CERN

Federated Identity Management for Research: **The Key is Collaboration**

Hannah Short
CERN, Identity Federation Manager
AARC Project Participant

With thanks to input from the FIM4R Community and AARC

Who am I?

- My job = making digital life for researchers more secure
- Based at CERN
- Spend most of my time working with others like me around the world →

The Past

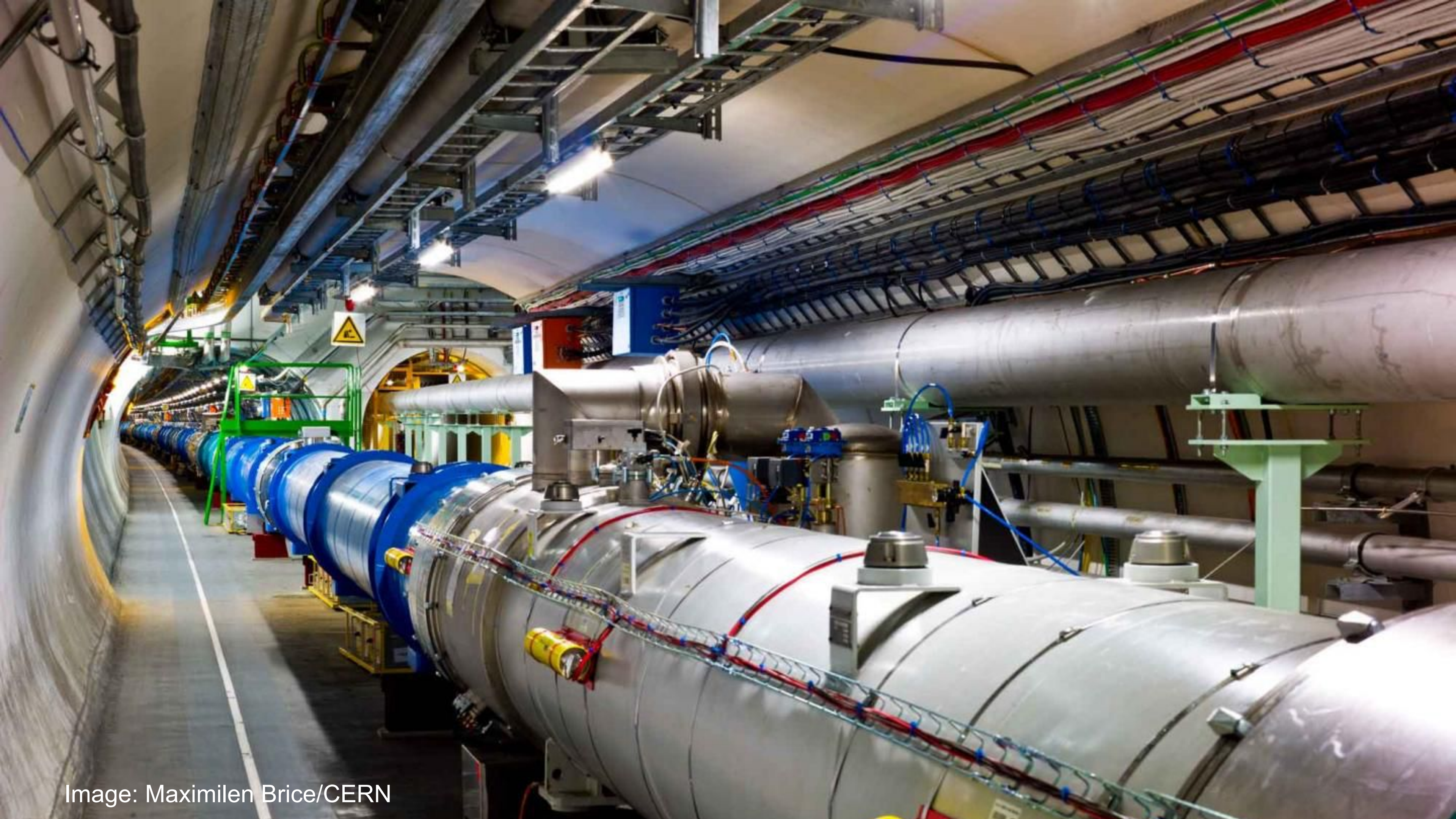
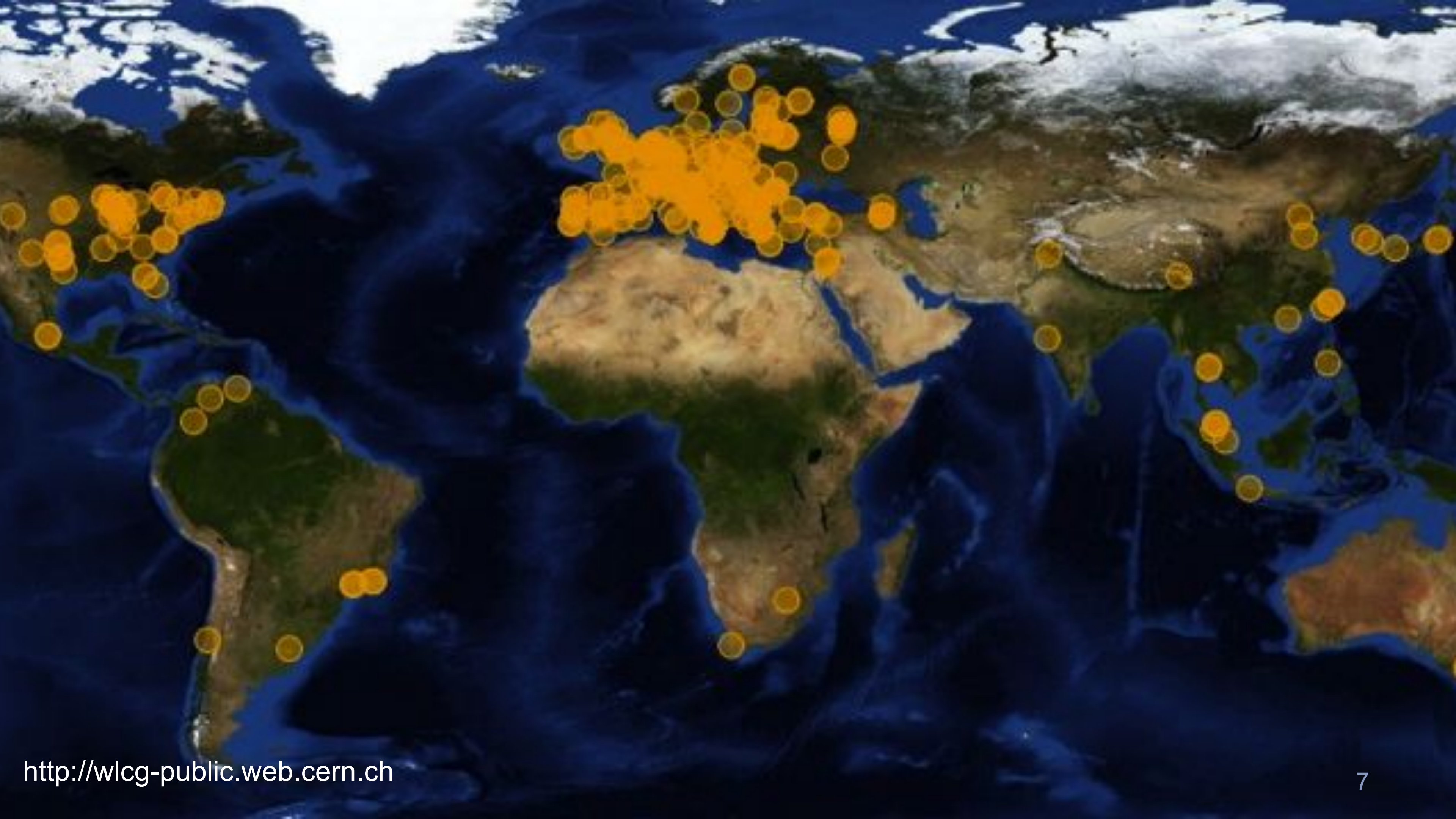
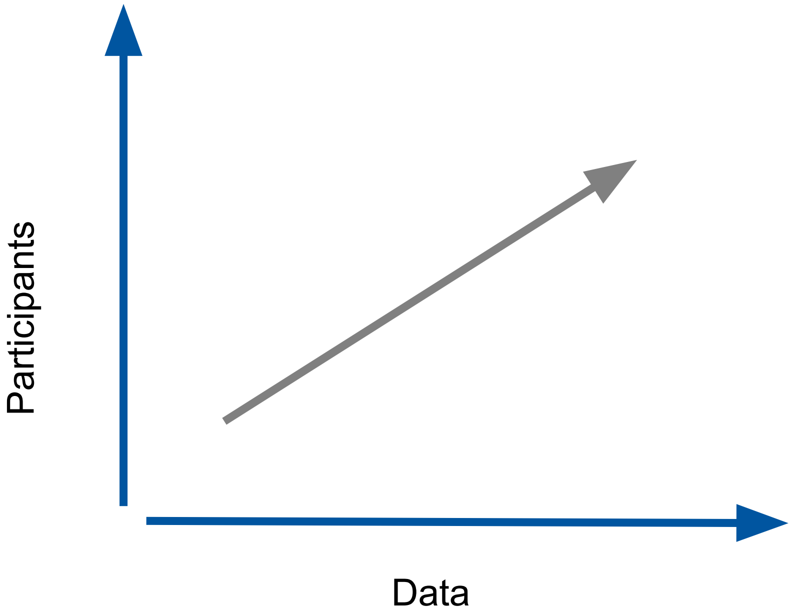


