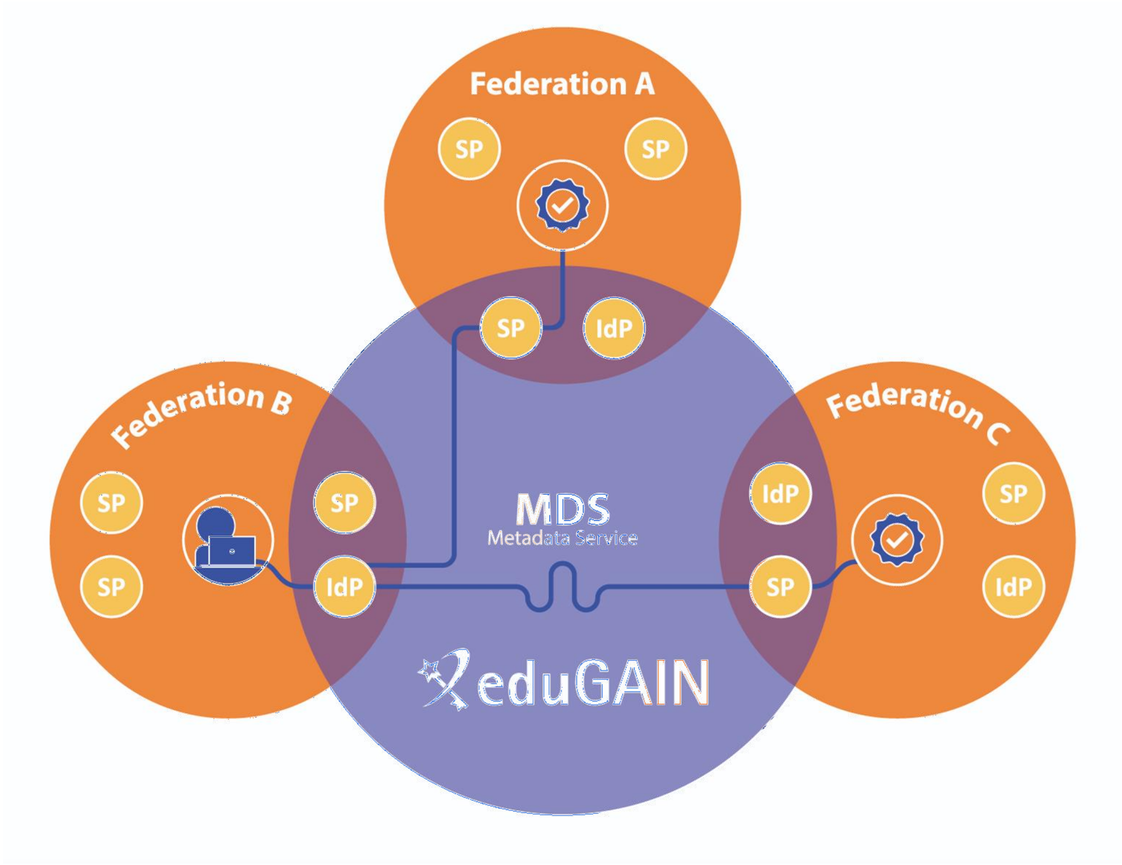
Listing of all entities (1572), 42 federations				
1	IdP	**29 Mayis University** Entity ID: https://kimlik.29mayis.edu.tr/simplesaml/saml2/idp/metadata.php Entity categories: Data Protection Code of Conduct v1; REFEDS Research and Scholarship Registrar: **YETKİM** Org: **Istanbul 29 Mayis University**	ECCS	Entity details
2	IdP	**A*STAR - Agency for Science, Technology and Research** Entity ID: https://a-star.singaren.net.sg/simplesaml/saml2/idp/metadata.php Entity categories: REFEDS Research and Scholarship Registrar: **Singapore Access Federation - SGAF** Org: **A*STAR - Agency for Science, Technology and Research**	ECCS	Entity details
3	IdP	**AAF Virtual Home** Entity ID: https://vho.aaf.edu.au/idp/shibboleth Entity categories: REFEDS Research and Scholarship SIRTFI: **asserted** Registrar: **AAF** Org: **AAF Virtual Home**	ECCS	Entity details
4	IdP	**AARNet** Entity ID: https://shibboleth.aarnet.edu.au/idp/shibboleth Entity categories: REFEDS Research and Scholarship SIRTFI: **asserted** Registrar: **AAF** Org: **Australian Academic and Research Network (AARNet)**	ECCS	Entity details
5	IdP	**ACCESS CI** Entity ID: https://access-ci.org/idp Entity categories: REFEDS Research and Scholarship; http://id.incommon.org/category/registered-by-incommon SIRTFI: **asserted** Registrar: **InCommon** Org: **National Center for Supercomputing Applications**	ECCS	⚠ Entity details
6	IdP	**ACOnet staff** Entity ID: https://idp.aco.net/idp/shibboleth Entity categories: Data Protection Code of Conduct v1; REFEDS Research and Scholarship Registrar: **ACOnet Identity Federation** Org: **ACOnet staff**	ECCS	Entity details
	IdP	**AIRCentre** Entity ID: https://idp.aircentre.org/idp/shibboleth	ECCS	

#credentials required?

from $\mathcal{O}(n_{users}) + \mathcal{O}(n_{services} * n_{home-orgs})$

to $\sim \boldsymbol{\mathcal{O}(n_{users}) + \mathcal{O}(n_{home-orgs}) + \mathcal{O}(n_{services})}$

MDS meta-data flow: https://wiki.geant.org/display/eduGAIN/Metadata+Flow+in+eduGAIN
eduGAIN meta-data https://mds.edugain.org/edugain-v2.xml ; table excerpt from https://technical.edugain.org/entities showing only R&S IdPs, i.e. those supporting research …



78

Identity Federations

5100+

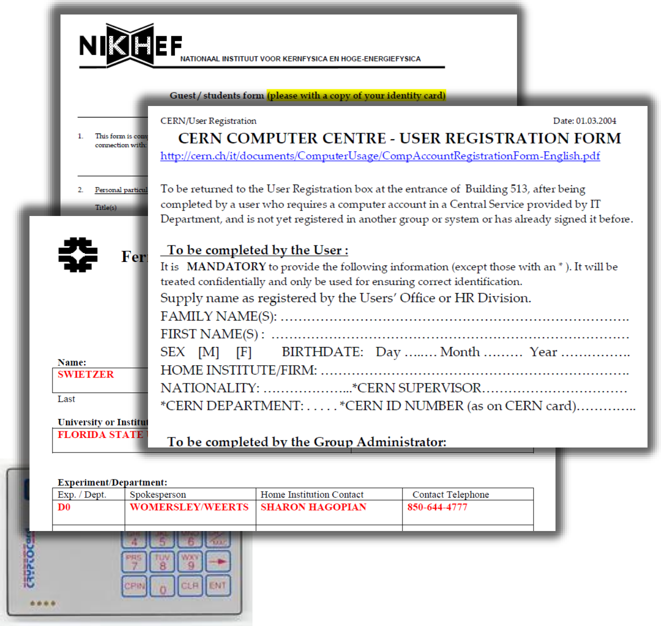
Identity Providers

3600+

Service Providers

eduGAIN image: Davide Vaghetti, GARR for GN*-*

We progressed a lot since 2003 with identity federation



NIKHEF NATIONAAL INSTITUUT VOOR KERNFYSICA EN HOGE-ENERGIEFYSICA

Guest / students form (please with a copy of your identity card)

1. This form is com connection with:

2. Personal particul

Title(s)

CERN/User Registration Date: 01.03.2004

CERN COMPUTER CENTRE - USER REGISTRATION FORM

http://cern.ch/it/documents/ComputerUsage/CompAccountRegistrationForm-English.pdf

To be returned to the User Registration box at the entrance of Building 513, after being completed by a user who requires a computer account in a Central Service provided by IT Department, and is not yet registered in another group or system or has already signed it before.

To be completed by the User :

It is MANDATORY to provide the following information (except those with an *). It will be treated confidentially and only be used for ensuring correct identification.

Supply name as registered by the Users' Office or HR Division.

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:

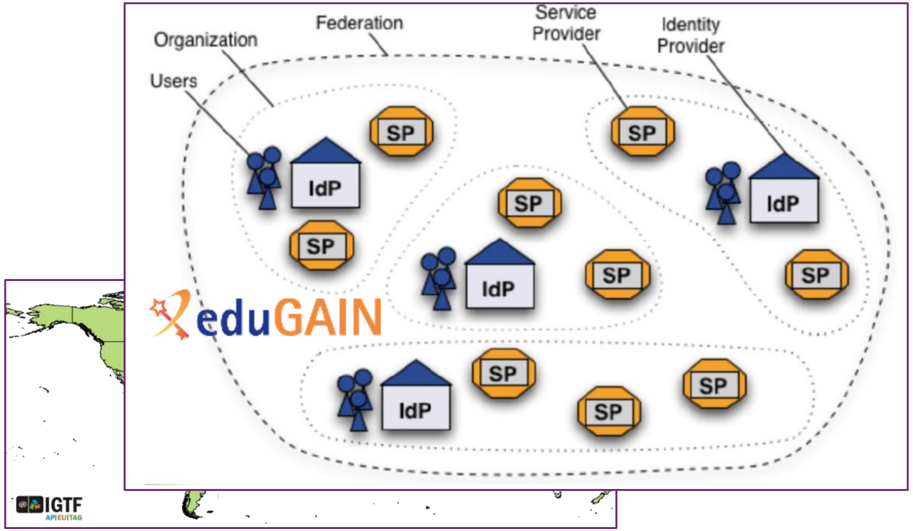
Fer

Name:
SWIETZER
Last

University or Institut
FLORIDA STATE

Experiment/Department:

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



For **eduGAIN federation** the IdPs provide **authentication** from the home organisation, for the user-centric PKIX IGTF trust fabric, the CAs do.
Then **Service providers** perform **authorization**,

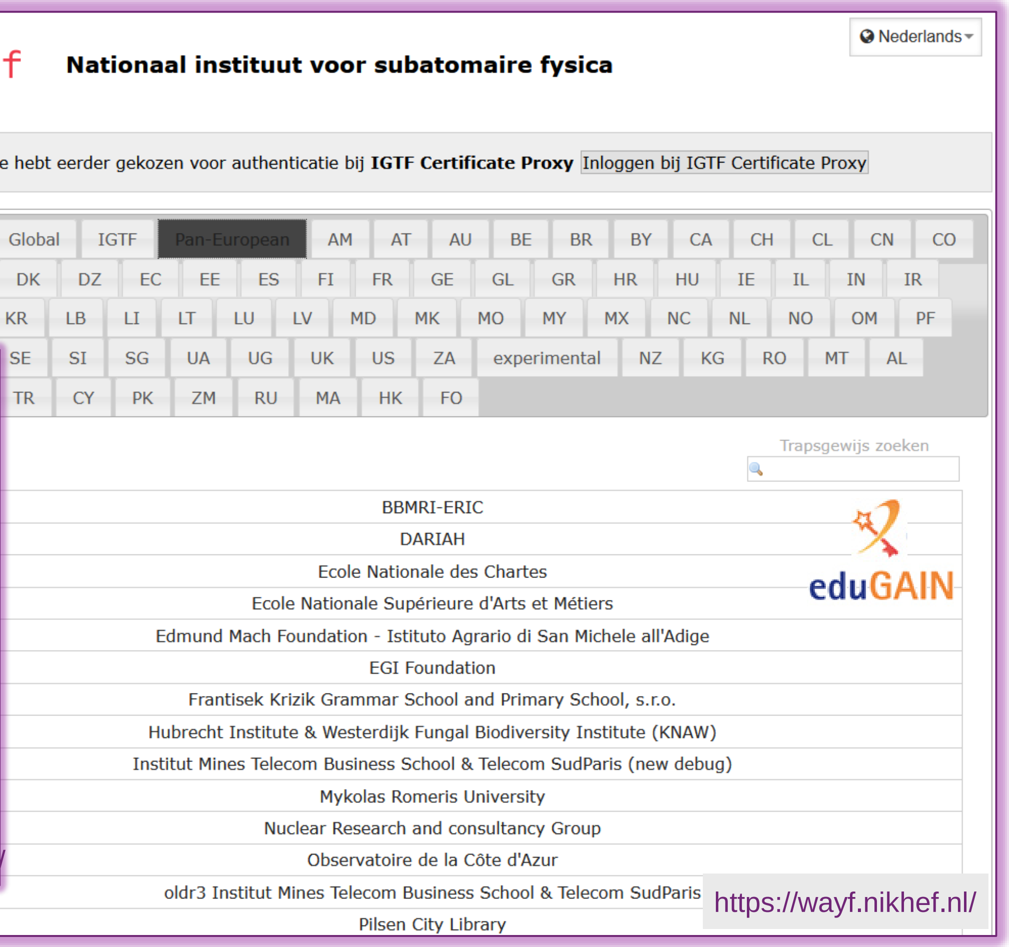
… maybe using attributes provided by the IdP. But do they get them??

Right-hand image: Shibboleth IdP federation, Lukas Hammerle, SWITCH (CH), user-centric PKI credentials: Interoperable Global Trust Federation, https://igtf.net/

Federated Success!

Login to GW’s ifosim.org, to gitlab, or … via the service proxy

with any eduGAIN IdP for user authentication



Nederlands

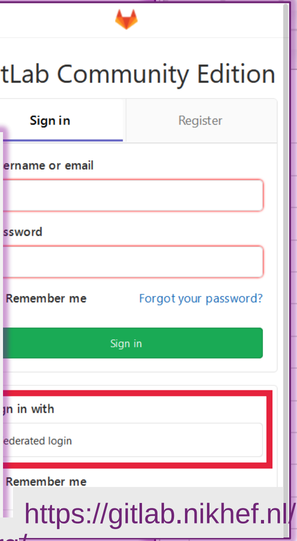
Nikhef Nationaal instituut voor subatomaire fysica

Je hebt eerder gekozen voor authenticatie bij **IGTF Certificate Proxy** Inloggen bij IGTF Certificate Proxy

Preferred Global IGTF Pan-European AM AT AU BE BR BY CA CH CL CN CO
CZ DE DK DZ EC EE ES FI FR GE GL GR HR HU IE IL IN IR
IT JP KR LB LI LT LU LV MD MK MO MY MX NC NL NO OM PF
SE SI SG UA UG UK US ZA experimental NZ KG RO MT AL
TR CY PK ZM RU MA HK FO
Trapsgewijs zoeken
eduGAIN

BBMRI-ERIC
DARIAH
Ecole Nationale des Chartes
Ecole Nationale Supérieure d'Arts et Métiers
Edmund Mach Foundation - Istituto Agrario di San Michele all'Adige
EGI Foundation
Frantisek Krizik Grammar School and Primary School, s.r.o.
Hubrecht Institute & Westerdijk Fungal Biodiversity Institute (KNAW)
Institut Mines Telecom Business School & Telecom SudParis (new debug)
Mykolas Romeris University
Nuclear Research and consultancy Group
Observatoire de la Côte d'Azur
oldr3 Institut Mines Telecom Business School & Telecom SudParis
Pilsen City Library

https://wayf.nikhef.nl/



GitLab Community Edition

ername or email

ssword

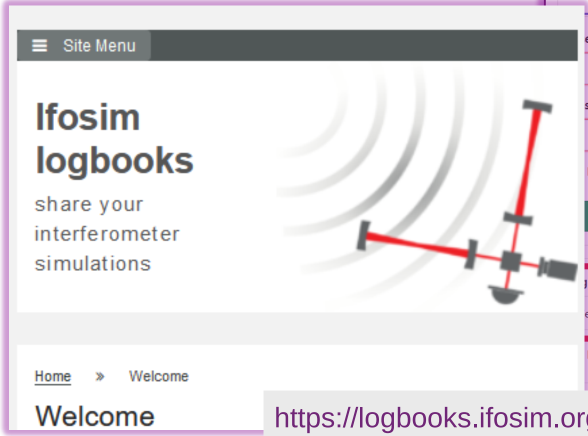
Remember me Forgot your password?

gn in with

ederated login

Remember me

https://gitlab.nikhef.nl/



Ifosim logbooks

share your interferometer simulations

Home » Welcome

Welcome

https://logbooks.ifosim.org/

ifosim federated AAI integration implementation by Mischa Sallé; per-country

Science infrastructures using our R&E ‘federated access’

About Services Solutions Projects Resources News & Events Participate

EMSO-ERIC

EMSO-ERIC, the European Multidisciplinary Seafloor and Water-Column Observatory to explore the Oceans. EGI Success Story.

Read more

EISCAT_3D

EISCAT_3D, the World's Leading Incoherent Scatter Radar. EGI Success Story.

