IGTF
Interoperable Global Trust Federation
AP | EU | TAG

Trust and Security in the EUGridPMA and EOSC

Enabling Communities through Trust, Identity, and Security in the Open Science era

David Groep
davidg@nikhef.nl

eugridpma Nikhef

part of the work programme of SURF - the Dutch National e-Infrastructure, GEANT 4-3 EnCo, EGI-ACE, and EOSC-Future

the work has received co-funding from the Horizon 2020 programme of the European Union

co-supported by Nikhef and the Dutch National e-Infrastructure coordinated by SURF

Meanwhile in Europe …

51st plenary proceedings
'consolidate & diversify'

TCS Elliptic Curves

ongoing SCI work items – *AUP and Policy Development Kit*

SCCC JWG – ensuring communications channels

BPA Policy Guidelines

Assurance Profiles
risk-based
…driven

wait for the ISGC presentation!

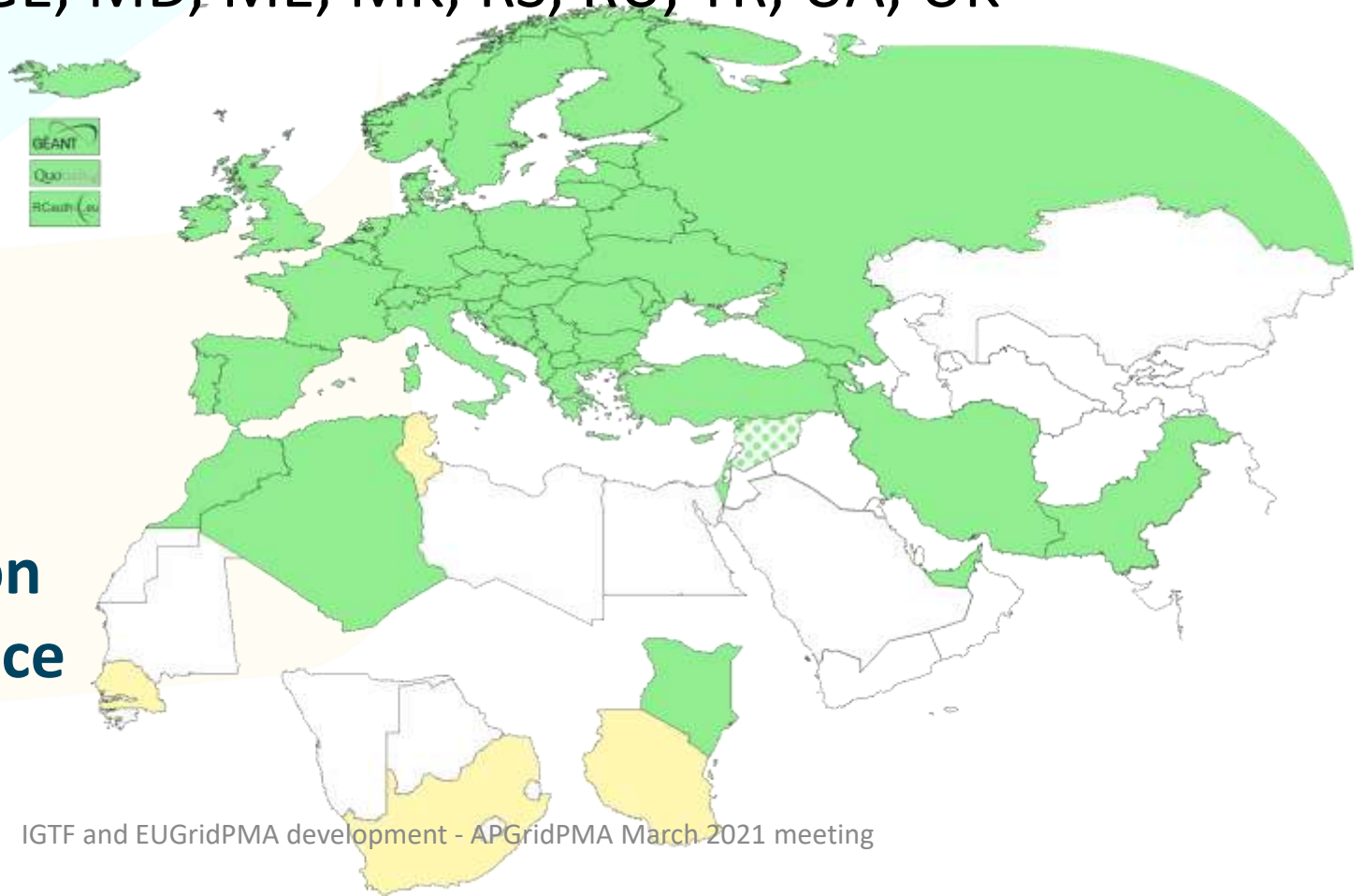
Secure Operations
for AAs & proxies

European Open Science Cloud – AAI for heterogeneous connected services

EOSC Trust & Security
a risk-based approach with a stong core

IGTF EMEA area membership evolution

- Europe: GEANT TCS and CZ, DE, DK(+FI+IS+NO+SE), FR, GR, HR, HU, NL, PL, PT, RO, SI, SK; AM, GE, MD, ME, MK, RS, RU, TR, UA, UK
- Middle East: AE, IR, PK
- Africa: DZ, KE, MA
- CERN, RCauth.eu, DigitalTrust (AE)



Emphasis on collaboration across the whole T&I space

Membership and other changes

- Identity providers: both reduction and growth
  - RCauth.eu distributed operations (GRNET, STFC, Nikhef)
    using a shared key (and some smart border-guard-proof distribution mechanisms)
  - TCS Gen 4 now operational – although with some rough edges
  - INFN discontinued (with unavailable CRL)

- Self-audit review
  - Cosmin Nistor as review coordinator
  - Self-audits are slacking a bit – fewer CAs …

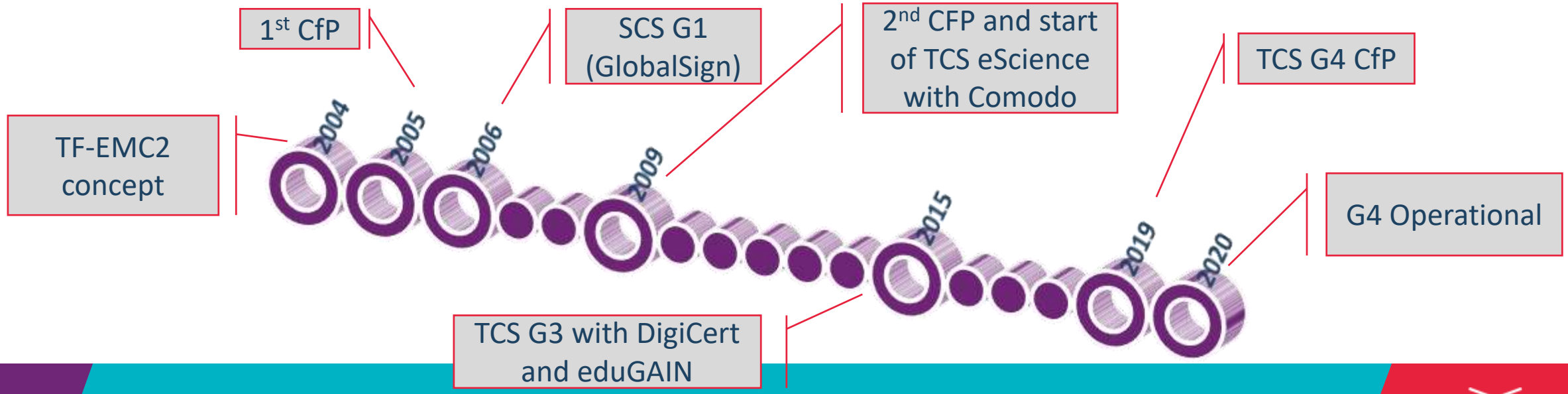
		Specific Policies and Practices			
TR-Grid CA (Turkey) *(Authority member)* (TACAR OK)	Feyza Eryol	CA TRGrid (accredited:classic): CERT CRL concerns: ca@grid.org.tr A2:31:9E:C8:90:AF:D9:6D:F4:4A:59:31:F2:E6:D2:D5:39:EC:1D:F0 Generic CP and CPS statements	2005-09-29	2016-01-20	2016-01-20 (0.2yr)
Trans-European Research and Educational Networking Association (TERENA) *(Relying Party member)*	Licia Florio (277707CC)	*CP and CPS are not relevant* About TERENA: http://www.terena.org/	2004-04-01	2015-09-09	
UK e-Science CAs *(Authority member)* (TACAR OK)	Jens Jensen (9210F006) David Kelsey	CA UKeScienceRoot-2007 (accredited:classic): CRL concerns: support@grid-support.ac.uk A1:39:B0:F3:04:6C:0B:F9:F5:0A:1B:33:00:06:4F:83:6B:7D:4F:3E CA UKeScienceCA-2A (accredited:classic): CRL concerns: support@grid-support.ac.uk 41:C7:C4:A0:31:F7:07:02:81:C7:61:D5:7E:92:48:01:DF:87:C9:06 CA UKeScienceCA-2B (accredited:classic): CRL concerns: support@grid-support.ac.uk DB:D9:5A:B4:E9:AD:74:26:E0:33:68:AA:B1:77:CC:5B:64:B2:CB:0E Generic CP and CPS statements	2000-12-04	2016-01-20	2014-01-14 (2.2yr)
Ukrainian Grid CA *(Authority member)* (TACAR FAILURE)	Sergii Stirenko Oleg Alienin	CA UGRID (accredited:classic): CERT CRL concerns: ca@ugrid.org 21:E7:0D:EE:D7:57:B6:47:A6:F5:04:29:76:81:FE:CD:E8:48:DD:9A Generic CP and CPS statements	2008-02-14	2013-09-11	2013-09-11 (2.5yr)

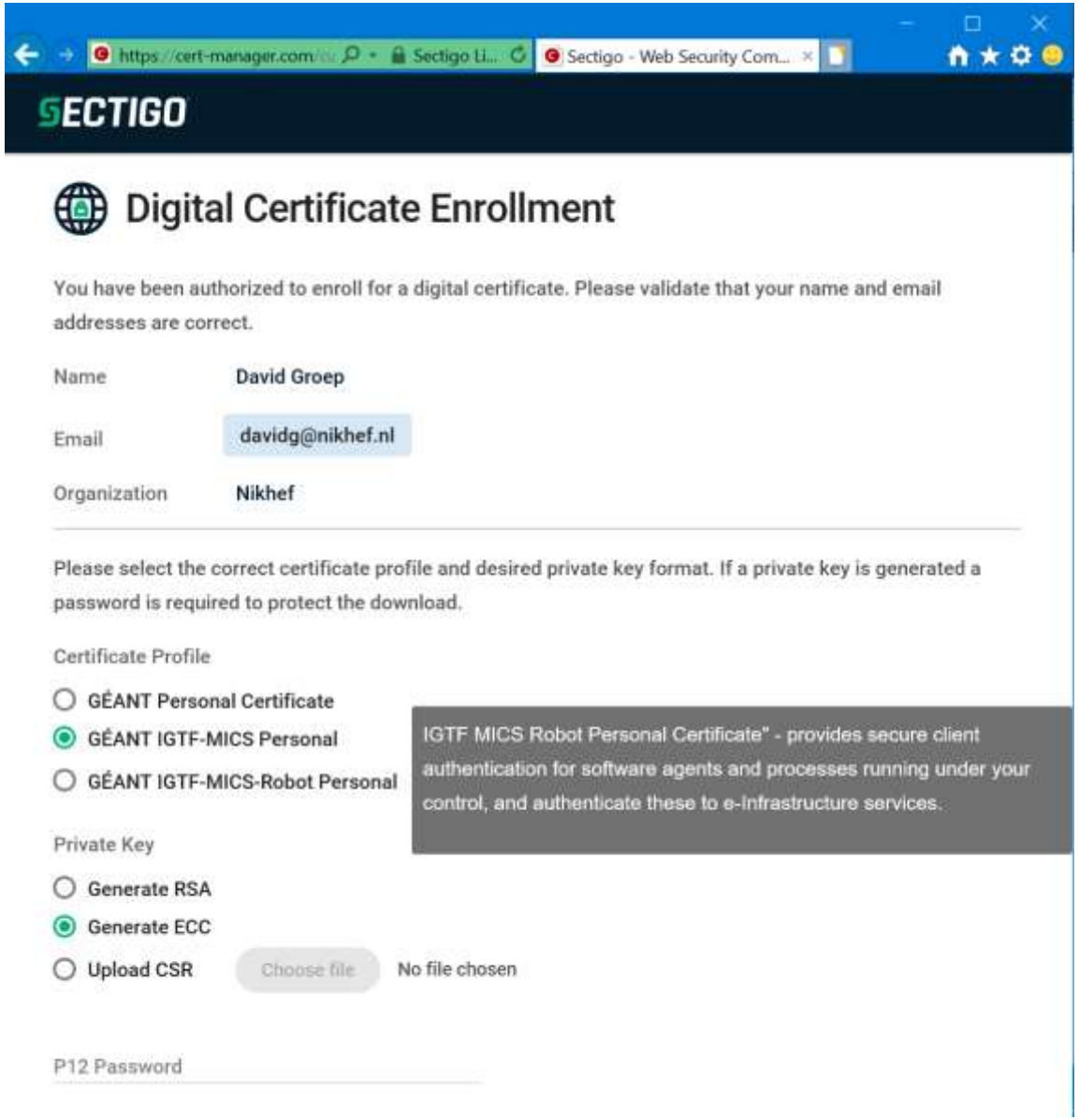
(TCS) EVOLUTION – AND ECC CERTS

15 years of TCS and going strong …

driven by public web trust, with the eScience use cases very much in mind

- NREN (GEANT constituency) relies on public trust, OV, today still EV, but also eIDAS
- in a way that scales to 45 countries and ~100k active certificates today, increasing steadily
- and also ~10k organisations, most of which cannot deal with certificates … nor with change
- now going to its 4th iteration: GlobalSign, Comodo, DigiCert, … and now Sectigo again





New 'SAML portal'

Newly developed by Murray @Sectigo

Picks profile and name form directly from product type

includes ePPN as uniqueID

Support .P12 generation and CSR …

… and … ECC!

A new thing: ECC IGTF certs

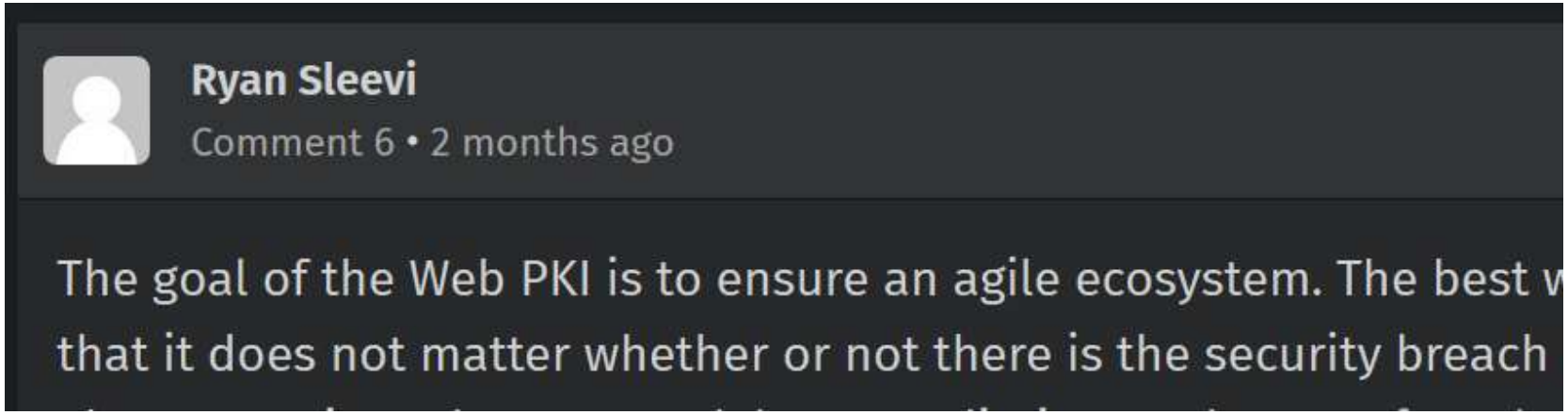
- Although ECC certs were available in TCSG3 as well, it was ‘a well-hidden option’ and never advertised and through the IGTF we never distributed the ECC variants of TCS G3
- New self-service portal for TCS G4 personal – since it generates key pairs on the CA side – now makes ECC certificates very prominent, and a first-class citizen of the ecosystem
- TCS G4 ECC intermediates, and the USERTrust ECC CA root, as ‘experimental’ CAs in the IGTF 1.106 release

ECC certs in the main RP contexts

- introduction of ECC anchors in 1.106 did not result in any issues
- at least *voms-proxy-init* in emi-ui >=3.7 does not explode, which is good™ (but the same in versions <=3.3 is known to get confused by them)
- Installing as extra trust anchors should be harmless, until a user trigger one

Validation remains challenging

Issue brought to new heights during enforced mass revocation in July 2020



https://bugzilla.mozilla.org/show_bug.cgi?id=1650910

and since people like Ryan continue to exert influence over end-relying parties …

(it would be nice if the goal of WebPKI were to have a secure ecosystem, instead of thinking agility is a goal in and of itself …)

and more useless agility is coming – in browser trust sphere, expect ~3mo validity!