Image: Maximilen Brice/CERN

supply - demand = ?



http://wlcg-public.web.cern.ch


Participants
Data

	Field	Users	Countries	Computing Sites
LIGO	Gravitational Waves	1,200	20	9
WLCG (CERN)	High Energy Physics	13,000	43	170
ESGF	Climate Science	17,000	13	18

Source: http://doi.org/10.5281/zenodo.129603

The challenge

- Large, global user community
- Working on a distributed infrastructure
- Don’t necessarily know each other
- Don’t necessarily ever meet

How can we securely provision digital identities that are trusted by the infrastructure?

Who knows the user best?

A: The Research Community

B: The Infrastructure

C: The Home Organisation

D: Nobody

Who knows the user best?

A: The Research Community

B: The Infrastructure

[✓ C: The Home Organisation]

D: Nobody

Who knows what they are working on?

A: The Research Community

B: The Infrastructure

C: The Home Organisation

D: Nobody

Who knows what they are working on?

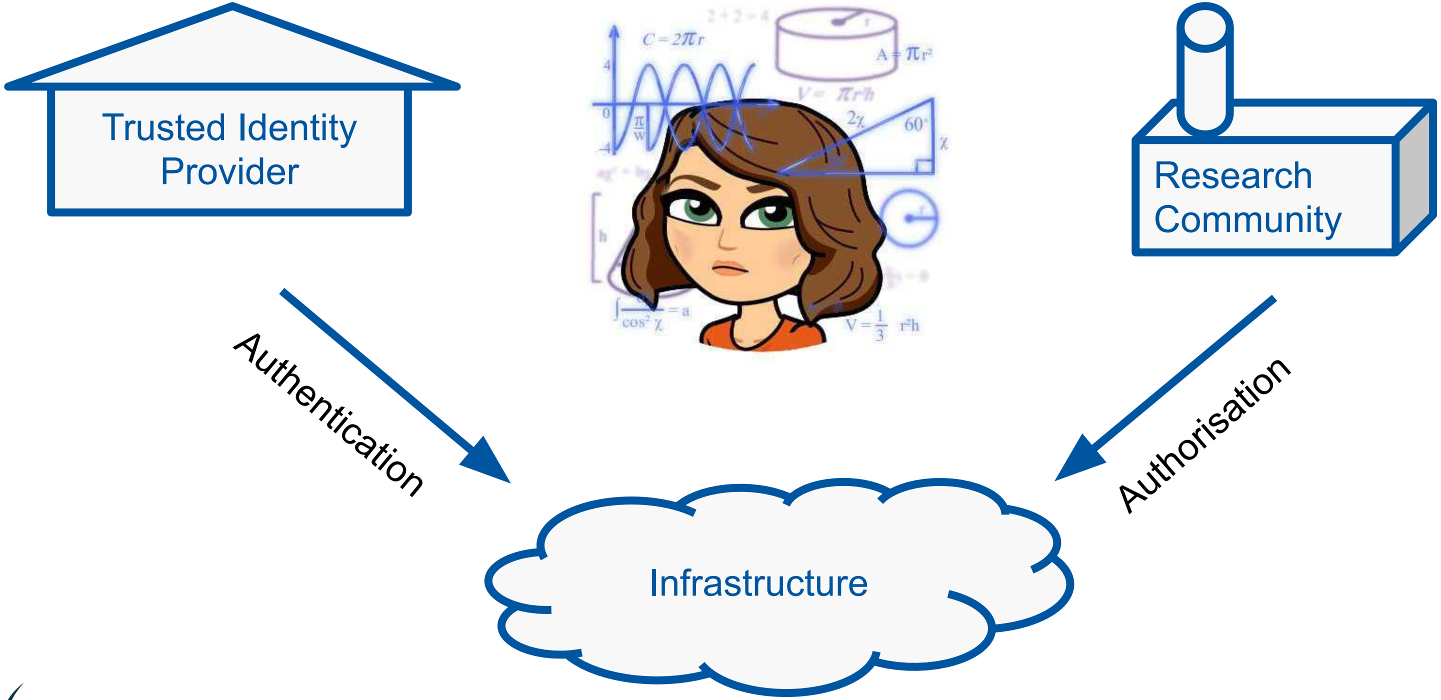
A: The Research Community

B: The Infrastructure

C: The Home Organisation

D: Nobody

Authentication vs Authorisation



Trusted Identity Provider

Research Community

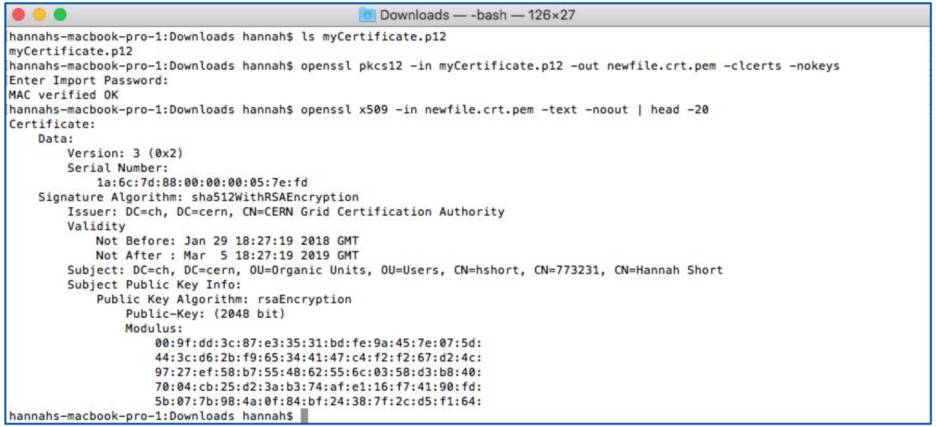
Authentication

Authorisation

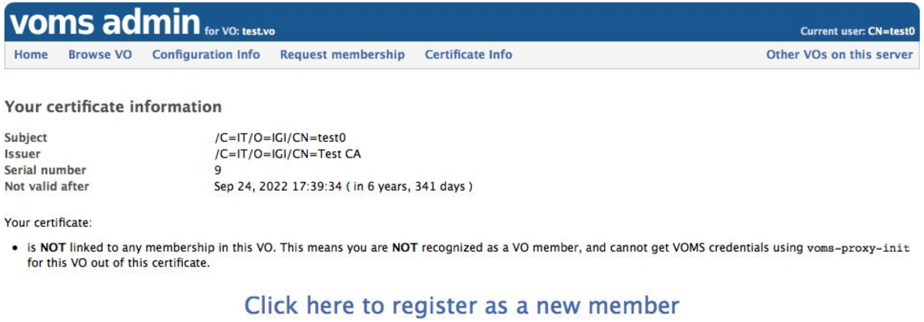
Infrastructure

2000s

- Authentication provided by X.509 certificates from trusted Certificate Authorities (ID vetting, strong policy set)
- Authorisation provided by Research Communities adding certificate extensions



```
hannahs-macbook-pro-1:Downloads hannah$ ls myCertificate.p12