Read more

OBSEA

OBSEA – Expandable Seafloor O... EGI Success Story

Read more

EOSC-WeNMR portals

Marketplace

300+ Content providers

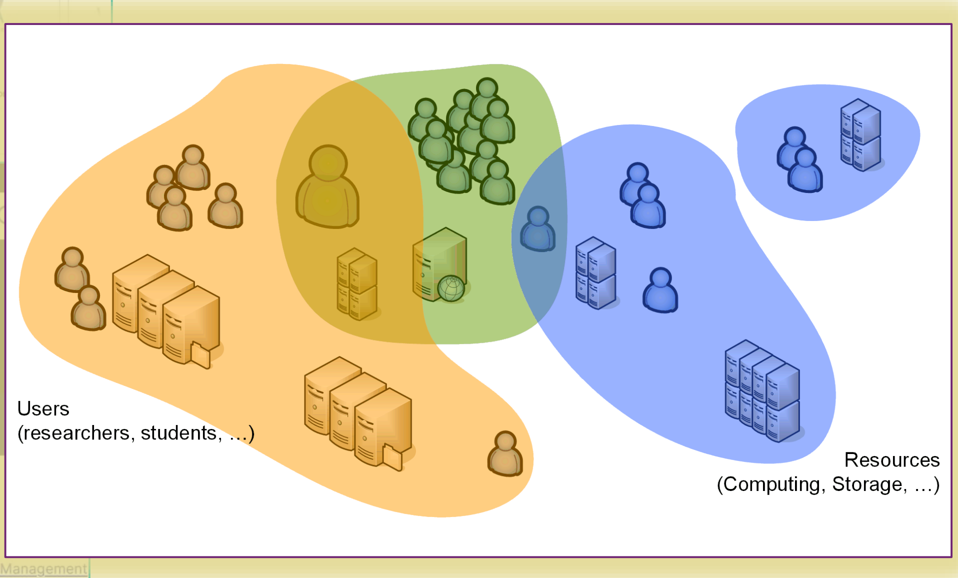
More

Storage

Research Data Management

science, cloud

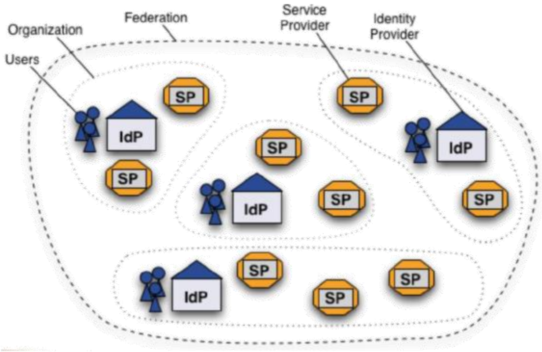
Research Infrastructures



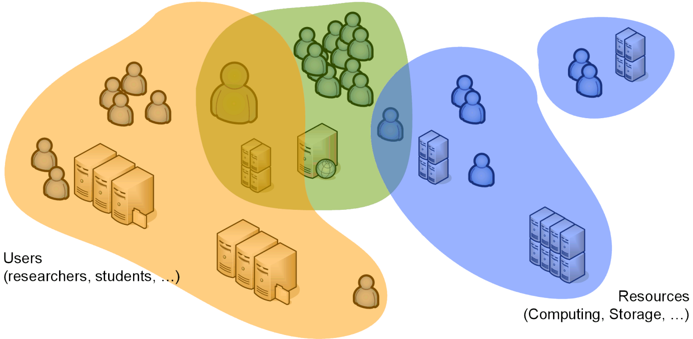
Images: CERN https://wlcg.web.cern.ch/; HADDOCK, WeNMR, @Bonvinlab https://wenmr.science.uu.nl/; Virgo, Pisa, IT; artist impression Einstein Telescope EMR region; EOSC portal in 2023, EGI catalogue https://www.egi.eu/

They look similar, yet they are not …

In the **Identity federation** picture, the source of authority is the *home organisation* via its IdP



In the **Community** picture, the source of authority is *the community itself*

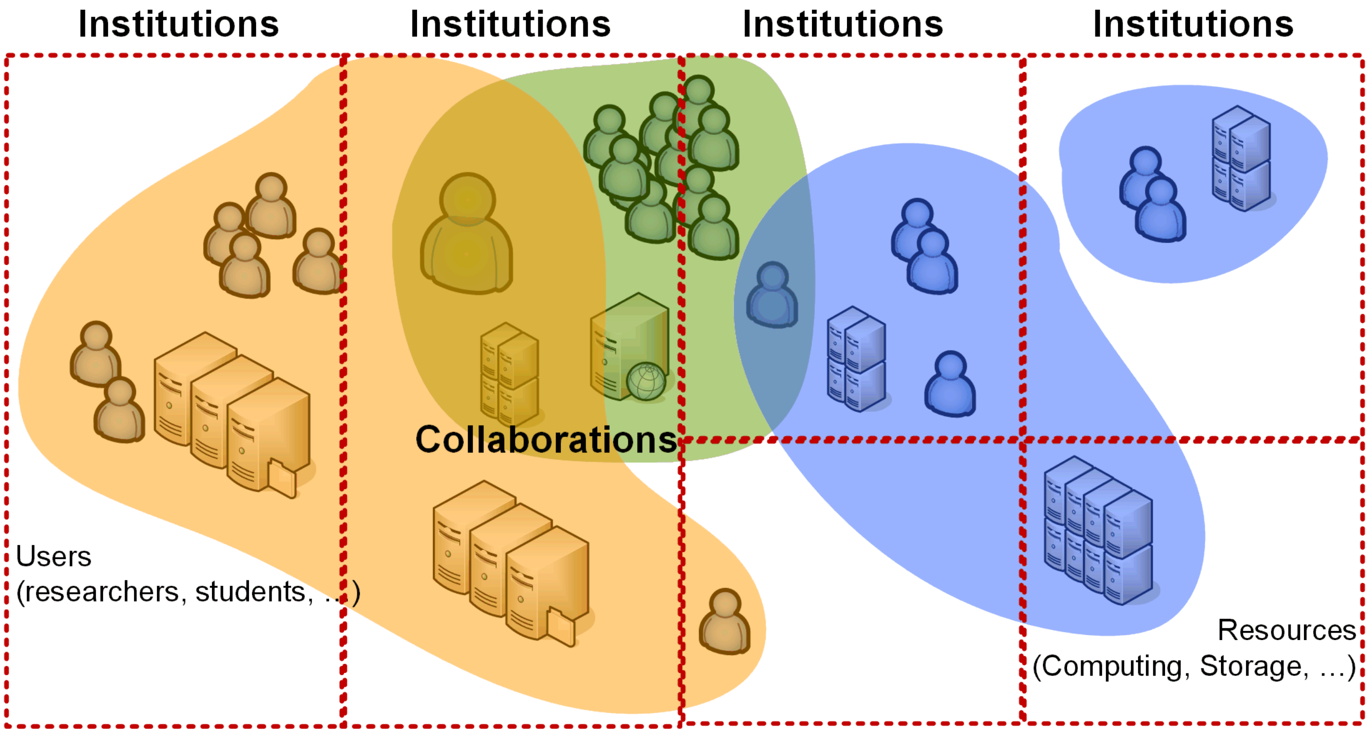


the AuthN-AuthZ separation is fundamental

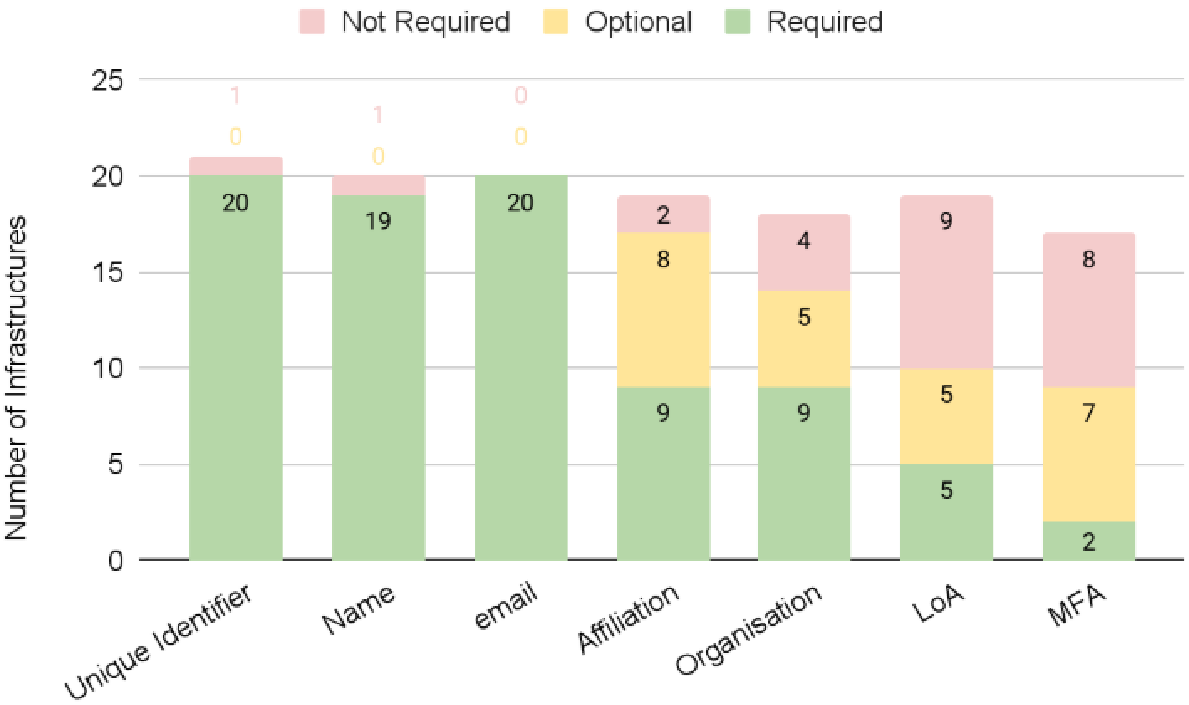
to the Federated (R&E) AAI, global IGTF PKI, VOMS, 'AARC BPA' AAI architecture …

Right-hand image: Shibboleth IdP federation, Lukas Hammerle, SWITCH (CH)

Since collaborations and institutions slice in different ways



Research Infrastructures: what they *actually* need from ‘home’



Glossary

Affiliation: what *type* of entity are you (student, faculty, alumnus, …)

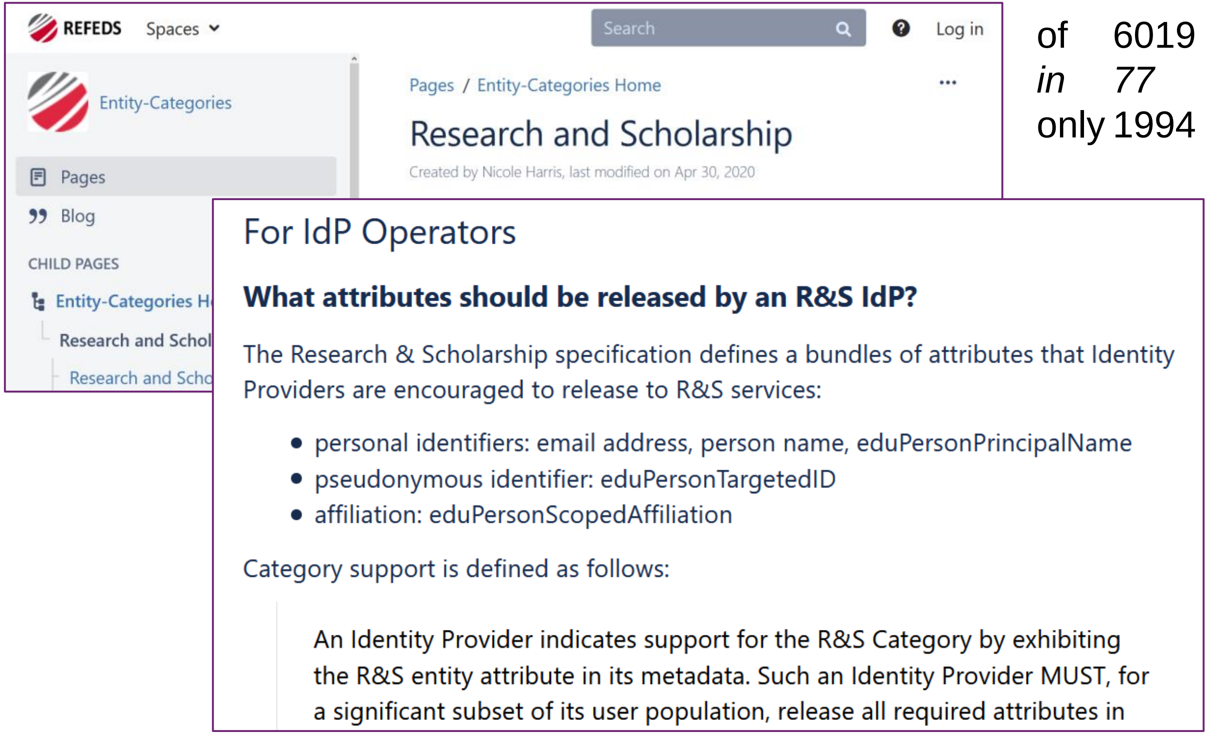
LoA: level of authentication assurance (like passport identity vetting and ‘freshness’ of data)

MFA: multi-factor authentication (password, 6-digit code, SMS, fingerprint)

Source: Marina Adomeit, Janos Mohasci, *et al.* AARC TREE Use-case collection and analysis (D3.2), 2025 (under review)

The one infra that did ‘not need a unique identifier’ actually stated: “<our infra> assingns own identifier upon registration” – so the unique identifier is *still* there!

For starters: sharing good user identifiers is non-trivial ☹



Pages / Entity-Categories Home

Research and Scholarship

Created by Nicole Harris, last modified on Apr 30, 2020

For IdP Operators

What attributes should be released by an R&S IdP?

The Research & Scholarship specification defines a bundles of attributes that Identity Providers are encouraged to release to R&S services:

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

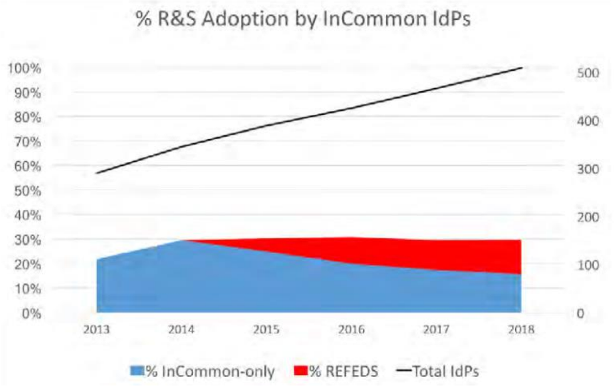
Category support is defined as follows:

> An Identity Provider indicates support for the R&S Category by exhibiting the R&S entity attribute in its metadata. Such an Identity Provider MUST, for a significant subset of its user population, release all required attributes in

of 6019 identity providers
in 77 federations,
only 1994 support R&S or Personalised access

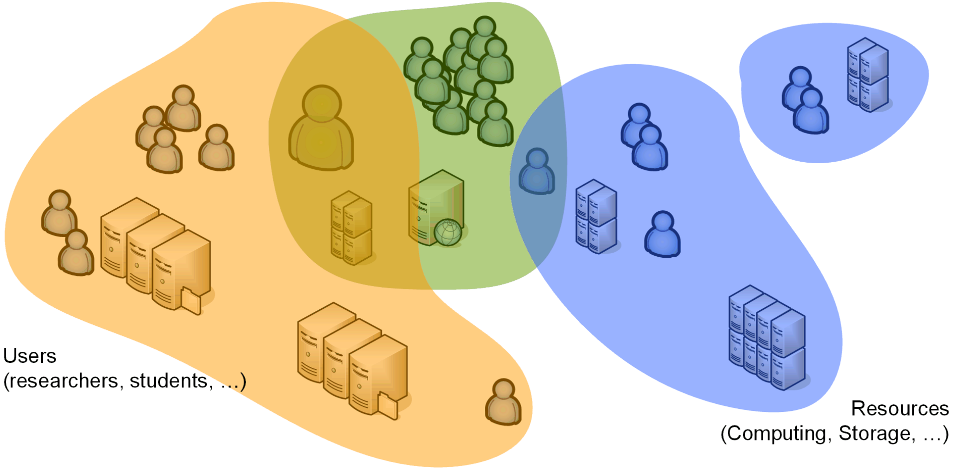
33%

~ constant since 2018 ☹

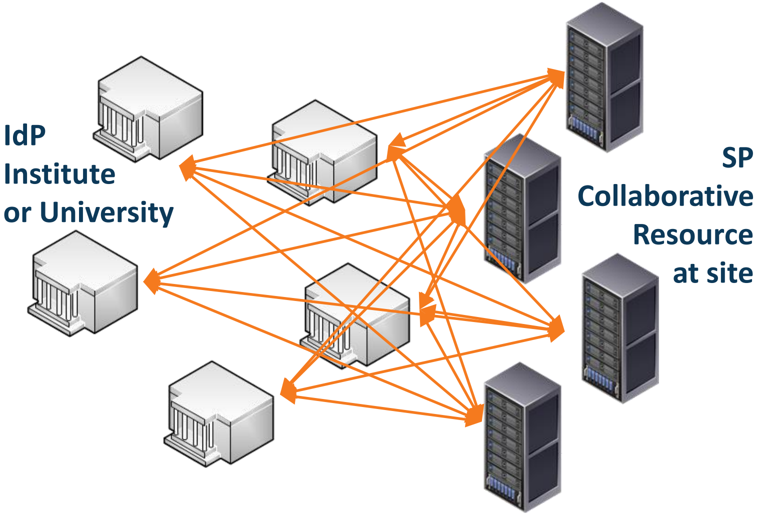


Graph: InCommon: Attributes-WG-Recommendations-May2018.pdf; Entity Category stats as per 2025-03-03, from https://technical.edugain.org/entities

