Authentication and Authorisation for Research and Collaboration

Linking research and infrastructures to federation – technology, policy, deployment

David Groep

AARC Policy and Best Practice Activity Lead

Nikhef

RDA FIM IG

September 2017

Montréal, QC, CA

Research Communities

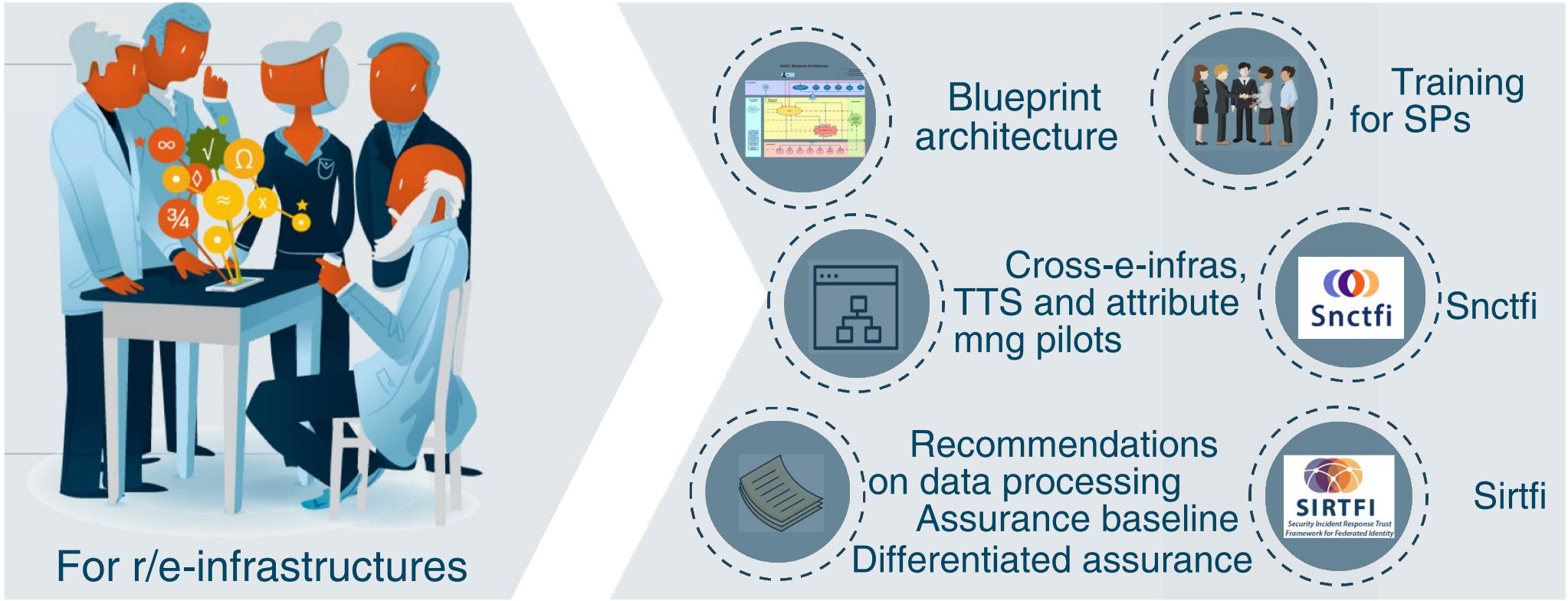
- The way researchers collaborate within scientific communities can vary significantly from community to community
- The ability to access and share resources is crucial for the success of any collaboration
- Research and Education (R&E) ICT there *also* to support collaboration
- Re-using existing identity management fabrics

Identified common challenges – beyond the old 'corporate IT' stuff

Communities / e-infrastructures surveyed in AARC

- Homeless user Home
- User friendliness
- Attribute Aggregation
- Community based AuthZ
- Non-Web Access
- Credential translation
- Bridging Communitie
- Identity Assurance
- Persistent non-reassigned ID

AARC: making federation work (also) for Research and e-Infrastructures

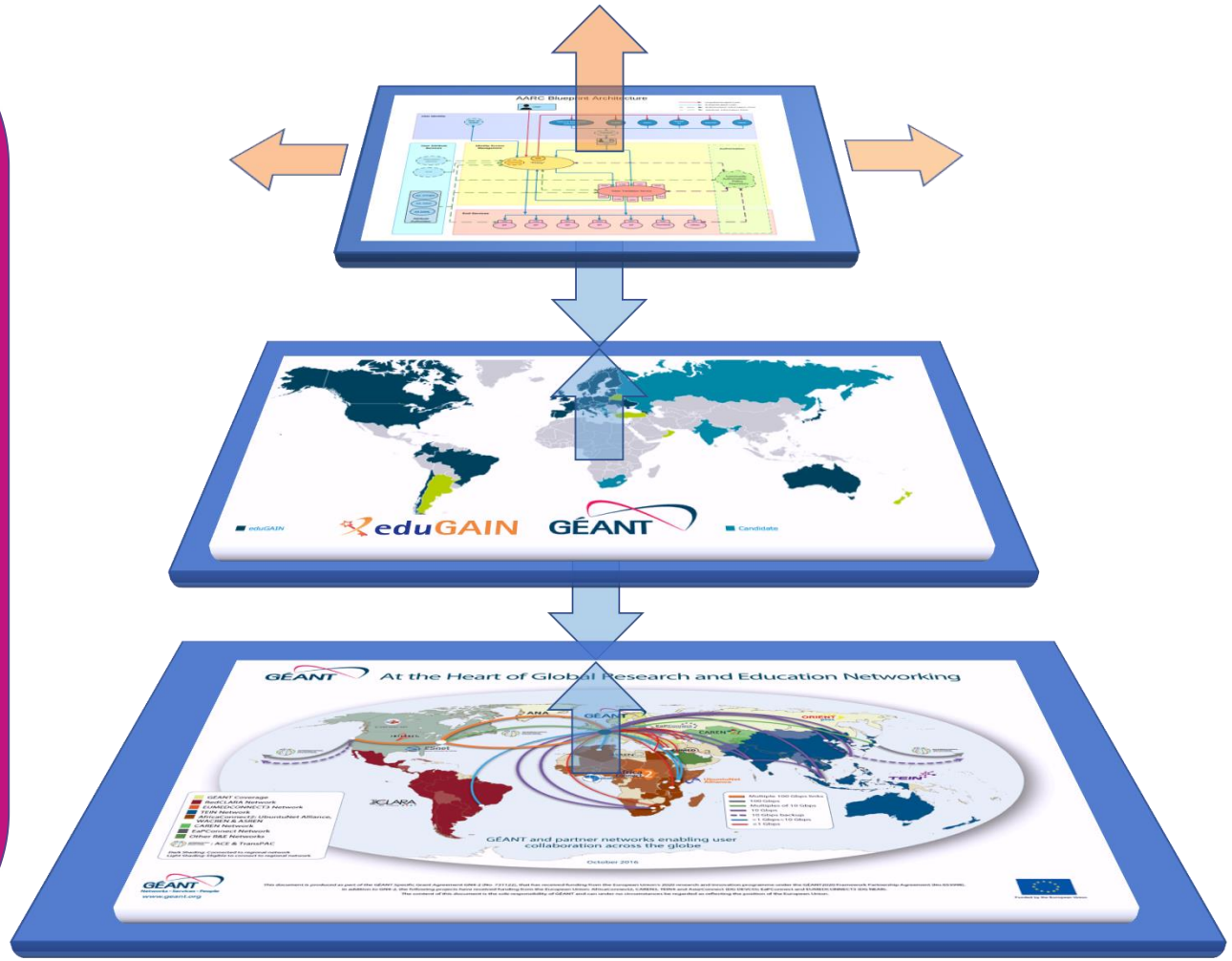


https://aarc-project.eu/infrastructures/
https://aarc-project.eu/pilots/piloted-solutions/