– so there you need prepare for ACME if you (also) need web trust

Baseline Acceptable Use Policy

Policy Development Kit

From IGTF RAT CC to ‘Security Communications Challenge Coordination’ - SCCC

WISE SCI INTERWORKING AND POLICY

https://www.eugridpma.org/meetings/2021-02/

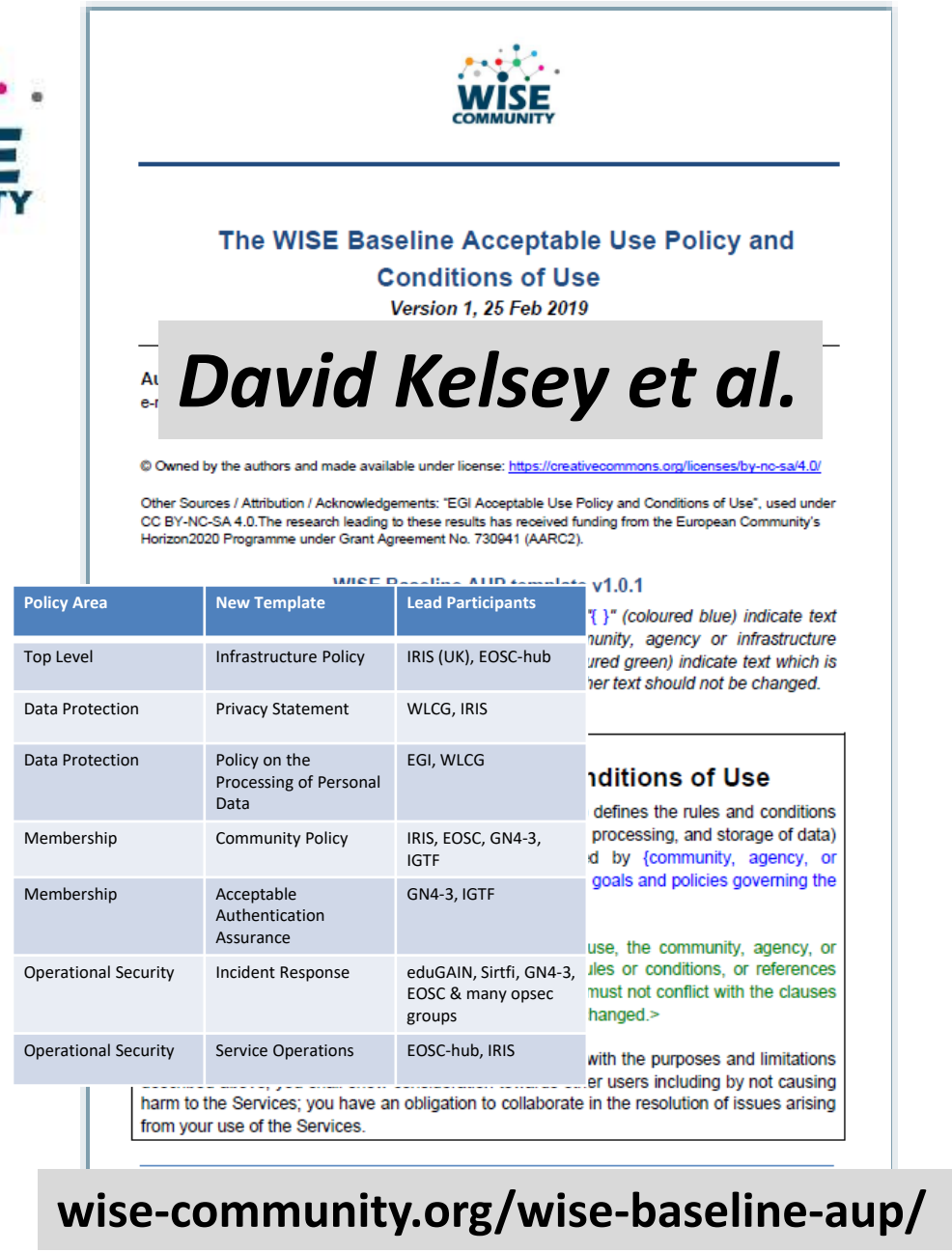
SCI - WISE AUP & PDK

AUP officially published, adopted by many

- relying parties can in the scheme can leverage user acceptance at any peer *specifically: at the community AAI*

Policy Development Kit

- broad work on new ‘top level’ with UK IRIS
- self-assessment review guidance & Implementer’s Guide



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

Communications Challenges – who picks up the call?

TI Reaction Test [TI-XI #107402165633] - Mozilla Thunderbird

File Edit View Go Message Enigmail Tools Help

Get Messages | Write | Chat | Address Book | Tag

Enigmail Good signature from Trusted Introduc

From ti@trusted-introducer.org

Subject TI Reaction Test [TI-XI #107402165633

To security@nikhef.nl

Dear TI Colleagues,

please take a short moment
by clicking on the URL bel
please contact someone tha
representative(s).

The time of your teams rea
member associated with the
teams reaction will be rec

Please visit the following
https://up.trusted-introdu

Best regards,
the Trusted Introducer

[EGI #16469] Site Security Contact Communication Challe

File Edit View Go Message Enigmail Tools Help

Get Messages | Write | Chat | Address B

From via RT <csirt@rt.egi.eu>

Subject [EGI #16469] Site Security Contact Communicatior

To security@nikhef.nl

Dear security contact for ** NIKHEF-ELPROD **,

=== Why you have received this message ===

To verify the security contact data set in the

=== What action is required ===

Confirm that this contact is still correct by

https://csirt-challenge.egi.eu/2020S-fe775a375

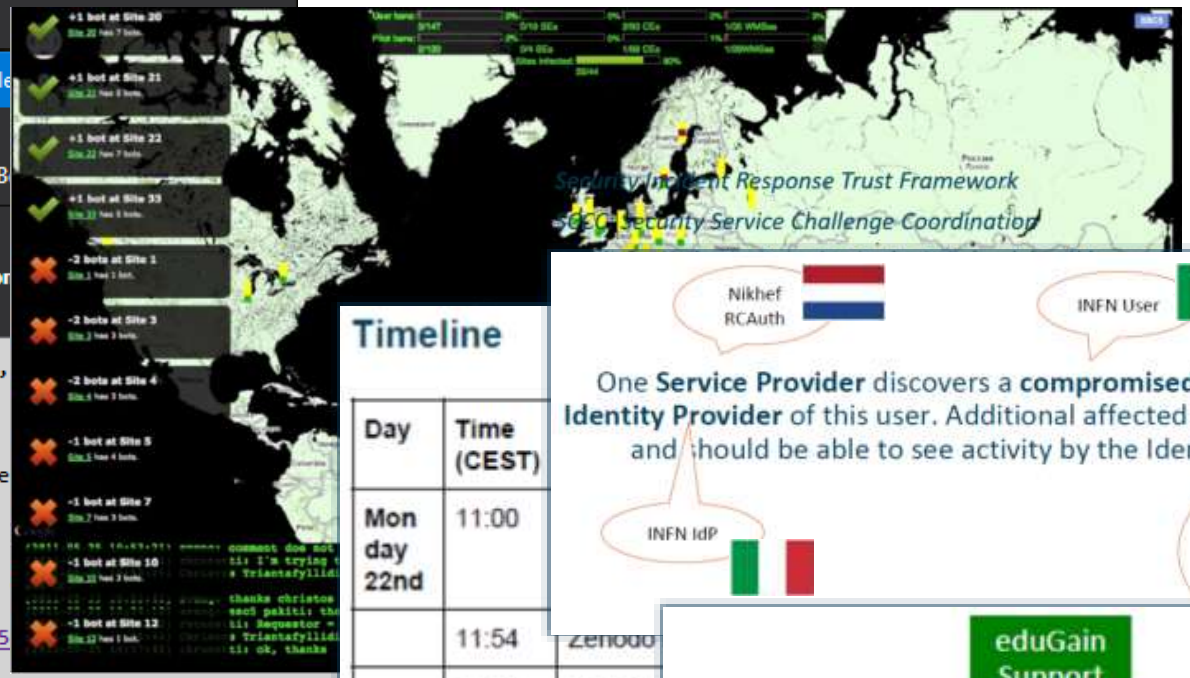
No further action is required except for the above.

=== Additional information ===

The EGI Security Incident Response Procedure requires sites to respond to requests from EGI CSIRT within 4 hours during an incident. For this reason it is essential that the contact information in GOC-DB is kept up to date and remains valid. Challenge emails such as this are used occasionally to test this validity.

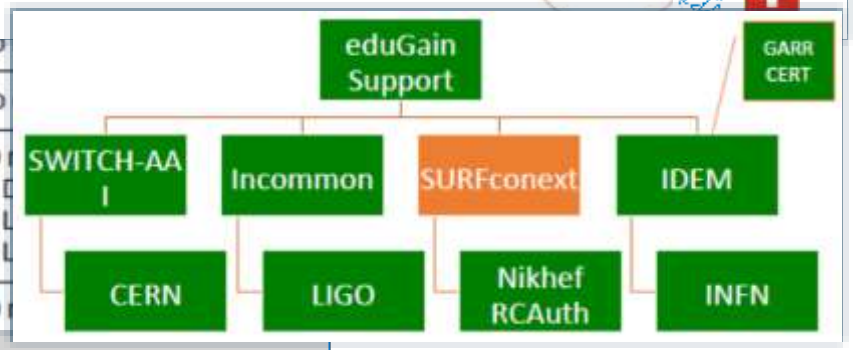
More information and links to the procedure are available here - https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting

Thank you



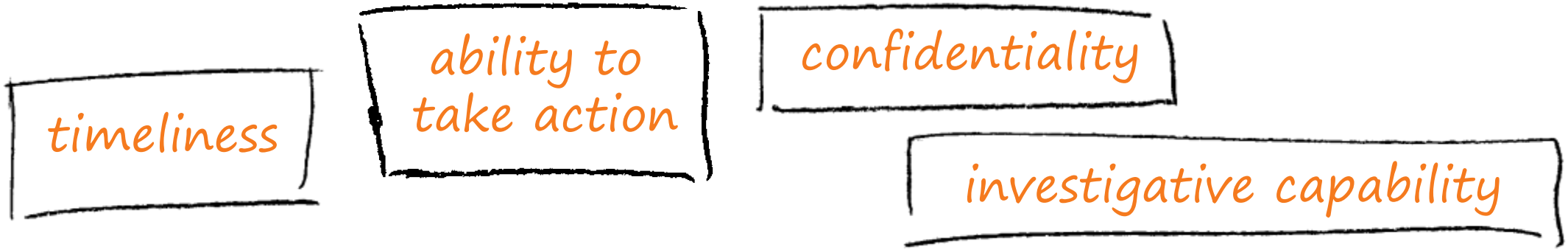
Timeline

Day	Time (CEST)	
Monday 22nd	11:00	
	11:54	Zenodo
	15:00	Zenodo
	15:44	ORCID
	15:56	ORCID



Challenge elements – what is valued or expected might differ …

A single test and challenge can answer one **or more** of these questions

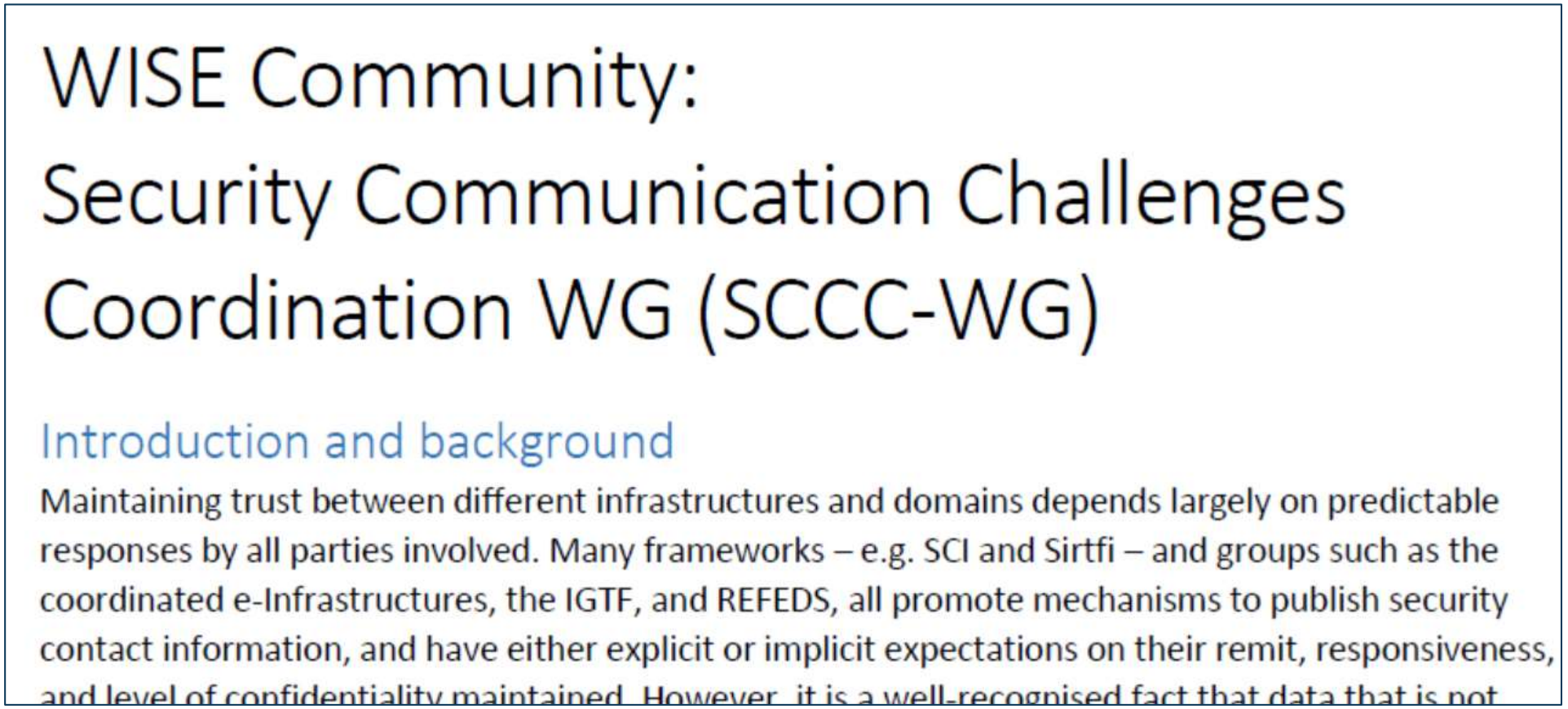


- when data available: infrastructure can set its *own level* of expectancy and gives *deep trust*
- assessment supported with community controls (suspension) gives a *baseline compliance*

Communications challenges build ‘confidence’ and trust – an important social aspect!

- different tests bring complementary results: responsiveness vs. ability act , or do forensics
- unless you run the test yourself, you may not be growing more trust in the entities tested
- for a ‘warm and fuzzy feeling of trust’, share results: but this is sociologically still challenging …

Continued engagement and coordination: WISE SCCC JOINT WG



WISE Community:
Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not

WISE
SIG-ISM
REFEDS
IGTF

https://wiki.geant.org/display/WISE/SCCC-JWG

Subsidiary aim: make security contacts less ‘scary’

The most basic response is to (sorry!) click on a harmless link: making it a challenge to respond ‘as fast as possible’ – a bit like a competition

Ask also a very simple ‘question’ to raise awareness,

> ‘for security contacts, do you want to be (proactively) informed if we have security information relevant to your organisation?’

***esp.* if the contact is the technical rep, i.e. there is no *Sirtfi* contact**

> ‘you got this message because there is no designated security contact for your organisation. Would you want to receive security information, or who (if not you) should be your security contact?
> Are you aware of Sirtfi?’

And we can add some ads for Sirtfi, although having *any* kind of contact is better than none …

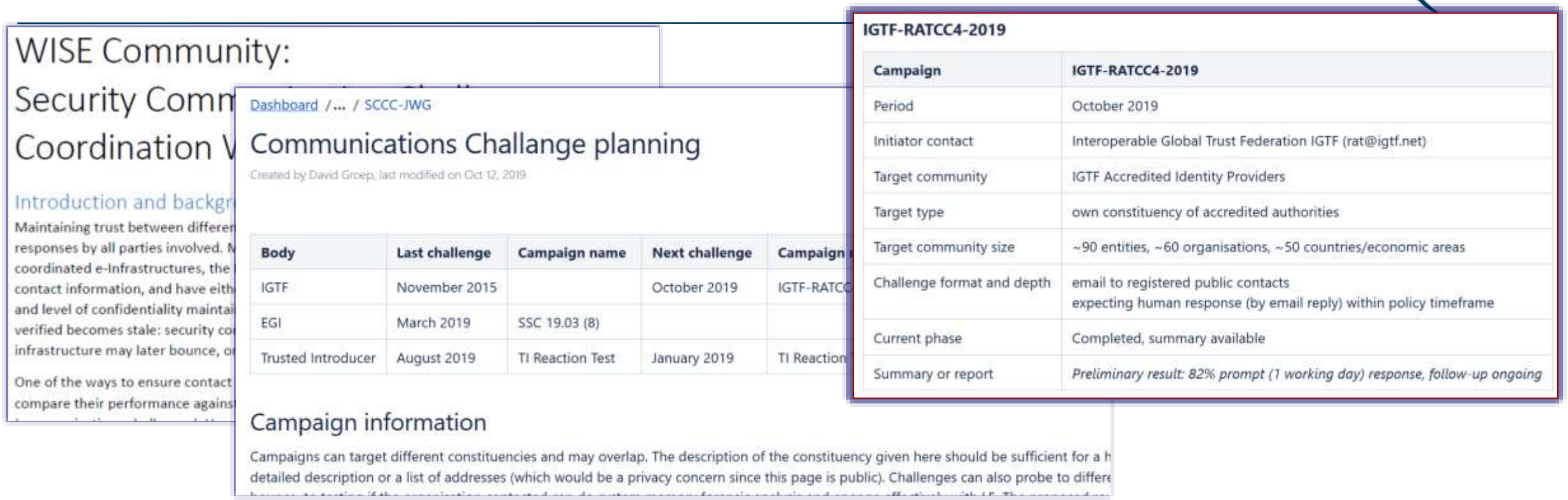
Would *you* like to be contacted?

