AARC 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

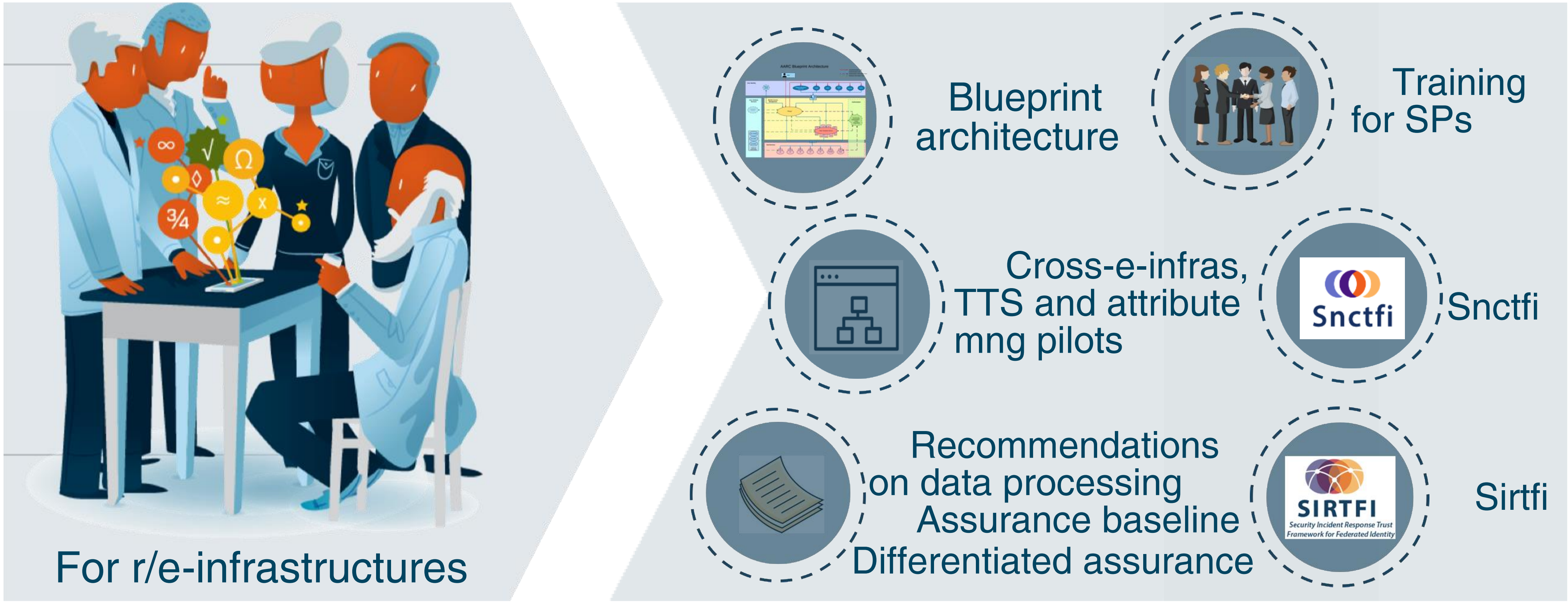
Identified common challenges – beyond the ‘corporate IT’ stuff

Communities / e-infrastructures surveyed in AARC

BBMRI Biobanking and Biomolecular Resources Research Infrastructure
CORBEL
instruct Integrating Biology
LIGO PROJECT
elixir
EPOS EUROPEANPLATEOBSERVINGSYSTEM
CLARIN
LifeWatch
INFRAFRONTIER
umbrella
BioVeL
cta cherenkov telescope array
WLCG Worldwide LHC Computing Grid
DARIAH-EU
HP
ARIADNE
EISCAT 3D
HELIX NEBULA THESCIENCECLOUD
PRACE
EUDAT
egi
GÉANT
CERN