myCertificate.p12
hannahs-macbook-pro-1:Downloads hannah$ openssl pkcs12 -in myCertificate.p12 -out newfile.crt.pem -clcerts -nokeys
Enter Import Password:
MAC verified OK
hannahs-macbook-pro-1:Downloads hannah$ openssl x509 -in newfile.crt.pem -text -noout | head -20
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1a:6c:7d:88:00:00:00:05:7e:fd
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: DC=ch, DC=cern, CN=CERN Grid Certification Authority
        Validity
            Not Before: Jan 29 18:27:19 2018 GMT
            Not After : Mar  5 18:27:19 2019 GMT
        Subject: DC=ch, DC=cern, OU=Organic Units, OU=Users, CN=hshort, CN=773231, CN=Hannah Short
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9f:dd:3c:87:e3:35:31:bd:fe:9a:45:7e:07:5d:
                    44:3c:d6:2b:f9:65:34:41:47:c4:f2:f2:67:d2:4c:
                    97:27:ef:58:b7:55:48:62:55:6c:03:58:d3:b8:40:
                    70:04:cb:25:d2:3a:b3:74:af:e1:16:f7:41:90:fd:
                    5b:07:7b:98:4a:0f:84:bf:24:38:7f:2c:d5:f1:64:
hannahs-macbook-pro-1:Downloads hannah$
```



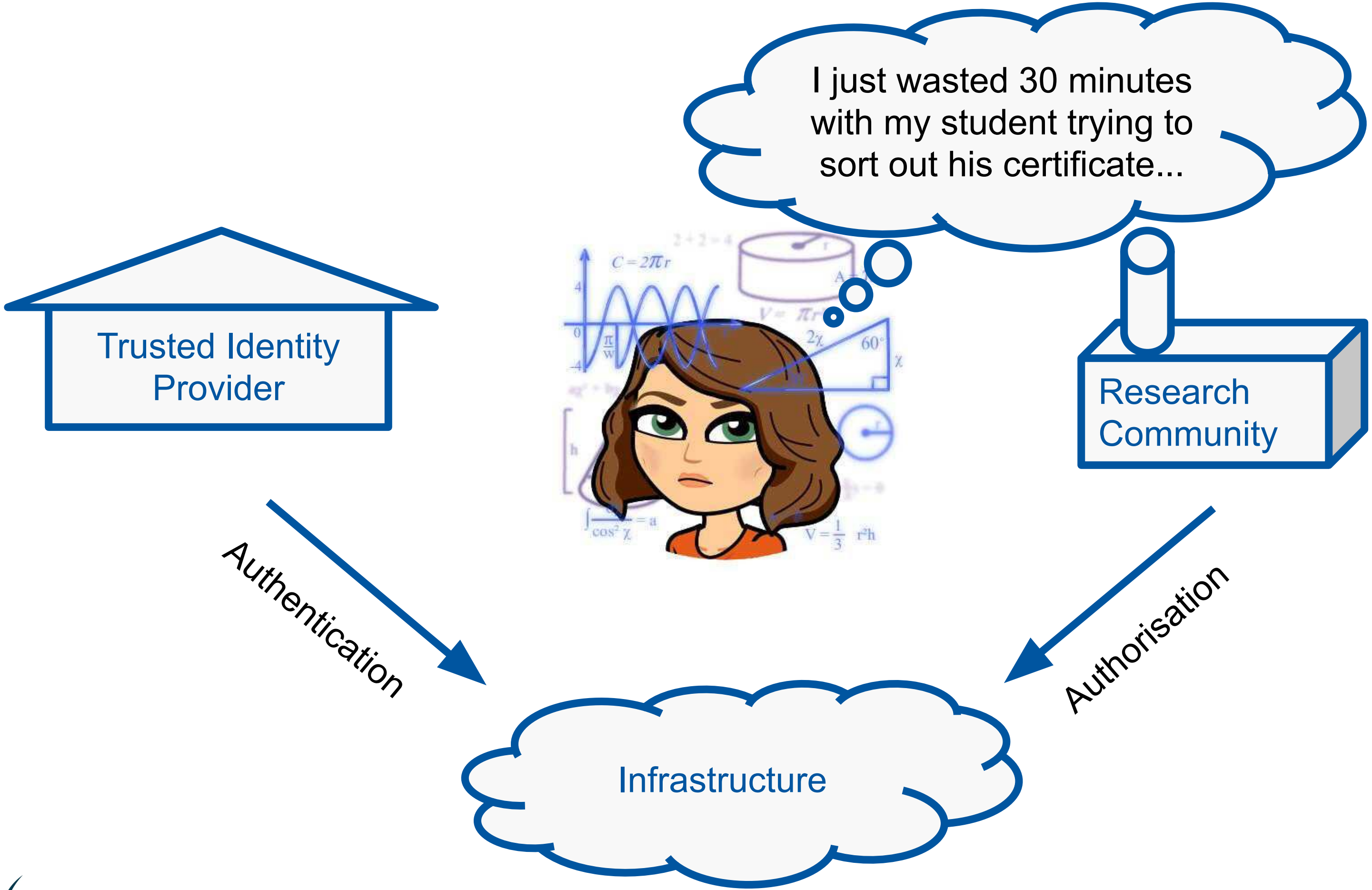
Your certificate information

Subject	/C=IT/O=IGI/CN=test0
Issuer	/C=IT/O=IGI/CN=Test CA
Serial number	9
Not valid after	Sep 24, 2022 17:39:34 (in 6 years, 341 days)

Your certificate:

- is **NOT** linked to any membership in this VO. This means you are **NOT** recognized as a VO member, and cannot get VOMS credentials using `voms-proxy-init` for this VO out of this certificate.