1. Do you have a security contact listed for your organisation?
   Is your CERT contact public?

2. Do you run (or control) an IdP, and do you support *Sirtfi*?

3. What kind of communications would *you* like to receive there?
   - information about **incidents in connected services**,
     where your users are actively involved?
   - information about incidents that are **currently affecting institutions like yours**
     and are spreading and attacking you soon?
   - information that **people with an email address** from your domain
     are using non-federated services?
   - **communications challenges**, to see whether you're awake?
   - **surveys** and questionnaires? ☺

WISE SCCC-WG – participate!



WISE Community:
Security Comm
Coordination V

Introduction and backgr
Maintaining trust between differen
responses by all parties involved. M
coordinated e-Infrastructures, the
contact information, and have eith
and level of confidentiality maintai
verified becomes stale: security co
infrastructure may later bounce, o

One of the ways to ensure contact
compare their performance agains

Dashboard / ... / SCCC-JWG

Communications Challange planning

Created by David Groep, last modified on Oct 12, 2019

Body	Last challenge	Campaign name	Next challenge	Campaign
IGTF	November 2015		October 2019	IGTF-RATC
EGI	March 2019	SSC 19.03 (8)		
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a h
detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to differe

IGTF-RATCC4-2019

Campaign	IGTF-RATCC4-2019
Period	October 2019
Initiator contact	Interoperable Global Trust Federation IGTF (rat@igtf.net)
Target community	IGTF Accredited Identity Providers
Target type	own constituency of accredited authorities
Target community size	~90 entities, ~60 organisations, ~50 countries/economic areas
Challenge format and depth	email to registered public contacts expecting human response (by email reply) within policy timeframe
Current phase	Completed, summary available
Summary or report	*Preliminary result: 82% prompt (1 working day) response, follow-up ongoing*

WISE, SIGISM, REFEDS, TI joint working group

see wise-community.org wiki and join!

https://wiki.geant.org/display/WISE/SCCC-JWG

co-chairs: Hannah Short (CERN) and David Groep (Nikhef)

voPersonAffiliation – can you heuristically create one?

AARC: ABOUT PROXIES AND THE BPA

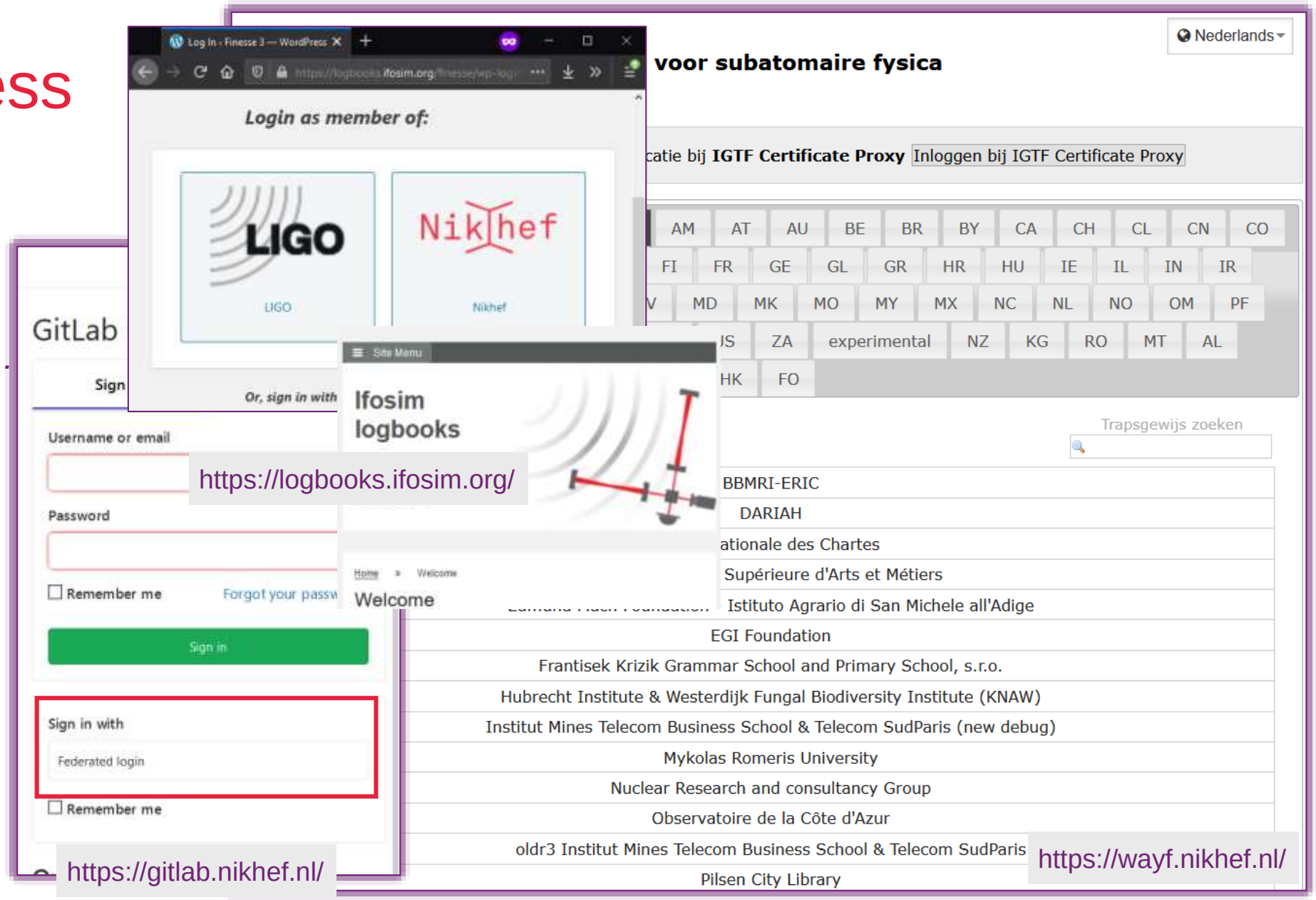
Federated Access

Login to services often via a service proxy

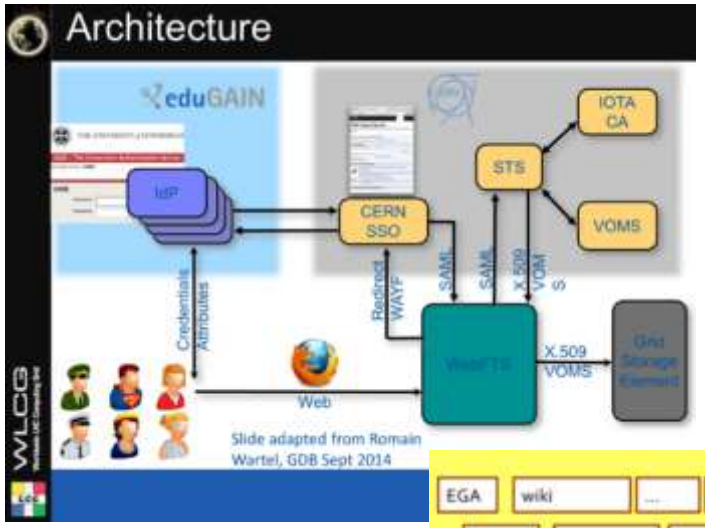
TERENA proxy was one of the first, but it's a common pattern …

"Where are you from"

discovery screen showing entities from the eduGAIN global interfederation

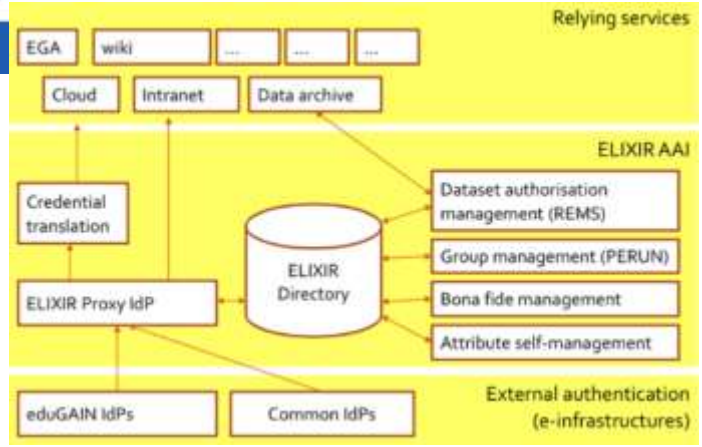


Managing complexities of distributed identity sources

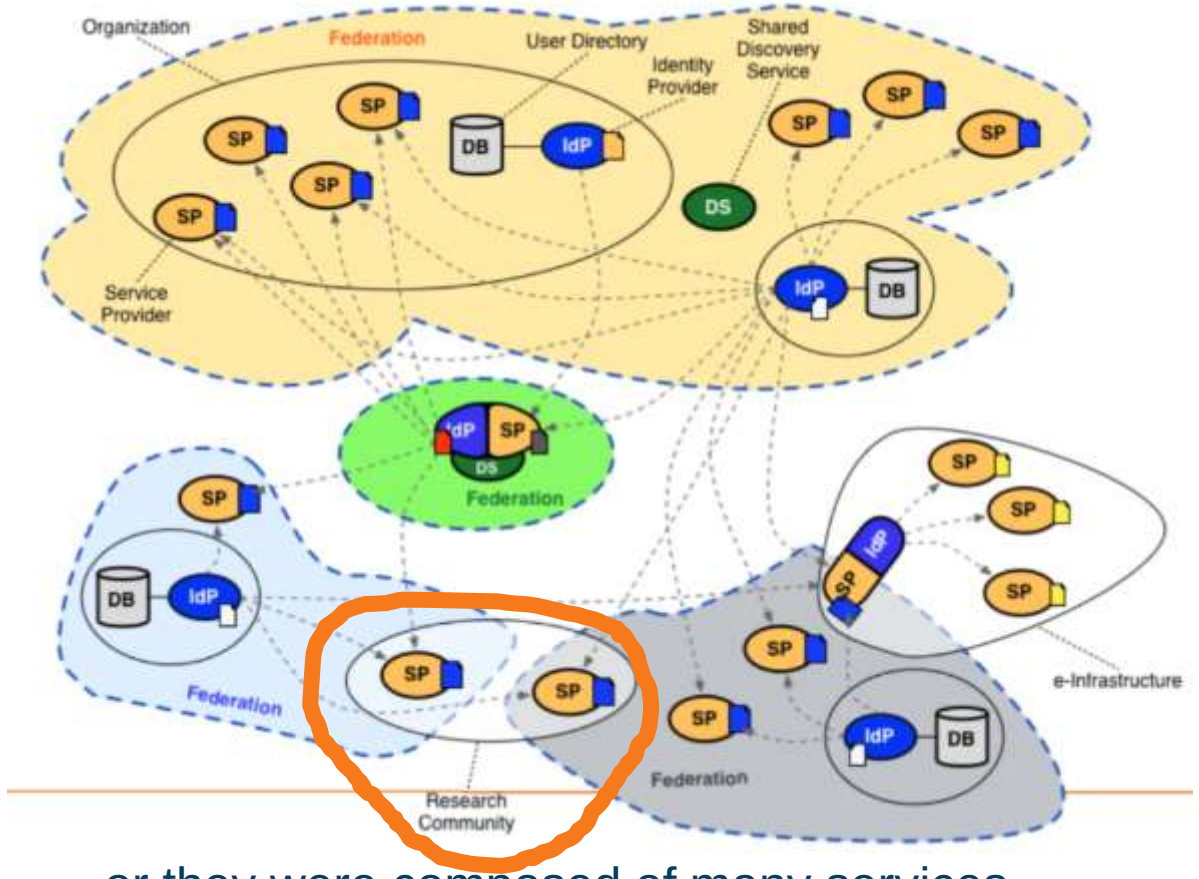


WebFTS prototype
'FIM4R' in wLCG
Romain Wartel et al.

ELIXIR reference architecture
Mikael Linden et al.



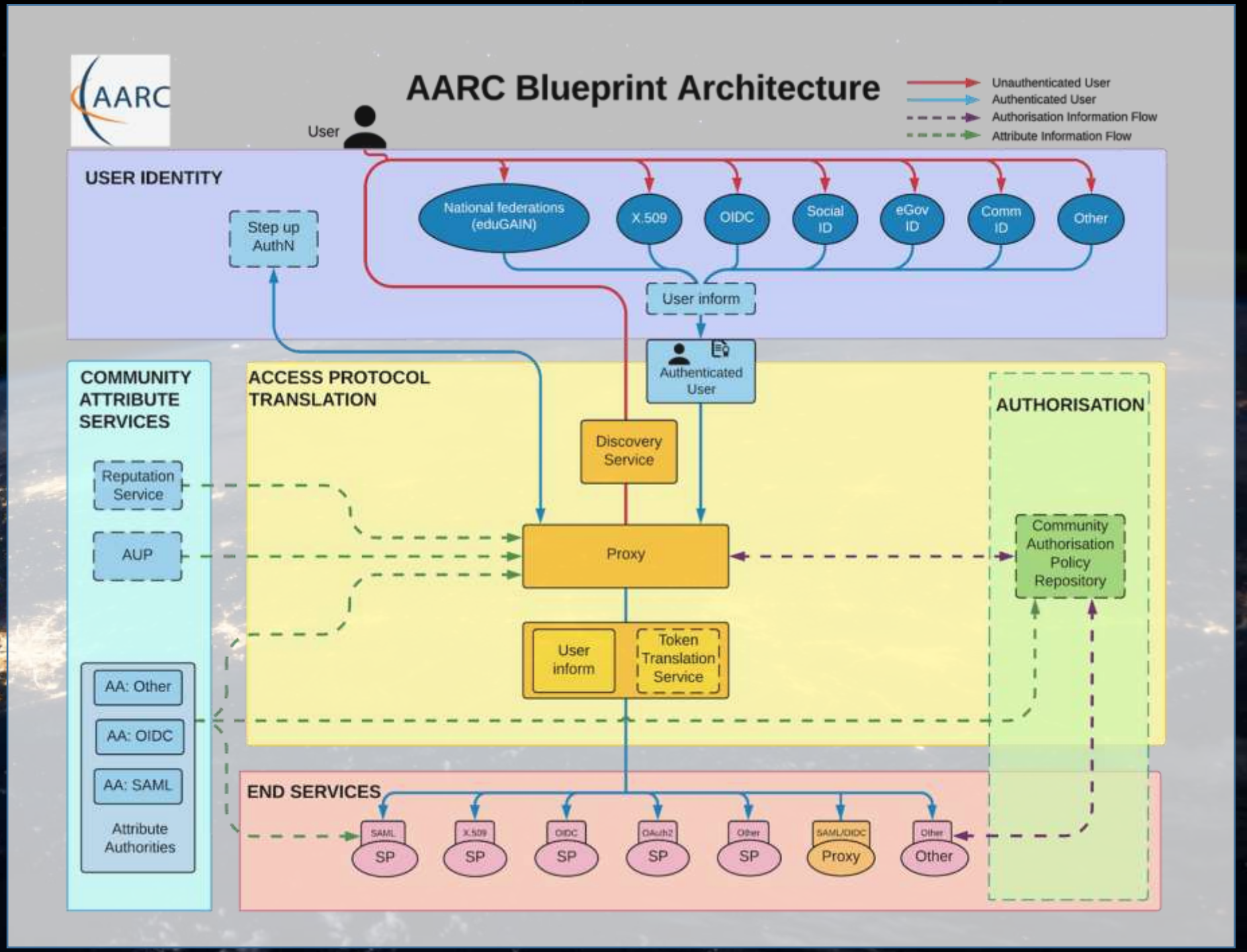
communities had either invented
their own 'proxy' model to abstract complexity



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

AARC BPA


AARC Blueprint Architecture
Unauthenticated User
Authenticated User
Authorisation Information Flow
Attribute Information Flow
User
USER IDENTITY
Step up AuthN
National federations (eduGAIN)
X.509
OIDC
Social ID
eGov ID
Comm ID
Other
User inform
Authenticated User
COMMUNITY ATTRIBUTE SERVICES
ACCESS PROTOCOL TRANSLATION
AUTHORISATION
Discovery Service
Reputation Service
AUP
Proxy
Community Authorisation Policy Repository
User inform
Token Translation Service
AA: Other
AA: OIDC
AA: SAML
Attribute Authorities
END SERVICES
SAML SP
X.509 SP
OIDC SP
OAuth2 SP
Other SP
SAML/OIDC Proxy
Other Other

All about the AARC BPA

Not sure how to begin with the AARC Blueprint Architecture? There are plenty of guidelines available but it can be a minefield at first. Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

Getting Started:

- How should I design my infrastructure? What is the AARC Blueprint Architecture? AARC-G045
- How should I approach performing a Data Protection Impact Assessment? AARC-G042
- How should my infrastructure support Federated Security Incident Response? AARC-I051

Access Protocol Translation:

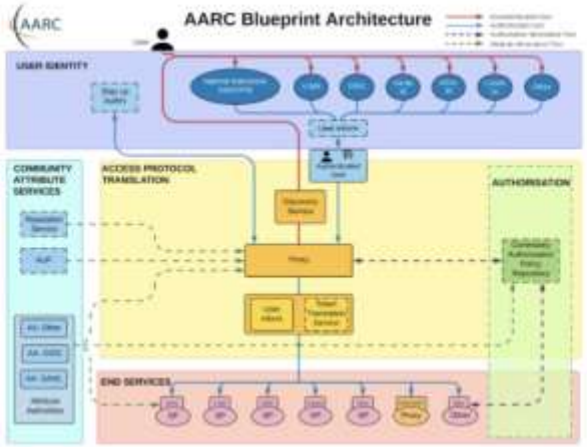
- Which best practices should I follow for my Token Translation Services? AARC-G004
- How should I translate from Identity Federation information to X.509 certificates? AARC-G010

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 assurance information for users when interacting with another proxy? AARC-G021

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
- What are the best practices for running my Attribute Authorities securely? AARC-G048
- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044



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

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

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.