- 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



For r/e-infrastructures

Blueprint architecture

Training for SPs

Cross-e-infras, TTS and attribute mng pilots

Snctfi

Recommendations on data processing

Assurance baseline

Differentiated assurance

Sirtfi

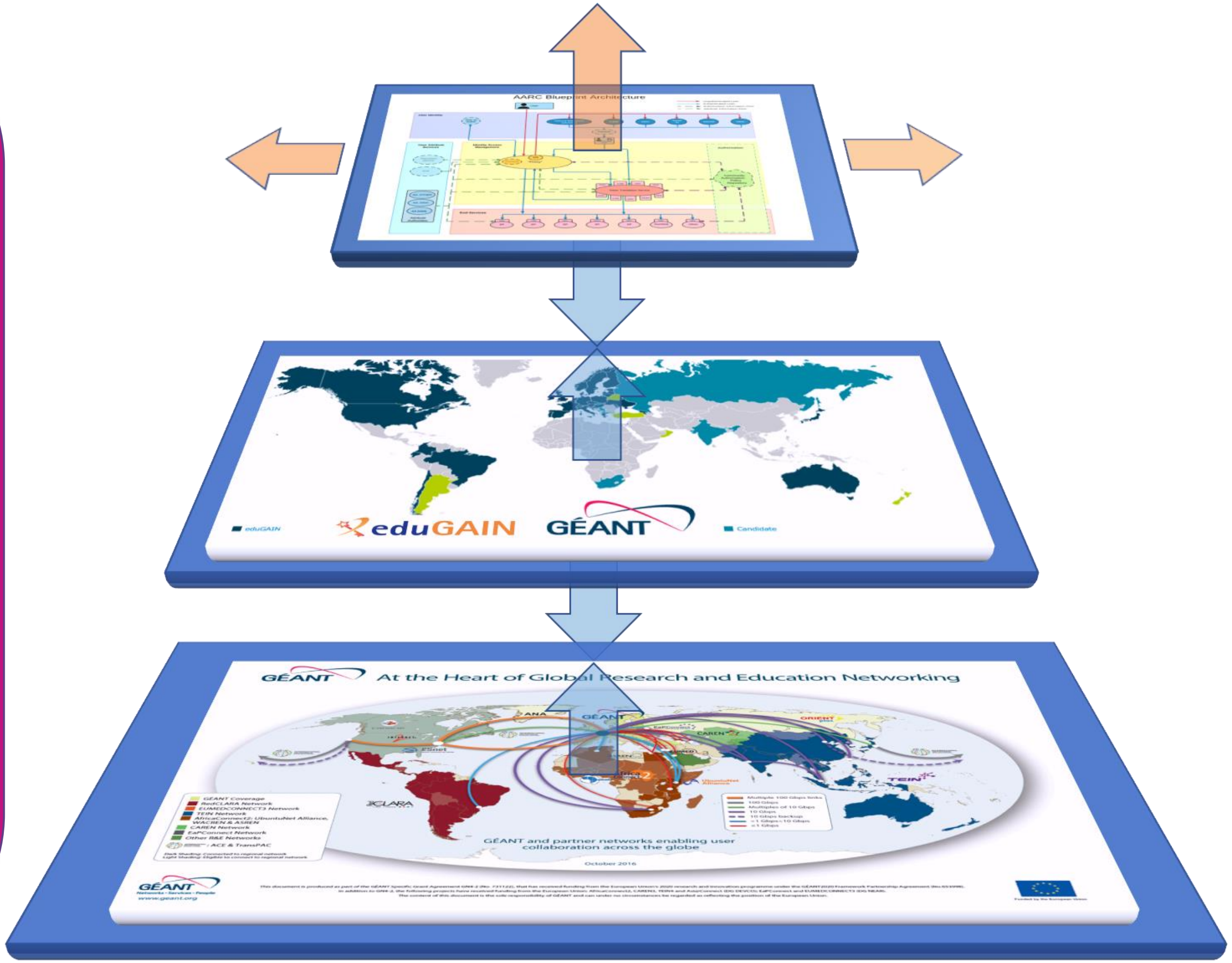
Snctfi
SIRTFI
Security Incident Response Trust Framework for Federated Identity