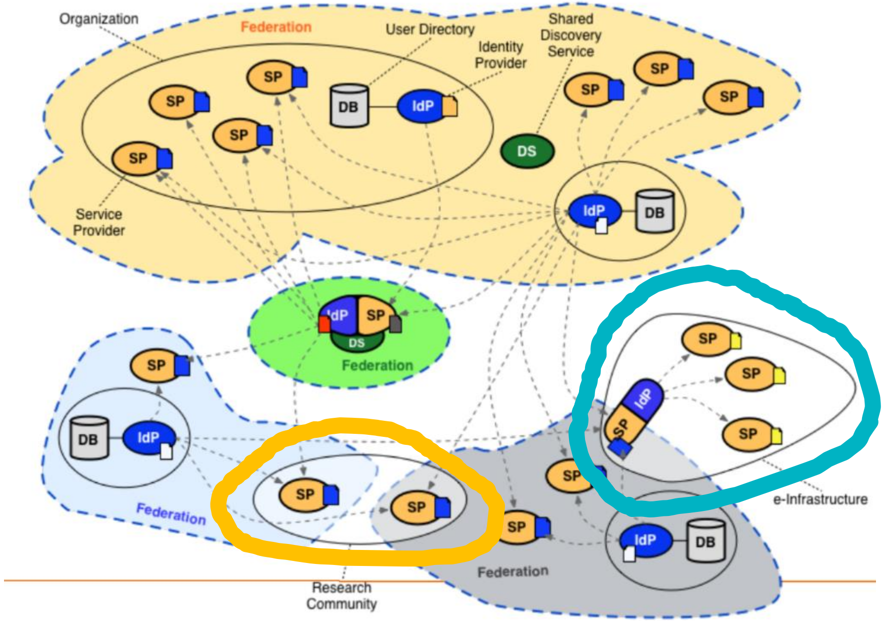
A fundamental scaling issue remained unique to research



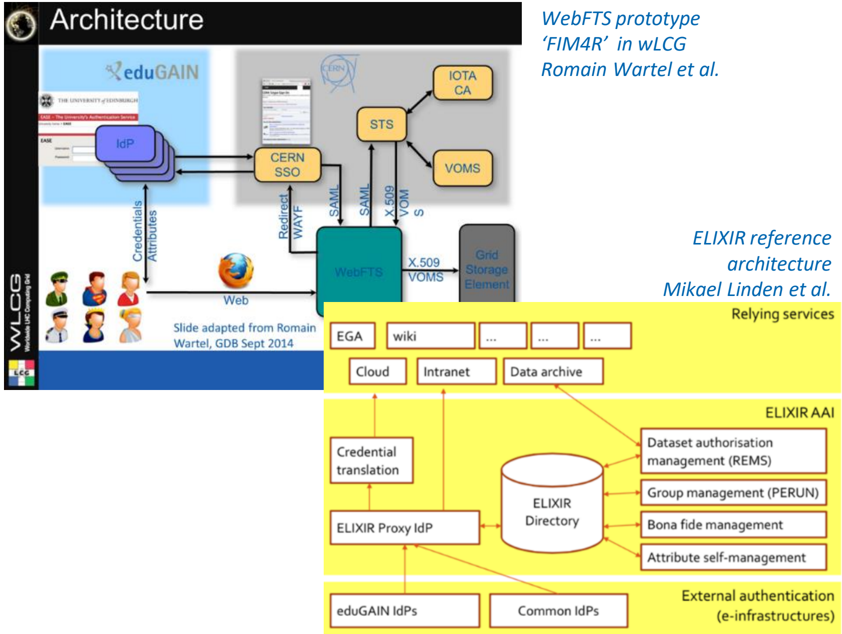
for identity and user data
‘n x m’ agreements remain(ed)



Managing complexity: distributed diverse identity sources



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



WebFTS prototype ‘FIM4R’ in wLCG Romain Wartel et al.

ELIXIR reference architecture Mikael Linden et al.

but most communities had started to invent their own ‘proxy’ model to abstract complexity

Community images: Romain Wartel, CERN; Mikael Linden, CSC; Federation image (R): Lukas Hammerle, SWITCH

The IdP-SP bridge

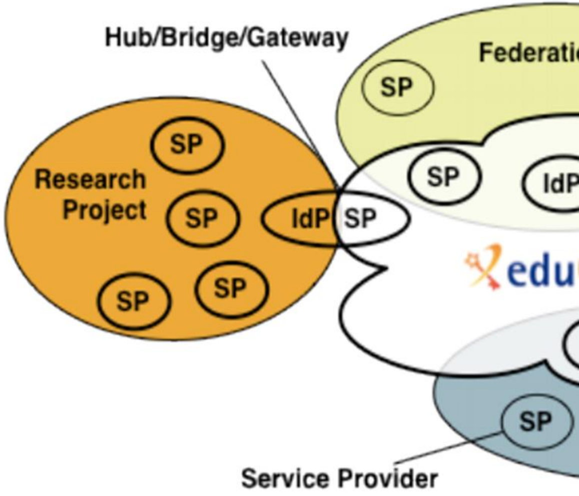
- Access services using **identities from users' Home Organizations**,
- but **hide complexity** of multiple IdPs, federations,

  and different technologies for authentication and authorisation
- **One persistent identity**

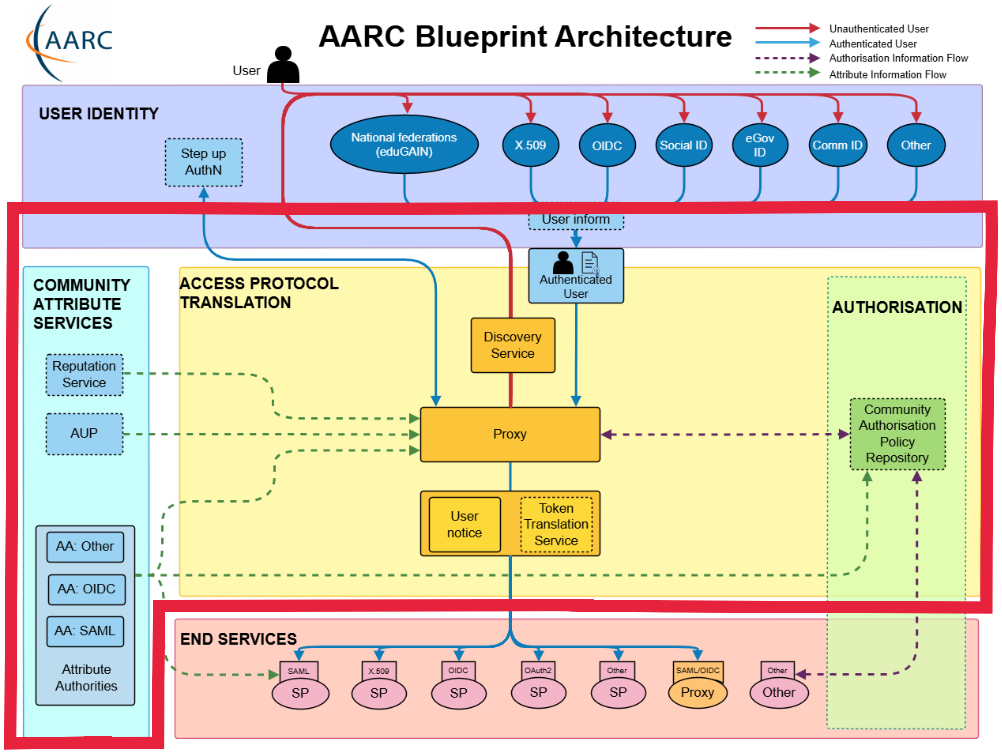
  across all the community's services through **account linking**
- **Access** services

  based on role(s) users have **in the collaboration**.
- For both **web** and **non-web** resources
- Integration of **guest identity solutions**
- **Support for stronger authentication assurance** mechanisms

often known as proxy!



AARC Blueprint – making the bridge a first-class citizen



AARC BPA 2019 ‘Community First’
https://aarc-community.org/guidelines/aarc-g045/

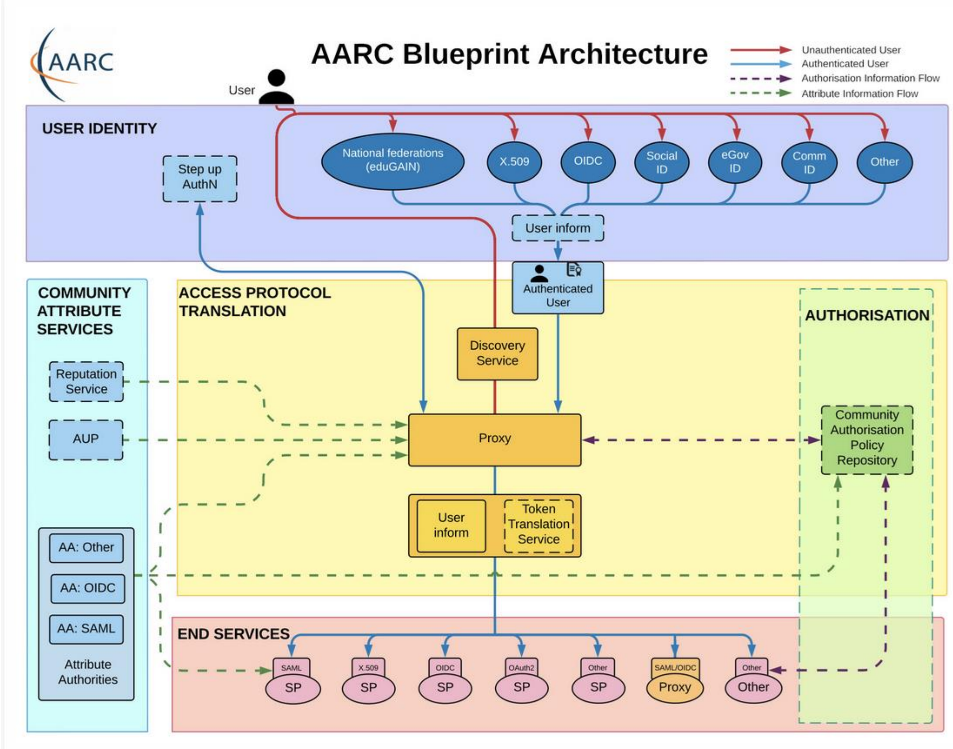
Manage users and access rights

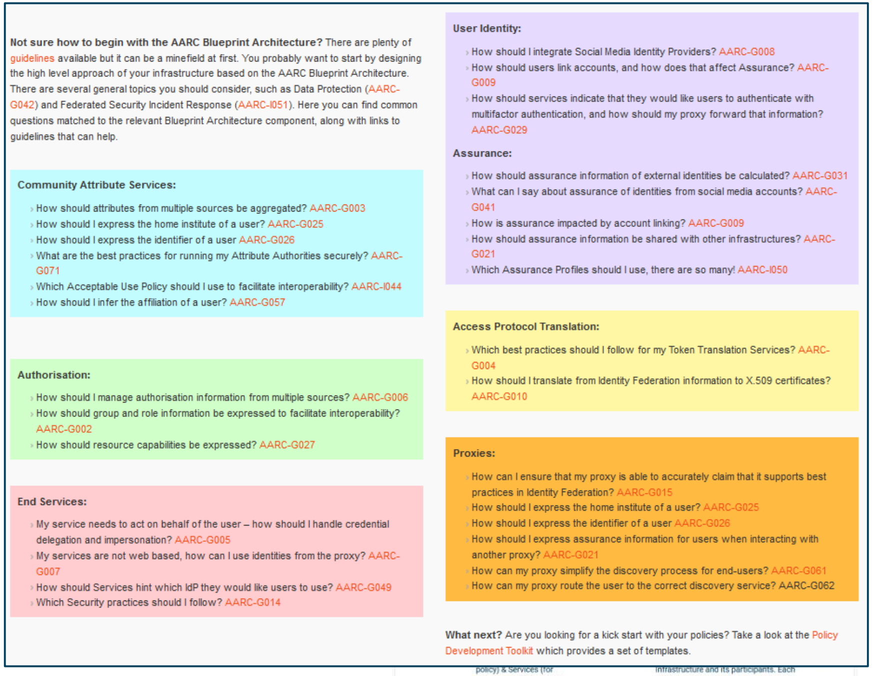
with interoperable **building blocks for ‘AAI infrastructure’ architects**

that are

- technology-agnostic
- have multiple implementations
- come with policy templates & good practice guides

More than just nice colours





Not sure how to begin with the AARC Blueprint Architecture? There are plenty of guidelines available but it can be a minefield at first. You probably want to start by designing the high level approach of your infrastructure based on the AARC Blueprint Architecture. There are several general topics you should consider, such as Data Protection (AARC-G042) and Federated Security Incident Response (AARC-I051). Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

Community Attribute Services:

- How should attributes from multiple sources be aggregated? AARC-G003
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- What are the best practices for running my Attribute Authorities securely? AARC-G071
- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044
- How should I infer the affiliation of a user? AARC-G057

Authorisation:

- How should I manage authorisation information from multiple sources? AARC-G006
- How should group and role information be expressed to facilitate interoperability? AARC-G002
- How should resource capabilities be expressed? AARC-G027

End Services:

- My service needs to act on behalf of the user – how should I handle credential delegation and impersonation? AARC-G005
- My services are not web based, how can I use identities from the proxy? AARC-G007
- How should Services hint which IdP they would like users to use? AARC-G049
- Which Security practices should I follow? AARC-G014

User Identity:

- How should I integrate Social Media Identity Providers? AARC-G008
- How should users link accounts, and how does that affect Assurance? AARC-G009
- How should services indicate that they would like users to authenticate with multifactor authentication, and how should my proxy forward that information? AARC-G029

Assurance:

- How should assurance information of external identities be calculated? AARC-G031
- What can I say about assurance of identities from social media accounts? AARC-G041
- How is assurance impacted by account linking? AARC-G009
- How should assurance information be shared with other infrastructures? AARC-G021
- Which Assurance Profiles should I use, there are so many! AARC-I050

Access Protocol Translation:

- Which best practices should I follow for my Token Translation Services? AARC-G004
- How should I translate from Identity Federation information to X.509 certificates? AARC-G010

Proxies:

- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? AARC-G015
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- How should I express assurance information for users when interacting with another proxy? AARC-G021
- How can my proxy simplify the discovery process for end-users? AARC-G061
- How can my proxy route the user to the correct discovery service? AARC-G062

What next? Are you looking for a kick start with your policies? Take a look at the Policy Development Toolkit which provides a set of templates.

	policy) & Services (for service specific policies)		Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.	
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.	Google Doc
Acceptable Use Policy	Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)	Users (abide by)	This is a template for the acceptable u policy that users must acce Research Infrastructure. It sh augmented by the Research C	oogle

Showing 1 to 9 of 9 entries

Previous Next

PDK

https://aarc-community.org/guidelines/

“Your attention to detail is appreciated”

Even a simple challenge …

“How to communicate affiliation of a user with the community”

needs standards for interoperability!

- AARC-G025 – Guidelines for expressing affiliation information
- AARC-G057 – Inferring and constructing voPersonExternalAffiliation

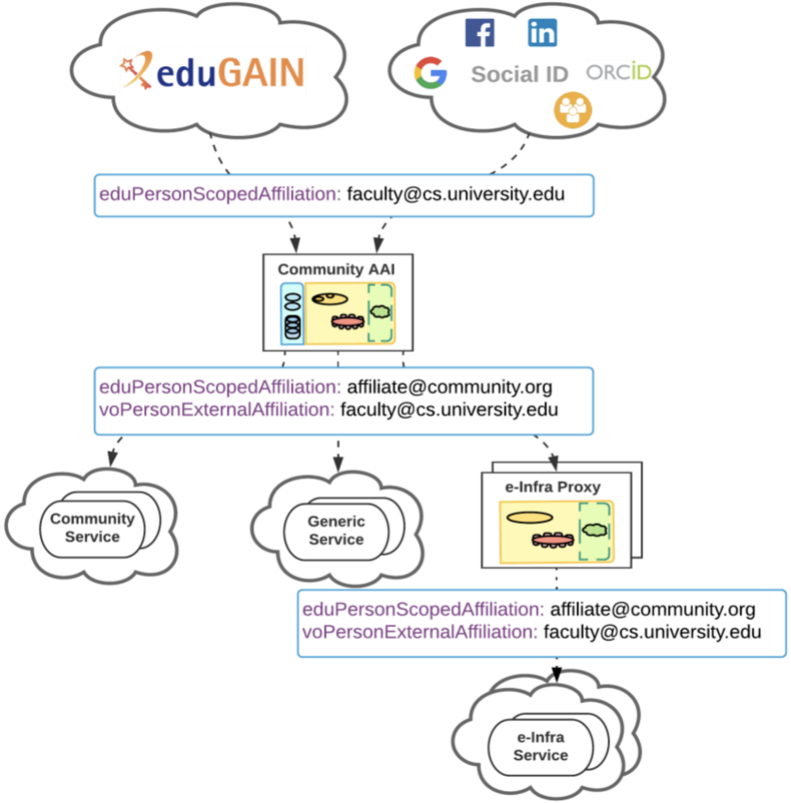
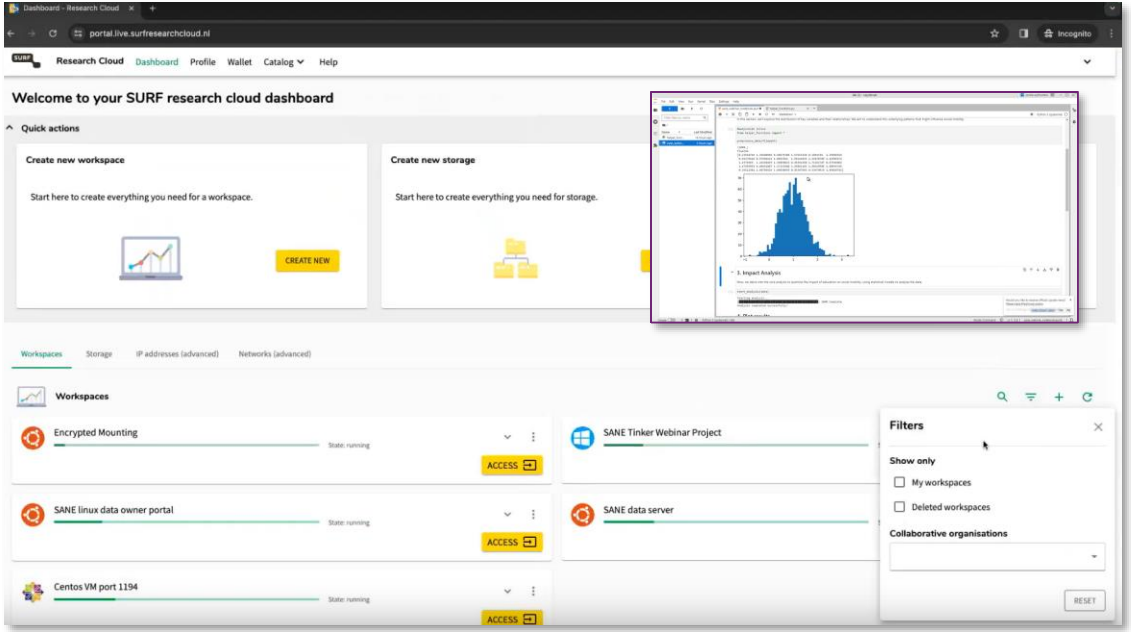

eduGAIN
Social ID
ORCID
eduPersonScopedAffiliation: faculty@cs.university.edu
Community AAI
eduPersonScopedAffiliation: affiliate@community.org
voPersonExternalAffiliation: faculty@cs.university.edu
Community Service
Generic Service
e-Infra Proxy
eduPersonScopedAffiliation: affiliate@community.org
voPersonExternalAffiliation: faculty@cs.university.edu
e-Infra Service

Image: Guideline AARC-G025 (AARC community); quote from the MoinMoin wiki software

Example: SURF Research Cloud Secure Supercomputing



Welcome to your SURF research cloud dashboard

Quick actions

Create new workspace

Start here to create everything you need for a workspace.