Certain guidelines are being adopted by the AEGIS community to support interoperability between infrastructures - consider prioritising these best practices.

On the AARC and FIM4R site

Many thanks to Hannah !

https://edu.nl/h3dm4

concept and publication: Hannah Short – slide inspired by Maarten Kremers

BPA Guidance

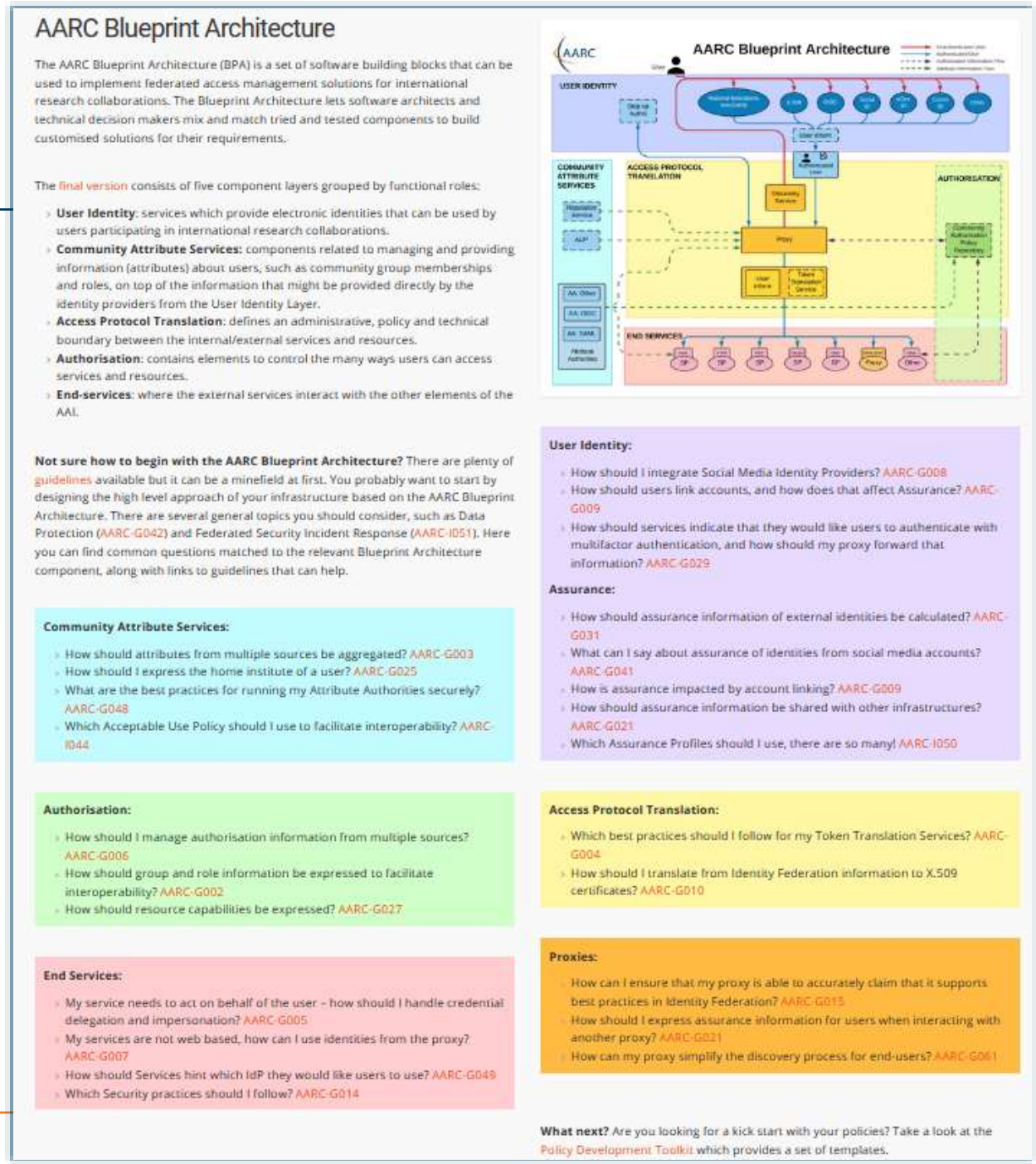
- Hannah Short made a great structured guide to the AARC Blueprint Architecture

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

- identifies relevant standards for each area

- links to the **Policy Development Toolkit PDK**

  available from both FIM4R and AARC



AARC Blueprint Architecture

The AARC Blueprint Architecture (BPA) is a set of software building blocks that can be used to implement federated access management solutions for international research collaborations. The Blueprint Architecture lets software architects and technical decision makers mix and match tried and tested components to build customised solutions for their requirements.

The final version consists of five component layers grouped by functional roles:

- **User Identity**: services which provide electronic identities that can be used by users participating in international research collaborations.
- **Community Attribute Services:** components related to managing and providing information (attributes) about users, such as community group memberships and roles, on top of the information that might be provided directly by the identity providers from the User Identity Layer.
- **Access Protocol Translation**: defines an administrative, policy and technical boundary between the internal/external services and resources.
- **Authorisation**: contains elements to control the many ways users can access services and resources.
- **End-services**: where the external services interact with the other elements of the AAI.

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
- What are the best practices for running my Attribute Authorities securely? AARC-G048
- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044

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-G069
- 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 assurance information for users when interacting with another proxy? AARC-G021
- How can my proxy simplify the discovery process for end-users? AARC-G061

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.

Example guideline G056: can you see ‘through’ the proxy to the home org?

Is the service dealing with a (university) researcher, a student, …?

Can the proxy infer some of this for the benefit of the SP?

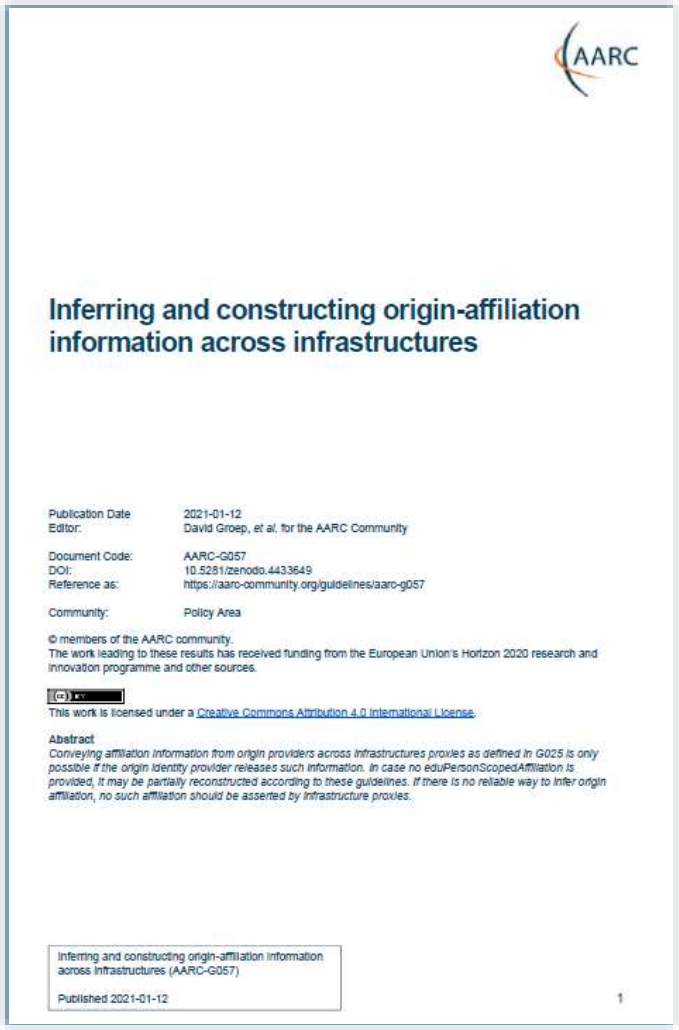
2. When to construct origin affiliation

A proxy SHOULD NOT assert *vPEA* unless the service provider requests this attribute. If no origin *ePSA* attribute is provided, and no *vPEA* is requested by the service provider, then a proxy MUST NOT construct a gratuitous *vPEA*.

If a service provider requests *vPEA*, but no *ePSA* is provided by the origin, a proxy SHOULD infer or construct a *vPEA*, and if it does, MUST do so only in accordance with this Guideline.

- get the *scope* right (e.g. using trusted meta-data or DCV)
- harmonise affiliation and ‘scoped’ affiliations
- allow both automated and verified enrolment by the proxy

should enable SPs to use and interpret voPersonExternalAffiliation



Inferring and constructing origin-affiliation information across infrastructures

Publication Date 2021-01-12
Editor: David Groep, *et al.* for the AARC Community

Document Code: AARC-G057
DOI: 10.5281/zenodo.4433649
Reference as: https://aarc-community.org/guidelines/aarc-g057

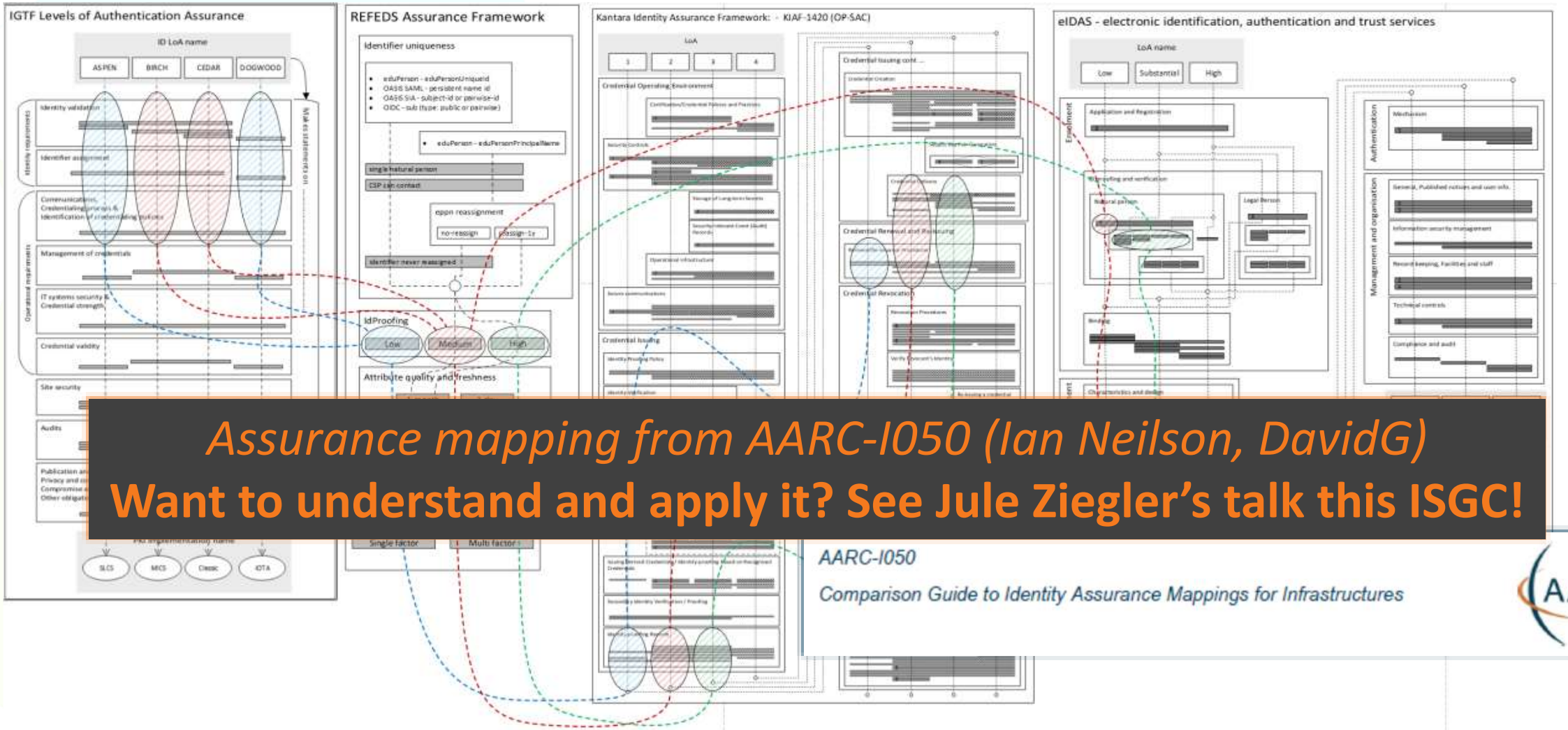
Community: Policy Area

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme and other sources.

Abstract

Conveying affiliation information from origin providers across infrastructures proxies as defined in G025 is only possible if the origin identity provider releases such information. In case no eduPersonScopedAffiliation is provided, it may be partially reconstructed according to these guidelines. If there is no reliable way to infer origin affiliation, no such affiliation should be asserted by infrastructure proxies.

Since even ‘Identity assurance’ components are already complex



Revising the Guidelines for Running a
Secure Membership Management Service and Proxy

ATTRIBUTE AUTHORITY OPERATIONS “REV 2”

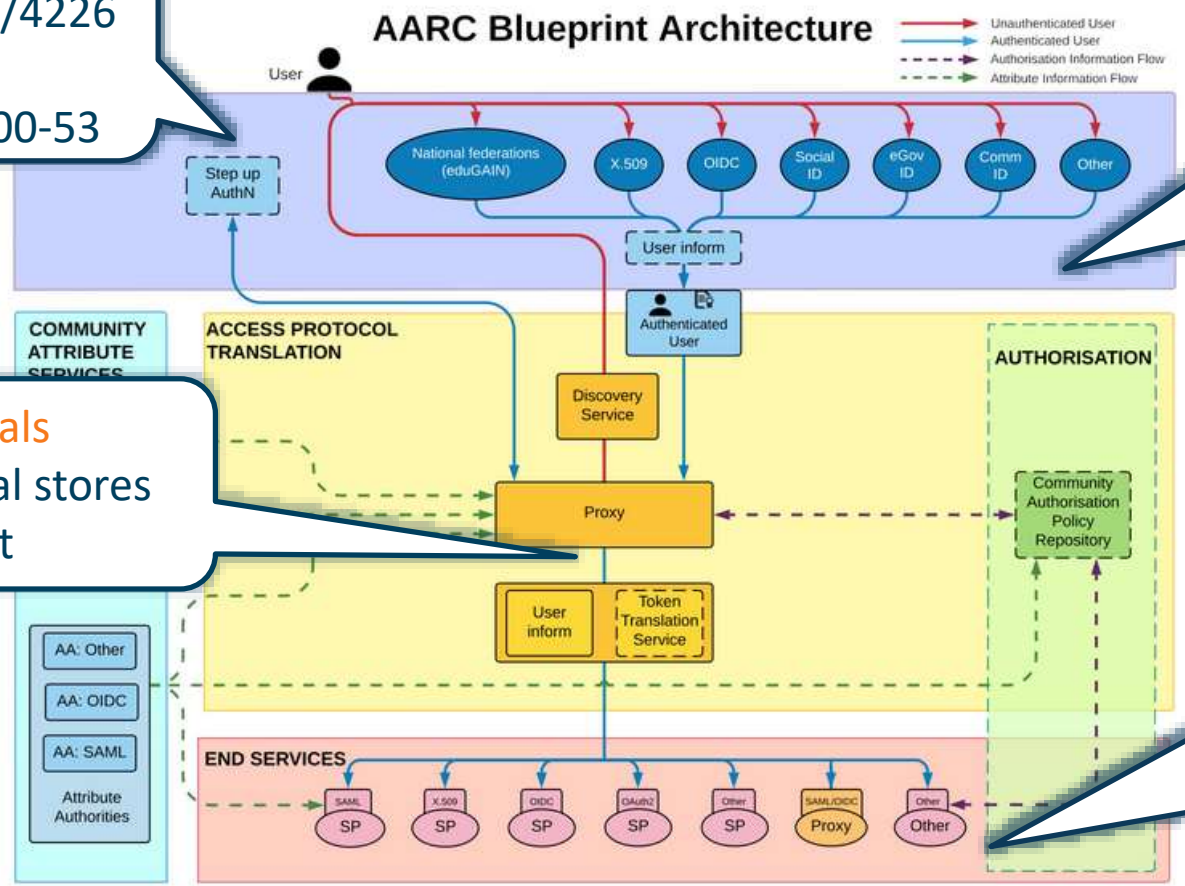
Policy guidance for proxy AAI components

MFA
RFC6238/4226
FIPS140
NISTSP800-53

Authentication/identity sources
Sirtfi
(eduGAIN) baselining
IGTF AP Profiles
NIST SP800-63
eduGAIN sec. team workflow