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

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

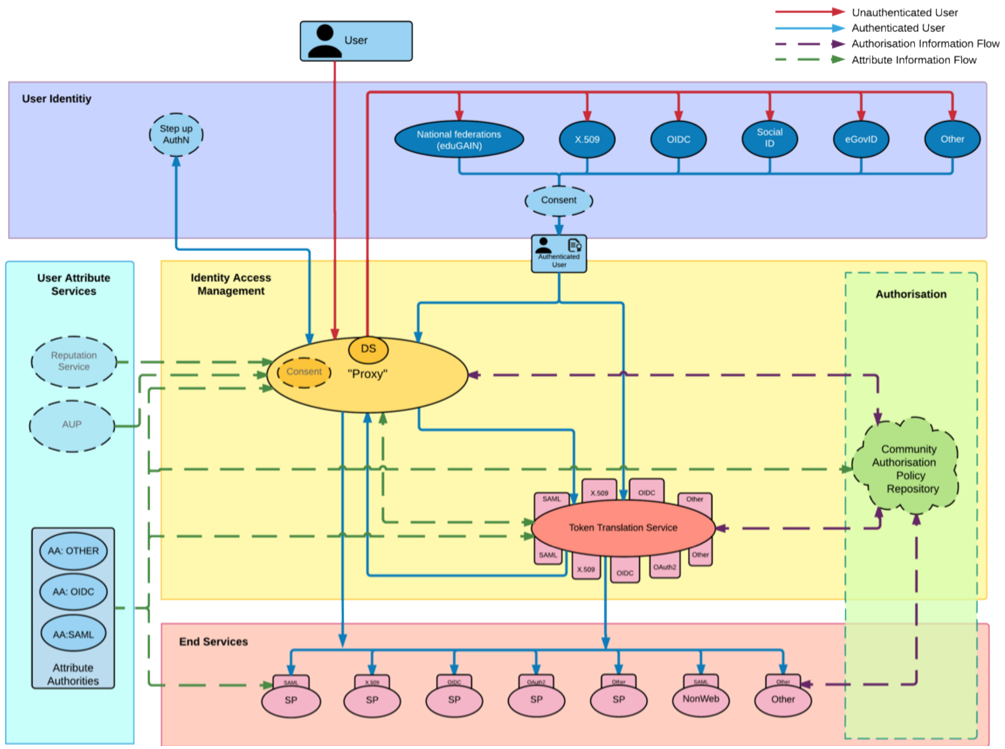
AARC Blueprint Architecture - Enabling an ecosystem of solution on top of eduGAIN

- 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
eduGAIN
eduGAIN
GÉANT
Candidate
GÉANT
At the Heart of Global Research and Education Networking
GÉANT and partner networks enabling user collaboration across the globe
October 2016
GÉANT
Networks • Services • People
www.geant.org