CREATE NEW

Create new storage

Start here to create everything you need for storage.

Workspaces | Storage | IP addresses (advanced) | Networks (advanced)

Workspaces

- Encrypted Mounting — State: running — ACCESS
- SANE Tinker Webinar Project
- SANE linux data owner portal — State: running — ACCESS
- SANE data server
- Centos VM port 1194 — State: running — ACCESS

Filters

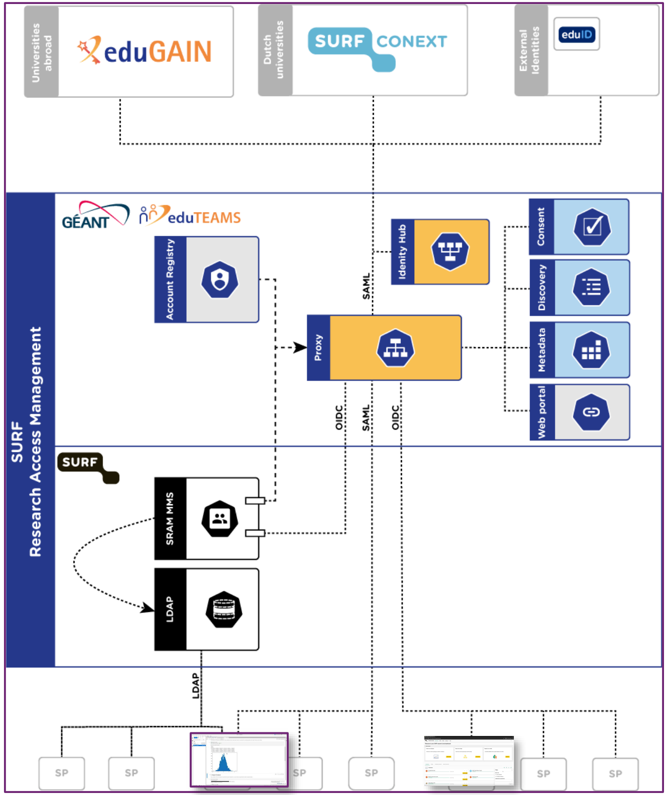
Show only

☐ My workspaces

☐ Deleted workspaces

Collaborative organisations

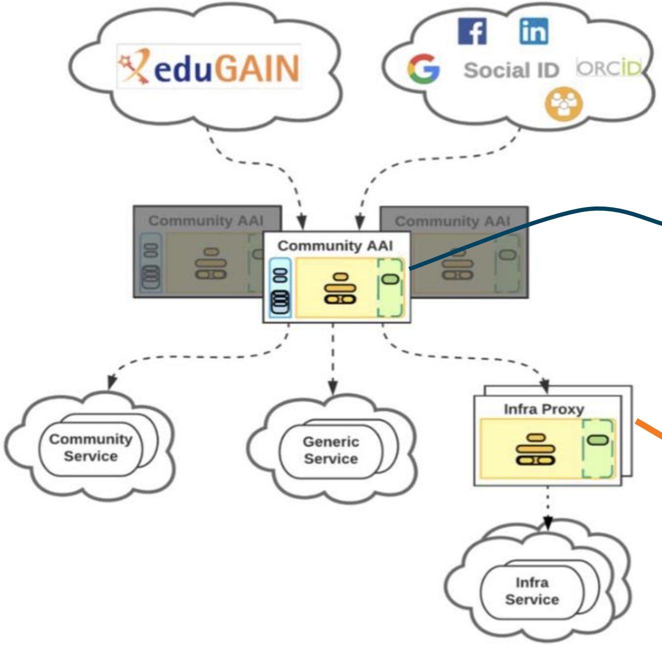
RESET



SURF SRAM architecture, Raoul Teeuwen *et al.* from https://servicedesk.surf.nl/wiki/display/IAM/Dienstbeschrijving+SURF+Research+Access+Management

SURF Research Cloud capture: from Introduction to SANE (Secure ANalysis Environment) webinar February 2024, by Martin Brandt et al., SURF https://www.surf.nl/themas/onderzoeksinfrastructuur/sane-veilige-omgeving-voor-analyse-van-gevoelige-data

… but one proxy is not enough in a research cloud



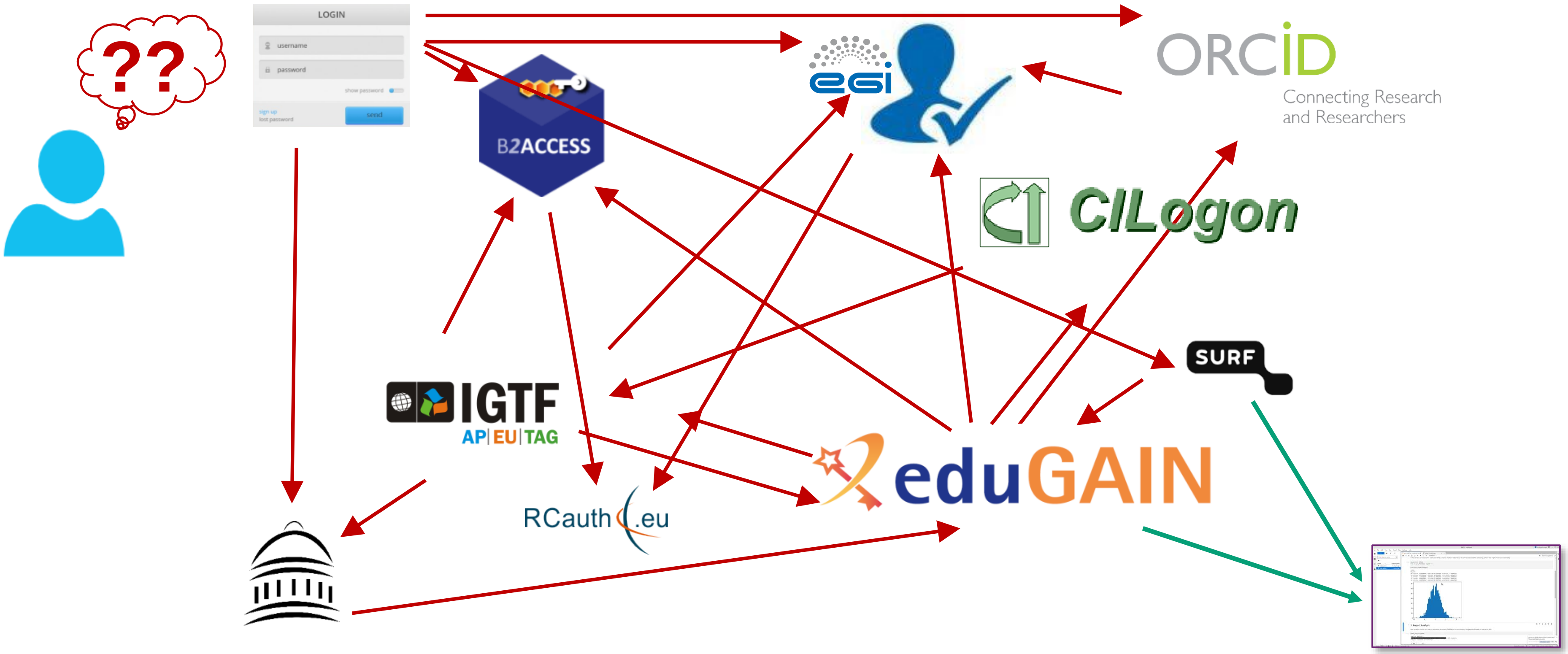
Community AAI

streamline researchers’ access to services,
both those provided by their own infrastructure
as well as the services provided
by shared infrastructures from other communities.

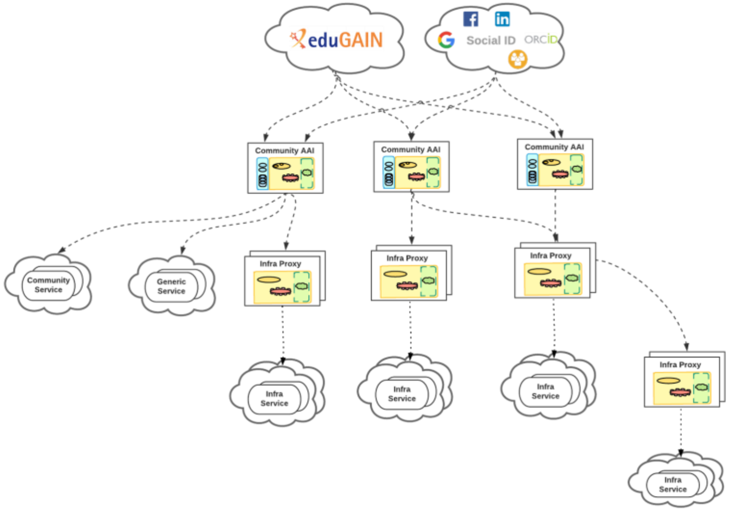
Infrastructure Proxy

enables Infrastructures with large number of resources,
to provide them through a single integration point,
where the Infrastructure can maintain centrally
all the relevant Policies and business logic
for making available resources to multiple communities

Identity spaghetti: 1-loop, 2-loop and higher order diagrams

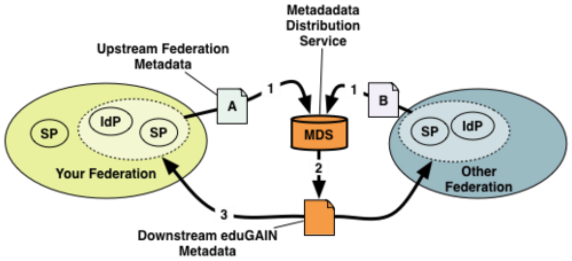


We have seen many arrows before … it needs federation!



Identity, community, infrastructure proxies and services form a ***federation of proxies***

- bilateral registration
  but then you have a scalability issue again
- meta-data distribution of trust paths
  - **OpenID Federation**
  - **SAML** meta-data



Metadadata Distribution Service
Upstream Federation Metadata
A
1
1
B
MDS
SP
IdP
SP
Your Federation
SP
IdP
Other Federation
2
3
Downstream eduGAIN Metadata

- discovery and identity provider hinting

European Open Science Cloud federation (2023 edition)

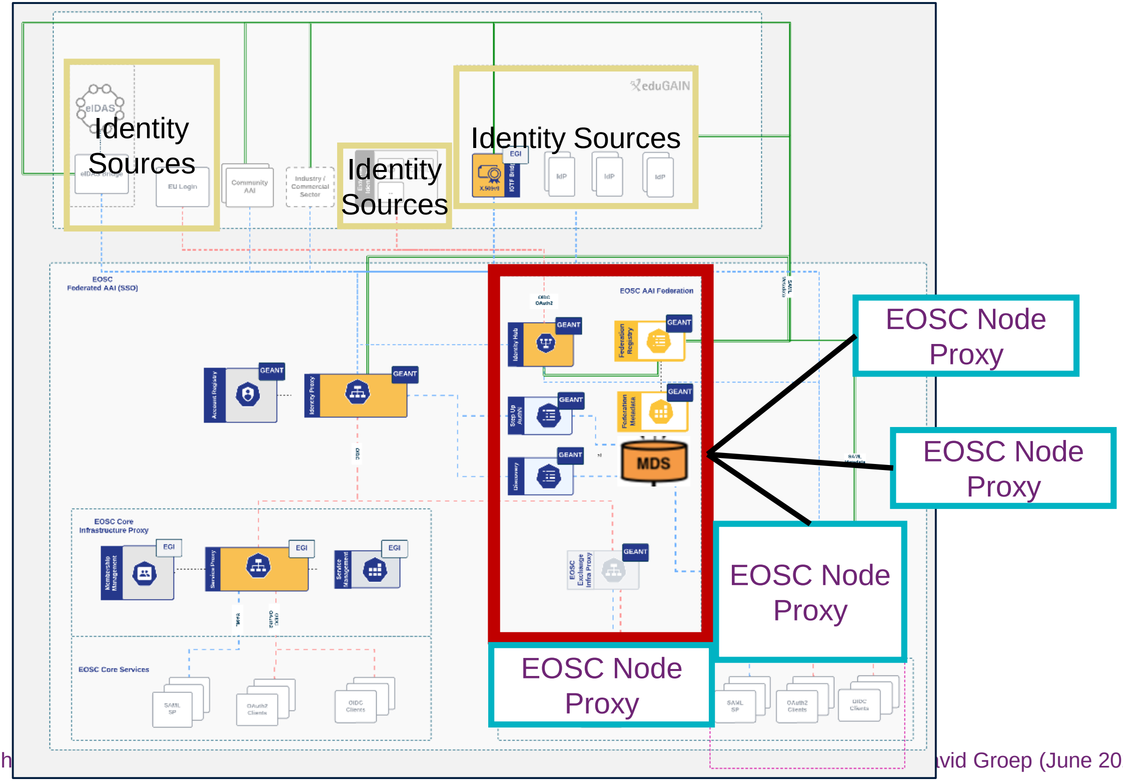
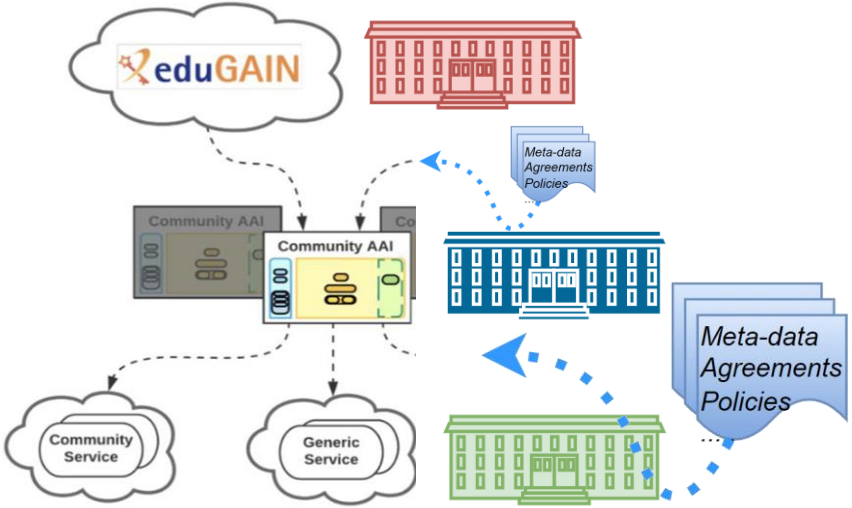


Image: EOSC AAI for the EOSC Core and Exch vid Groep (June 2023)