Ephemeral credentials
- trusted credential stores
- protection at rest

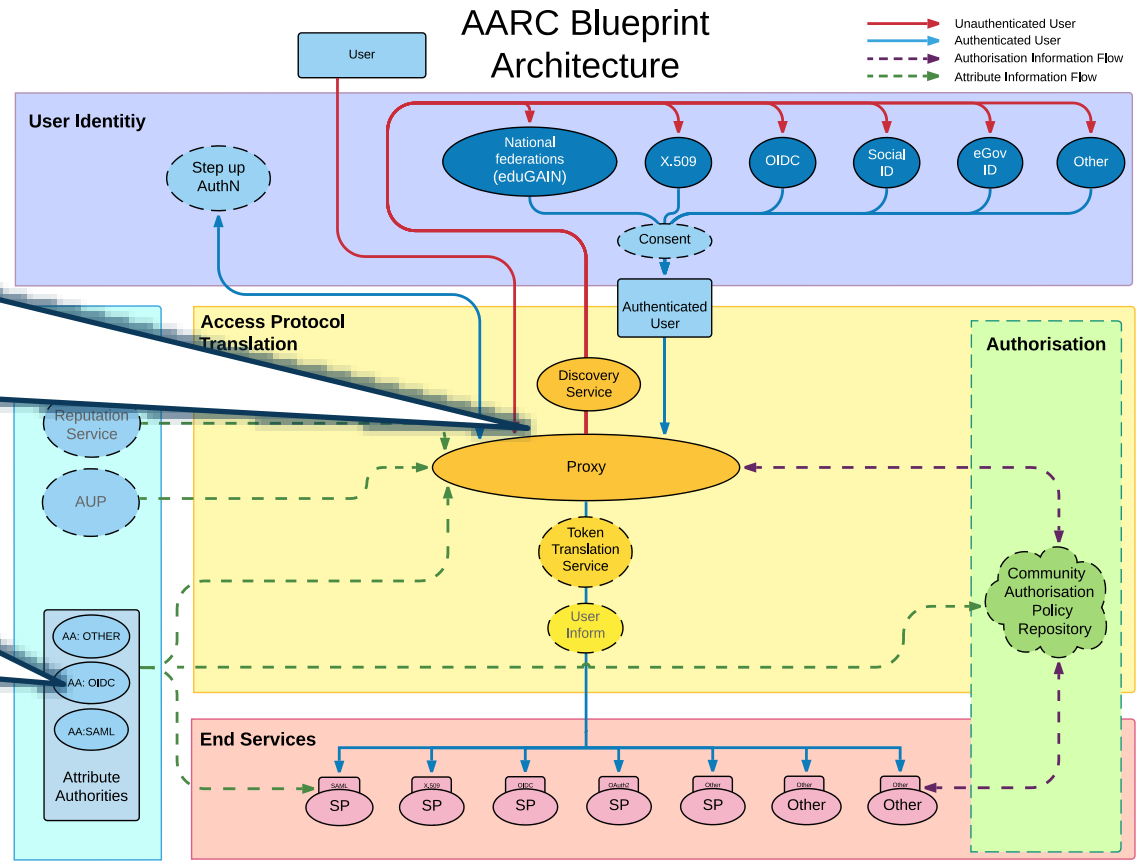
Service provider operations
ISO27k
Sirtfi
Infrastructure response plans



Operational security in the BPA: beyond IdPs and SPs

Membership management attribute authorities
+ credential proxying

- integrity of membership
- identification and naming
- assertion integrity
- traceability and logging

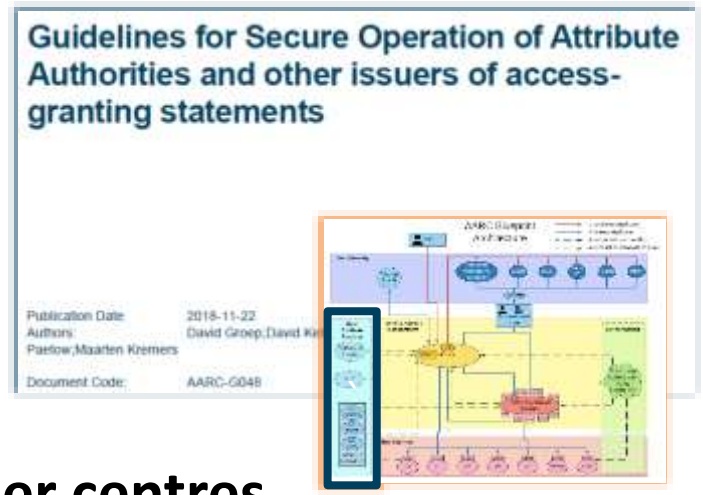


Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements
(AARC-I048, in collaboration with IGTF AAOPS)

AARC-G048: protecting the proxies users and services

trusted delegation of response from communities to operators, and from services to communities in recognizing their assertions

Structured around concept of "**AA Operators**",
operating "**Attribute Authorities**" (technological entities),
on behalf of, one or more, **Communities**



Many recommendations already implemented 'implicitly' in proper centres

- common software implements it: e.g. signing SAML assertions and JWTs
- a good data centre already has network monitoring and central logging in place
- since the proxy signed up to Sirtfi (didn't you?) – so you collaborate in incident response

or best practice, and knowledge worth sharing

- like assigning a unique and lasting names, putting in transparency and sharing controls
- privacy notices and personal data protection are already mandatory

https://www.igtf.net/guidelines/aaops/ **https://aarc-community.org/guidelines/aarc-g048/**

Balancing generalisation and actionable guidance

G048 Revision 2 Process

2. In addition to ~~The AA should~~ meeting its own regulatory obligations, the AA must respect data protection requirements of the ~~Infrastructure and~~ Community. It is recommended ~~This may mean~~ that AAs require client-side authentication, in addition to the encryption of the messages and the communication channel. The ...data than requested by the RP.

2 ~~... a virtual environment only where the virtual environment has ... better level of security than required for the AA itself, and for all services running in this environment, and it must not leave this security context. Any virtualization techniques employed (including the hosting environment) must not degrade the security context.~~

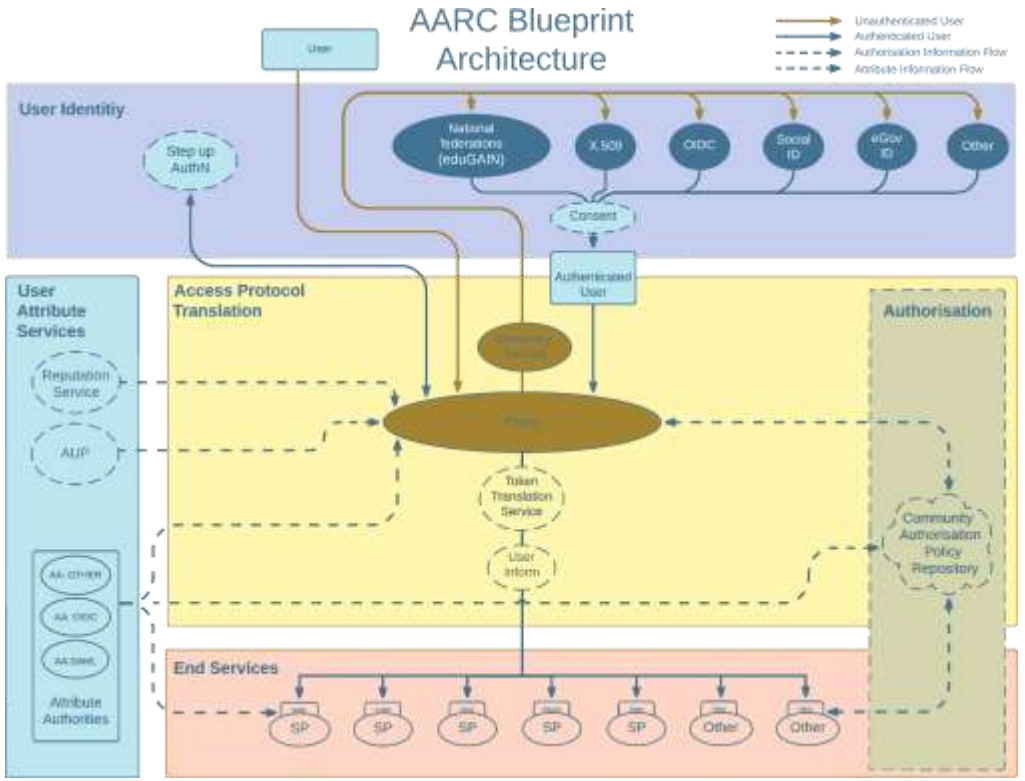
Through its personnel or by contractual measures, ~~the~~ AA operator should ensure appropriate controls are in place over the security context ~~AA Operator should have control over the virtualised security context of the AA~~.

3. The AA must be located in a physically secure environment where access is controlled and limited to specific trained personnel.

... registration model, the protection put in place to prevent ... data from the OpenID Connect Provider (OP) is the ...ge at the ~~interstitial~~ user authentication point and asking ...om the user. This constitutes an implementation of 'client

Implementers of AAs SHOULD use placement policies to ensure physical and/or virtual separation of sensitive and non-sensitive services, containers, or VMs to reduce the risk of cross-compromise. In all cases, the environment itself must be protected according to current best practice, and a risk assessment of the environment should be performed[e.g. based on the WISE SCI and Sirtfi requirements], taking into account both the integrity of the AA as well as the requirements of the communities hosted on the AA and the relying parties receiving attributes.

wiki.geant.org/display/AARC/Attribute+Authority+and+Proxy+operational+security



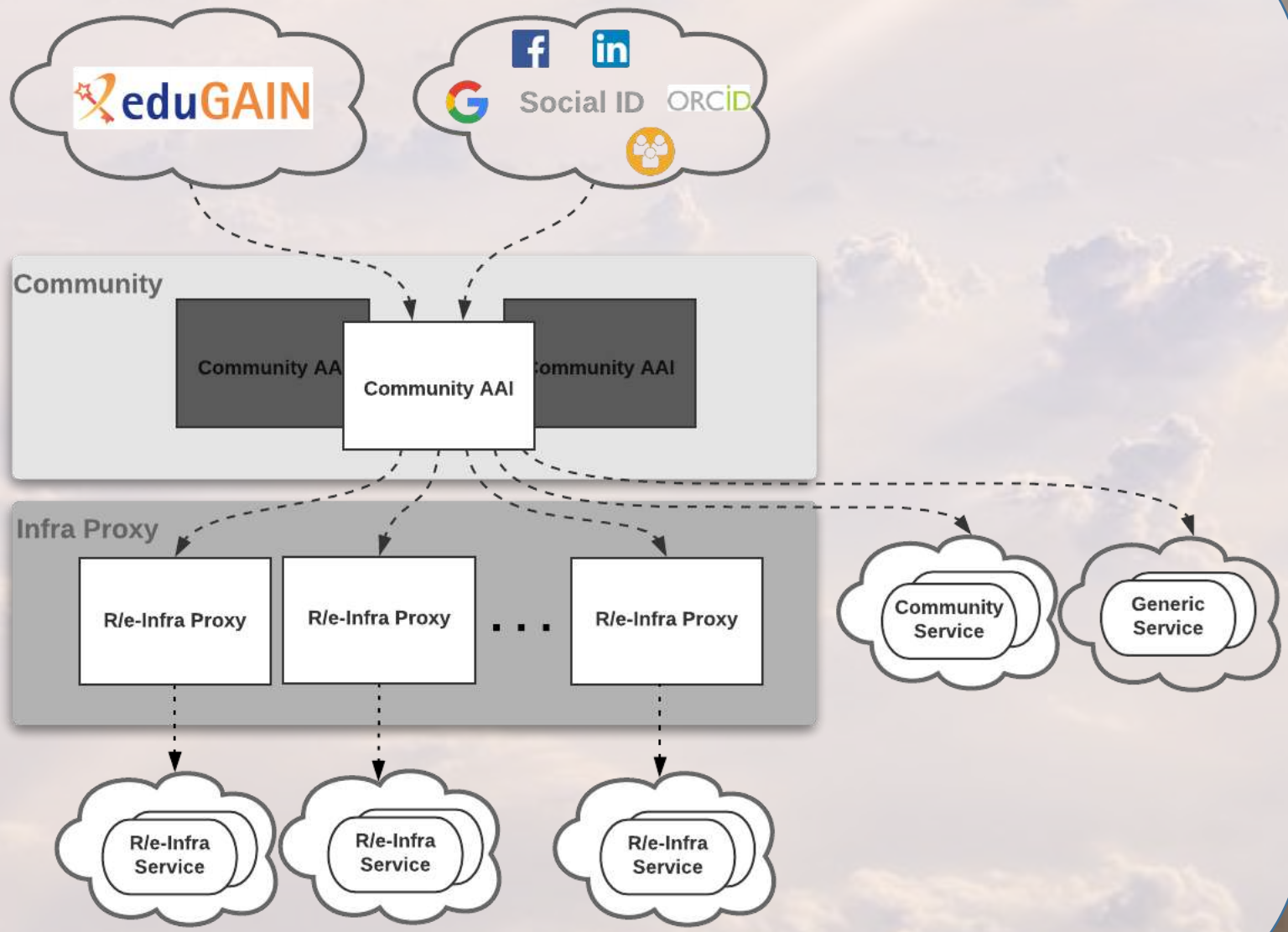
AARC BPA ‘Community First’ model and the EOSC

Weaving participants, services, and infrastructures

An ecosystem of fair services and data

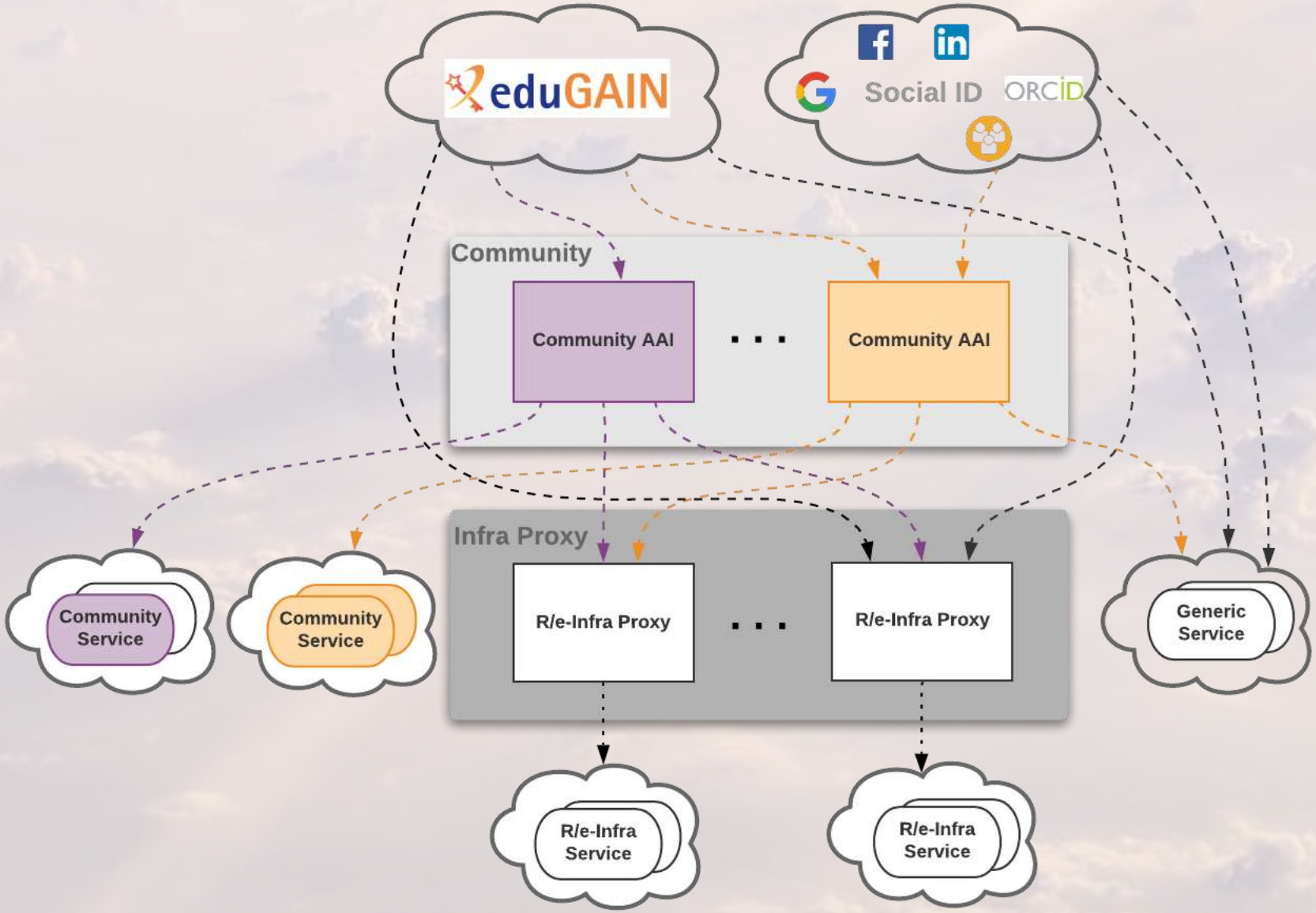
AARC BLUEPRINT ARCHITECTURE AND THE EUROPEAN OPEN SCIENCE CLOUD “EOSC”