AARC Blueprint Architecture

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



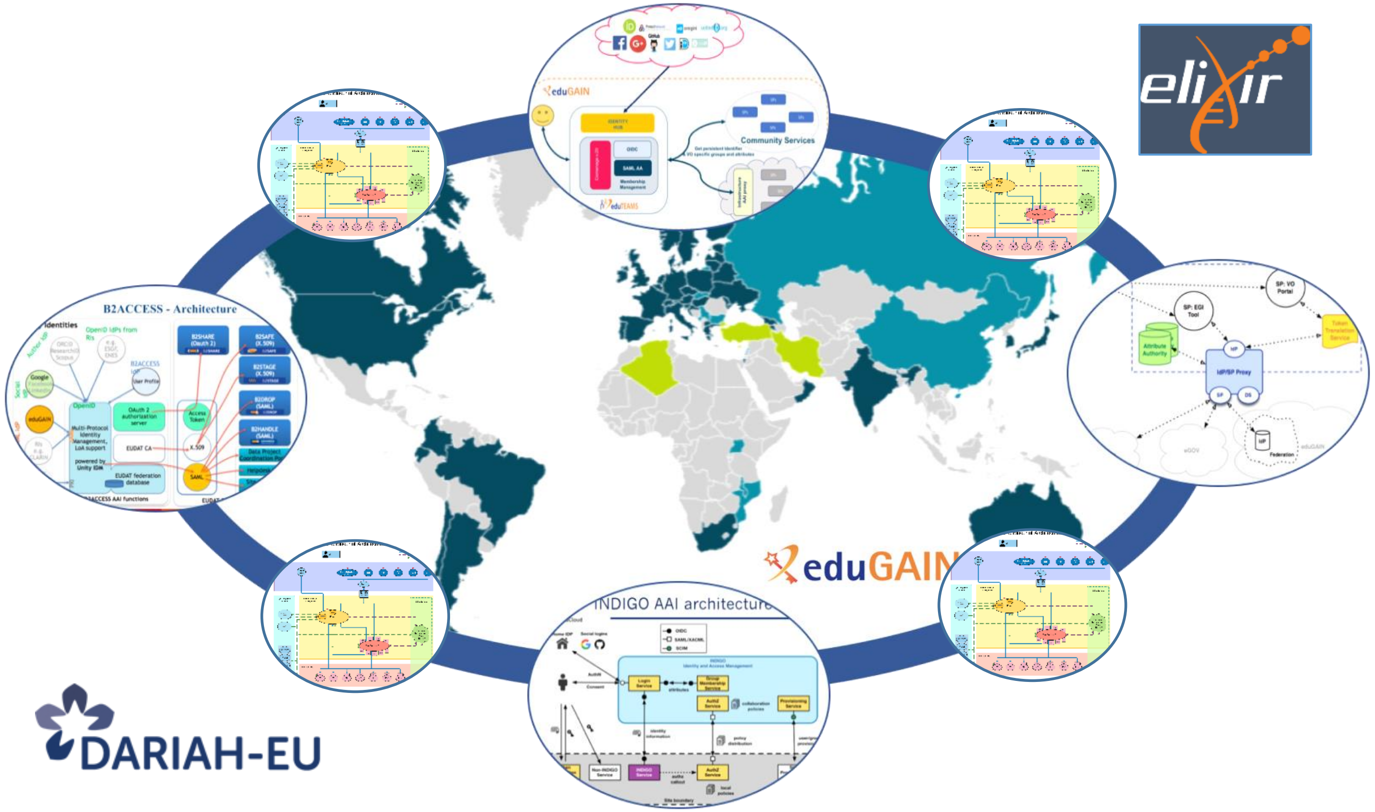
Guidelines and support documents

- 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

GÉANT

elixir

EUDAT



egi

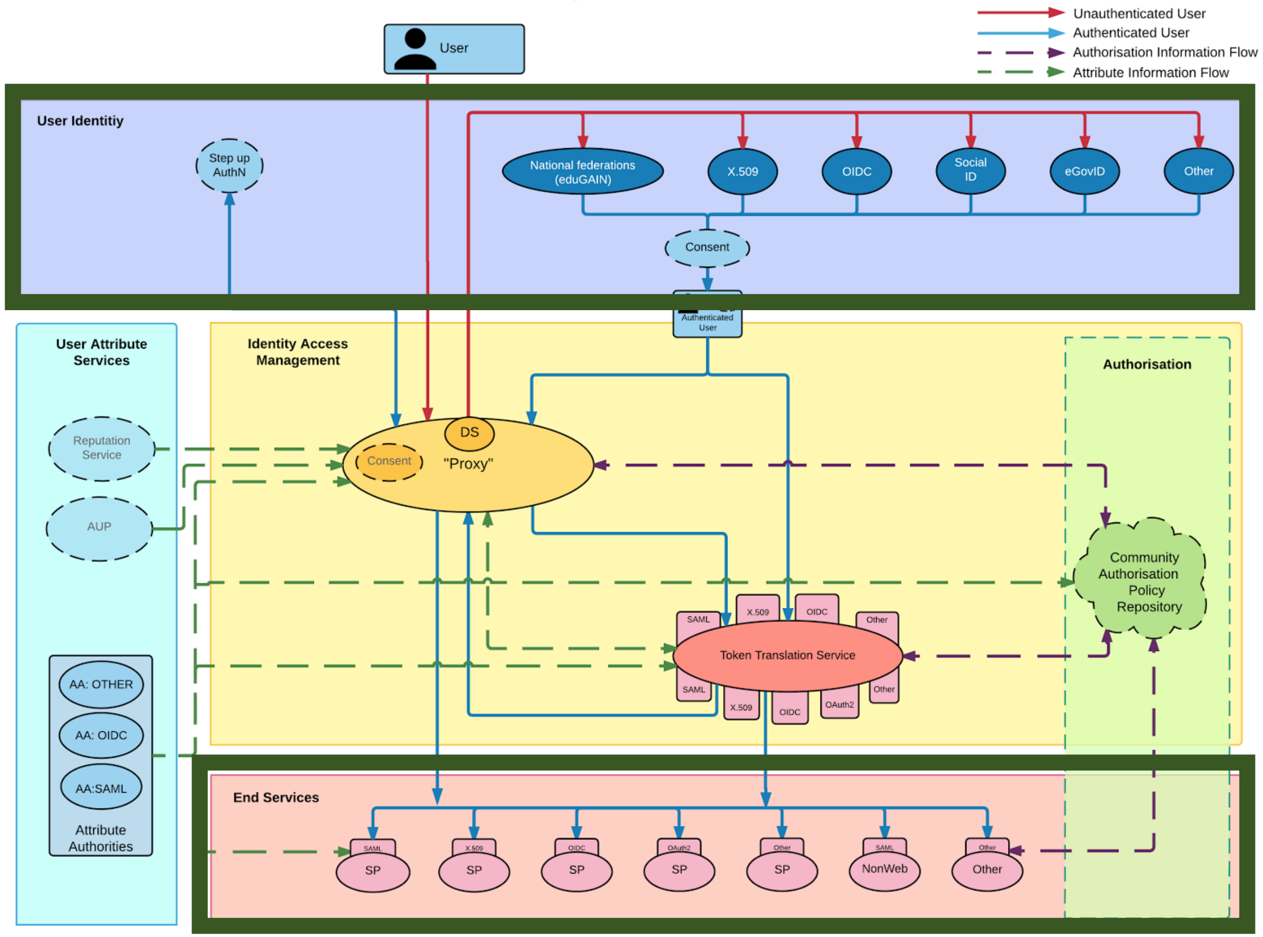
DARIAH-EU

INDIGO - DataCloud
Better Software for Better Science

and over 20 pilots with user communities and Infrastructures

Easing linking of research to infrastructure services with good practice

AARC Blueprint Architecture



'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:

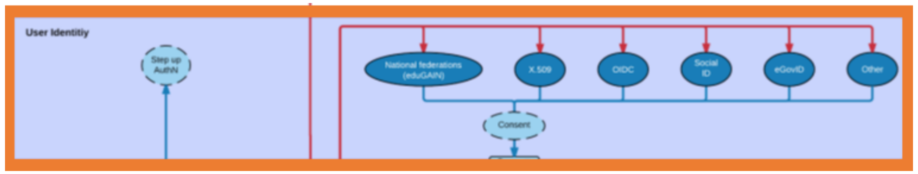
- *Filtering function for policy and assurance*
- *Present harmonized view to existing federations to get 'useful' data from them*