And we need to ‘decorate’ the arrows with trust

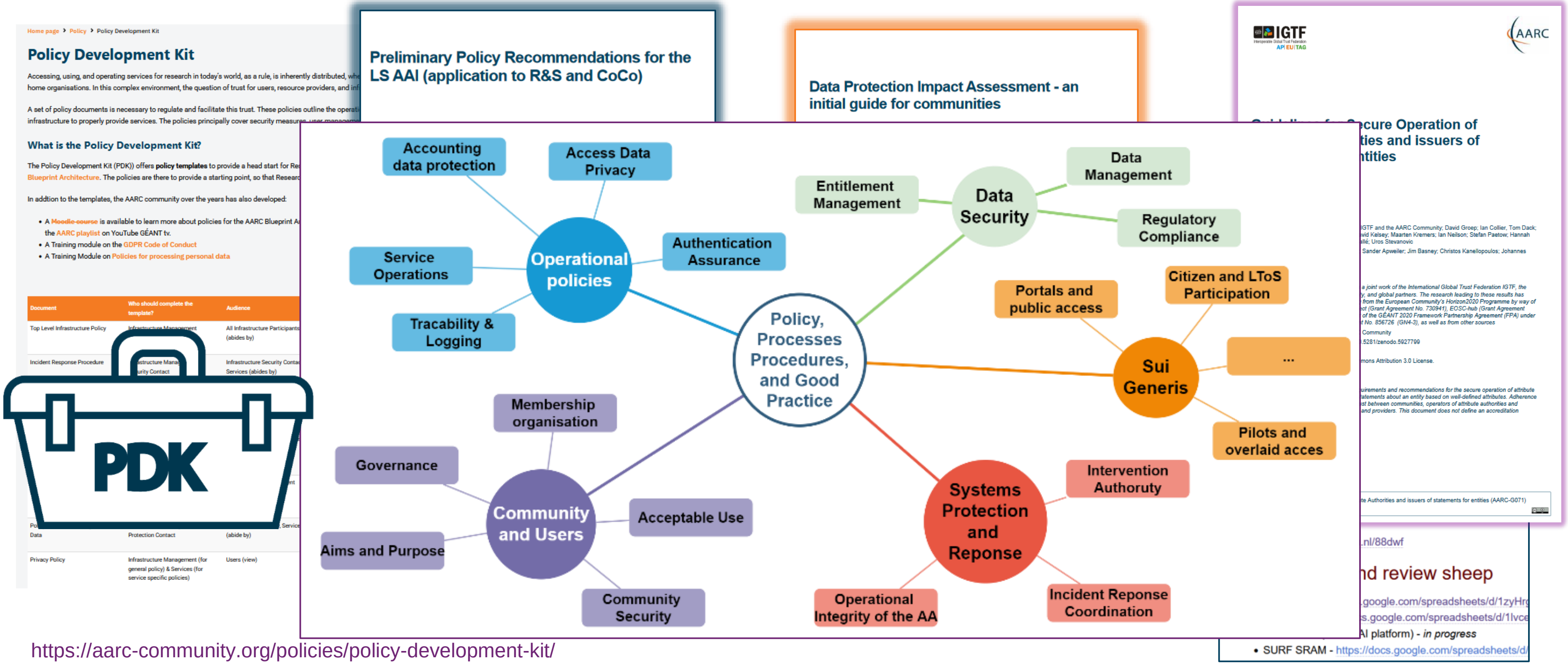


Each side of each arrow has *independent* parties

- we allow *them* to do part of the work *we* would otherwise do
- to make it easier and faster for users to perform their research
- but **we relinquish some control** beyond our organisation, our own policies, our own jurisdiction

***Why* would we trust them to do that?**

Structuring trust 'between boxes and arrows' is complex!



Home page › Policy › Policy Development Kit

Policy Development Kit

Accessing, using, and operating services for research in today's world, as a rule, is inherently distributed, whe
home organisations. In this complex environment, the question of trust for users, resource providers, and inf

A set of policy documents is necessary to regulate and facilitate this trust. These policies outline the operati
infrastructure to properly provide services. The policies principally cover security measures, user manageme

What is the Policy Development Kit?

The Policy Development Kit (PDK)) offers **policy templates** to provide a head start for Re
Blueprint Architecture. The policies are there to provide a starting point, so that Researc

In addtion to the templates, the AARC community over the years has also developed:

- A ~~Moodle course~~ is available to learn more about policies for the AARC Blueprint A
the AARC playlist on YouTube GÉANT tv.
- A Training module on the GDPR Code of Conduct
- A Training Module on Policies for processing personal data

Document	Who should complete the template?	Audience
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)
Incident Response Procedure	astructure Manag urity Contact	Infrastructure Security Conta Services (abides by)
		ent
Po Data	Protection Contact	, Service (abide by)
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)

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

Data Protection Impact Assessment - an initial guide for communities

IGTF
API EU TAG
AARC

cure Operation of
ties and issuers of
ntities

IGTF and the AARC Community; David Groep; Ian Collier, Tom Dack;
vid Kelsey; Maarten Kremers; Ian Neilson; Stefan Paetow; Hannah
allé; Uros Stevanovic

Sander Apweiler; Jim Basney; Christos Kanellopoulos; Johannes

a joint work of the International Global Trust Federation IGTF, the
y, and global partners. The research leading to these results has
from the European Community's Horizon2020 Programme by way of
ct (Grant Agreement No. 730941), EOSC-hub (Grant Agreement
of the GÉANT 2020 Framework Partnership Agreement (FPA) under
t No. 856726 (GN4-3), as well as from other sources

Community

.5281/zenodo.5927799

mons Attribution 3.0 License.

uirements and recommendations for the secure operation of attribute
tatements about an entity based on well-defined attributes. Adherence
st between communities, operators of attribute authorities and
and providers. This document does not define an accreditation

te Authorities and issuers of statements for entities (AARC-G071)

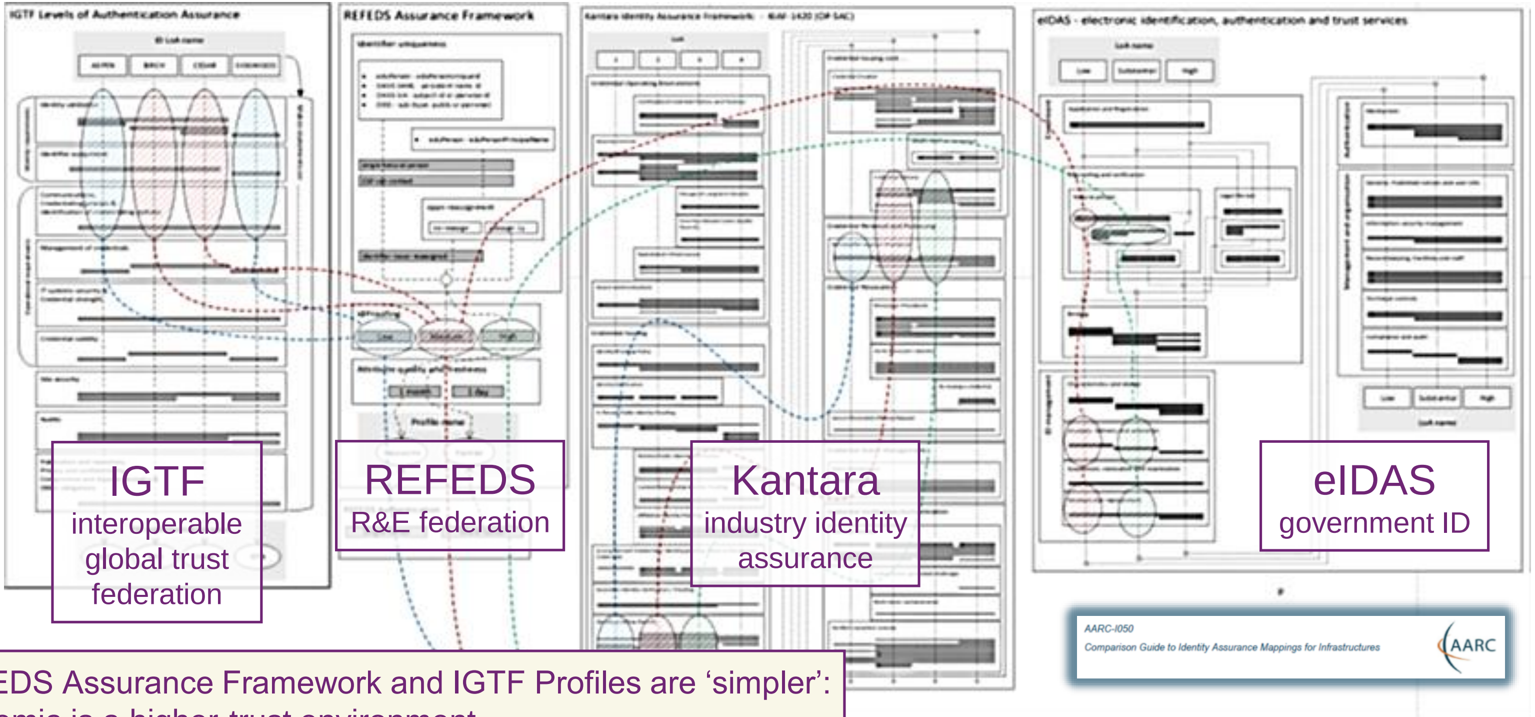
.nl/88dwf

nd review sheep

- google.com/spreadsheets/d/1zyHrg
- s.google.com/spreadsheets/d/1lvce
- AI platform) - *in progress*
- SURF SRAM - https://docs.google.com/spreadsheets/d/

https://aarc-community.org/policies/policy-development-kit/

And even a simple ‘Who are you?’ is not always easy …


IGTF Levels of Authentication Assurance
REFEDS Assurance Framework
Kantara Identity Assurance Framework
eIDAS - electronic identification, authentication and trust services
AARC-I050
Comparison Guide to Identity Assurance Mappings for Infrastructures
AARC

IGTF
interoperable
global trust
federation

REFEDS
R&E federation

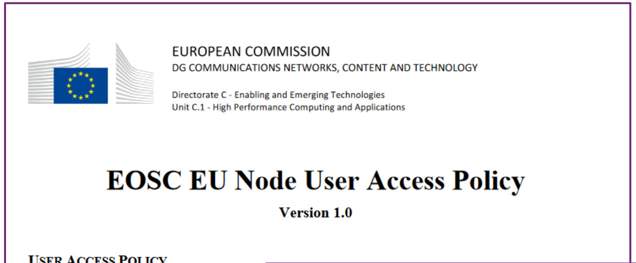
Kantara
industry identity
assurance

eIDAS
government ID

REFEDS Assurance Framework and IGTF Profiles are ‘simpler’:
academia is a higher-trust environment,
leveraging self-assessed peer review

Source: https://aarc-community.org/guidelines/aarc-i050, Ian Neilson et al.

Helping community and users: how much clicking through?



EUROPEAN COMMISSION
DG COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

Directorate C - Enabling and Emerging Technologies
Unit C.1 - High Performance Computing and Applications

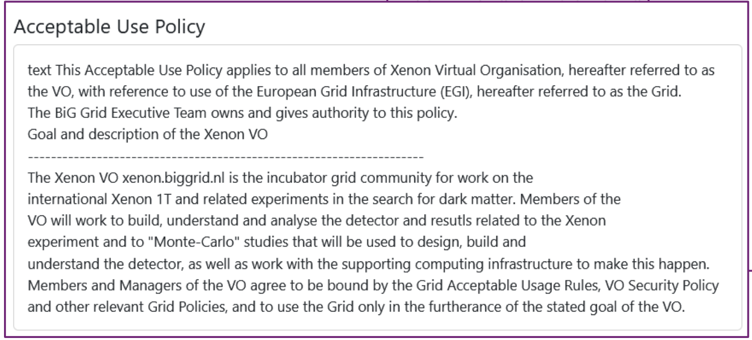
EOSC EU Node User Access Policy

Version 1.0

USER ACCESS POLICY

1. **Purpose**

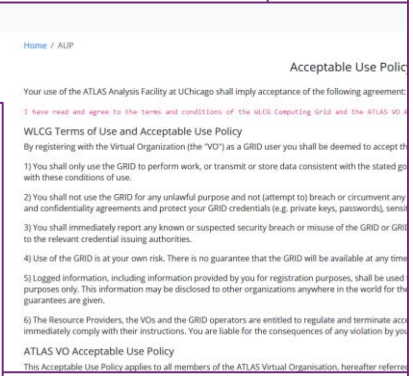
This User Access Policy ("UAP") defi



Acceptable Use Policy

text This Acceptable Use Policy applies to all members of Xenon Virtual Organisation, hereafter referred to as the VO, with reference to use of the European Grid Infrastructure (EGI), hereafter referred to as the Grid.
The BiG Grid Executive Team owns and gives authority to this policy.
Goal and description of the Xenon VO

The Xenon VO xenon.biggrid.nl is the incubator grid community for work on the international Xenon 1T and related experiments in the search for dark matter. Members of the VO will work to build, understand and analyse the detector and resutls related to the Xenon experiment and to "Monte-Carlo" studies that will be used to design, build and understand the detector, as well as work with the supporting computing infrastructure to make this happen.
Members and Managers of the VO agree to be bound by the Grid Acceptable Usage Rules, VO Security Policy and other relevant Grid Policies, and to use the Grid only in the furtherance of the stated goal of the VO.



Home / AUP

Acceptable Use Polic

Your use of the ATLAS Analysis Facility at UChicago shall imply acceptance of the following agreement:

`I have read and agree to the terms and conditions of the WLCG Computing Grid and the ATLAS VO A`

WLCG Terms of Use and Acceptable Use Policy

By registering with the Virtual Organization (the "VO") as a GRID user you shall be deemed to accept th

1) You shall only use the GRID to perform work, or transmit or store data consistent with the stated go with these conditions of use.

2) You shall not use the GRID for any unlawful purpose and not (attempt to) breach or circumvent any and confidentiality agreements and protect your GRID credentials (e.g. private keys, passwords), sensi

3) You shall immediately report any known or suspected security breach or misuse of the GRID or GRI to the relevant credential issuing authorities.

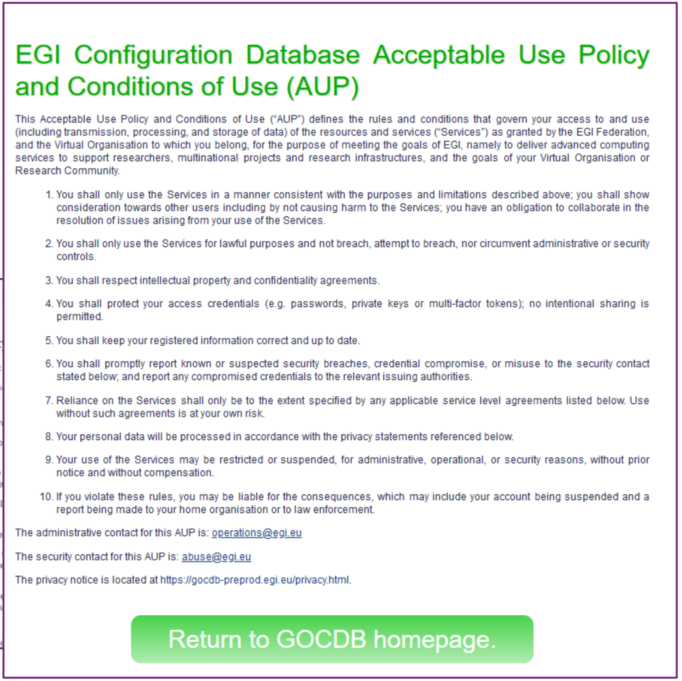
4) Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time

5) Logged information, including information provided by you for registration purposes, shall be used purposes only. This information may be disclosed to other organizations anywhere in the world for the guarantees are given.

6) The Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate acc immediately comply with their instructions. You are liable for the consequences of any violation by you

ATLAS VO Acceptable Use Policy

This Acceptable Use Policy applies to all members of the ATLAS Virtual Organisation, hereafter referre



EGI Configuration Database Acceptable Use Policy and Conditions of Use (AUP)

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by the EGI Federation, and the Virtual Organisation to which you belong, for the purpose of meeting the goals of EGI, namely to deliver advanced computing services to support researchers, multinational projects and research infrastructures, and the goals of your Virtual Organisation or Research Community.

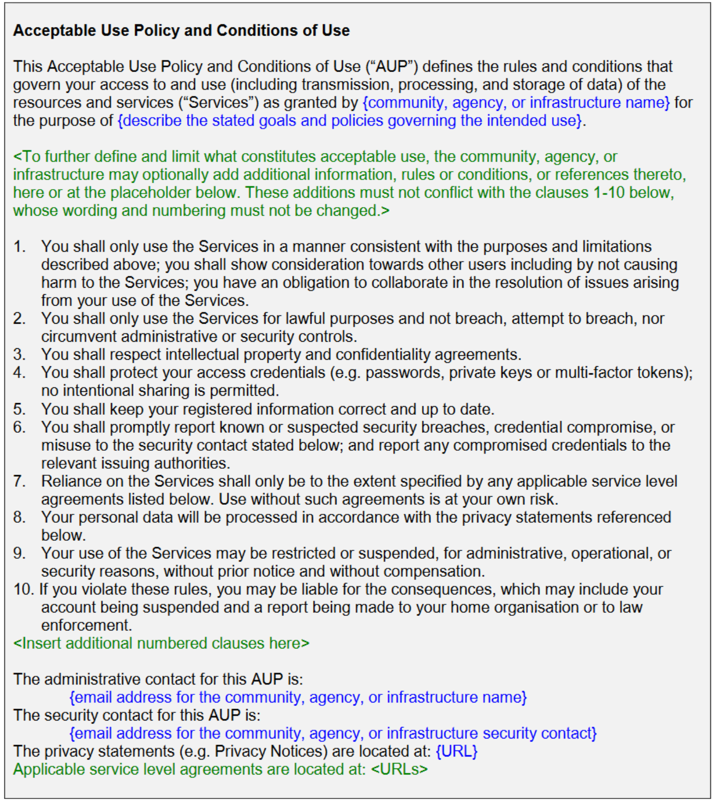
1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.

The administrative contact for this AUP is: operations@egi.eu

The security contact for this AUP is: abuse@egi.eu

The privacy notice is located at https://gocdb-preprod.egi.eu/privacy.html.

Good common practice: the WISE Baseline AUP



Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use (“AUP”) defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services (“Services”) as granted by {community, agency, or infrastructure name} for the purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed.>

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.