Click here to register as a new member



Trusted Identity Provider

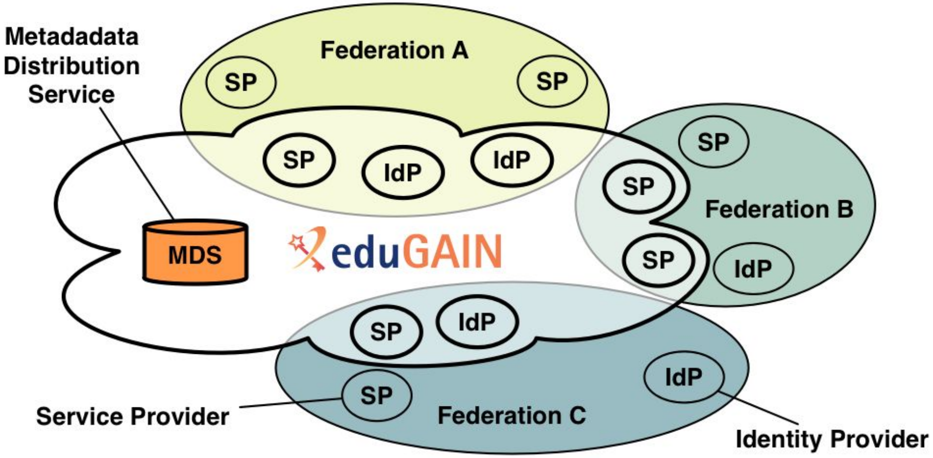
Research Community

Infrastructure

Authentication

Authorisation

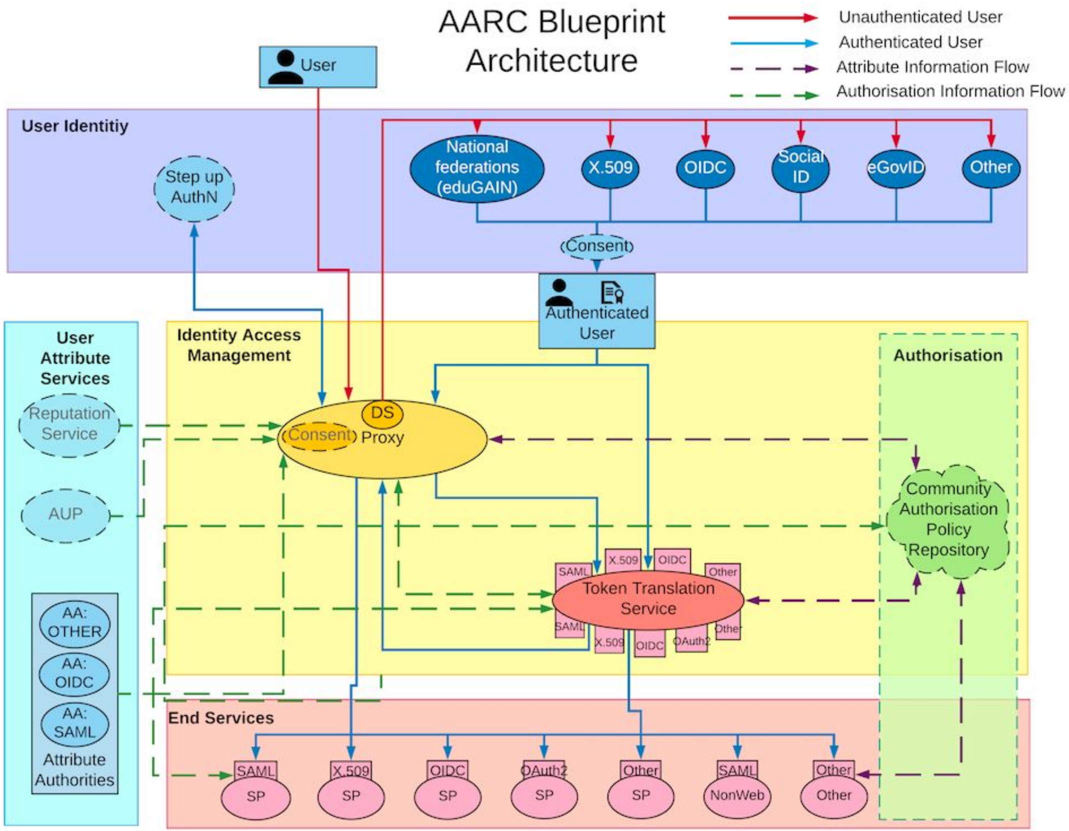
I just wasted 30 minutes with my student trying to sort out his certificate...



2010s

The hope that SAML federations (and Interfederation through eduGAIN) could provide a better solution

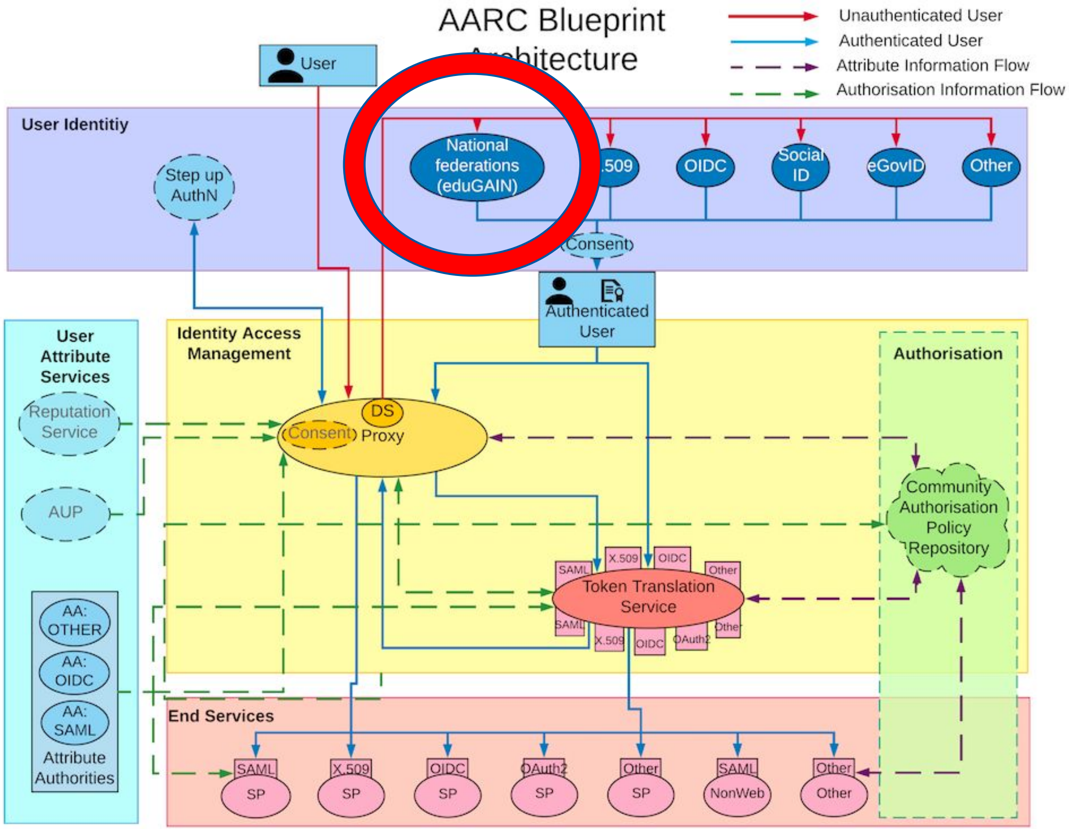
https://www.geant.org/Services/Trust_identity_and_security/eduGAIN/Pages/About-eduGAIN.aspx