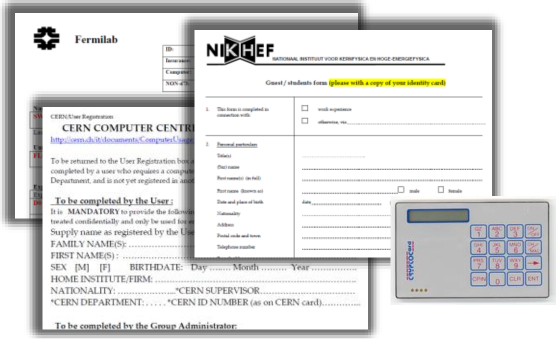
Service Infrastructure

- ***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





Fermilab

ID:
Insurance:
Computer:
NON-473:

NIKHEF NATIONAAL INSTITUUT VOOR KERNFYSICA EN HOGE-ENERGIEFYSICA

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

1. This form is completed in connection with: □ work experience □ otherwise, viz. ....

2. Personal particulars
Title(s)
(Sur) name
First name(s) (in full)
First name (known as) □ male □ female
Date and place of birth date ....
Nationality
Address
Postal code and town
Telephone number

CERN/User Registration

CERN COMPUTER CENTR

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

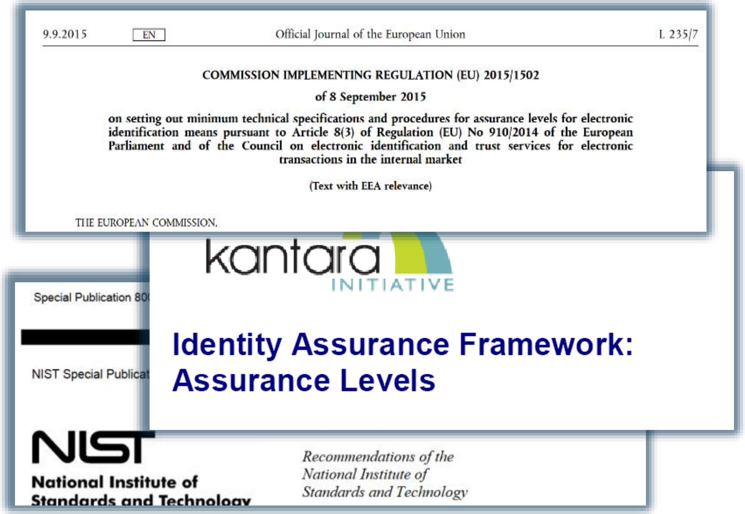
To be returned to the User Registration box a
completed by a user who requires a compute
Department, and is not yet registered in ano

To be completed by the User :

It is MANDATORY to provide the followin
treated confidentially and only be used for
Supply name as registered by the Use
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:

CRYPTOCard
QZ 1
ABC 2
DEF 3
ON/OFF
GHI 4
JKL 5
MNO 6
CH/MAC
PRS 7
TUV 8
WXY 9
CPIN
0
CLR
ENT



9.9.2015 EN Official Journal of the European Union L 235/7

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

of 8 September 2015

on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

kantara INITIATIVE

Identity Assurance Framework: Assurance Levels

Special Publication 80

NIST Special Publicat

NIST National Institute of Standards and Technology

Recommendations of the National Institute of Standards and Technology

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 a (Research) Infrastructure viewpoint

‘low-risk’ use cases

few unalienable expectations by research and collaborative services

Milestone MNA3.1: Recommendations on Minimal Assurance Level Relevant for Low-risk Research Use Cases

Baseline Assurance

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

generic e-Infrastructure services

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

Slice includes:

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

protection of sensitive resources

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

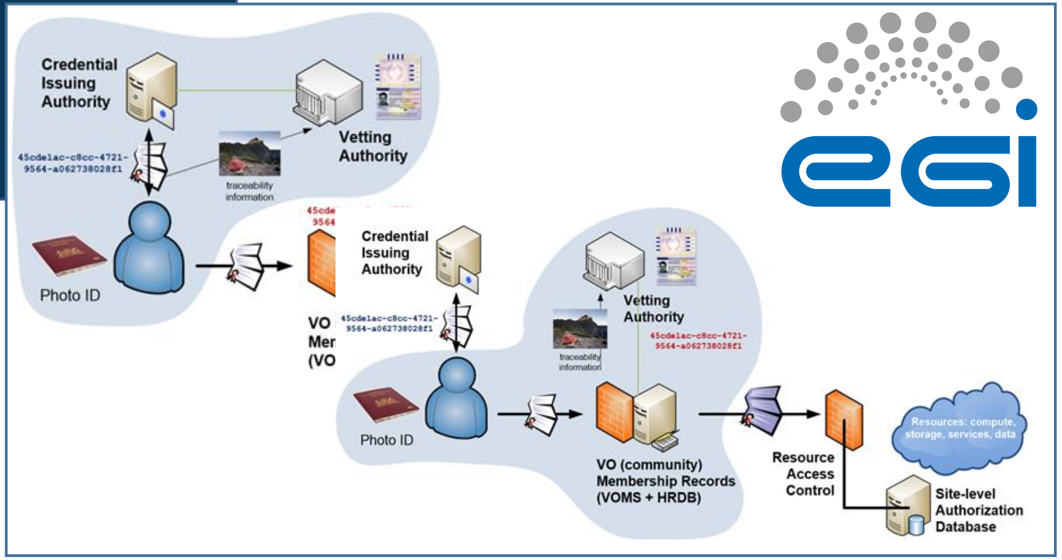
Slice includes:

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

Using Assurance in practice: “Espresso” for sensitive data

Identifiers	ID proofing	Authentication	Attributes
ID is unique, personal and traceable	Good enough for institution’s local systems	Good entropy passwords	Accurate and fresh affiliation information
ePPN is unique, personal and traceable	Assumed (e.g. postal credential delivery)	Multi-factor authentication	
	Verified (e.g. F2F)		

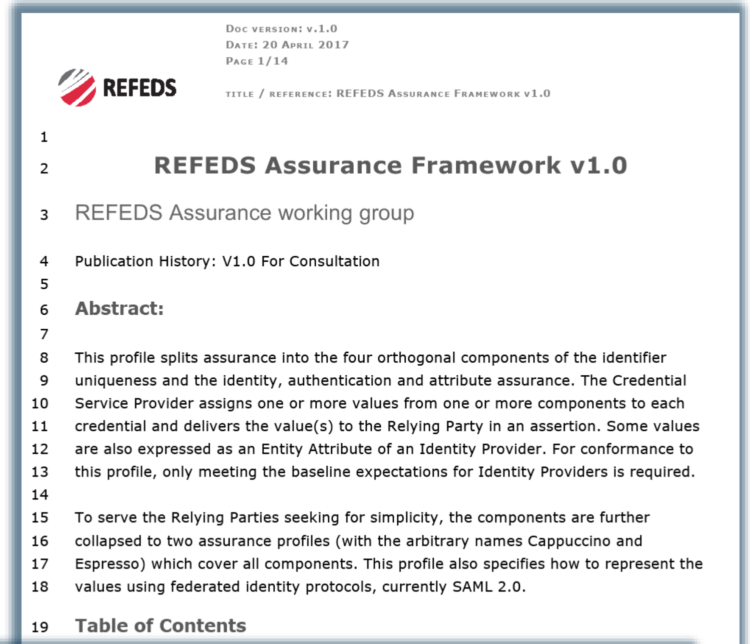
Assurance can come from a single source …
… or be a combined/collaborative assurance by identifier source and vetting attributes