AARC BPA



slides: thanks to Christos Kanellopoulos, GEANT

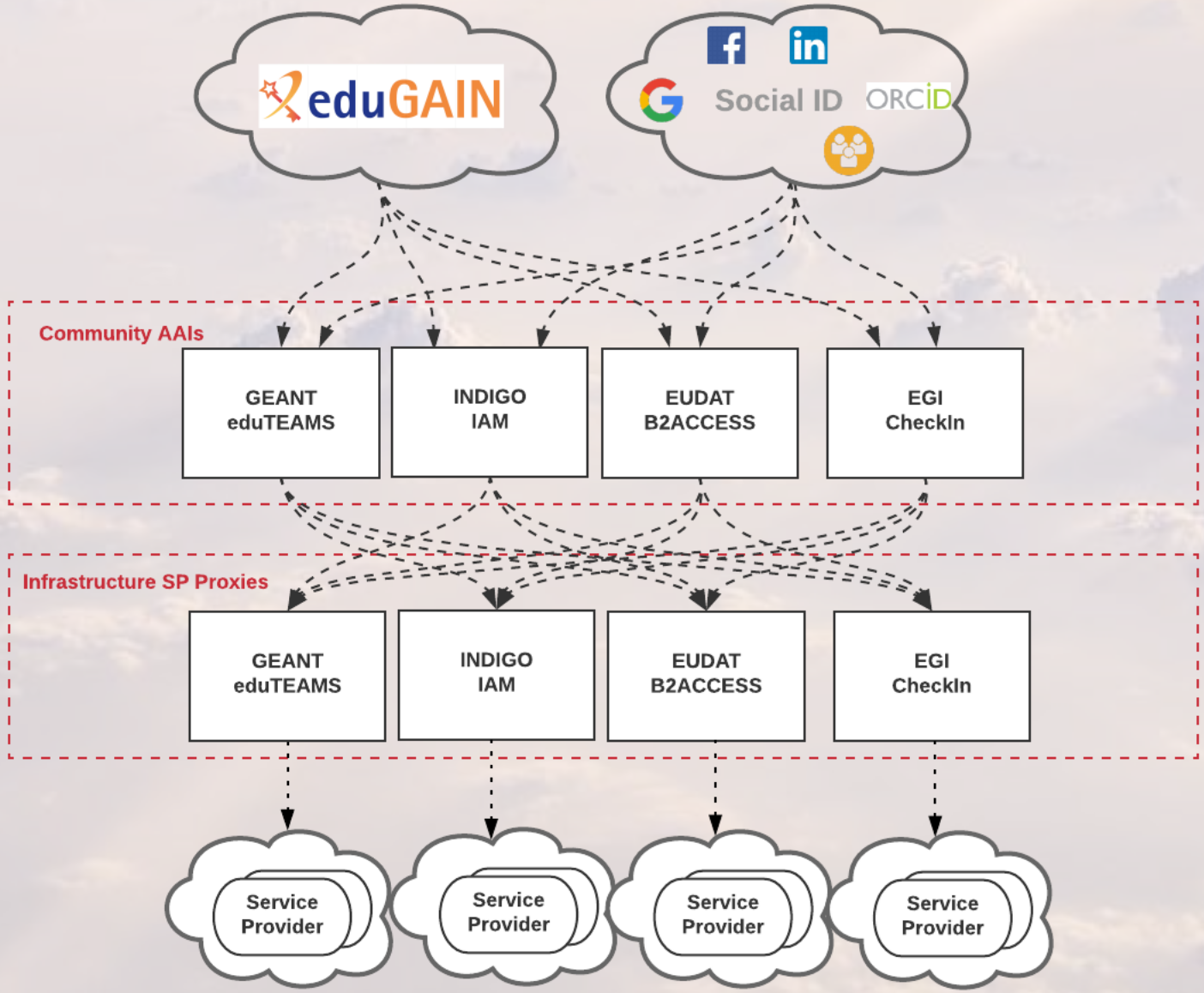
AARC BPA



slides: thanks to Christos Kanellopoulos, GEANT

GÉANT
Networks • Services • People

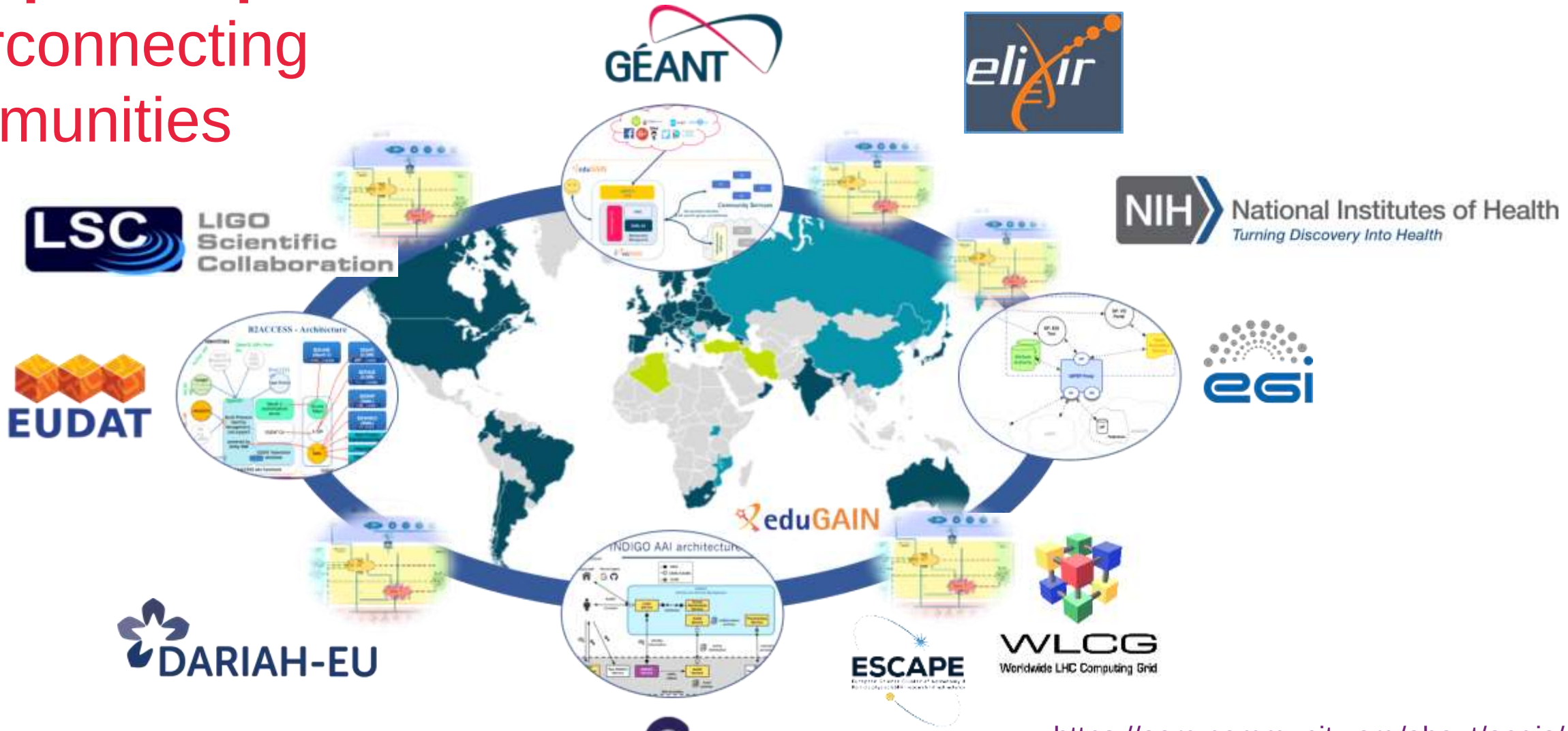
EOSC Hub



slides: thanks to Christos Kanellopoulos, GEANT

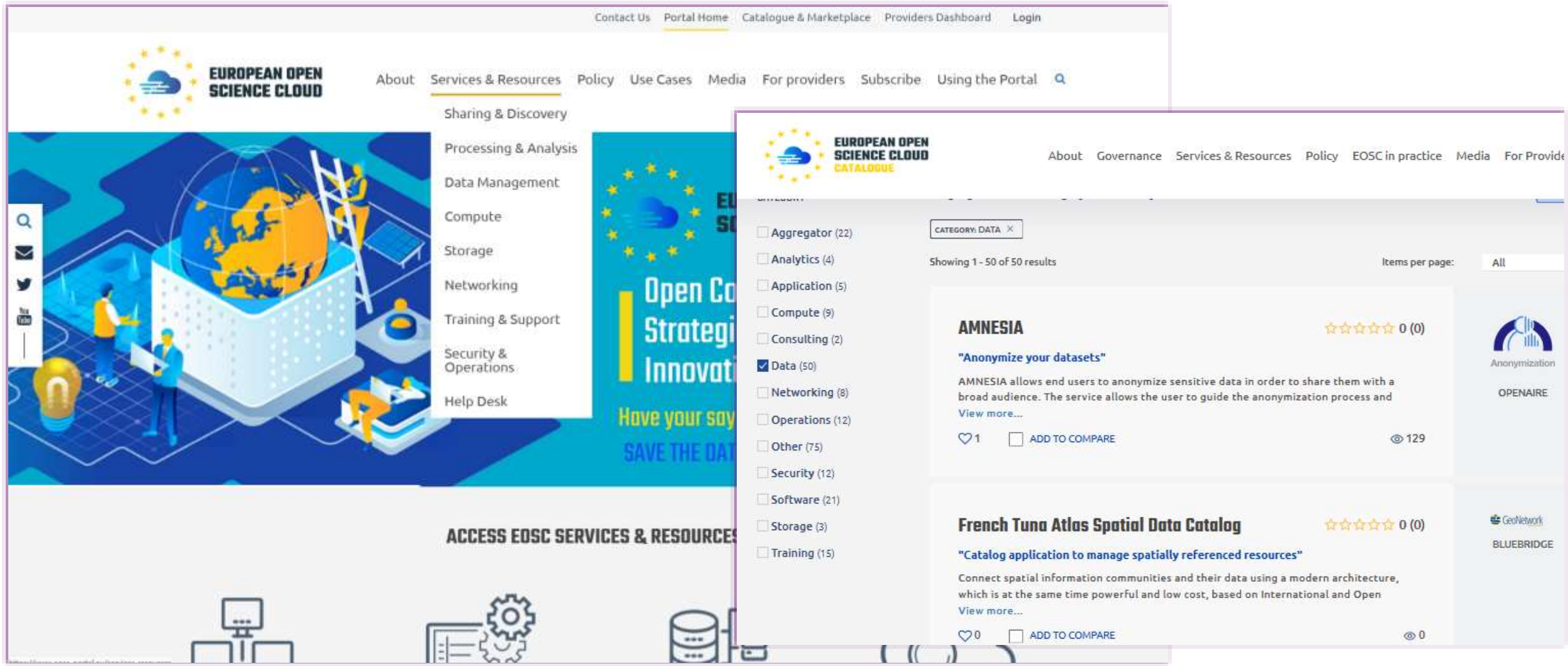
European Open Science Cloud

Interconnecting communities



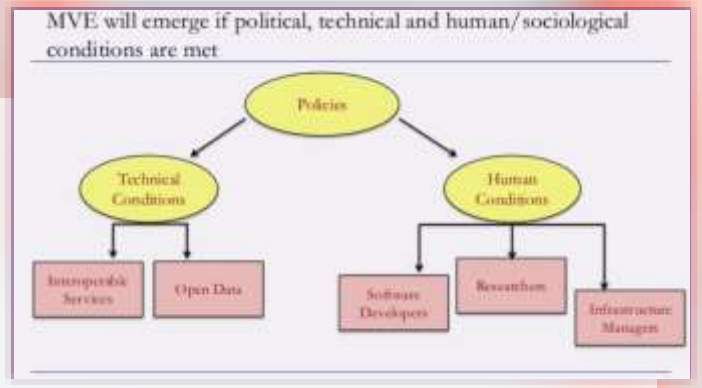
https://aarc-community.org/about/aegis/

An ecosystem more than just the infrastructure



EOSC Portal (https://www.eosc-portal.eu/) – as built by EOSChub

Minimum Viable … EOSC



Great Expectations … but what about requirements?

‘MVE – MINIMUM VIABLE EOSC’

includes some *Rules of Participation* to aid security & trust

Core

- ‘distributed and participatory’
- ‘collaborative consensus’
- ‘interoperability standards, […] and implementation via best practices’

Exchange & Portal

- ‘research-enabling services’
- ‘national, regional, institutional, domain based, … and commercial’
- ‘catalogue …[for] research life cycle’

- it will be a mix, and in any case service providers will need to contribute
- *Sirtfi shows that is not completely unrealistic*

Sirtfi – security incident response trust framework for federated identity – see refeds.org/sirtfi

graphic: Prompting an EOSC in Practice – Isabel Campos, CSIC & EOSC HLEG

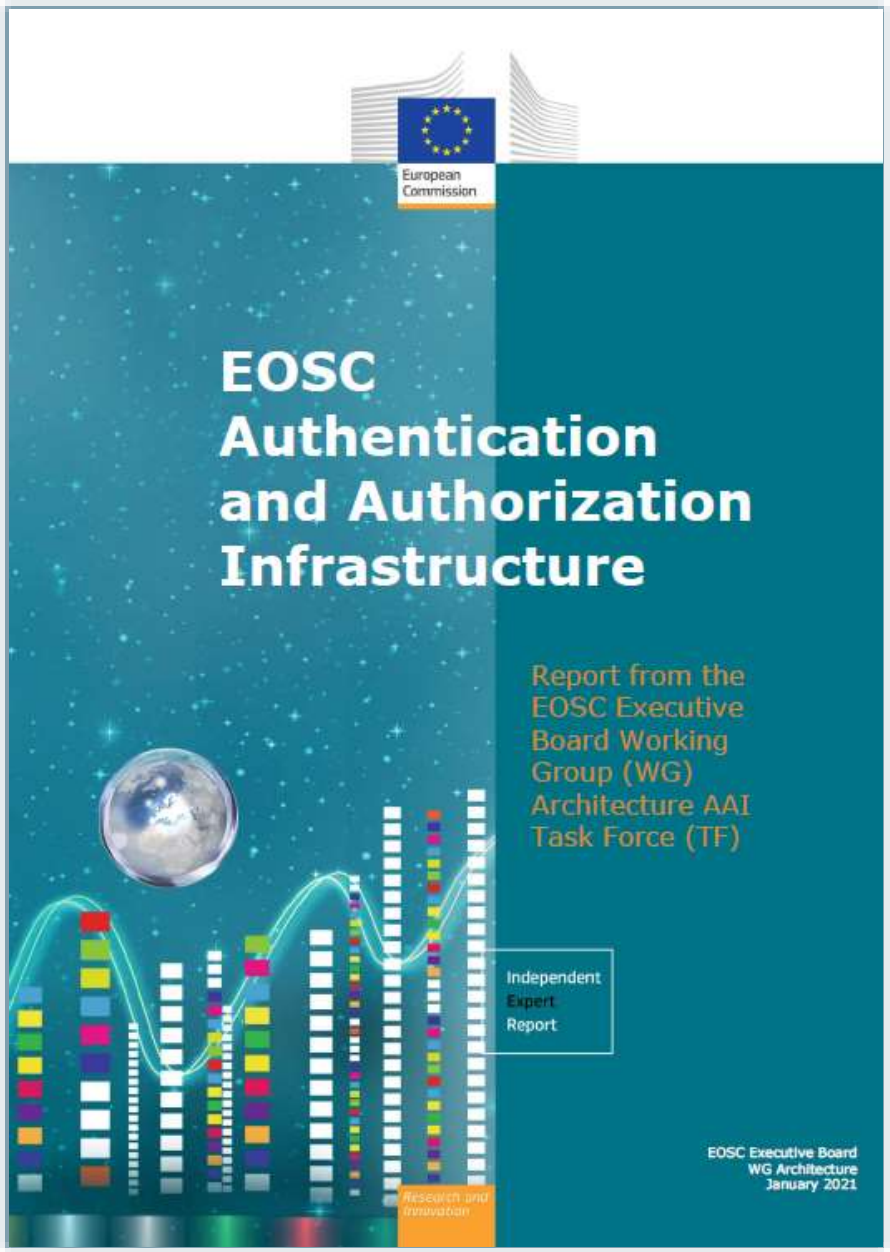
Photo: Patrick Perkins (Unsplash)

EOSC AAI Core Principles

In order to outline a globally viable, scalable and secure EOSC AAI, the group defined the following three core principles, on which to base their work:

- **User experience** is the only touchstone.
- All trust flows from **communities.**
- **There is no centre** in a distributed system**.**

“The human element was the starting point of our exploration. We believe that providing a good user experience and making use of the existing trust relations that users already have within their research communities are the key factors for delivering a successful EOSC AAI.” [Klaas Wieringa, EOSC AAI TF chair]