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

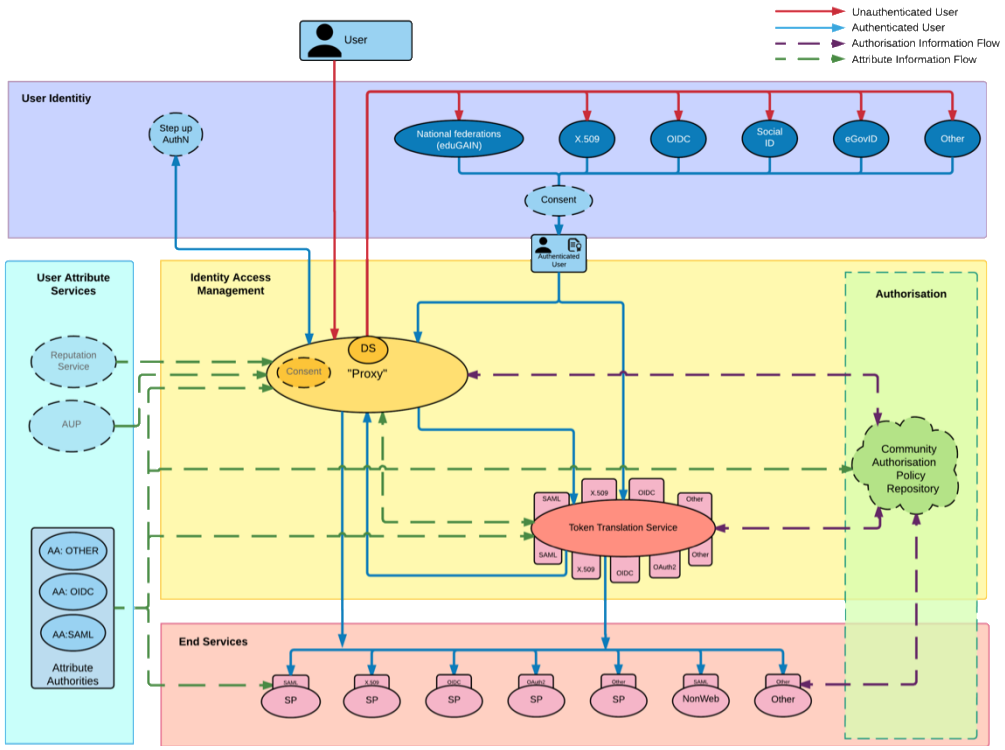
AARC Blueprint Architecture - Enabling an ecosystem of solution on top of eduGAIN

- A Blueprint **Architecture** for authentication and authorization
  - A set of architectural and policy building blocks on top of eduGAIN
- eduGAIN and the Identity Federations
  - A solid foundation for federated access in Research and Education