<Insert additional numbered clauses here>

The administrative contact for this AUP is:
{email address for the community, agency, or infrastructure name}
The security contact for this AUP is:
{email address for the community, agency, or infrastructure security contact}
The privacy statements (e.g. Privacy Notices) are located at: {URL}
Applicable service level agreements are located at: <URLs>

Purpose binding
ensure use is as intended for access grant

Terms and Conditions
research data access conditions, permits, grant conditions

WISE Baseline AUP
common 10 commandments that allow seamless cross-sectoral user movement

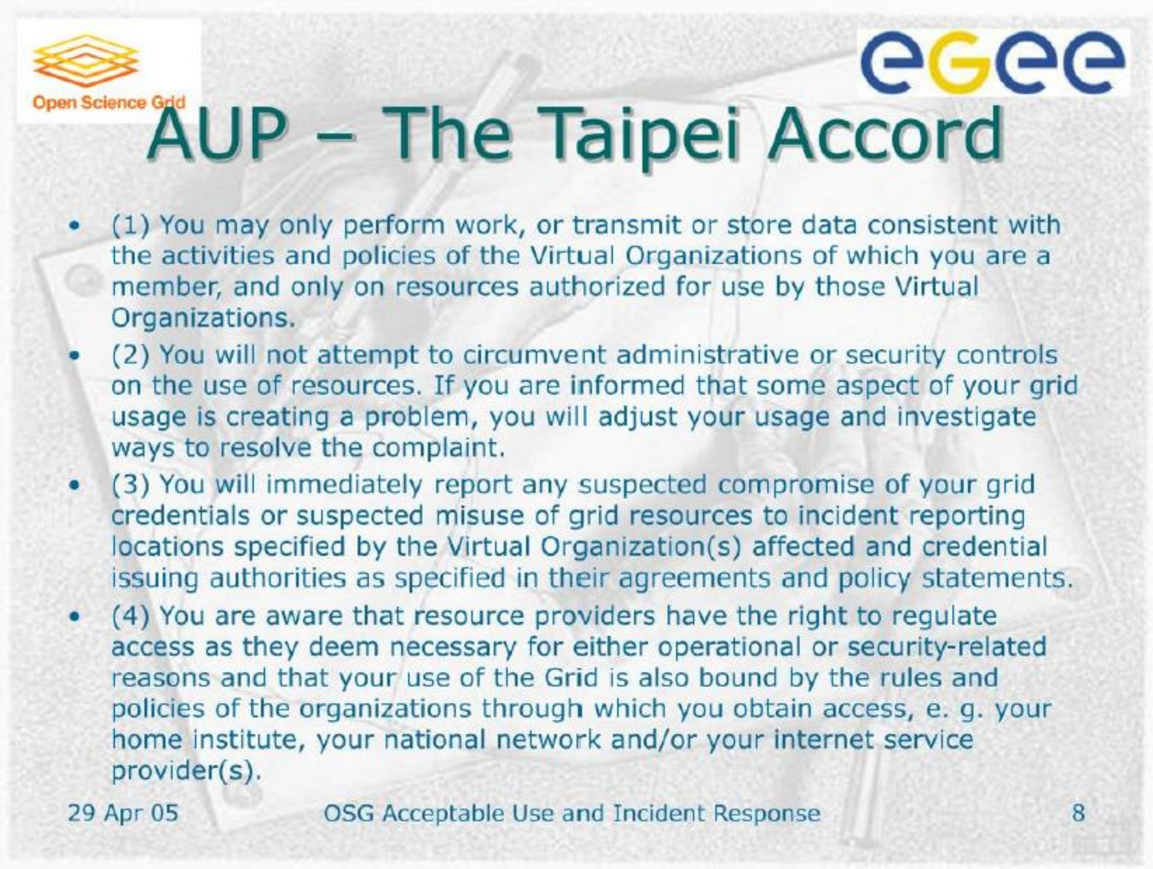
Service level agreements
promises and recourse

Privacy notice references
for *access* personal data policies

Guidance for Notice Management by Proxies

https://wise-community.org/wise-baseline-aup/

It all started here!



Open Science Grid

egee

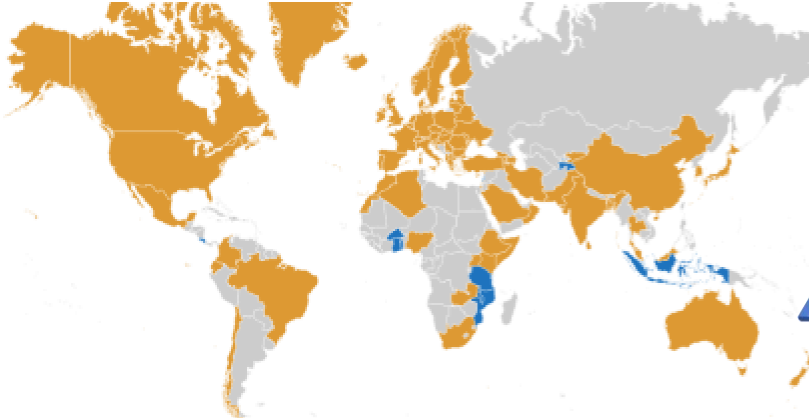
AUP – The Taipei Accord

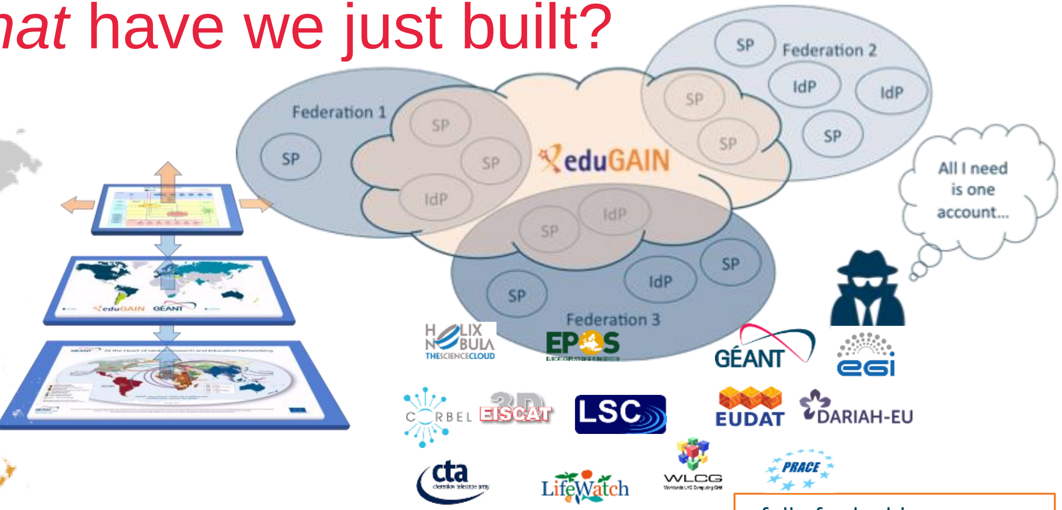
- (1) You may only perform work, or transmit or store data consistent with the activities and policies of the Virtual Organizations of which you are a member, and only on resources authorized for use by those Virtual Organizations.
- (2) You will not attempt to circumvent administrative or security controls on the use of resources. If you are informed that some aspect of your grid usage is creating a problem, you will adjust your usage and investigate ways to resolve the complaint.
- (3) You will immediately report any suspected compromise of your grid credentials or suspected misuse of grid resources to incident reporting locations specified by the Virtual Organization(s) affected and credential issuing authorities as specified in their agreements and policy statements.
- (4) You are aware that resource providers have the right to regulate access as they deem necessary for either operational or security-related reasons and that your use of the Grid is also bound by the rules and policies of the organizations through which you obtain access, e. g. your home institute, your national network and/or your internet service provider(s).

29 Apr 05 OSG Acceptable Use and Incident Response 8

Bob Cowles *Acceptable Use Policy and Security Incident Response Strategy in the Open Science Grid* – ISGC, 29 April 2005

What about *unacceptable* use? “who dunnit” essential for incident response, but *what* have we just built?





full of valuable resources (data, network, services)

So we have federation and single sign-on …
… but can we respond if something goes haywire?
… can we share security incident information when needed?
… timely and confidentially, protecting everyone’s reputation?

left: eduGAIN interfederation in 2025 (https://technical.edugain.org/status); logos on the right from the European e-Infrastructures and ESFRIs; center graphic: AARC

‘Sirtfi’ – what makes federated security different?

SIRTFI
Security Incident Response Trust Framework for Federated Identity

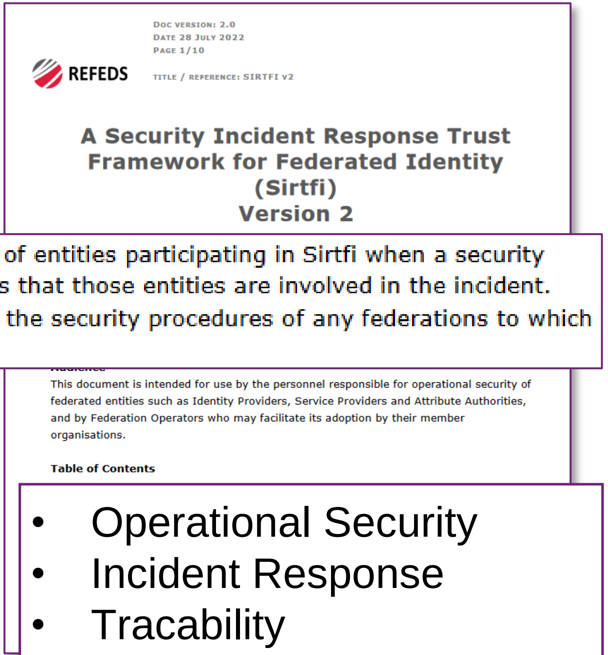
Organisations probably do ‘something reasonable’ for their own security ... but may not realise the implications for others

Sirtfi targets coordinated **response in a federated context**:

1. Enable **communication** and coordination in managing federated security incidents
2. Relevant **event data** is available to help collaborating incident responders.
3. **Security protections are applied** to federated transactions

Define capabilities for security incident response an IdP or SP **organisation can self-asserts** in federation meta-data

https://refeds.org/sirtfi



REFEDS

DOC VERSION: 2.0
DATE 28 JULY 2022
PAGE 1/10

TITLE / REFERENCE: SIRTFI v2

A Security Incident Response Trust Framework for Federated Identity (Sirtfi) Version 2

This document is intended for use by the personnel responsible for operational security of federated entities such as Identity Providers, Service Providers and Attribute Authorities, and by Federation Operators who may facilitate its adoption by their member organisations.

Table of Contents

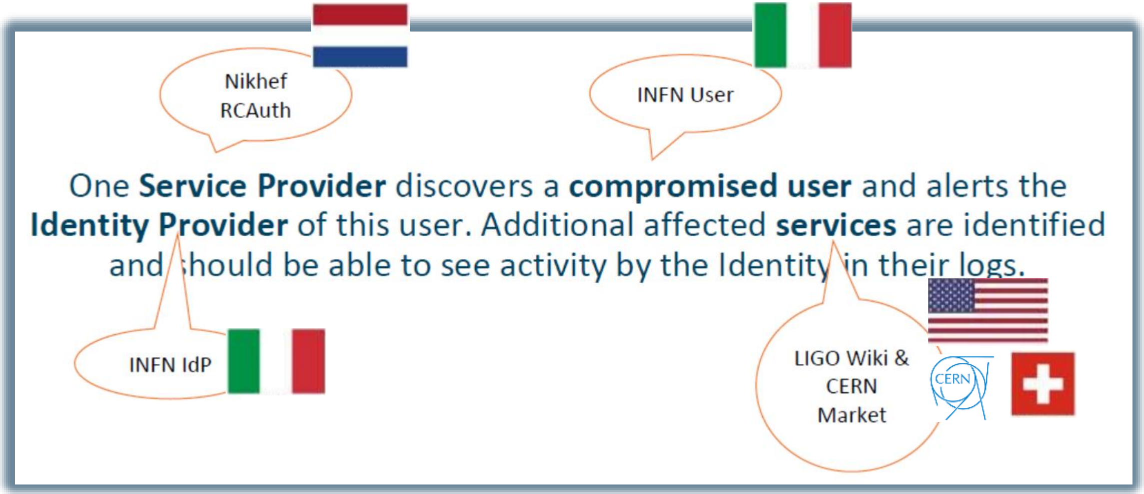
- [IR3] Notify security contacts of entities participating in Sirtfi when a security incident investigation suggests that those entities are involved in the incident. Notification should also follow the security procedures of any federations to which your organisation belongs.

- Operational Security
- Incident Response
- Tracability
- User Rules & Conditions

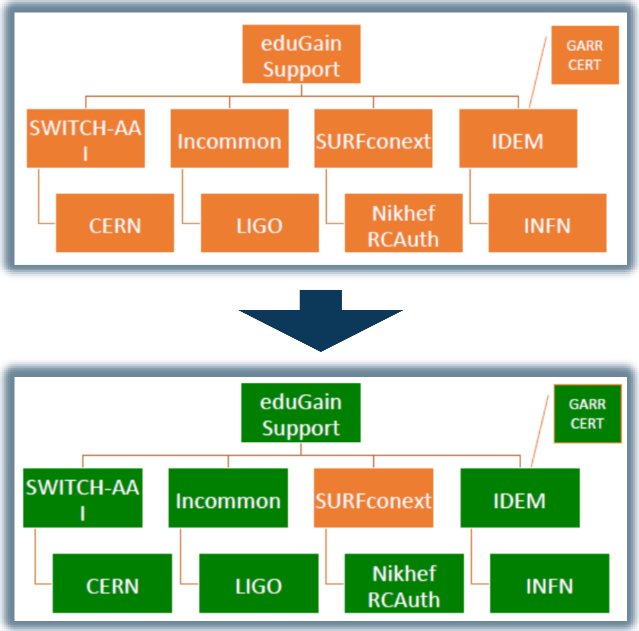
A federated community security challenge

Can we coordinate our collective R&E response?

‘security challenges’ based on the *Sirtfi* contact model



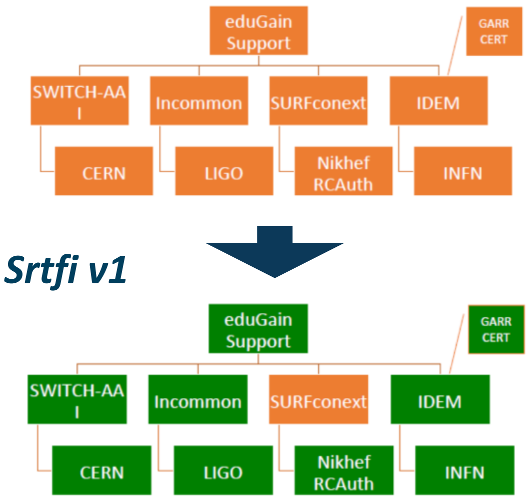
One **Service Provider** discovers a **compromised user** and alerts the **Identity Provider** of this user. Additional affected **services** are identified and should be able to see activity by the Identity in their logs.