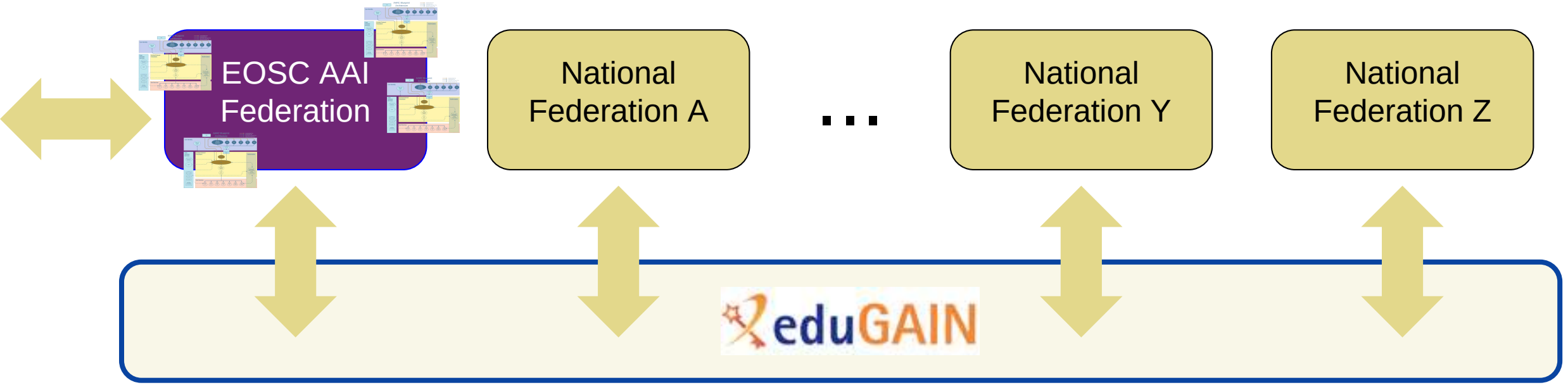


doi:10.2777/8702 – ISBN 978-92-76-28113-9

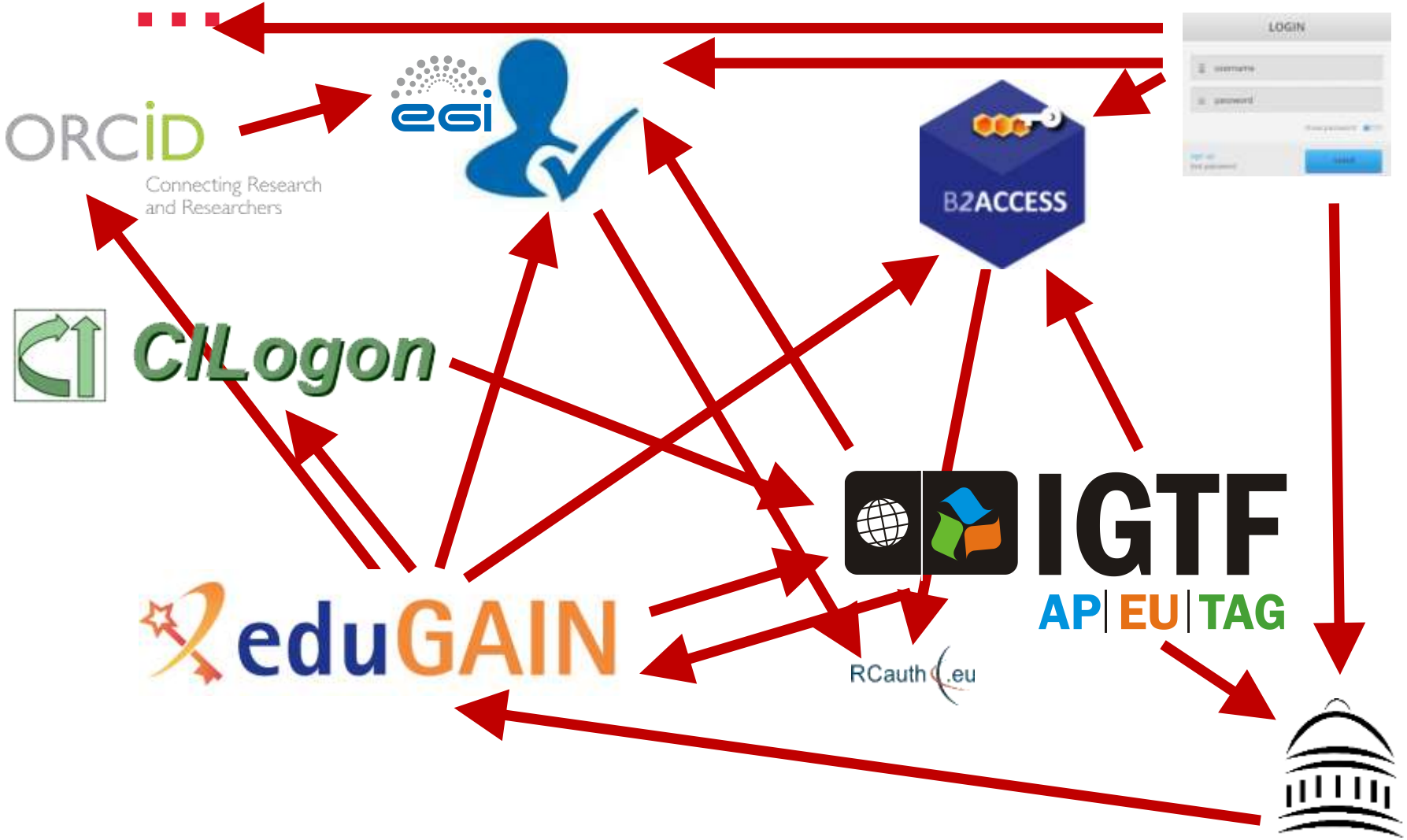
Linking the providers and users together

AARC BPA's 'community-first' model does not cover all EOSC cases, e.g. *infrastructures acting as providers **and** suppliers **and** as attribute authority*

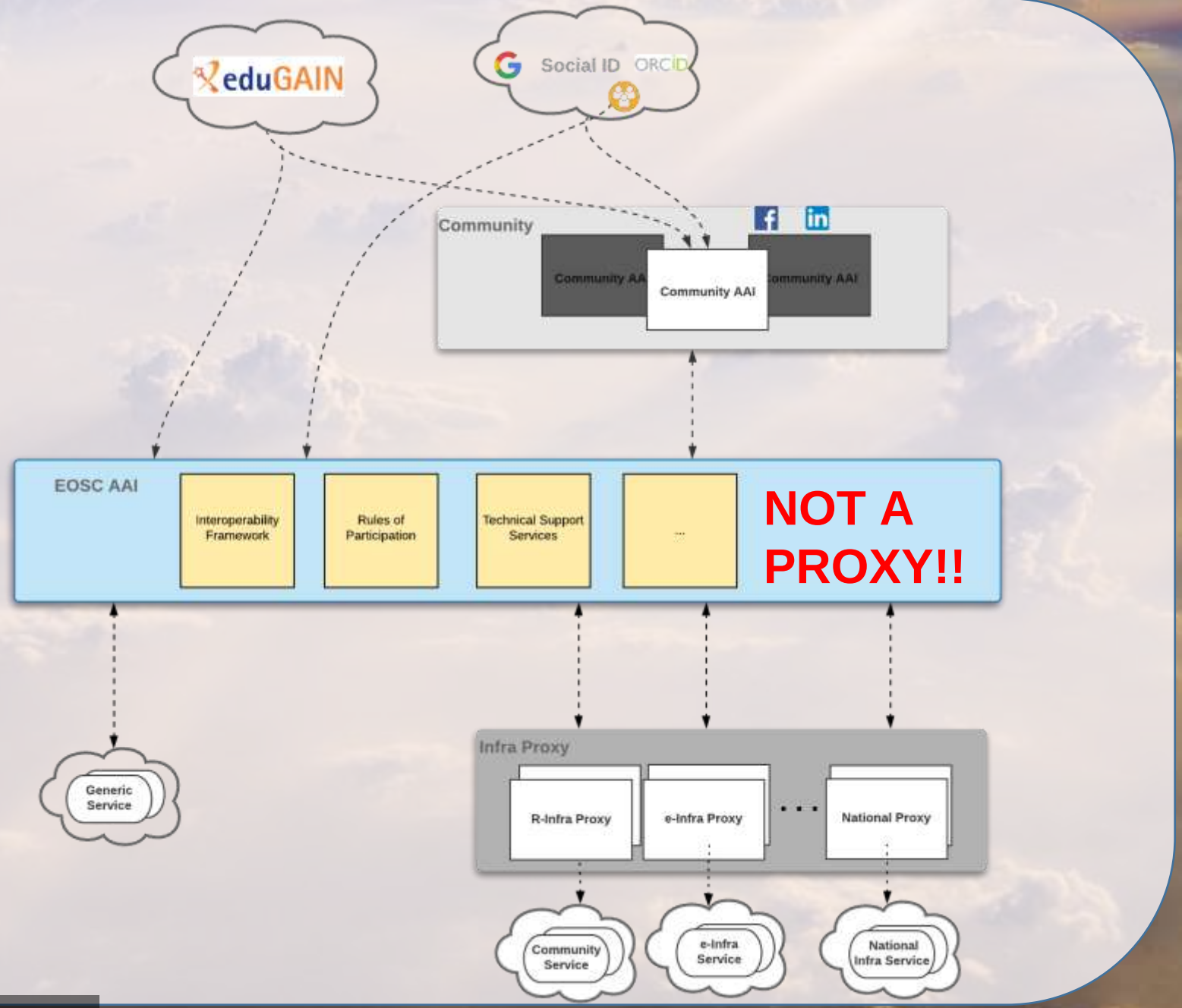
You need to turn the EOSC entities into a federation in itself, with carefully forged links to eduGAIN to prevent 'user loop' inconsistencies



Confusing the user … *and, yes, these paths all work* ☹

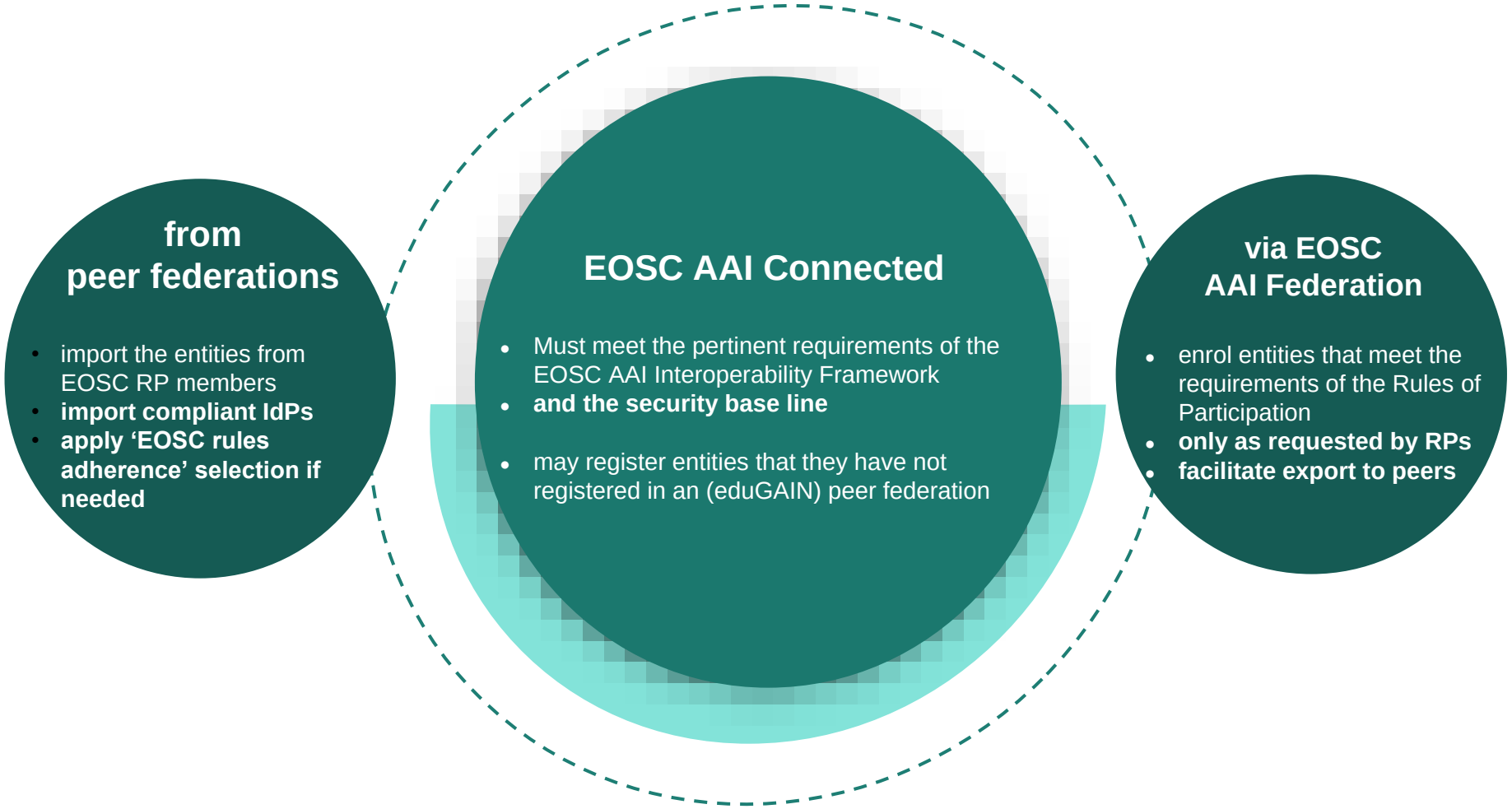


EOSC AAI



slides: thanks to Christos Kanellopoulos, GEANT

EOSC AAI Federation participation policy

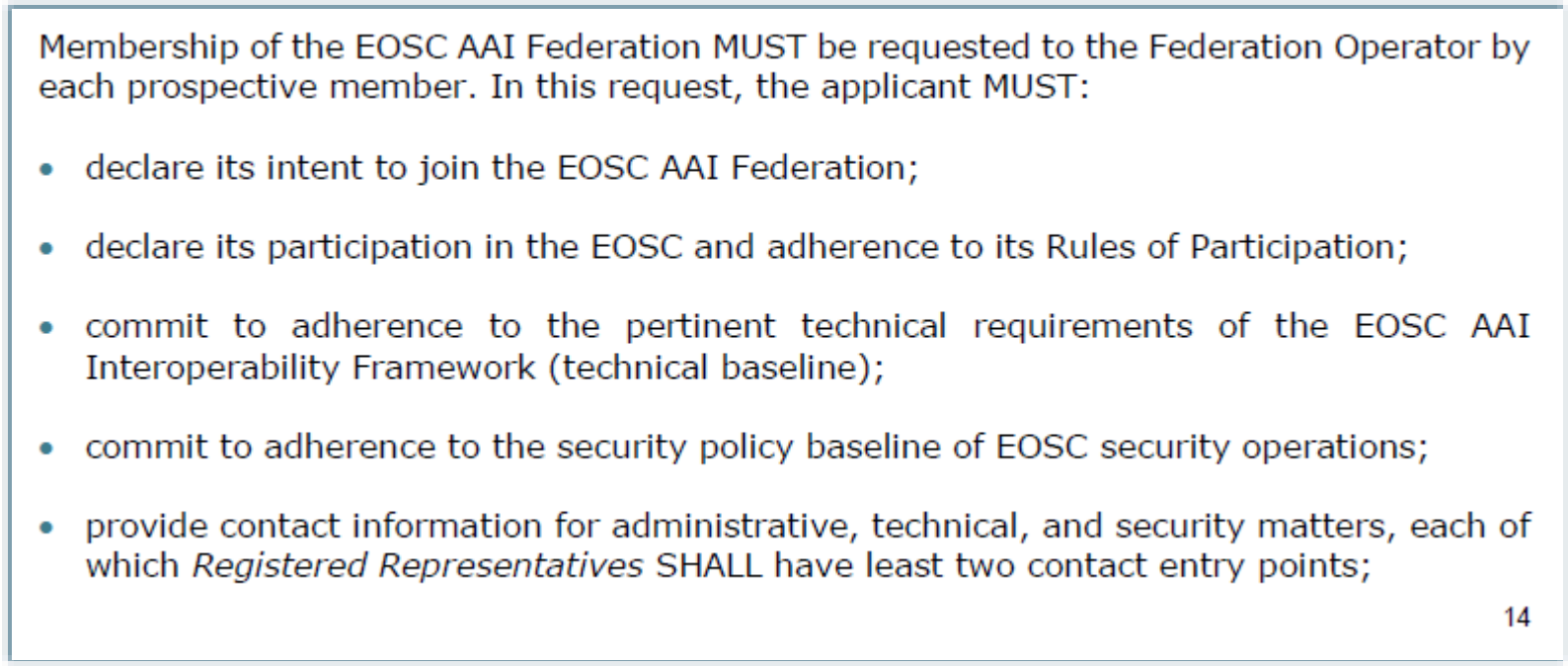


Linked to peer federations (including eduGAIN) - EOSC and eduGAIN mutually strengthen each other

Given the broad reach of the EOSC, it may well contain new entities, both from the private sector and from international collaborations and research infrastructures

But now … turtles all the way down

… now that new 'EOSC' federation needs policies and a base line



Membership of the EOSC AAI Federation MUST be requested to the Federation Operator by each prospective member. In this request, the applicant MUST:

- declare its intent to join the EOSC AAI Federation;
- declare its participation in the EOSC and adherence to its Rules of Participation;
- commit to adherence to the pertinent technical requirements of the EOSC AAI Interoperability Framework (technical baseline);
- commit to adherence to the security policy baseline of EOSC security operations;
- provide contact information for administrative, technical, and security matters, each of which *Registered Representatives* SHALL have least two contact entry points;

14

- inspired by eduGAIN constitution and other sources
- leveraging existing trust frameworks
- and not repeating earlier mistakes so implement a baseline at the start

A risk-based approach to service composition

Baselining and federated trust

Actionable security for the Core and Exchange-wide incidents

EOSC TRUST AND OPERATIONAL SECURITY

A challenging landscape

Entities of all kinds – diversity in the EOSC range
from *data sets* to *storage* to *computing* to *publications & digital objects*

An open ecosystem – rules of participation will favour low barrier to entry regarding operational maturity, service management quality, &c

A diverse ecosystem – providers will come from e-Infrastructures, from member states, from research infrastructures, and private sector

An *interdependent* ecosystem – aiming for composability and collective service design through an open, core AAI federation

Back to Basics: the few tenets for the EOSC ecosystem security

From *promoting and monitoring capabilities* **to** *managing core risk*

A service provider should

- **do no harm** to interests & assets of users
- **not expose *other*** service providers in the EOSC ecosystem to enlarged risk as a result of *their* participation in EOSC
- **be transparent** about its infosec maturity and risk to its customers and suppliers

this will mean *some minimum requirements* in the Rules of Participation

Photo Hippokrates tomb: Melania Stubos, CC-BY-SA-3.0
http://himetop.wikidot.com/hippocrates-funeral-monument

Making the EOSC a trusted place

Risk-centric self-assessment framework
- based on federated InfoSec guidance including WISE SCI

Baselining security policies & common assurance
- AARC, REFEDS, IGTF, PDK & practical implementation measures

An incident coordination hub and a trust posture
- spanning providers and core, based on experience & exercises

Actionable operational response to incidents
- EOSC core expertise to support resolution of cross-provider issues

Fostering trust through a known skills programme
- so that your peers may have confidence in service provider abilities