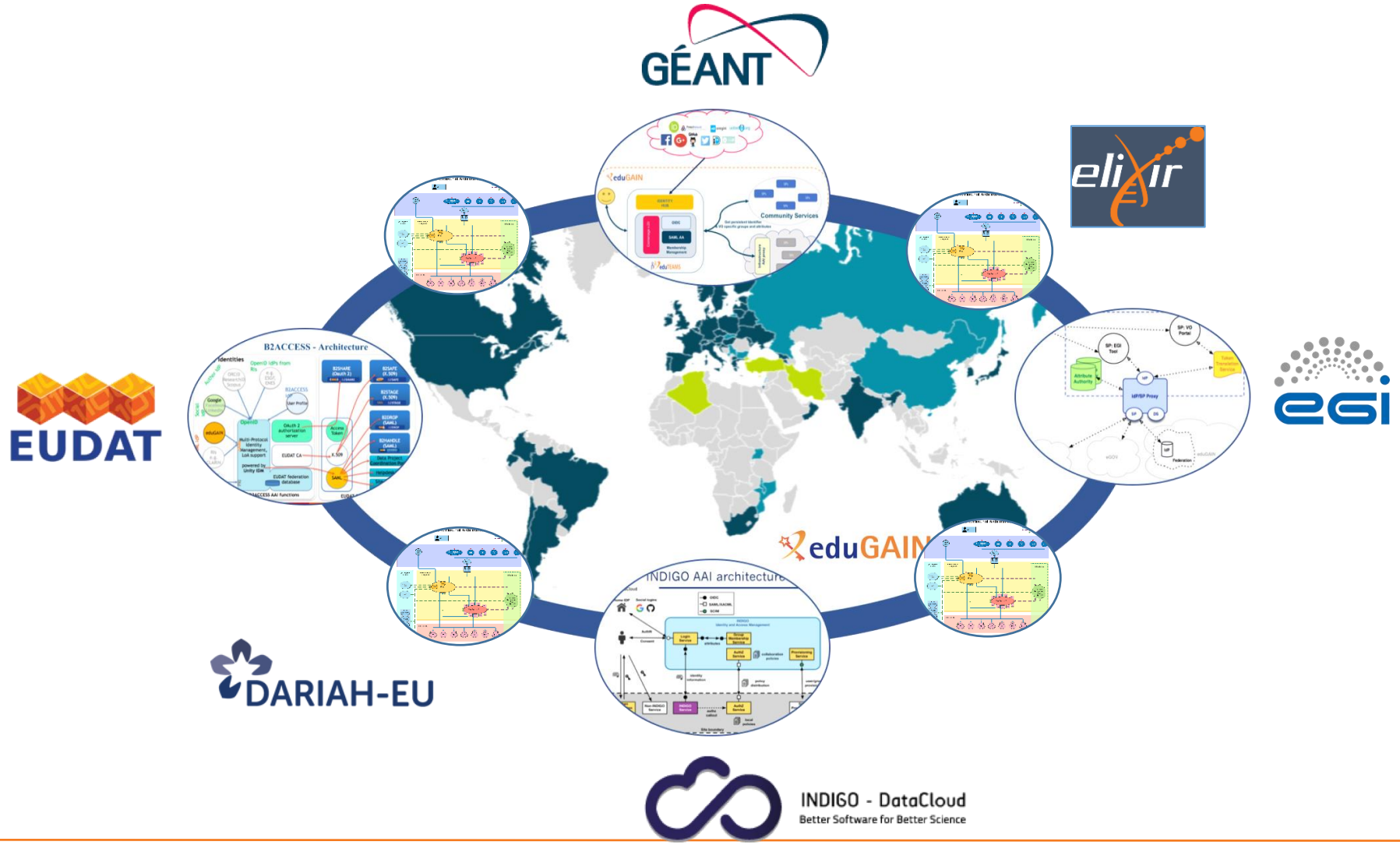
AARC Blueprint Architecture

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



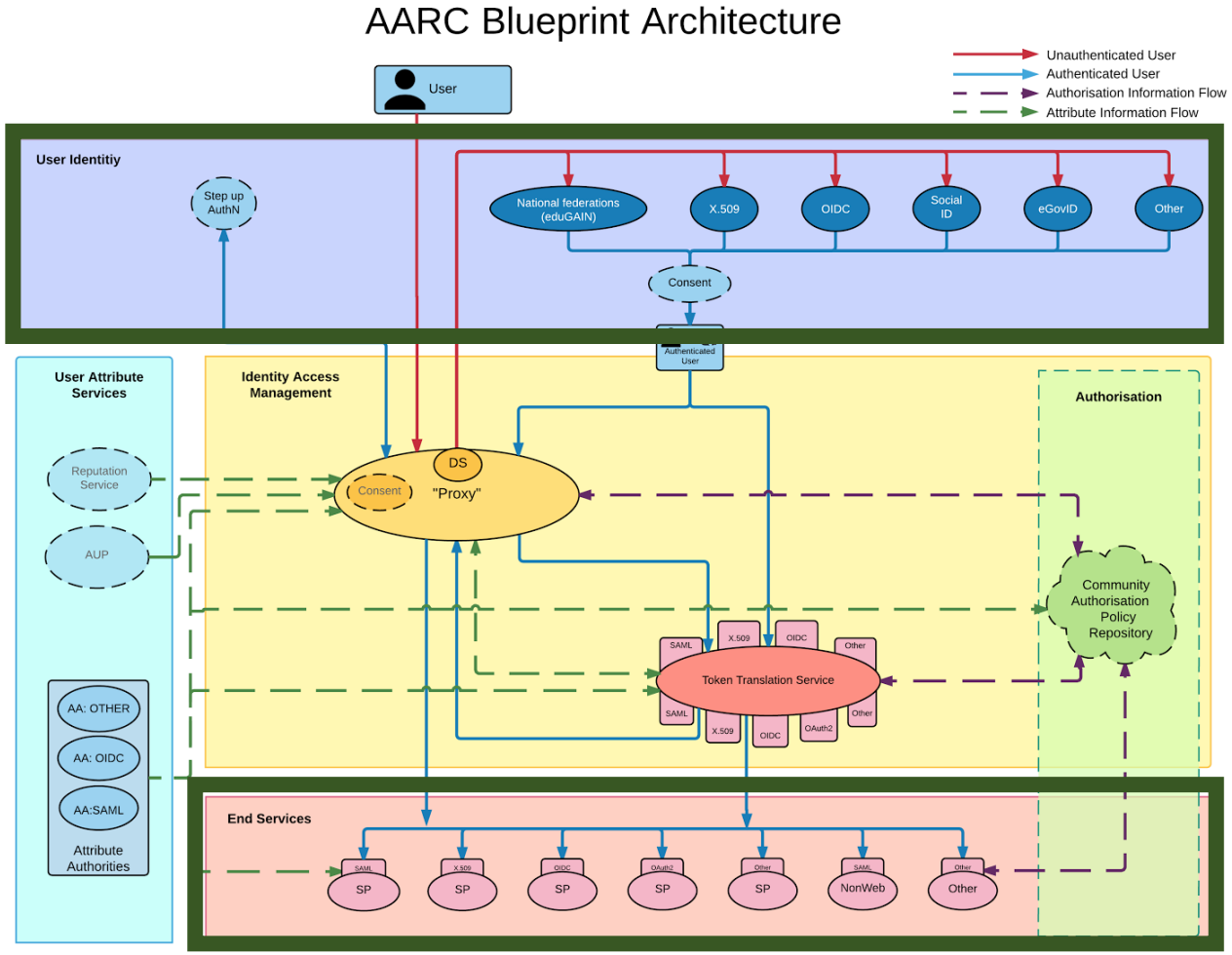
Guidelines and support documents

- Best practices for managing authorisation
- Expressing group membership and role information
- Scalable attribute aggregation
- Implementation of token TTS
- Credential delegation
- Non-web access
- Social media IdPs
- Use cases for account linking
- Use cases for LoA elevation via step-up authentication



and over 20 pilots with user communities and Infrastructures

Easing linking of research to infrastructure services with good practice



'Researcher (user)-centric' policy

Identify the source of your identity, will your provider stand by that identifier, and will it be yours forever?

The Blueprint SP-IdP Proxy as key component, also policy-wise:

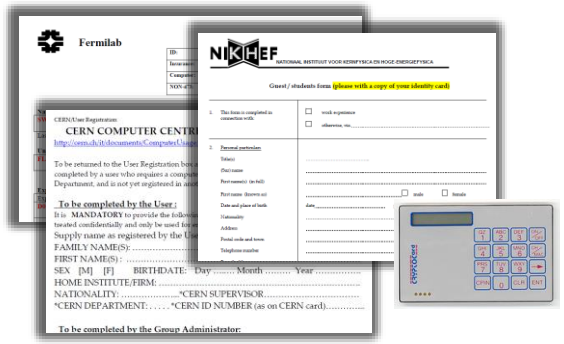
- *Filtering function for policy and assurance*
- *Present harmonized view to existing federations to get 'useful' data from them*

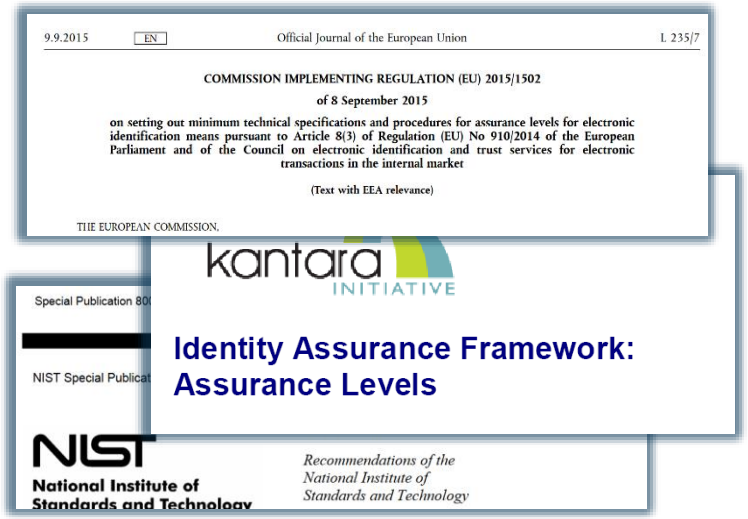
Service Infrastructure

- ***Incident response***
  "Sirtfi adoption will be critical"
- ***"A" baseline "LoA" will be critical, (demonstrable but not necessary by audit)***

Basically: **your, FIM4R, requirements!**

Trusting the User's Authentication





Many layered models (3-4 layers)

but: specific levels don't match needs of Research- and e-Infrastructures:

- Specific combination 'authenticator' and 'vetting' assurance doesn't match research risk profiles
- Disregards existing trust model between federated R&E organisations
- Cannot accommodate distributed responsibilities

but also national (eduGAIN) R&E federations lacked a documented, agreed assurance level