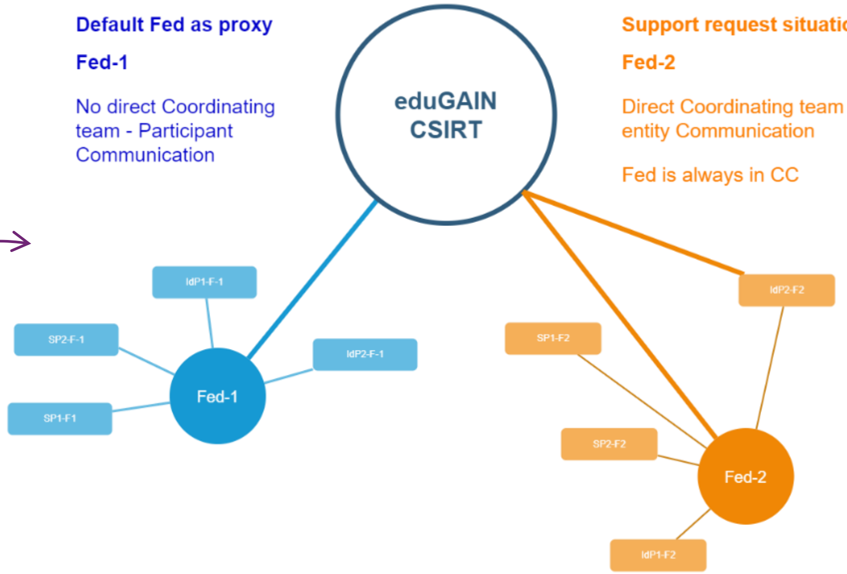


parties involved in response challenge

Report-outs see **https://wiki.geant.org/display/AARC/Sirtfi+Communications+Challenges%2C+AARC2-TNA3.1**

Response across IdP-SP Proxies: the limits of Sirtfi version 1





Default Fed as proxy

Fed-1

No direct Coordinating team - Participant Communication

Support request situation

Fed-2

Direct Coordinating team - end entity Communication

Fed is always in CC

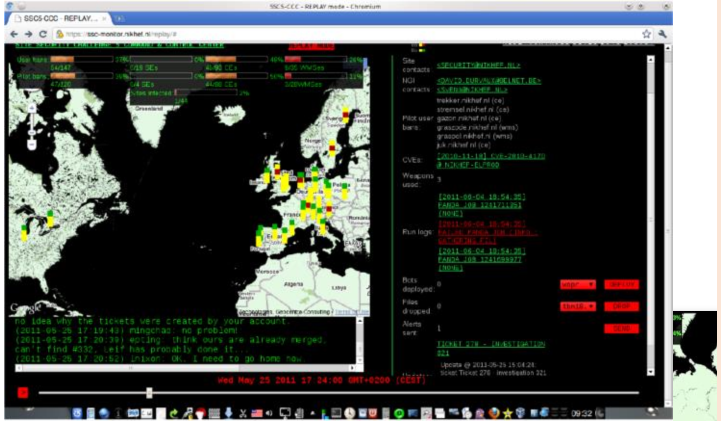
GÉANT | eduGAIN | CSIRT

joint work with GN5 EnCo and eduGAIN CSIRT

eduGAIN Security Incident Response Handbook

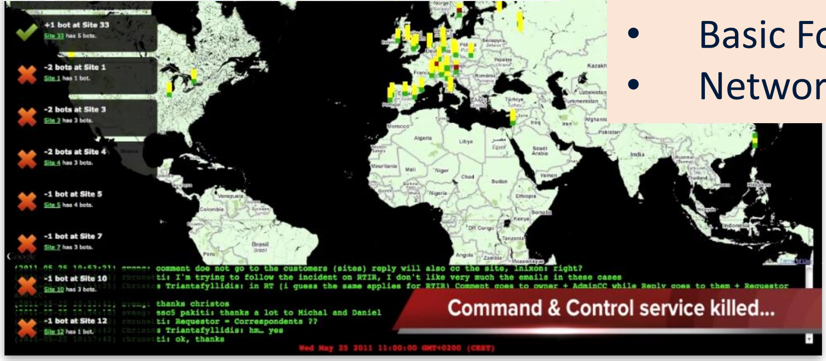
Preface

Trust … but verify


SSC5-CCC - REPLAY mode - Chromium
Bots deployed: 0
Files dropped: 0
Alerts sent: 1
TICKET 278 - INVESTIGATION 321
Update @ 2011-05-25 15:04:28: ticket Ticket 278 - Investigation 321

```
no idea why the tickets were created by your account.
(2011-05-25 17:19:43) mingchao: no problem!
(2011-05-25 17:20:39) epting: think ours are already merged,
can't find #332, Leif has probably done it...
(2011-05-25 17:20:52) lnixon: OK. I need to go home now.
```

Wed May 25 2011 17:24:00 GMT+0200 (CEST)



```
(2011-05-25 10:53:21) svengj: comment doe not go to the customers (sites) reply will also cc the site, lnixon: right?
ti: I'm trying to follow the incident on RTIR, I don't like very much the emails in these cases
s Triantafyllidis: in RT (i guess the same applies for RTIR) Comment goes to owner + AdminCC while Reply goes to them + Requestor
thanks christos
ssc5 pakiti: thanks a lot to Michal and Daniel
ti: Requestor = Correspondents ??
s Triantafyllidis: hm… yes
ti: ok, thanks
```

Wed May 25 2011 11:00:00 GMT+0200 (CEST)

Command & Control service killed...

Communication:

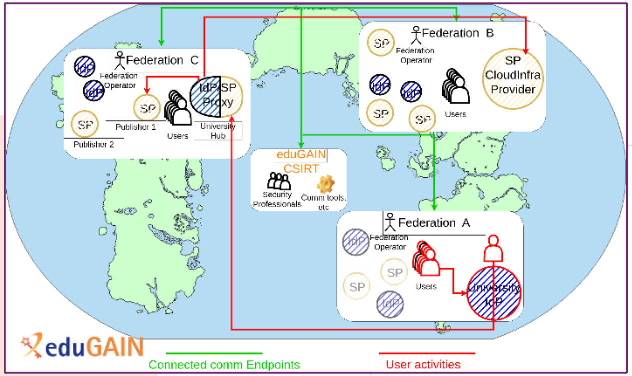
- Endpoints valid?
- Form/Content OK ?

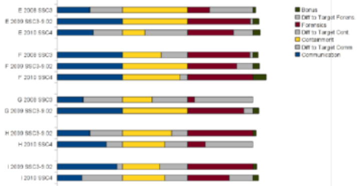
Containment

- Ban ”malicious” users
- Find/Stop malicious processes
- Find submission IP

Forensics

- Basic Forensics on binary
- Network traffic





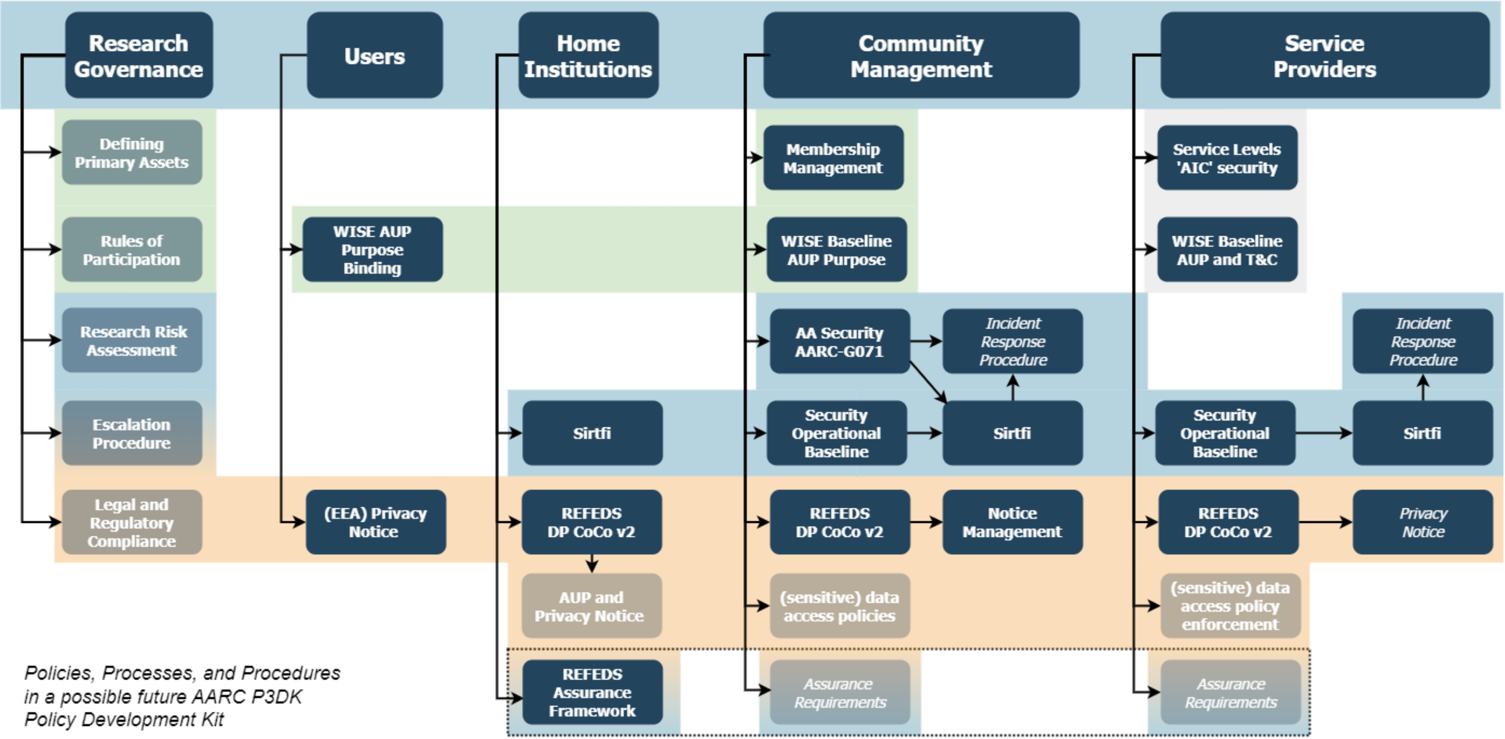
Nikhef CSIRT Traceability Challenge

Introduction

Deze Traceability Challenge bestaat uit drie onderdelen, in (naar verwachting) oplopende moeilijkheidsgraad. Iedere challenge begint met een externe 'trigger' – aan het eind van dit document staan de hints en de goede (of in ieder geval: de 'gewenste') oplossing.

Veel plezier!

Policy Development Kit: simplify by re-using good practice



Research Governance
- Defining Primary Assets
- Rules of Participation
- Research Risk Assessment
- Escalation Procedure
- Legal and Regulatory Compliance

Users
- WISE AUP Purpose Binding
- (EEA) Privacy Notice

Home Institutions
- Sirtfi
- REFEDS DP CoCo v2 → AUP and Privacy Notice
- REFEDS Assurance Framework

Community Management
- Membership Management
- WISE Baseline AUP Purpose
- AA Security AARC-G071 → *Incident Response Procedure*; AA Security AARC-G071 → Sirtfi
- Security Operational Baseline → Sirtfi → *Incident Response Procedure*
- REFEDS DP CoCo v2 → Notice Management
- (sensitive) data access policies
- *Assurance Requirements*

Service Providers
- Service Levels 'AIC' security
- WISE Baseline AUP and T&C
- Security Operational Baseline → Sirtfi → *Incident Response Procedure*
- REFEDS DP CoCo v2 → *Privacy Notice*
- (sensitive) data access policy enforcement
- *Assurance Requirements*

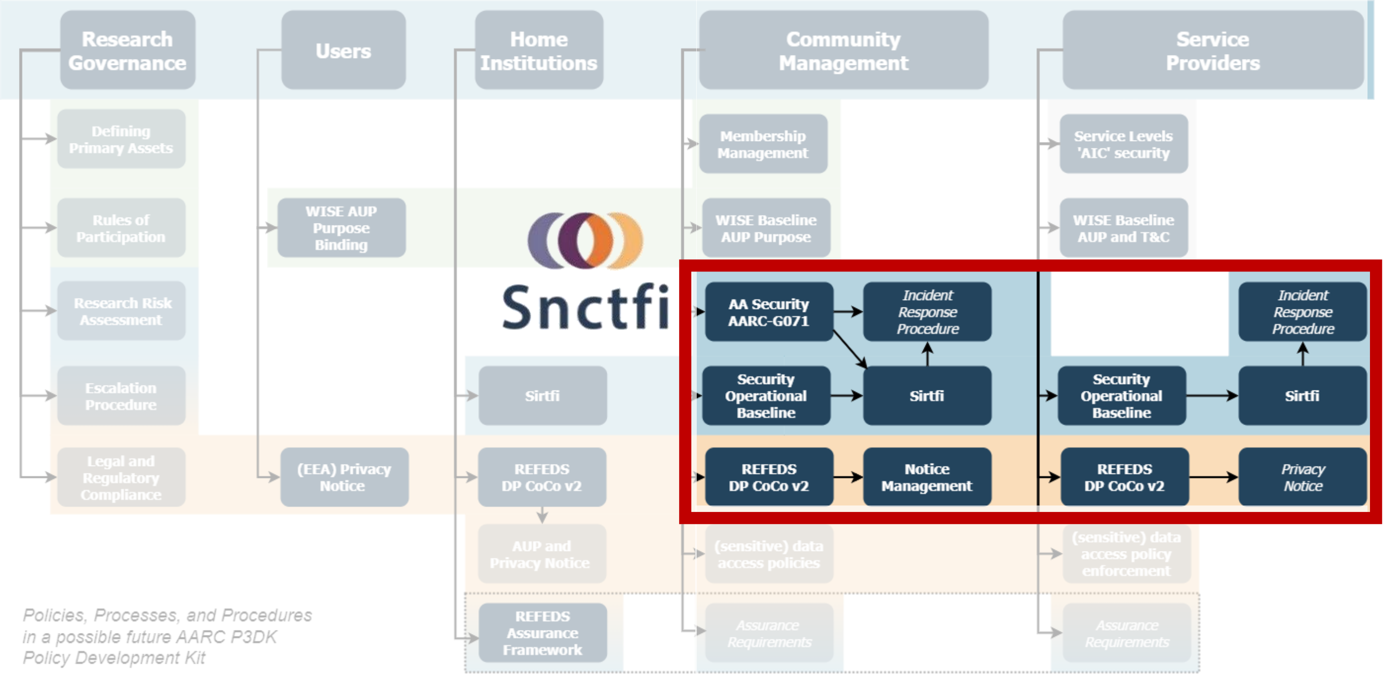
Policies, Processes, and Procedures in a possible future AARC P3DK Policy Development Kit

🟩 **Purpose of the collaboration**

🟦 **Protection of the collaboration, its ICT services and resources**

🟧 **Protection of the collaborating users (and any sensitive research data)**

Providers manage complexity for research communities



Policies, Processes, and Procedures in a possible future AARC P3DK Policy Development Kit

🟩 **Purpose of the collaboration**

🟦 **Protection of the collaboration, its ICT services and resources**

🟧 **Protection of the collaborating users (and any sensitive research data)**

communities sourcing ‘well-operated’ community platforms

eduTEAMS

B2ACCESS

SURF (SRAM)

CILogon

and a few more …

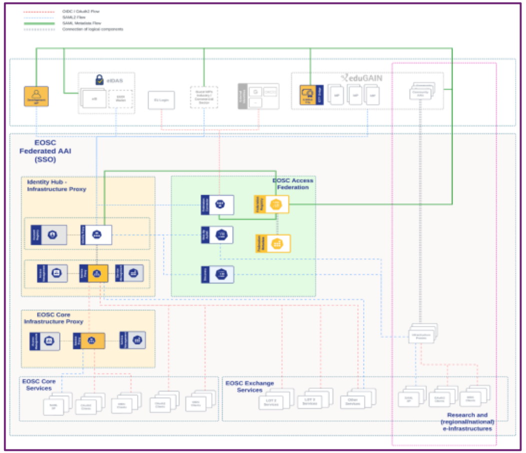
through their scale gets federations to trust our AARC ‘middle boxes’

Enabling research: using the ‘EOSC’ with federated login

AARC compliant federation of ‘national’ and ‘thematic’ nodes in the European Open Science Cloud

linked with other ‘data spaces’ and infrastructures

eosc | Federation



OIDC / OAuth2 Flow
SAML2 Flow
SAML Metadata Flow
Connection of logical components
eIDAS
eduGAIN
EOSC Federated AAI (SSO)
Identity Hub - Infrastructure Proxy
EOSC Access Federation
EOSC Core Infrastructure Proxy
EOSC Core Services
EOSC Exchange Services
Research and (regional/national) e-Infrastructures

ESRF
panosc
Italian National Research Council
eosc | Blue-Cloud2026
CERN
NATIONAL SCIENCE CENTRE POLAND
ICSC Centro Nazionale di Ricerca in HPC, Big Data and Quantum Computing
nfdi Nationale Forschungsdaten Infrastruktur
cnrs
DATA TERRA
EUDAT
CSC
SURF
BBMRI-ERIC
elixir
EMBL
EURO BIOIMAGING
instruct ERIC

The organisations invited to join the March 2025 kick-off workshop for the build-up phase of the EOSC Federation. All of the organisations are among the membership of the EOSC Association.

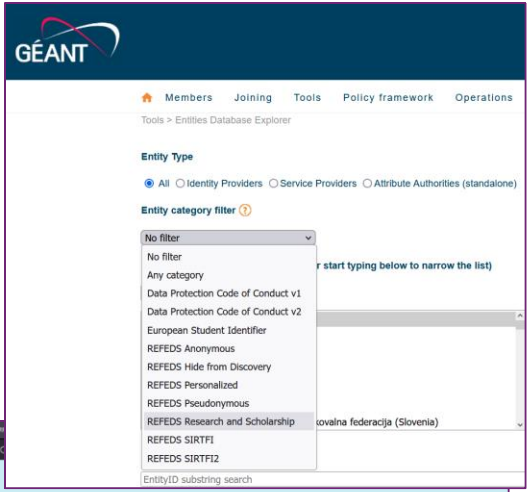
https://eosc.eu/eosc-about/building-the-eosc-federation/contributing-to-the-build-up-phase-of-the-eosc-federation/; See also https://wiki.geant.org/display/AARC/EOSC+AAI

And it needs everyone to work together

To scale trust in research infrastructures,
we need to keep challenging ourselves …

- *for eduGAIN: do we choose more trustworthiness and target baseline assurance, or more inclusiveness, but maybe less trust?*
- *for your university IT department: prioritize the primary mission of education and research, as both are now globally connected*
  - ‘we can *use* existing services from outside’
  - ‘we can *contribute* in collaborations in education and research’
  - ‘we teach our students to understand, study, and work with interconnected services and systems that are globally connected’

  … rather than get stuck in an enterprise egg-shell approach?
- *do our networks support a perimeter ‘fit for collaboration’?*



GÉANT

Members Joining Tools Policy framework Operations

Tools > Entities Database Explorer

Entity Type

● All ○ Identity Providers ○ Service Providers ○ Attribute Authorities (standalone)

Entity category filter

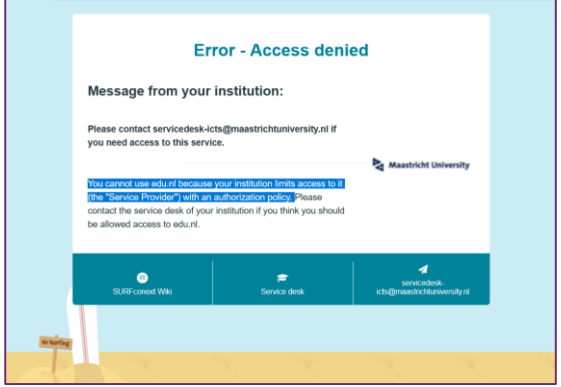
No filter

- No filter
- Any category
- Data Protection Code of Conduct v1
- Data Protection Code of Conduct v2
- European Student Identifier
- REFEDS Anonymous
- REFEDS Hide from Discovery
- REFEDS Personalized
- REFEDS Pseudonymous
- REFEDS Research and Scholarship
- REFEDS SIRTFI
- REFEDS SIRTFI2

r start typing below to narrow the list)

ovalna federacija (Slovenia)

EntityID substring search



Error - Access denied

Message from your institution:

Please contact servicedesk-icts@maastrichtuniversity.nl if you need access to this service.