2015+

The realisation that SAML Federations were one small piece of the puzzle

https://aarc-project.eu/architecture/



2015+

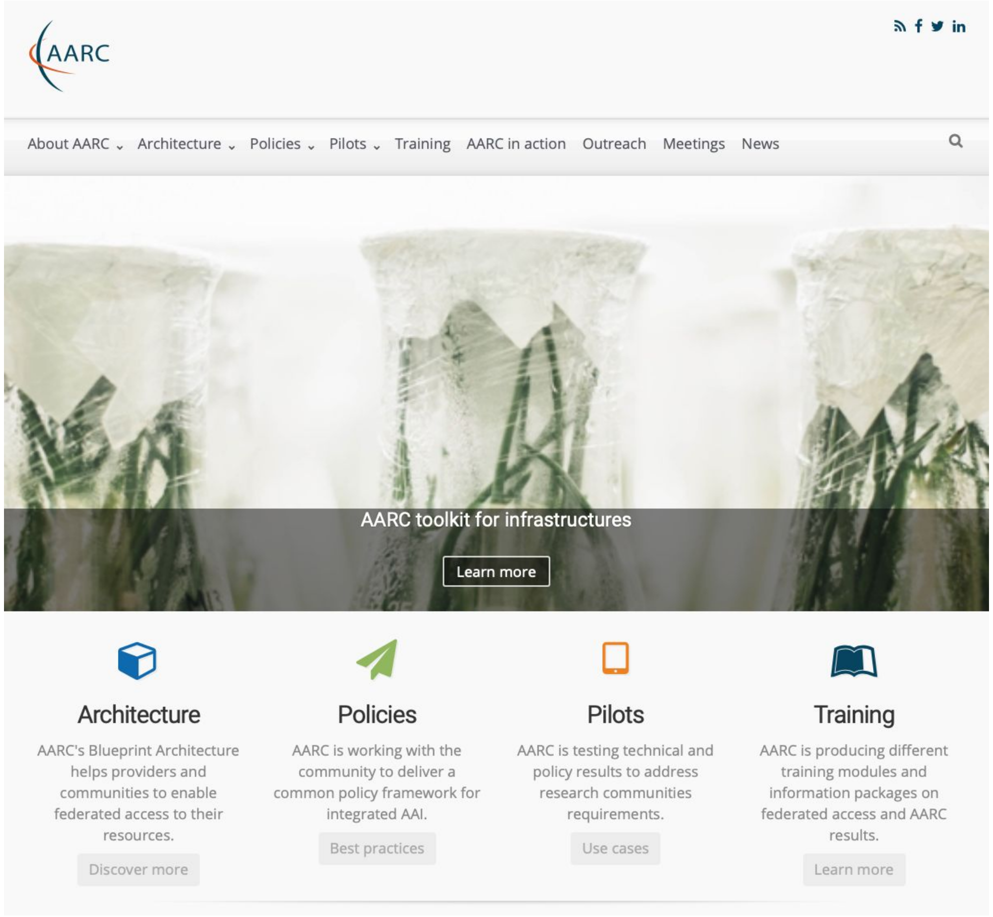
The realisation that SAML Federations were one small piece of the puzzle

https://aarc-project.eu/architecture/

The Present

AARC

Authentication and Authorisation for Research and Collaboration



AARC toolkit for infrastructures

Architecture

AARC's Blueprint Architecture helps providers and communities to enable federated access to their resources.

Policies

AARC is working with the community to deliver a common policy framework for integrated AAI.

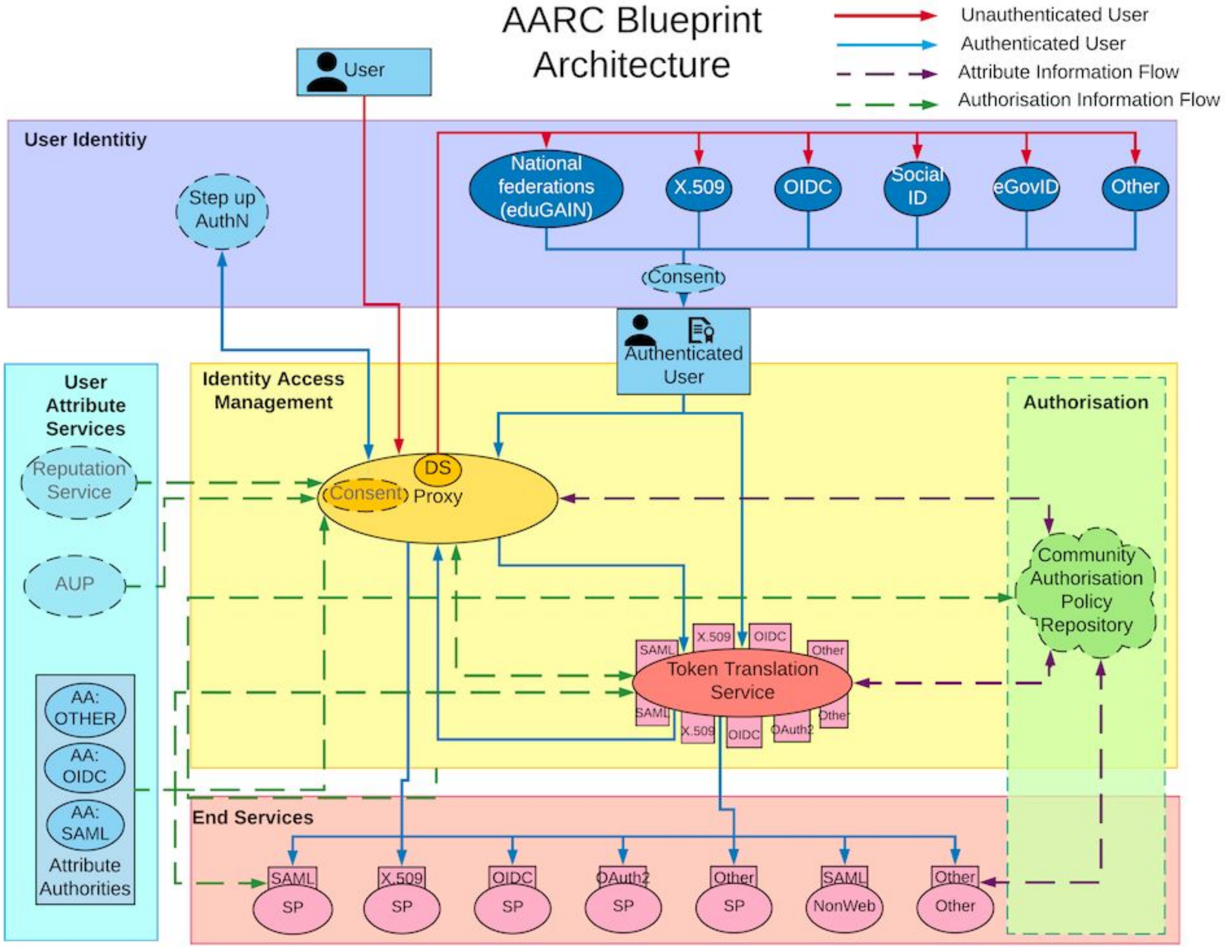
Pilots

AARC is testing technical and policy results to address research communities requirements.

Training

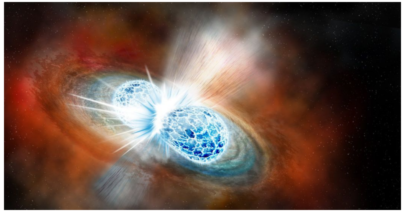
AARC is producing different training modules and information packages on federated access and AARC results.