Beyond uncontrolled identifiers:

***baseline* assurance for research use cases**

Differentiated assurance from an (Research) Infrastructure viewpoint

‘low-risk’ use cases

few unalienable expectations by research and collaborative services

generic e-Infrastructure services

access to common compute and data services that do not hold sensitive personal data

protection of sensitive resources

access to data of real people, where positive ID of researchers and 2-factor authentication is needed

Baseline Assurance

1. known individual
2. Persistent identifiers
3. Documented vetting
4. Password authenticator
5. Fresh status attribute
6. Self-assessment

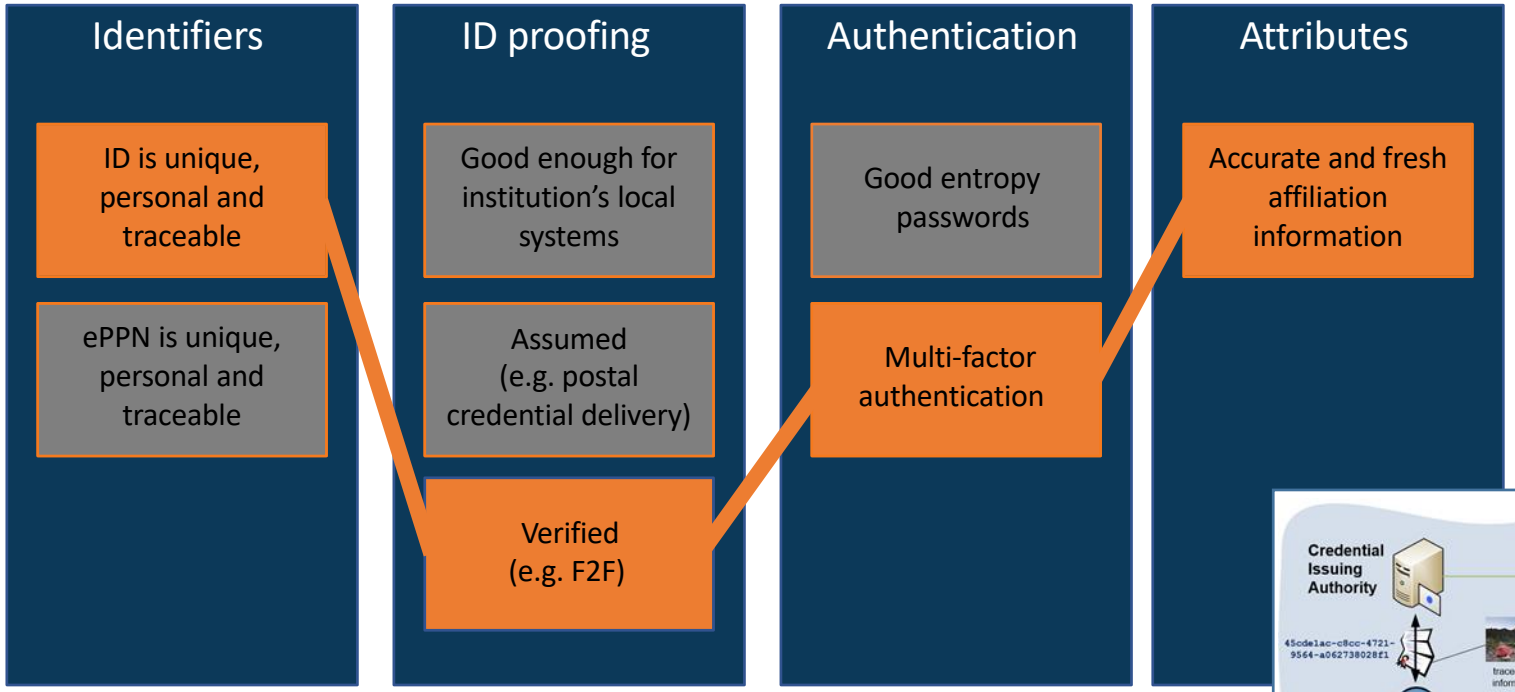
Slice includes:

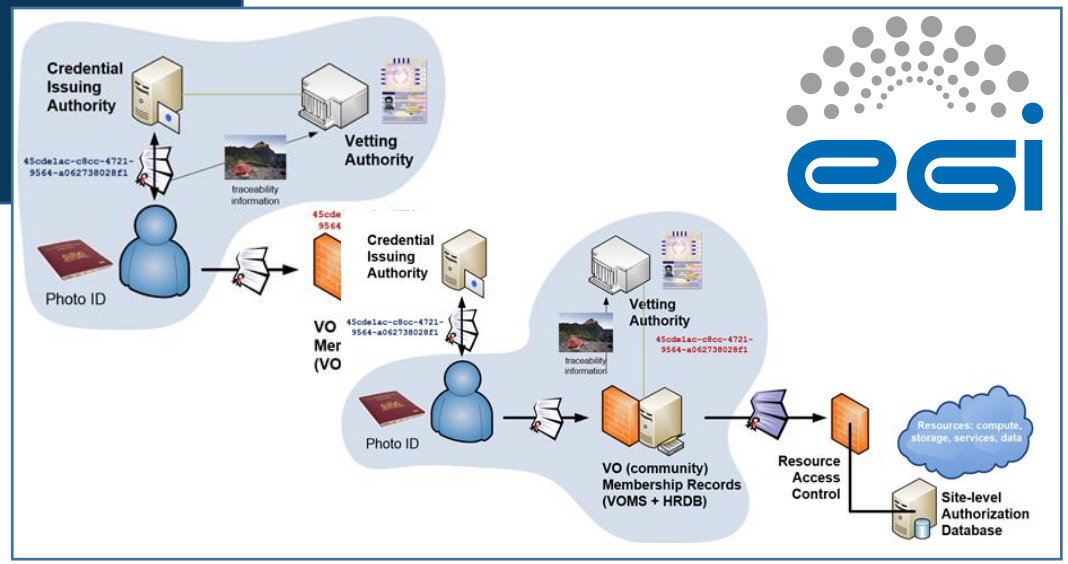
1. assumed ID vetting
   ‘Kantara LoA2’, ‘eIDAS low’, or ‘IGTF BIRCH’
2. Good entropy passwords
3. Affiliation freshness
   better than 1 month

Slice includes:

1. Verified ID vetting
   ‘eIDAS substantial’, ‘Kantara LoA3’
2. Multi-factor authenticator

Using Assurance in practice: “Espresso” for sensitive data



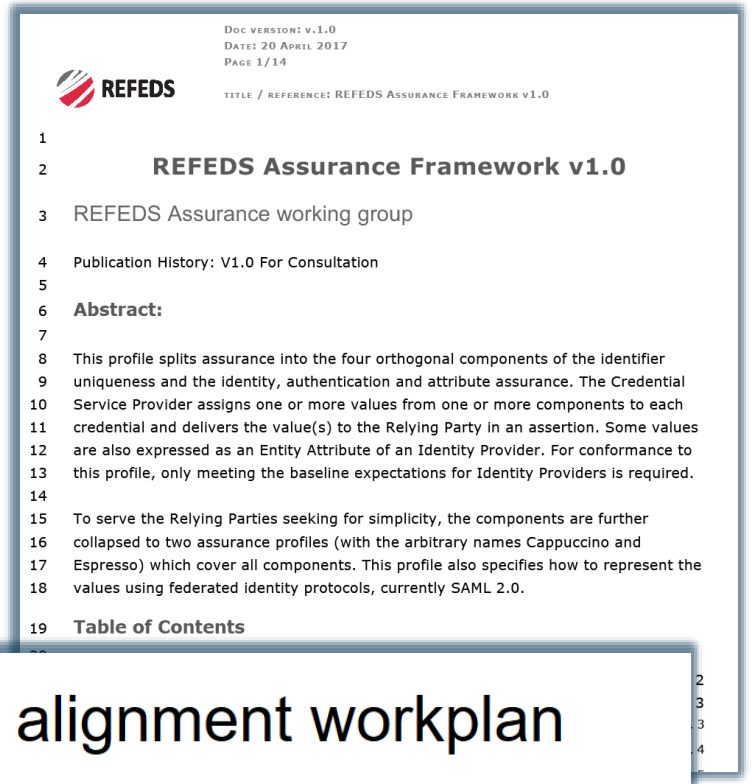


Assurance can come from a single source …
… or be a combined/collaborative assurance by identifier source and vetting attributes

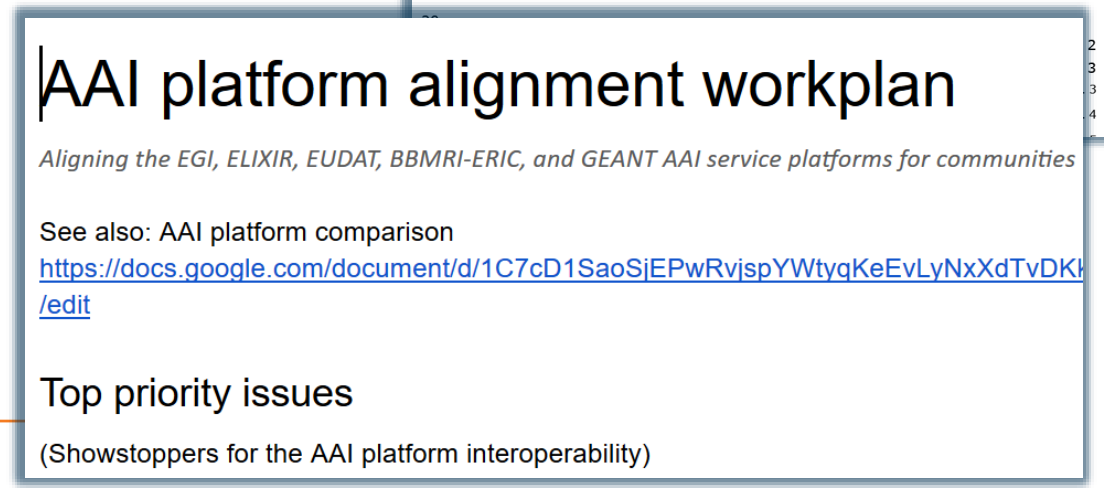
Gaining global adoption: REFEDS Assurance Framework

https://wiki.refeds.org/display/GROUPS/Assurance+Working+Group

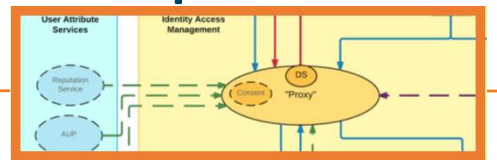
- open, international forum
- link to identity federations –
  adoption needs IdP to act and federations to communicate
- Add new eduGAIN *metadata* and new *attributes* for IdPs
- implementation guidance in normative form helps



Also used to align the e-Infrastructure providers
so that you can move between proxied infrastructures



… and now: how to apply it to attribute provenance?

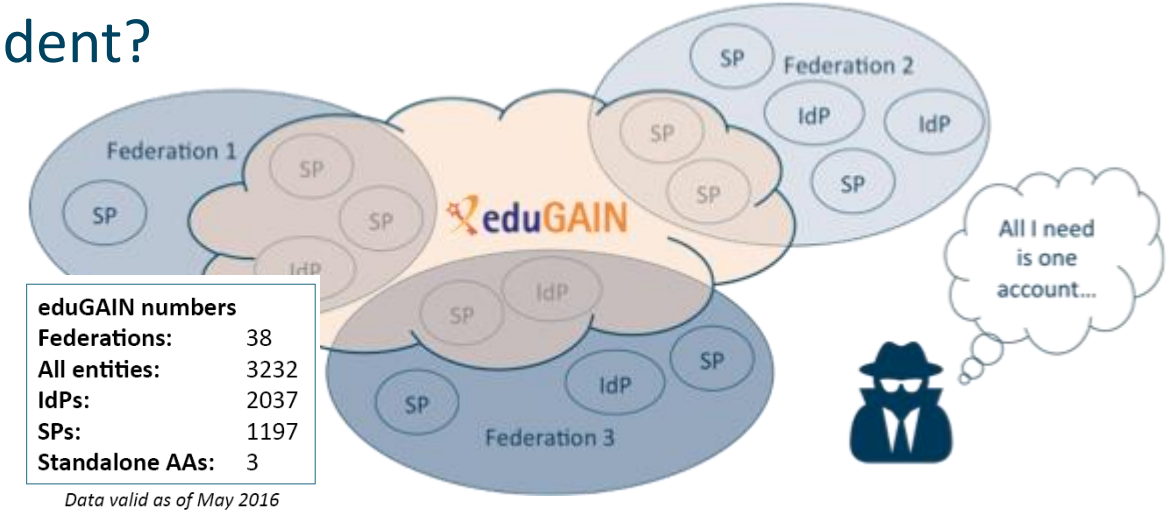


Security Incident Response in the Federated World

SIRTFI
Security Incident Response Trust Framework for Federated Identity

AARC

- How could we determine the scale of the incident?
  - Do useful logs exist?
  - Could logs be shared?
- Who should take responsibility for resolving the incident?
- How could we alert the identity providers and service providers involved?



eduGAIN numbers	
Federations:	38
All entities:	3232
IdPs:	2037
SPs:	1197
Standalone AAs:	3

Data valid as of May 2016

- Could we ensure that information is shared confidentially, and reputations protected?

Security Incident Response Trust Framework for Federated Identity

Sirtfi – *based on Security for Collaborating Infrastructures (SCI) & FIM4R Recommendations*

A Security Incident Response Trust Framework – Sirtfi summary

Operational Security

- Require that a security incident response capability exists with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.