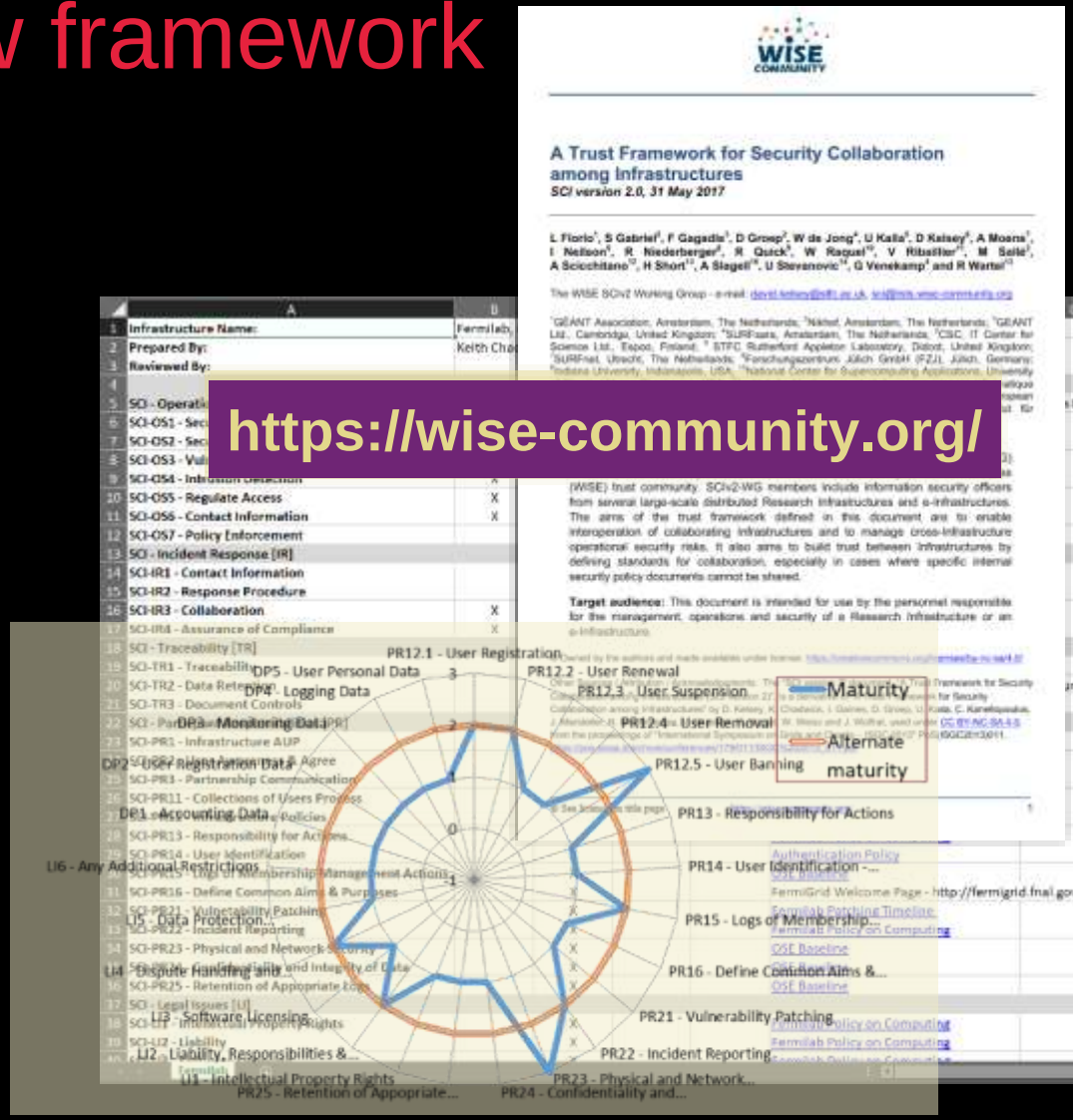
WISE SCI: wise-community.org/sci
AARC&c: aarc-community.org, refeds.org, igtf.net
PDK: aarc-community.org/policies/policy-development-kit

Assessing risk … in a peer-review framework

InfoSec **risk assessment framework**
for EOSC services based on
a federated evolution of WISE SCI and
a multi-tier maturity model,
also addressing data security and protection

- risks ‘play out’ differently
  in different infrastructures
- more than storage or compute, but also
  risks for (open) data and for reputation

Many risks are generic, some need context and expertise to assess. Or are under regulated regime



this spider diagram is fictional – idea by Urpo Kaila, CSC

Start with baselining

baselining has been very effective with Sirtfi, for R&S, and for InCommon …

Trust marks or seals
for specific service levels, access classes, types of data, regulatory domains, &c

SCI-based policy mapping
leverage common templates like the WISE Acceptable Use Policy, or membership management …

Good Practice
policy implementation guidance
small number of assurance profiles (REFEDS, IGTF, eIDAS), AARC secure operations standards, AEGIS recommendations, CSIRT capability

Technical guidance
e.g. expression of identity assurance

Rules of Participation
minimal set of capabilities – initially maybe just contact information, responsiveness, confidentiality

Image credit: ZULTAX, https://www.youtube.com/watch?v=NRznoYCJOHg

Establishing the trust basis for response

Collaboration frameworks, processes, exercises – the basis of trust
since not everything can be done on personal trust and 'blind faith'

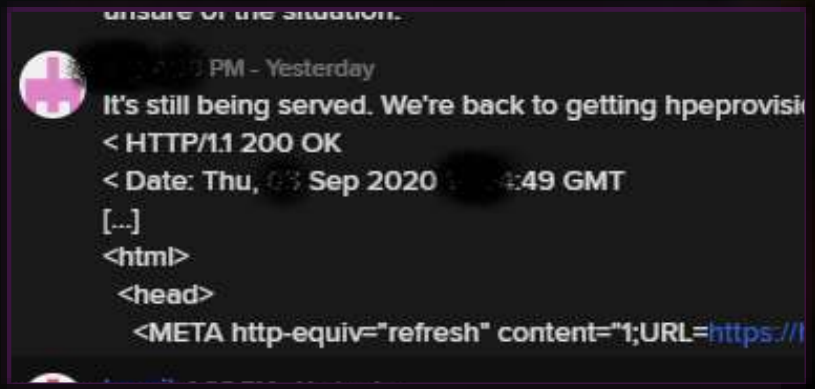
sources: GEANT CLAW, https://connect.geant.org/2020/02/19/claw-2020-save-the-date
Sirtfi: Hannah Short et al. https://wiki.geant.org/pages/viewpage.action?pageId=123766092

Actionable Response – coordination involving the Core

We *know* we cannot address all needs, but we can make progress

‘in the end, the same people do the same work, together, and regardless of the project of funding label’

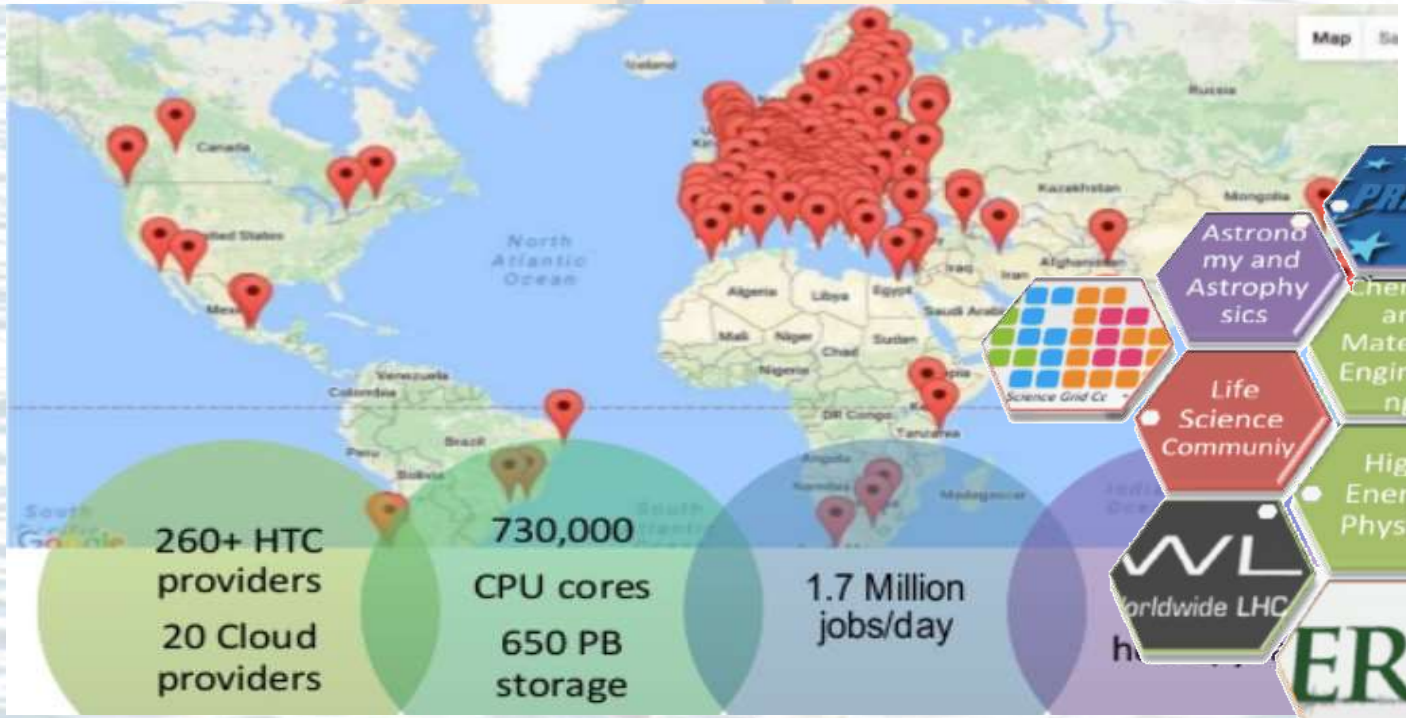
- EOSC core will itself be a significant hub
- tightly-knit team of experts
  looking after the security of the core
- who can work collaboratively
  with peer infrastructures and groups

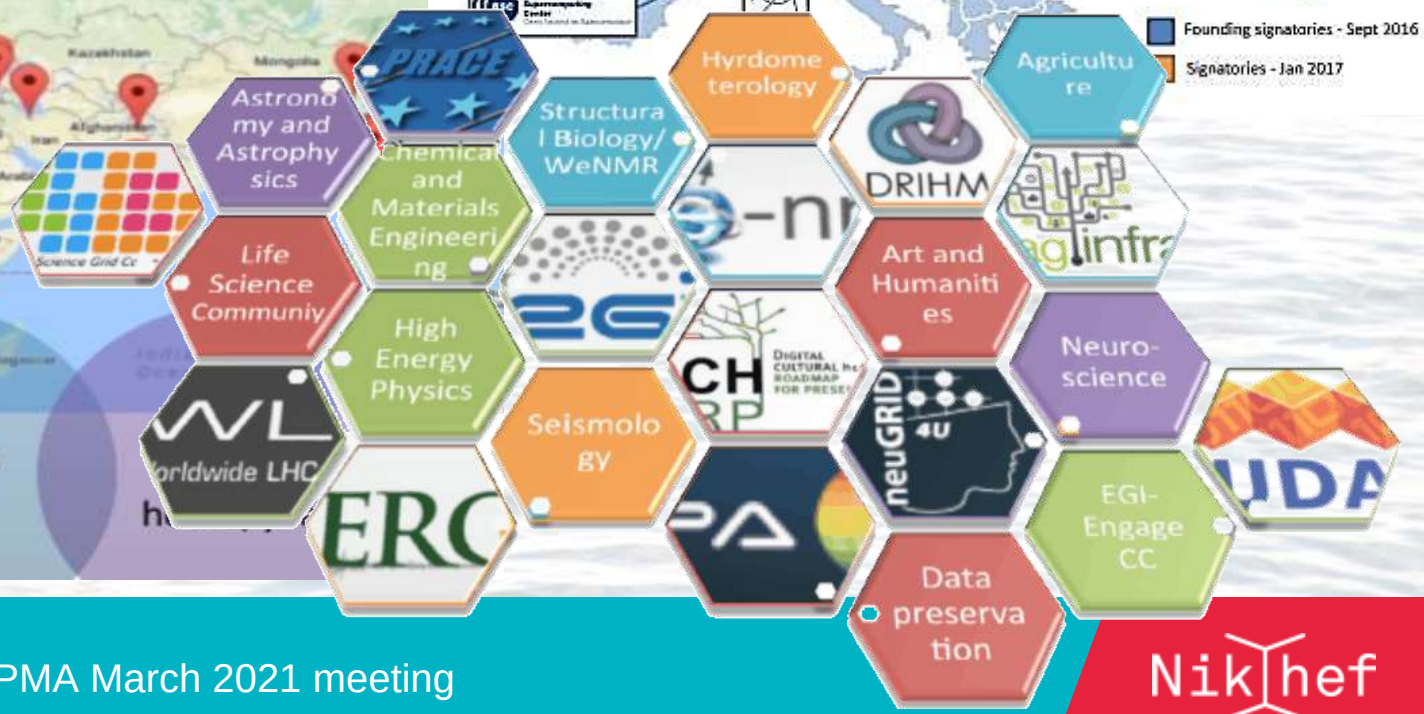


this team is essential to glue together the information during incidents – leveraging the trust built up before through engagement

But is an EOSC-level mechanisms the only piece?

we must leverage the ecosystem …





Thus even generic capabilities will be widely distributed

EOSC 'Portal' and ecosystem

security for a loosely coupled ecosystem

- risk management for collective services
- security baselining and trust marking
- coherence of response, community readiness/collaboration, and information sharing
- resolution, forensics, resolution and remediation for core and stakeholders
- training and capability enhancement

Core in EOSC-Future

(e-)Infrastructures, services, content

- service security & integrity, responsiveness, compliance monitoring
- vulnerability management and pro-active security management
- incident response and resolution within the infrastructure or service

EGI | EUDAT | GEANT | OpenAIRE | *ServiceX* | ..

See also *Trust Coordination for Research Collaboration in the EOSC era,* February 2020, https://g.nikhef.nl/eosc-sec-wp; https://doi.org/10.5281/zenodo.3674676

Common questions – open answers

Will any EOSC core drown?

Or can the EOSC do better?

- a baseline policy bringing enough trust to keep an EOSC-like ecosystem secure?
- will service providers also act collectively in the common interest?
- does the AAI technical and policy baseline provide a sufficient incentive?
- will provider self-assessment and mitigation of key risks, be seen as ‘good value’?

And … do the users care?

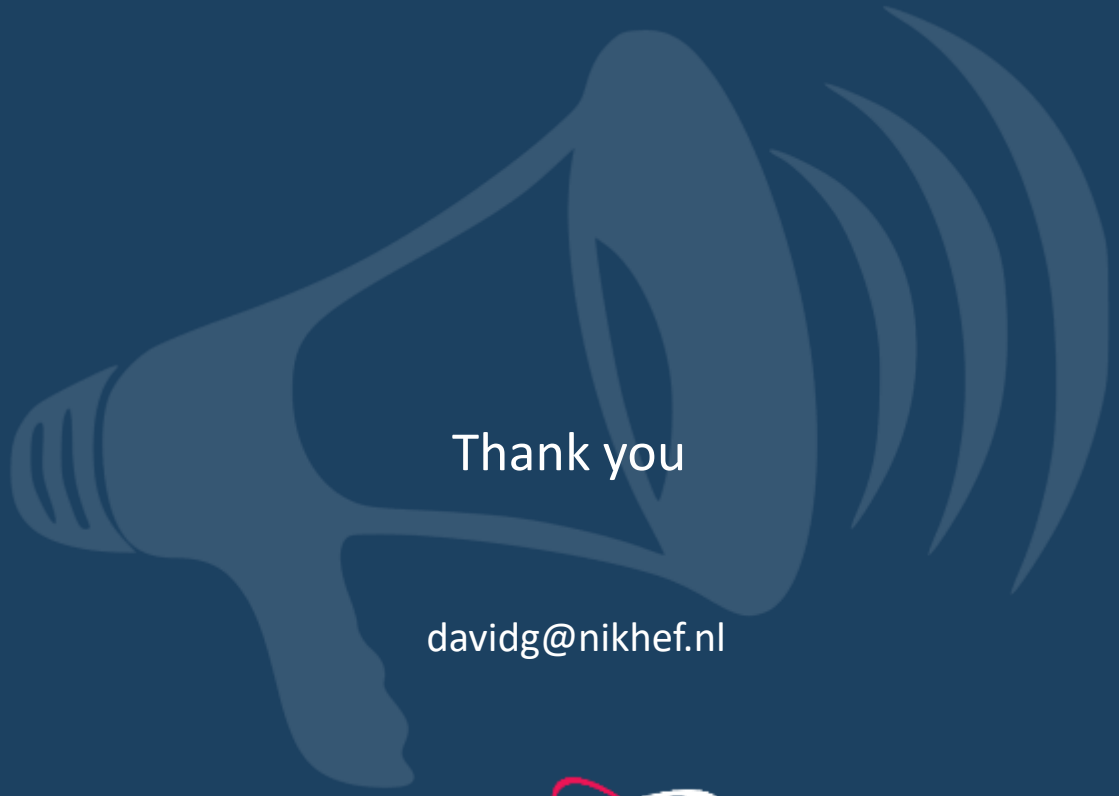
- and: *care enough* to make trust and security worth the cost for service providers?

Photo by Yash Prajapati on Unsplash

Questions?

BUILDING A GLOBAL TRUST FABRIC

this work is co-supported by the Trust and Identity workpackage of the GEANT4 project - phase 3



Thank you

davidg@nikhef.nl

GÉANT
Networks · Services · People
www.geant.org

with material from Christos Kanellopoulos, Hannah Short, Maarten Kremers, Dave Kelsey, Nicolas Liampotis, Uros Stevanovic, and others

This work IS ALSO SUPPORTED BY A project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).