AARC Blueprint Architecture



Many success stories

- gw-astronomy.org
- Collaboration hub for gravitational-wave and multi-messenger astronomy (MMA)
- Used to manage collaboration around the August 17, 2017 kilonova event



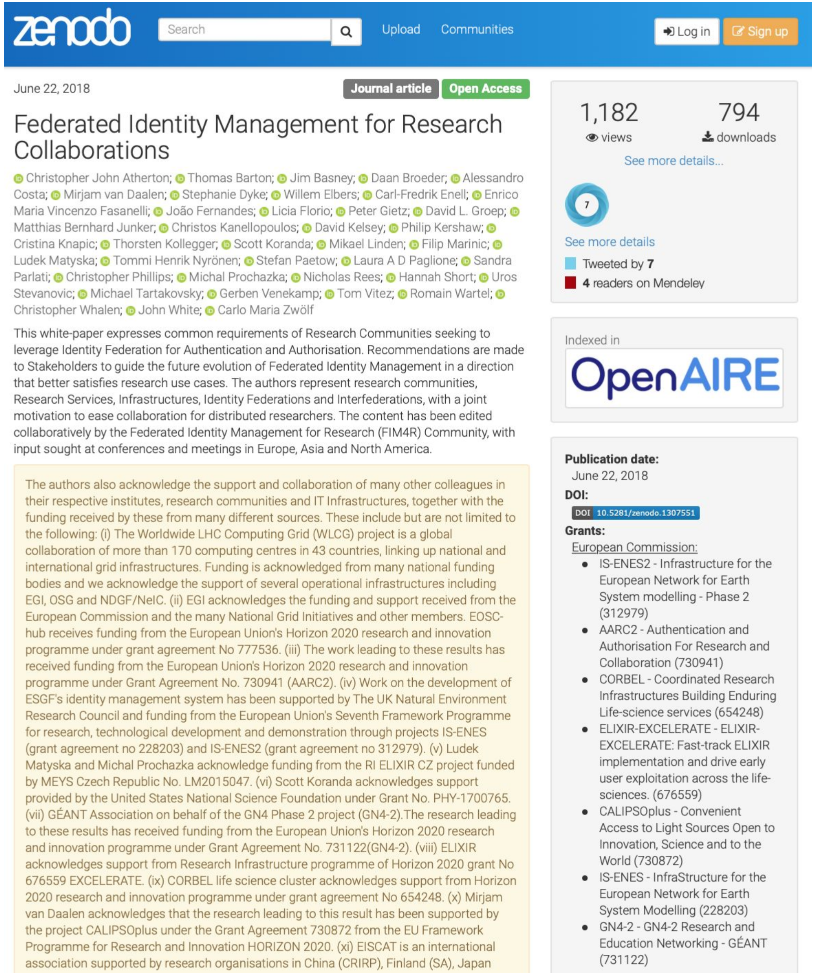
- EU Photon & Neutron facilities
- Single Sign On for 16 light sources
- Steady growth rate of 20% per year

Slide taken from FIM4R Session, TNC2018

Is the challenge now solved?

LIGO VIRGO
EISCAT SCIENTIFIC ASSOCIATION
umbrella
DARIAH-EU
WLCG
Worldwide LHC Computing Grid
elixir
SKA
SQUARE KILOMETRE ARRAY
KAGRA
CLARIN
INFN
Istituto Nazionale di Fisica Nucleare
VAMDC
Virtual Atomic and Molecular Data Centre
FAIR
LIGO
cta
cherenkov telescope array
HELIX NEBULA
THESCIENCECLOUD
CORBEL
ESGF
Earth System Grid Federation
esa
National Institute
of Allergy and
Infectious Diseases

*** Not all contributors' logos represented*



June 22, 2018

Journal article Open Access

Federated Identity Management for Research Collaborations

Christopher John Atherton; Thomas Barton; Jim Basney; Daan Broeder; Alessandro Costa; Mirjam van Daalen; Stephanie Dyke; Willem Elbers; Carl-Fredrik Enell; Enrico Maria Vincenzo Fasanelli; João Fernandes; Licia Florio; Peter Gietz; David L. Groep; Matthias Bernhard Junker; Christos Kanellopoulos; David Kelsey; Philip Kershaw; Cristina Knapic; Thorsten Kollegger; Scott Koranda; Mikael Linden; Filip Marinic; Ludek Matyska; Tommi Henrik Nyrönen; Stefan Paetow; Laura A D Paglione; Sandra Parlati; Christopher Phillips; Michal Prochazka; Nicholas Rees; Hannah Short; Uros Stevanovic; Michael Tartakovsky; Gerben Venekamp; Tom Vitez; Romain Wartel; Christopher Whalen; John White; Carlo Maria Zwölf

This white-paper expresses common requirements of Research Communities seeking to leverage Identity Federation for Authentication and Authorisation. Recommendations are made to Stakeholders to guide the future evolution of Federated Identity Management in a direction that better satisfies research use cases. The authors represent research communities, Research Services, Infrastructures, Identity Federations and Interfederations, with a joint motivation to ease collaboration for distributed researchers. The content has been edited collaboratively by the Federated Identity Management for Research (FIM4R) Community, with input sought at conferences and meetings in Europe, Asia and North America.

The authors also acknowledge the support and collaboration of many other colleagues in their respective institutes, research communities and IT Infrastructures, together with the funding received by these from many different sources. These include but are not limited to the following: (i) The Worldwide LHC Computing Grid (WLCG) project is a global collaboration of more than 170 computing centres in 43 countries, linking up national and international grid infrastructures. Funding is acknowledged from many national funding bodies and we acknowledge the support of several operational infrastructures including EGI, OSG and NDGF/NeIC. (ii) EGI acknowledges the funding and support received from the European Commission and the many National Grid Initiatives and other members. EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 777536. (iii) The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2). (iv) Work on the development of ESGF's identity management system has been supported by The UK Natural Environment Research Council and funding from the European Union's Seventh Framework Programme for research, technological development and demonstration through projects IS-ENES (grant agreement no 228203) and IS-ENES2 (grant agreement no 312979). (v) Ludek Matyska and Michal Prochazka acknowledge funding from the RI ELIXIR CZ project funded by MEYS Czech Republic No. LM2015047. (vi) Scott Koranda acknowledges support provided by the United States National Science Foundation under Grant No. PHY-1700765. (vii) GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122(GN4-2). (viii) ELIXIR acknowledges support from Research Infrastructure programme of Horizon 2020 grant No 676559 EXCELERATE. (ix) CORBEL life science cluster acknowledges support from Horizon 2020 research and innovation programme under grant agreement No 654248. (x) Mirjam van Daalen acknowledges that the research leading to this result has been supported by the project CALIPSOplus under the Grant Agreement 730872 from the EU Framework Programme for Research and Innovation HORIZON 2020. (xi) EISCAT is an international association supported by research organisations in China (CRIRP), Finland (SA), Japan

1,182 views

794 downloads

See more details...