Incident Response

- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration

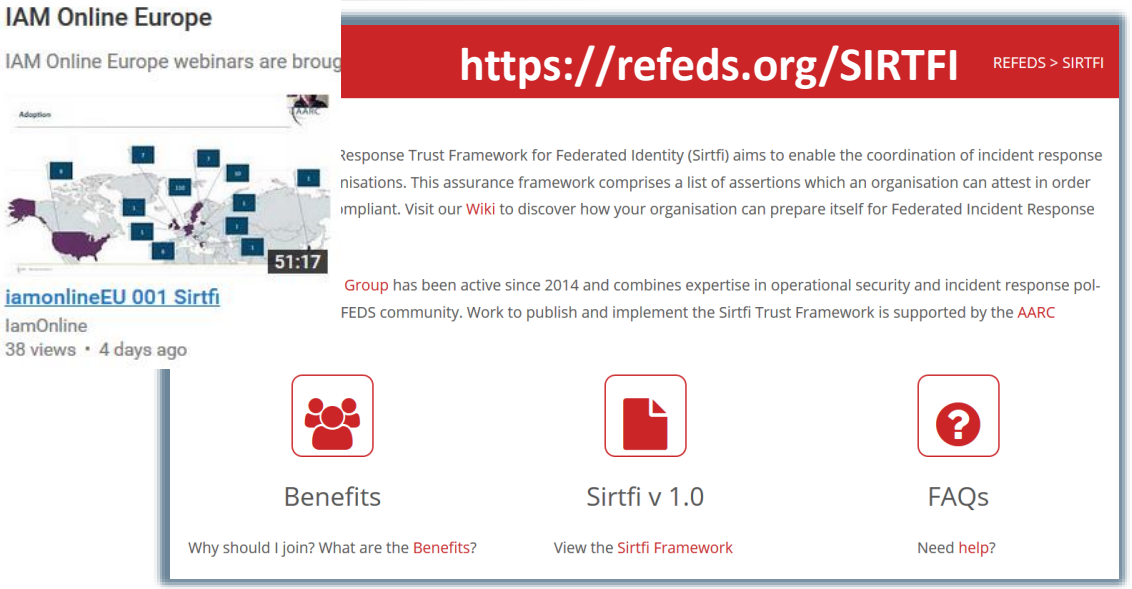
Traceability

- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

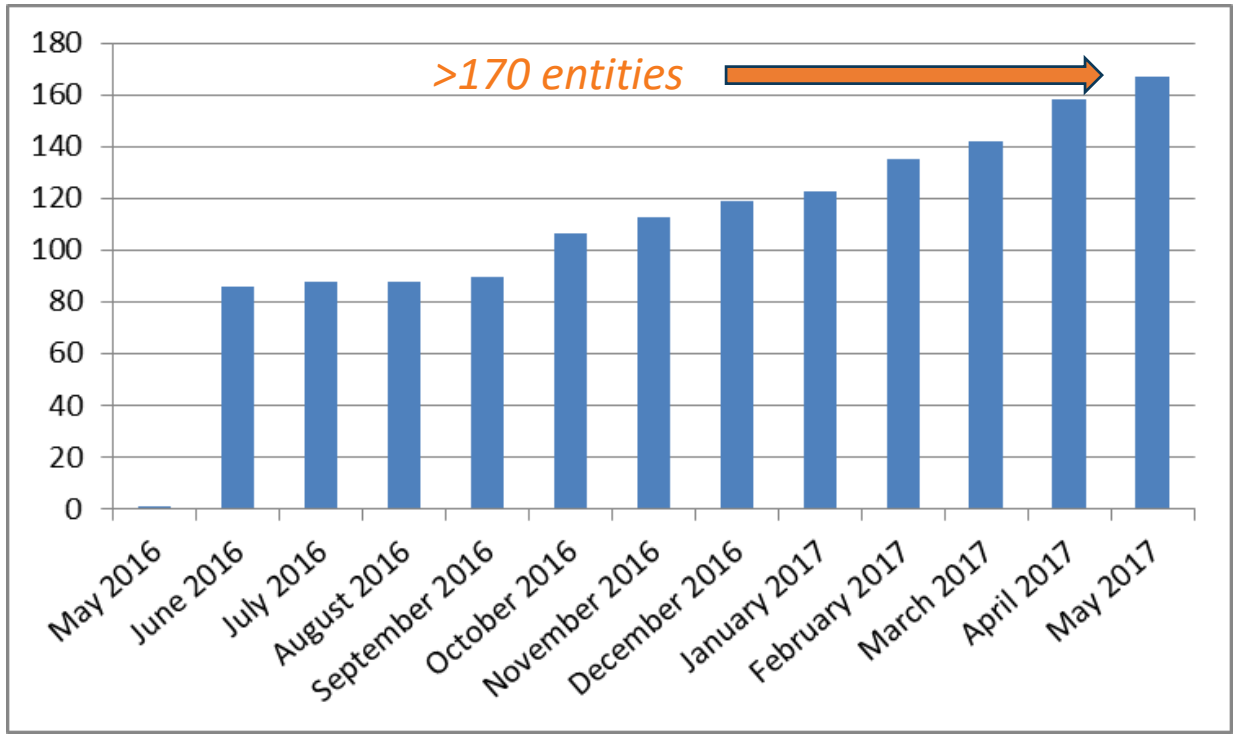
Sirtfi adoption by authentication providers and services



- adds **security contact** meta-data in eduGAIN
- with R&S meets **baseline assurance** and IGTF "assured identifier" profile
  … *IGTF-to-eduGAIN bridge asserts R&S+Sirtfi*

Used for filtering (with R&S) by proxies & services

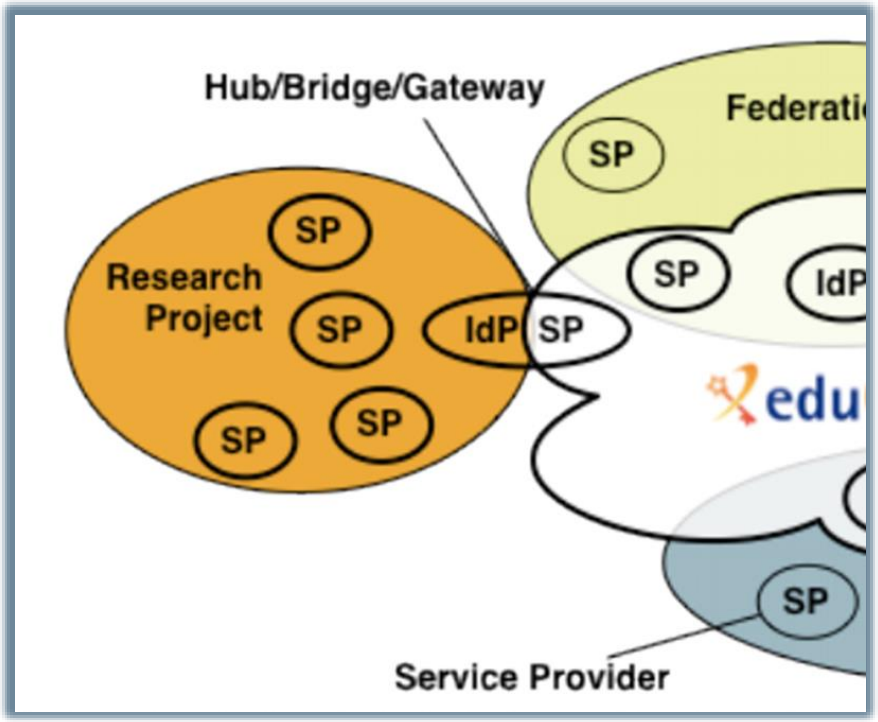
EGI operational services, RCauth.eu bridge, CERN SSO, CILogon Basic services, …



Combine with 407 REFEDS R&S IdPs (May '17)

Snctfi: aiding Infrastructures achieve policy coherency

- ✓ allow SPIdP Proxies to assert ‘qualities’, categories, based on assessable trust
- ✓ Develop recommendations for an Infrastructure’s coherent policy set




Scalable Negotiator for a Community Trust Framework in Federated Infrastructures (Snctfi)

Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp (SURFsara)

AARC - Version 1.0 - 26 Apr 2017

e-mail: david.kelsey@stfc.ac.uk

Abstract: This paper identifies operational and policy requirements to help establish trust between an Infrastructure and identity providers either in an R&E Federation or in another Infrastructure, in each case joined via a Service Provider to Identity Provider proxy.