Maastricht University

You cannot use edu.nl because your institution limits access to it (the "Service Provider") with an authorization policy. Please contact the service desk of your institution if you think you should be allowed access to edu.nl.

Images: https://technical.edugain.org/entities, Maastricht University blocking access to … a privacy-friendly URI shortener ☹,

Make and treat computing as the research instrument it is today – institutionally and globally

Institutional:
Nikhef “Stoomboot”
Analysis Facility

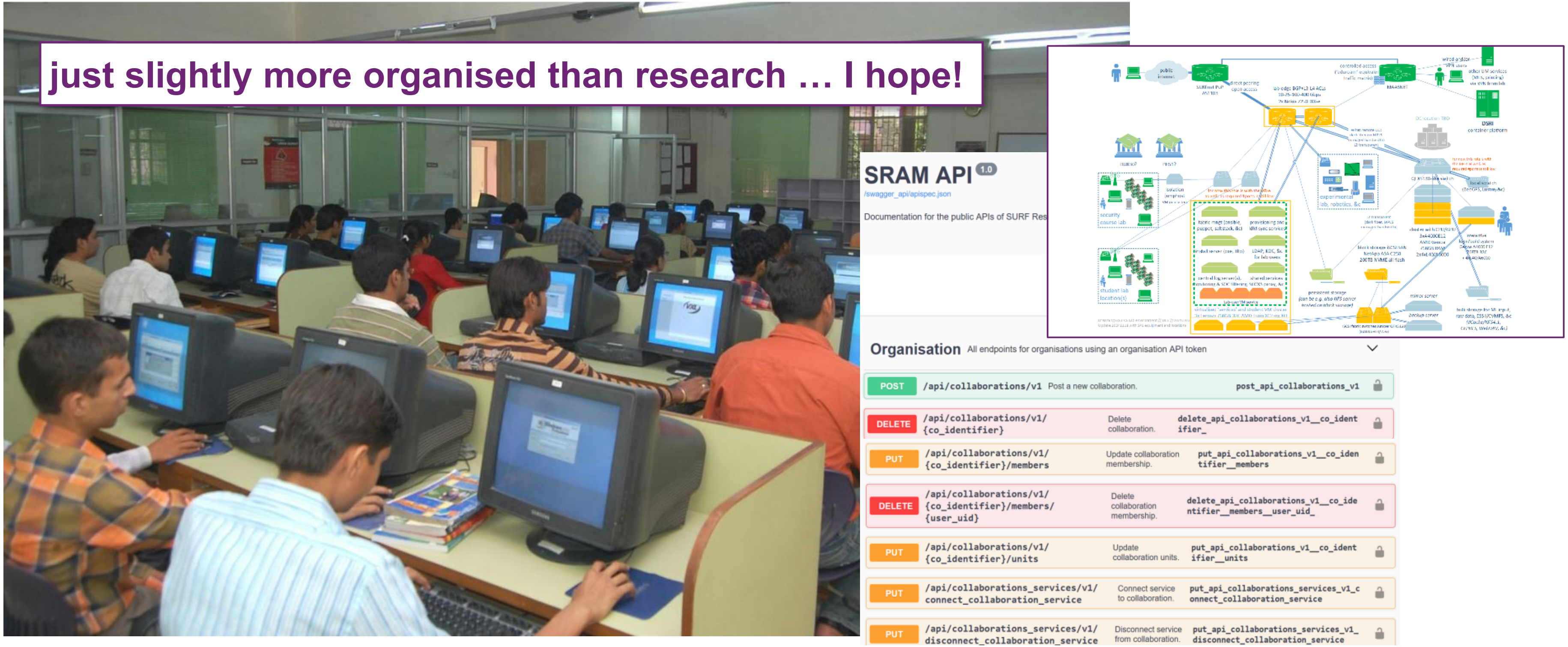
National Infrastructure
SURF Snellius HPC

as well as JP’s HPCI,
US’s AccessCI, &c of course!

There are today as much part of science as detectors are to physics
and: users should move seamlessly between tiers

Photos: Nikhef NDPF, DelftBlue/TUDelft, SURF Data Repository, Snellius, SURF @ DigitalRealty; EuroHPC images: EuroHPC, LUMI Consortium, Jules Verne consortium

And education labs are much like ad-hoc research collaboration



just slightly more organised than research … I hope!

SRAM API 1.0

/swagger_api/apispec.json

Documentation for the public APIs of SURF Res

Organisation All endpoints for organisations using an organisation API token

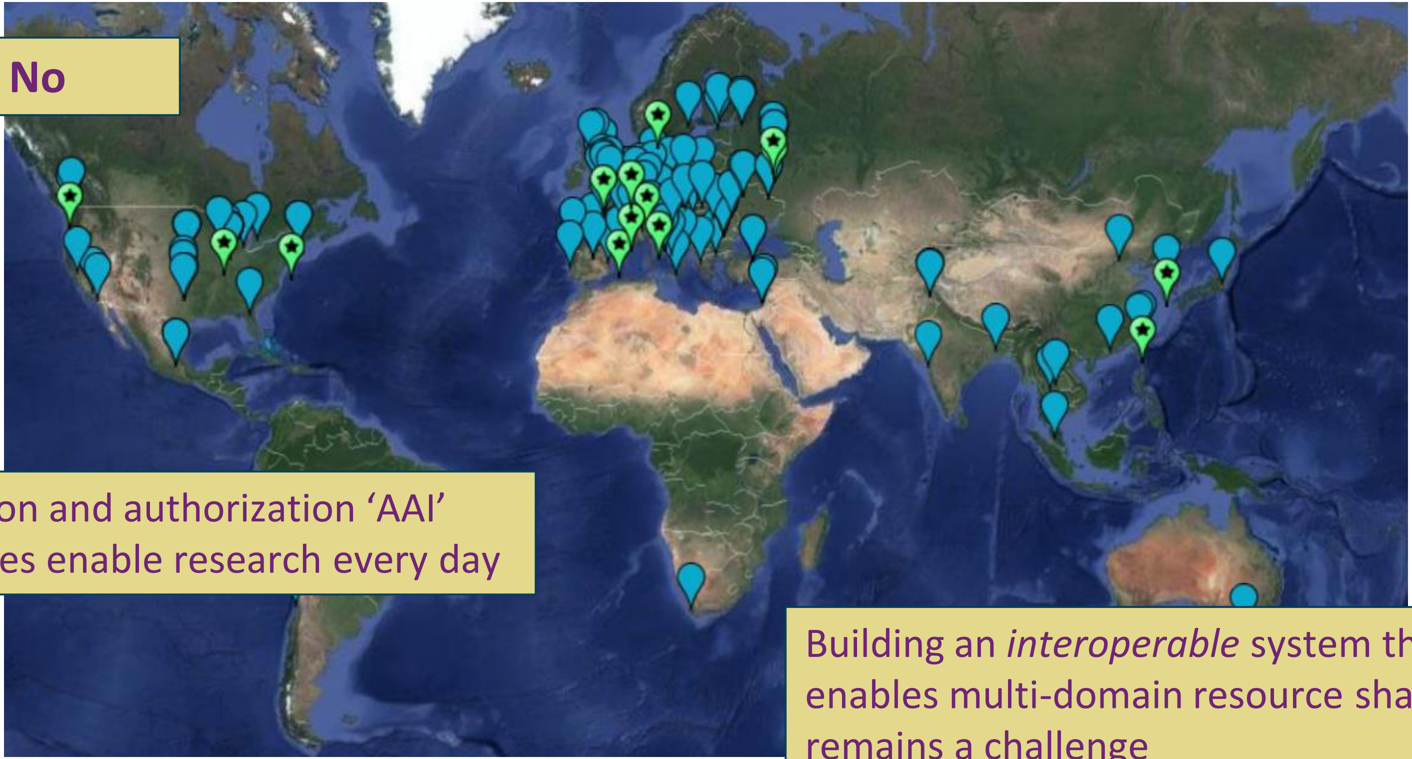
POST	/api/collaborations/v1	Post a new collaboration.	post_api_collaborations_v1
DELETE	/api/collaborations/v1/{co_identifier}	Delete collaboration.	delete_api_collaborations_v1__co_identifier_
PUT	/api/collaborations/v1/{co_identifier}/members	Update collaboration membership.	put_api_collaborations_v1__co_identifier__members
DELETE	/api/collaborations/v1/{co_identifier}/members/{user_uid}	Delete collaboration membership.	delete_api_collaborations_v1__co_identifier__members__user_uid_
PUT	/api/collaborations/v1/{co_identifier}/units	Update collaboration units.	put_api_collaborations_v1__co_identifier__units
PUT	/api/collaborations_services/v1/connect_collaboration_service	Connect service to collaboration.	put_api_collaborations_services_v1_connect_collaboration_service
PUT	/api/collaborations_services/v1/disconnect_collaboration_service	Disconnect service from collaboration.	put_api_collaborations_services_v1_disconnect_collaboration_service

public internet
SURFnet PoP
direct peering open access
controlled access ('eduroam'-equivalent traffic matrix)
MAASNET
wired and/or VPN users
other UM services (MFA, printing) via VPN from lab
lab edge BGP+L3 L4 ACLs
DSRI container platform
DC location TBD
isolation jumphost
security course lab
student lab location(s)
experimental lab, robotics, &c
fabric mngt (ansible, puppet, saltstack, &c)
provisioning and IdM sync services
LDAP, KDC, &c for lab users
central log server(s), monitoring & SOC filtering
shared services SOCKS proxy, &c
persistent storage (can be e.g. also NFS server hosted on block storage)
block storage iSCSI SAN NetApp ASA C250 200TB NVME all flash
mirror server
backup server
bulk storage for ML input, raw data, EESSI/CVMFS, &c
local scratch (BeeGFS, Lustre, &c)

Photo by sunrise University on Unsplash; network diagram: FSE CSLab, Maastricht University; SRAM API: https://sram.surf.nl/apidocs/

So: did we solve this inherently-cross-domain issue … ?

Both Yes and No



Authentication and authorization ‘AAI’ infrastructures enable research every day

Building an *interoperable* system that enables multi-domain resource sharing remains a challenge

site map: WLCG sites 2021, visualization: CERN IT

The AARC Blueprint – a very digestible architecture … so

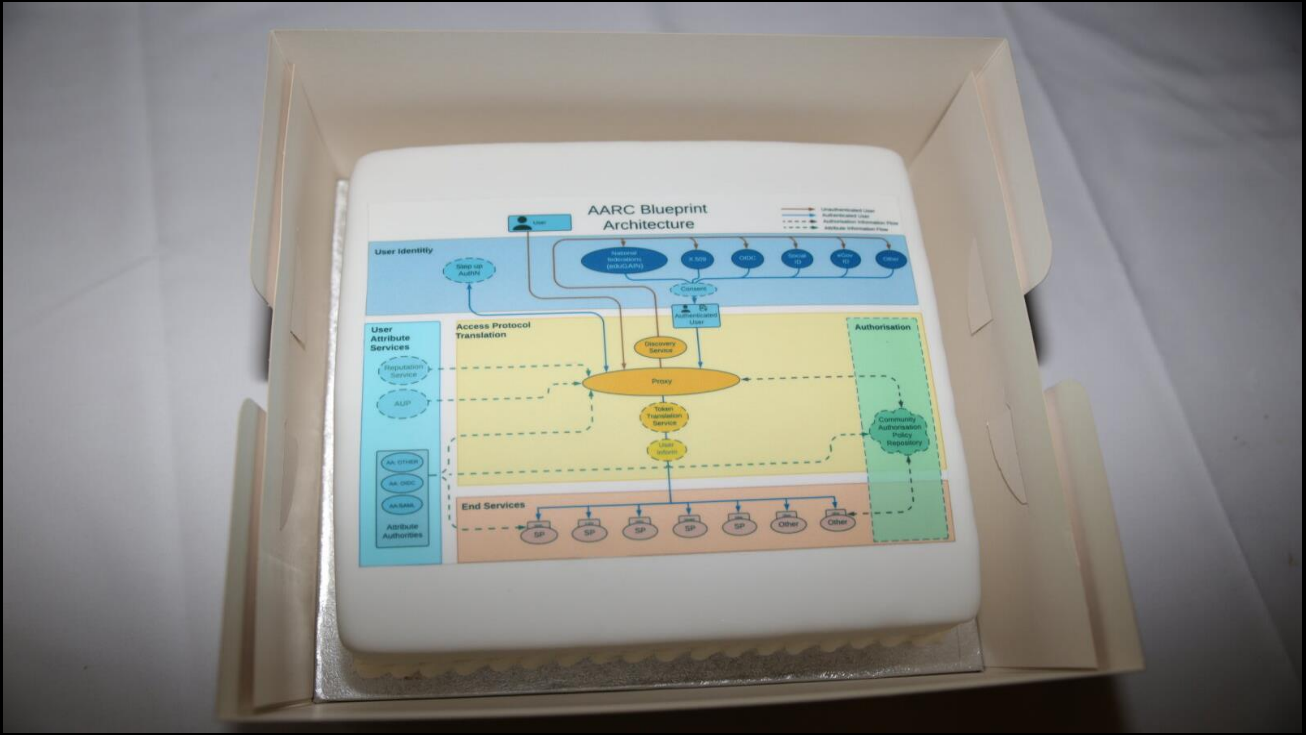


Photo credit: Marcus Hardt

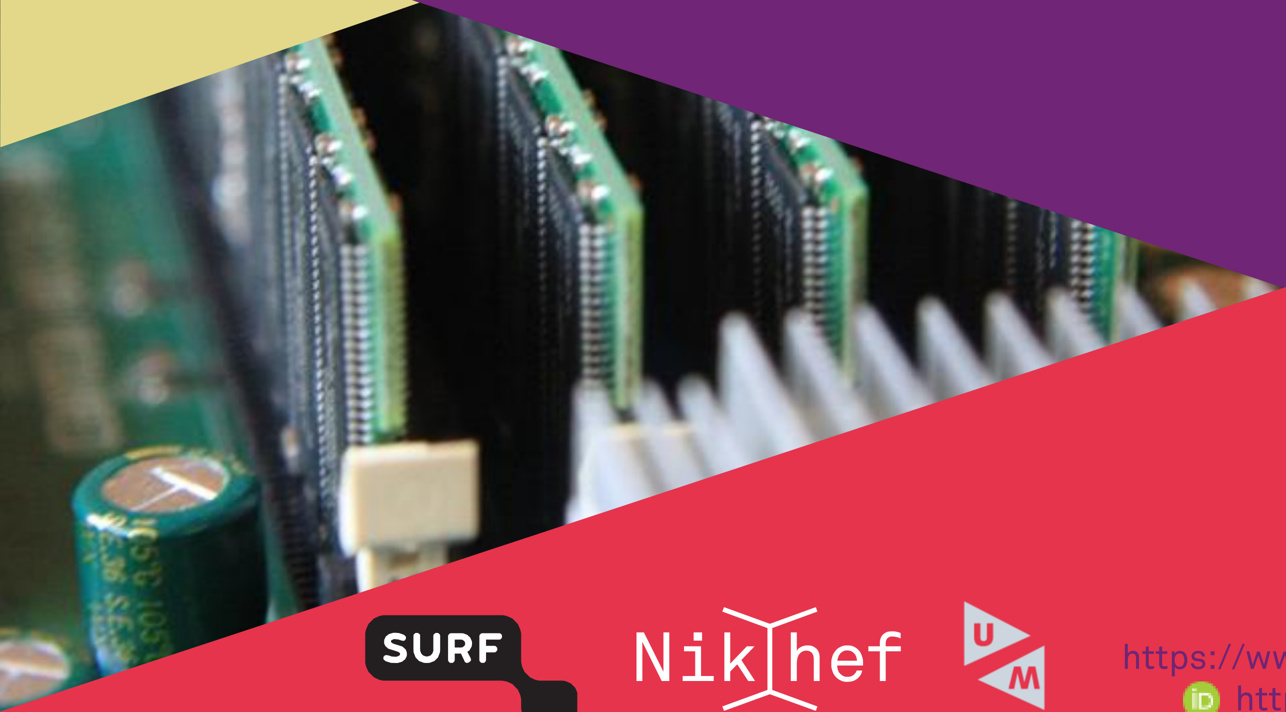
The AARC Blueprint – take a piece and feed collaboration!

Photo credit: Marcus Hardt

This work has also been co-supported by projects that have received funding from the European Union's Horizon programmes through grants AARC TREE and GEANT 5-2

Thanks to the AARC and global T&I Community, including folk from whom I re-used graphics in this overview. In random order: Licia Florio, Nicolas Liampotis, Christos Kanellopoulos, Marina Adomeit, Janos Mohacsi, Slavek Licehammer, Dave Kelsey, Ian Neilson, Marcus Hardt, Mischa Salle, Oscar Koeroo, Jouke Roorda, Davide Vaghetti, Floris Fokkinga, Sven Gabriel, Hannah Short, Maarten Kremers, and many others!

So let's digest all this …



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

this work co-funded by and contributing to the Dutch National e-Infrastructure coordinated by SURF