7

See more details

🟦 Tweeted by **7**

🟥 **4** readers on Mendeley

Indexed in

OpenAIRE

Publication date:
June 22, 2018

DOI:
DOI 10.5281/zenodo.1307551

Grants:
European Commission:
- IS-ENES2 - Infrastructure for the European Network for Earth System modelling - Phase 2 (312979)
- AARC2 - Authentication and Authorisation For Research and Collaboration (730941)
- CORBEL - Coordinated Research Infrastructures Building Enduring Life-science services (654248)
- ELIXIR-EXCELERATE - ELIXIR-EXCELERATE: Fast-track ELIXIR implementation and drive early user exploitation across the life-sciences. (676559)
- CALIPSOplus - Convenient Access to Light Sources Open to Innovation, Science and to the World (730872)
- IS-ENES - InfraStructure for the European Network for Earth System Modelling (228203)
- GN4-2 - GN4-2 Research and Education Networking - GÉANT (731122)

FIM4R Recommendations

Governance & Sustainability

Research representation, funding for sustainable operation, ongoing coordination

Baseline of User Experience

Attribute release, remove interoperability barriers, non-legal status, user mobility

Security Incident Response Readiness

For federations, interfederation and organisations

Harmonisation of Proxy Operations & Practices

Reuse generic services, follow best practices for interoperability

Sensitive Research User Experience

Support multifactor authentication and publish Assurance Profiles

Slide taken from FIM4R Session, TNC2018

Nine Stakeholder Groups to address

- General Stakeholders
  - Network coordinators and operators:
    GÉANT (Europe), Internet2 (US)
  - Research funding bodies
  - REFEDS (Research and Education FEDerations group)
- Identity federation stakeholders
  - Researchers’ Home organisations
  - National R&E federations
  - eduGAIN operators providing the Interfederation
- Research stakeholders
  - Generic e-infrastructures
  - Research community proxies in particular
  - Research communities

Slide taken from FIM4R Session, TNC2018

Nine Stakeholder Groups to address

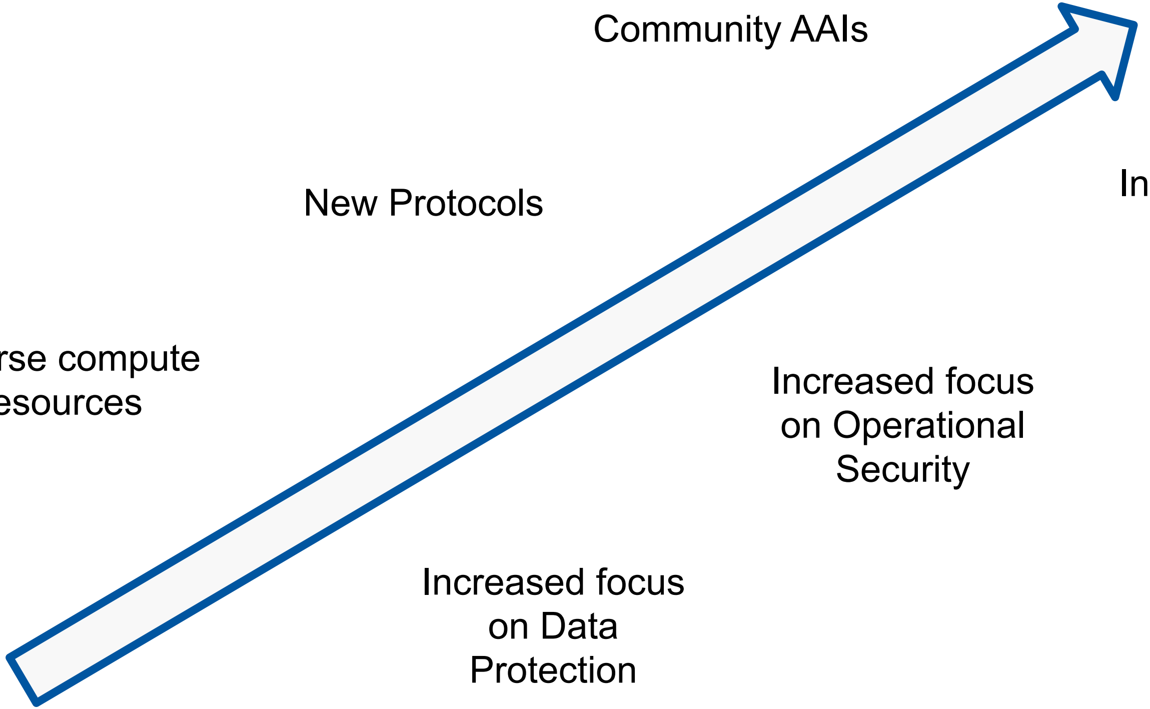
- General Stakeholders
  - Network coordinators and operators:
    GÉANT (Europe), Internet2 (US)
  - Research funding bodies
  - REFEDS (Research and Education FEDerations group)
- Identity federation stakeholders
  - Researchers’ Home organisations
  - National R&E federations
  - eduGAIN operators providing the Interfederation
- Research stakeholders
  - Generic e-infrastructures
  - Research community proxies in particular
  - Research communities