Audience: This document is intended for use by the personnel responsible for the management, operation and security of an Infrastructure and those wishing to assess its trustworthiness.

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

- Derived from SCI, the framework on *Security for Collaboration among Infrastructures*
- Complements Sirtfi with requirements on internal consistent policy sets for Infrastructures
- Aids Infrastructures to assert *existing* categories to IdPs: REFEDS R&S, Sirtfi, DPCoCo, …

See FIM4R presentation by David Kelsey!

Graphics inset: Ann Harding and Lukas Hammerle, GEANT and SWITCH

Snctfi infrastructure requirements, a summary

Operational Security

- State common security requirements: AAI, security, incident and vulnerability handling
- Ensure *constituents* comply: through MoUs, SLA, OLA, policies, or even contracts, &c

User Responsibilities

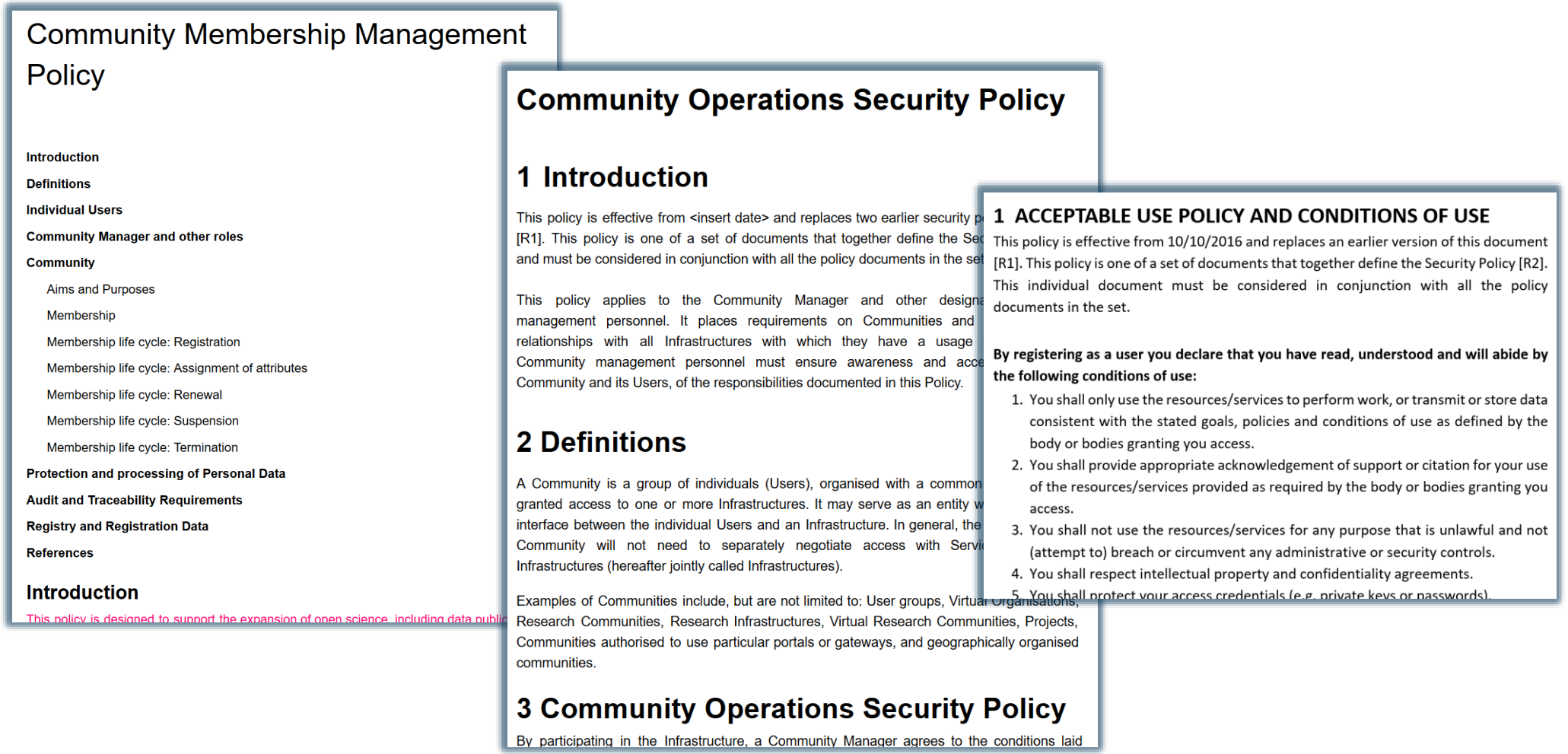
- Awareness: users and communities need to know there are policies
- Have an AUP covering the usual
- Community registration and membership should be managed
- Have a way of identifying both individuals and communities
- Define the common aims and purposes *(that really helps for data protection …)*

Protection and Processing of Personal Data

- Have a data protection policy that binds the infrastructure together, e.g. AARCs recommendations or DP CoCo
- Make sure every ‘back-end’ provider has a visible and accessible Privacy Policy

https://igtf.net/snctfi

Evolving the Policy Development Kit for communities around Snctfi



Community Membership Management Policy

Introduction
Definitions
Individual Users
Community Manager and other roles
Community
- Aims and Purposes
- Membership
- Membership life cycle: Registration
- Membership life cycle: Assignment of attributes
- Membership life cycle: Renewal
- Membership life cycle: Suspension
- Membership life cycle: Termination

Protection and processing of Personal Data
Audit and Traceability Requirements
Registry and Registration Data
References

Introduction

This policy is designed to support the expansion of open science, including data public

Community Operations Security Policy

1 Introduction

This policy is effective from <insert date> and replaces two earlier security p
[R1]. This policy is one of a set of documents that together define the Se
and must be considered in conjunction with all the policy documents in the se

This policy applies to the Community Manager and other designa
management personnel. It places requirements on Communities and
relationships with all Infrastructures with which they have a usage
Community management personnel must ensure awareness and acce
Community and its Users, of the responsibilities documented in this Policy.

2 Definitions

A Community is a group of individuals (Users), organised with a common
granted access to one or more Infrastructures. It may serve as an entity w
interface between the individual Users and an Infrastructure. In general, the
Community will not need to separately negotiate access with Servi
Infrastructures (hereafter jointly called Infrastructures).

Examples of Communities include, but are not limited to: User groups, Virtual Organisations,
Research Communities, Research Infrastructures, Virtual Research Communities, Projects,
Communities authorised to use particular portals or gateways, and geographically organised
communities.

3 Community Operations Security Policy

By participating in the Infrastructure, a Community Manager agrees to the conditions laid

1 ACCEPTABLE USE POLICY AND CONDITIONS OF USE

This policy is effective from 10/10/2016 and replaces an earlier version of this document [R1]. This policy is one of a set of documents that together define the Security Policy [R2]. This individual document must be considered in conjunction with all the policy documents in the set.

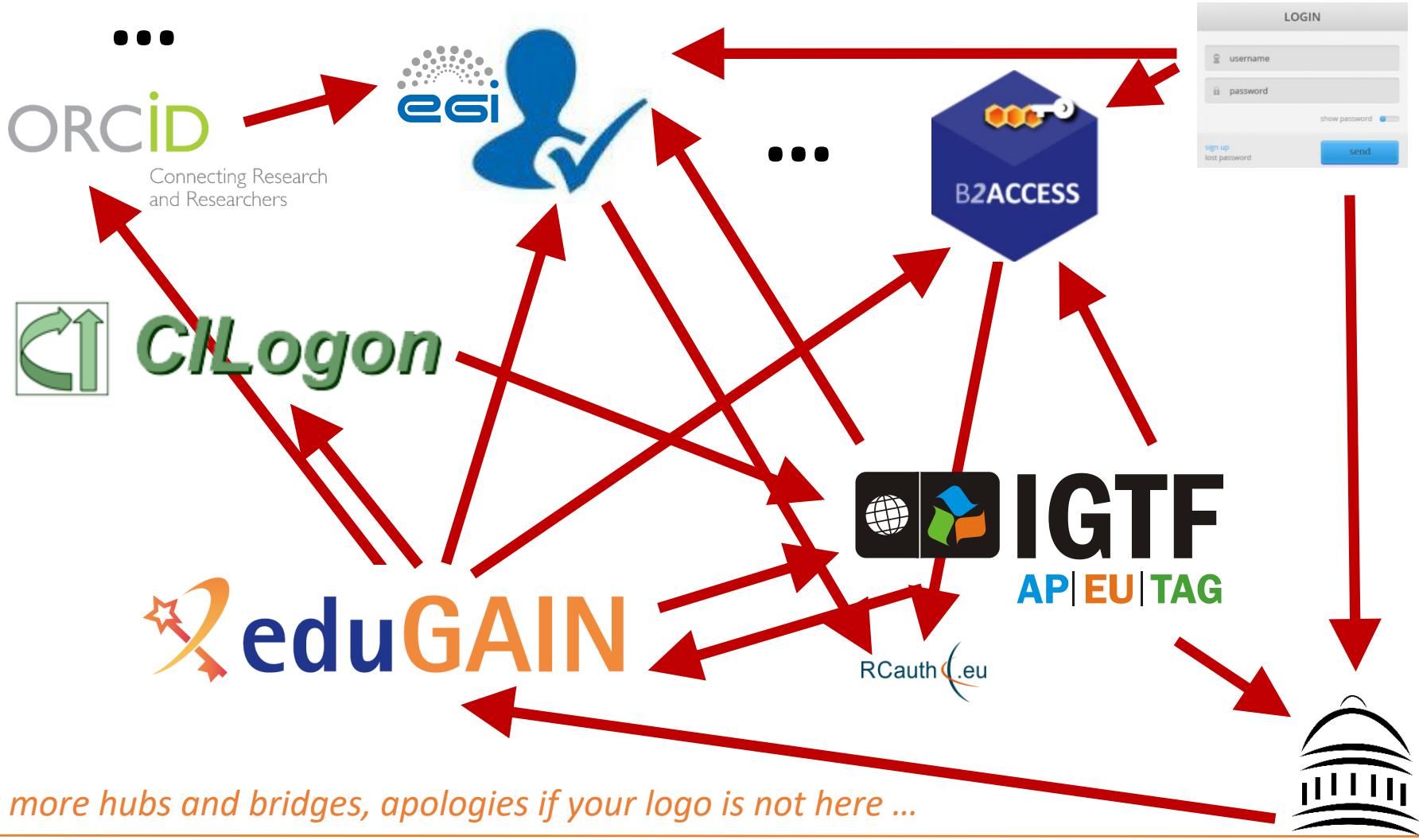
By registering as a user you declare that you have read, understood and will abide by the following conditions of use:

1. You shall only use the resources/services to perform work, or transmit or store data consistent with the stated goals, policies and conditions of use as defined by the body or bodies granting you access.
2. You shall provide appropriate acknowledgement of support or citation for your use of the resources/services provided as required by the body or bodies granting you access.
3. You shall not use the resources/services for any purpose that is unlawful and not (attempt to) breach or circumvent any administrative or security controls.
4. You shall respect intellectual property and confidentiality agreements.
5. You shall protect your access credentials (e.g. private keys or passwords).

...

https://wiki.geant.org/display/AARC/Policy+Engagement+and+Coordination

Everything can be meshed together …



and many more hubs and bridges, apologies if your logo is not here …

& WISE COMMUNITY

Collect Recommendations – both for Infrastructures & Federations

For your Research and generic e-Infrastructures

- Following AARC Blue Print Architecture and the recommendations – makes it easier for you
- Support Personal Data Protection (EU) + tag R&S – IdPs could giving you useable identifiers
- Assess if Sirtfi + R&S is sufficient for access. Or add a REFEDS Assurance Profile.
- Apply policy frameworks inside your Infrastructure, *'Snctfi'*, or re-use the policy kit

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Snctfi

For Federations, REFEDS, and eduGAIN

- Support an omnidirectional, non-reassigned ID for users that is standard everywhere
- Don't filter authentication to only services you know about: allow meta-data to flow
- Support attribute release through R&S, and collaborate in Sirtfi
- Help eduGAIN operate a support desk to help international research and collaboration

Recommendations go to REFEDS, eduGAIN – and the Infrastructures through FIM4R & IGTF

We have a lot to do still … ENGAGE through FIM4R, IGTF, REFEDS, WISE!

Operational Security and Incident Response

- Evolve beyond *Sirtfi* by adding automated (volume) **sharing of data and indicators of compromise**
- Cross-domain **trust groups** spanning Infrastructures (and the eduGAIN Support Desk)

Supporting Research Service Providers and Infrastructures: Service-centric guidance

- **Adoption of *Snctfi***, helping communities and infrastructure to express trust
- Accounting data in complex communities, **access control to accounting data** in Infrastructures?

Movement of people and collaboration: e-Researcher-centric guidance

- Align **attribute management practices & provenance** for self-hosting and managed communities
- Beyond Espresso: review complex Assurance Profile cases – in light of the GDPR and beyond

Policy Development Engagement and Coordination

- Guidance for communities: policy development and engagement 'kit'
- **SCIv3**: aligning *Snctfi*, *Sirtfi*, and *Recommendations* through WISE, IGTF, and FIM4R & FIMIG

And if I want to get to AARC?

- A bilateral channel to:
  - Report on AARC recommendations and pilots with research collaborations in AARC
  - Get feedback on AARC solutions from the wider FIM4R community
- Explore possibility to pilot solutions more widely
- Effectively supporting FIM4R
  - AARC supports participation of AARC research collaborations at FIM4R

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

Thank you

Any Questions?

davidg@nikhef.nl

http://aarc-project.eu/

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).