Collaboration
is critical

Slide taken from FIM4R Session, TNC2018

The Future

Trends



Research Community AAIs

New Protocols

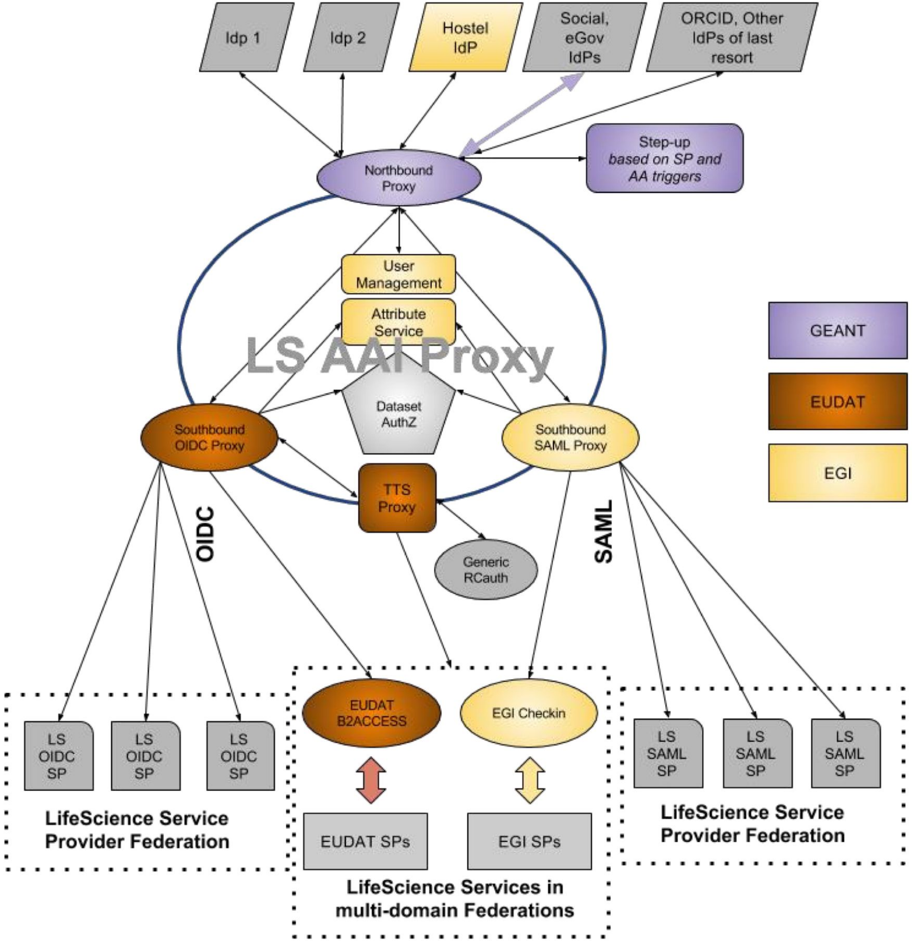
Infrastructure AAIs

Diverse compute resources

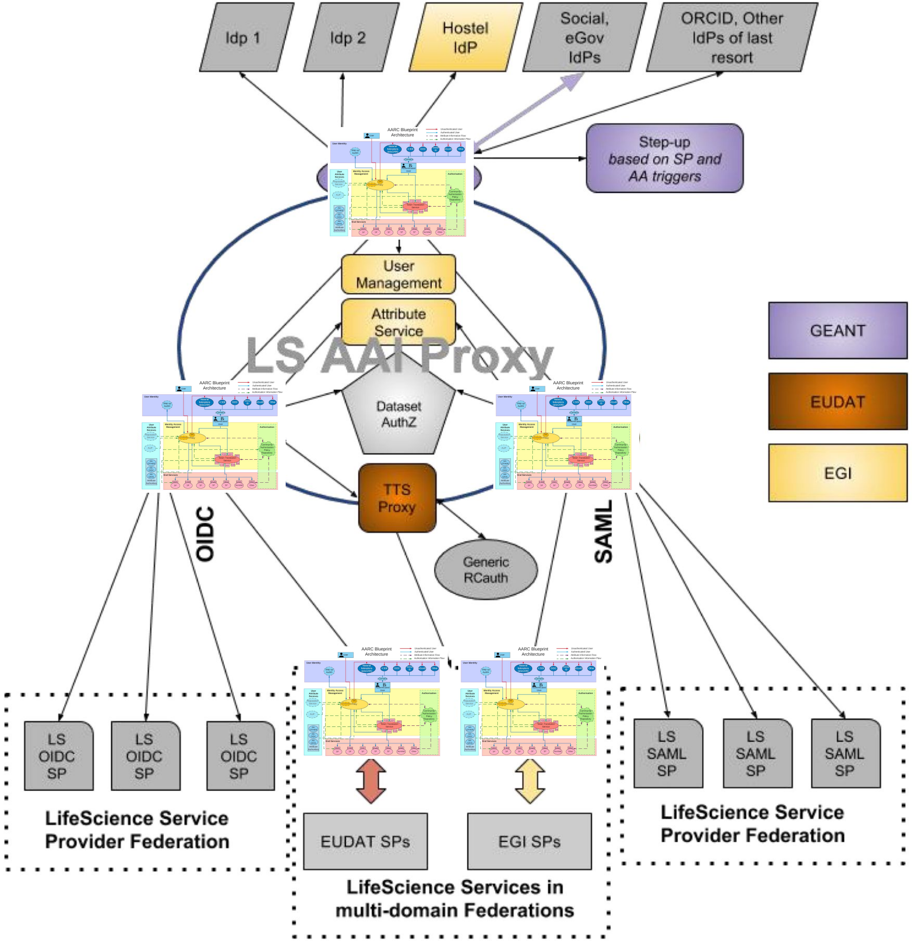
Increased focus on Operational Security

Increased focus on Data Protection

What does this mean for Research Infrastructures?

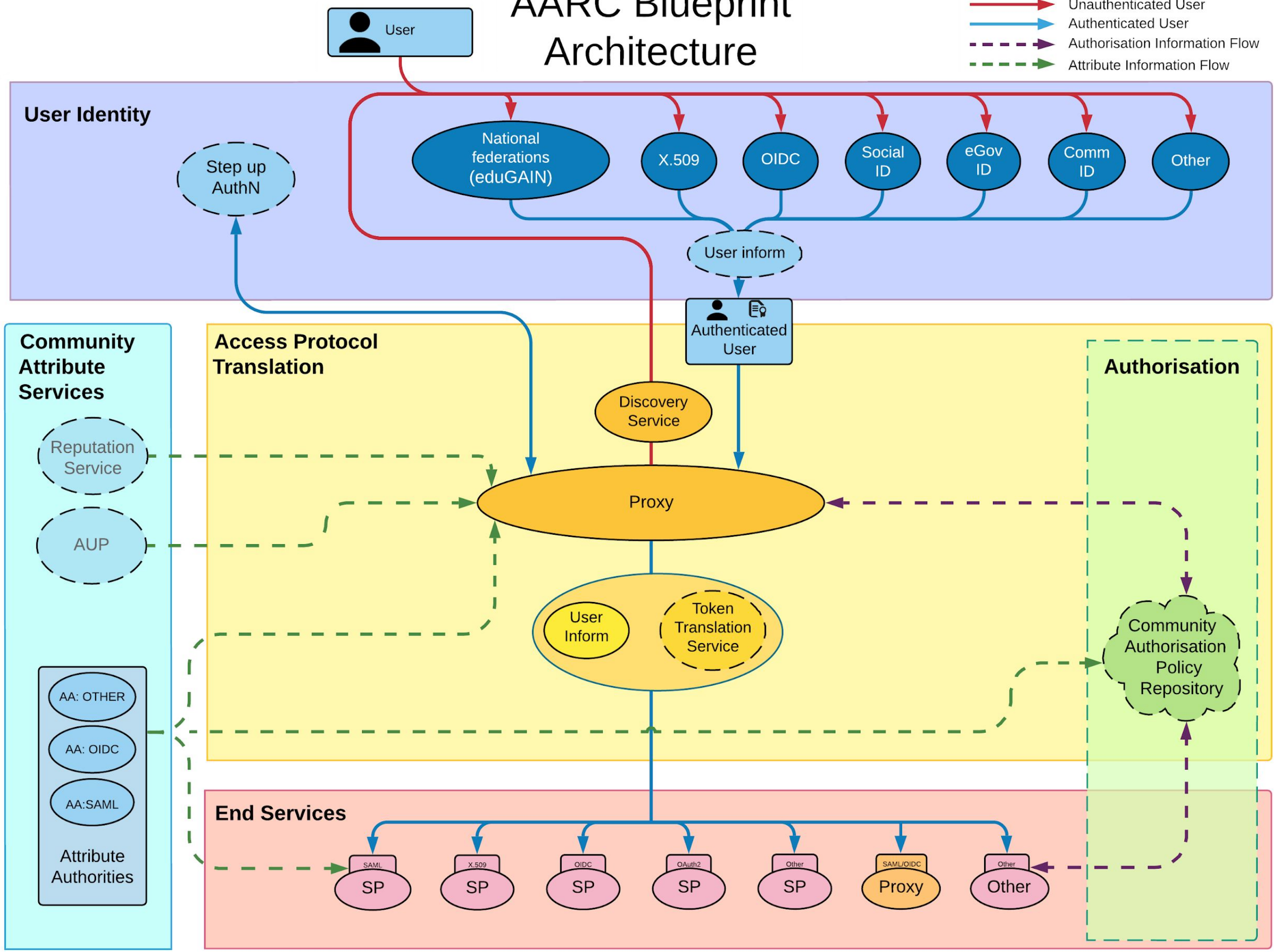


https://aarc-project.eu/wp-content/uploads/2018/09/AARC2-DJRA1.1-V3-v3FINAL.pdf



https://aarc-project.eu/wp-content/uploads/2018/09/AARC2-DJRA1.1-V3-v3FINAL.pdf

AARC Blueprint Architecture



Impact

- Interoperability fundamental
    - Technical
    - Policy
- Overhead of AAI significant
    - Hosted options will be critical
    - Sustainable support for key components required

The FIM4R Recommendations go some way to defining the path towards an interoperable future

What can you do?

A: Read the FIM4R Paper

B: Tell others to

C: Do your bit for Research

D: Nothing

What can you do?

A: Read the FIM4R Paper

B: Share with others

C: Do your bit for Research

D: Nothing

“Every researcher is entitled to focus on their work and not be impeded by needless obstacles nor required to understand anything about the FIM infrastructure enabling their access to research services.” **FIM4R version 2**

CERN