Credential Issuing Authority
45cdelac-c8cc-4721-9564-a062738028f1
traceability information
Vetting Authority
Photo ID
45cde
9564
VO
Mer
(VO
Credential Issuing Authority
45cdelac-c8cc-4721-9564-a062738028f1
Vetting Authority
traceability information
45cdelac-c8cc-4721-9564-a062738028f1
Photo ID
VO (community) Membership Records (VOMS + HRDB)
Resource Access Control
Resources: compute, storage, services, data
Site-level Authorization Database
egi

Gaining global adoption: REFEDS Assurance Framework

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

- open, international forum (gave us R&S spec with 'some' UniqueID)
- 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



Doc version: v.1.0
Date: 20 April 2017
Page 1/14

REFEDS

title / reference: REFEDS Assurance Framework v1.0

REFEDS Assurance Framework v1.0

REFEDS Assurance working group

Publication History: V1.0 For Consultation

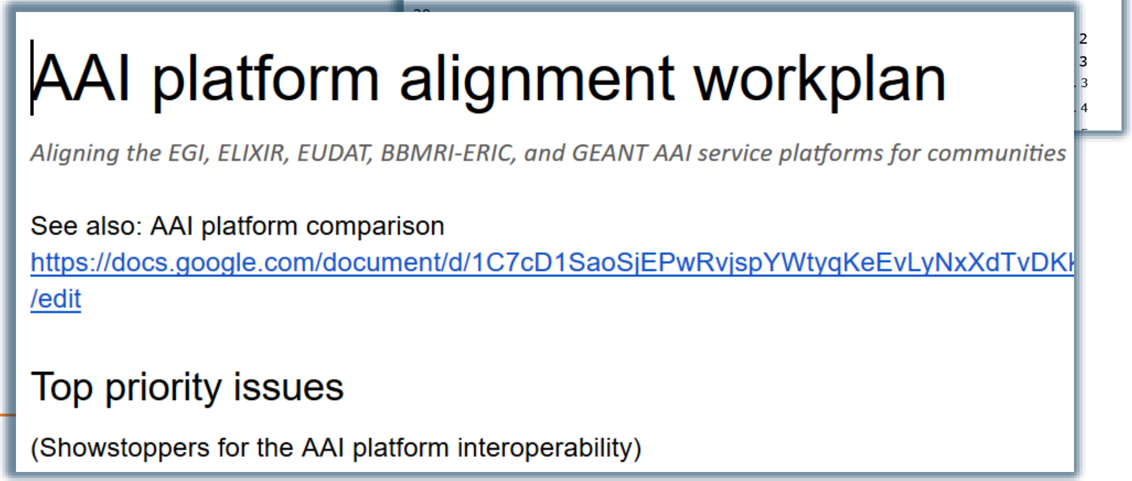
Abstract:

This profile splits assurance into the four orthogonal components of the identifier uniqueness and the identity, authentication and attribute assurance. The Credential Service Provider assigns one or more values from one or more components to each credential and delivers the value(s) to the Relying Party in an assertion. Some values are also expressed as an Entity Attribute of an Identity Provider. For conformance to this profile, only meeting the baseline expectations for Identity Providers is required.

To serve the Relying Parties seeking for simplicity, the components are further collapsed to two assurance profiles (with the arbitrary names Cappuccino and Espresso) which cover all components. This profile also specifies how to represent the values using federated identity protocols, currently SAML 2.0.

Table of Contents

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



AAI platform alignment workplan

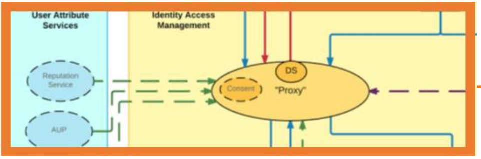
Aligning the EGI, ELIXIR, EUDAT, BBMRI-ERIC, and GEANT AAI service platforms for communities

See also: AAI platform comparison
https://docs.google.com/document/d/1C7cD1SaoSjEPwRvjspYWtyqKeEvLyNxXdTvDKk
/edit

Top priority issues

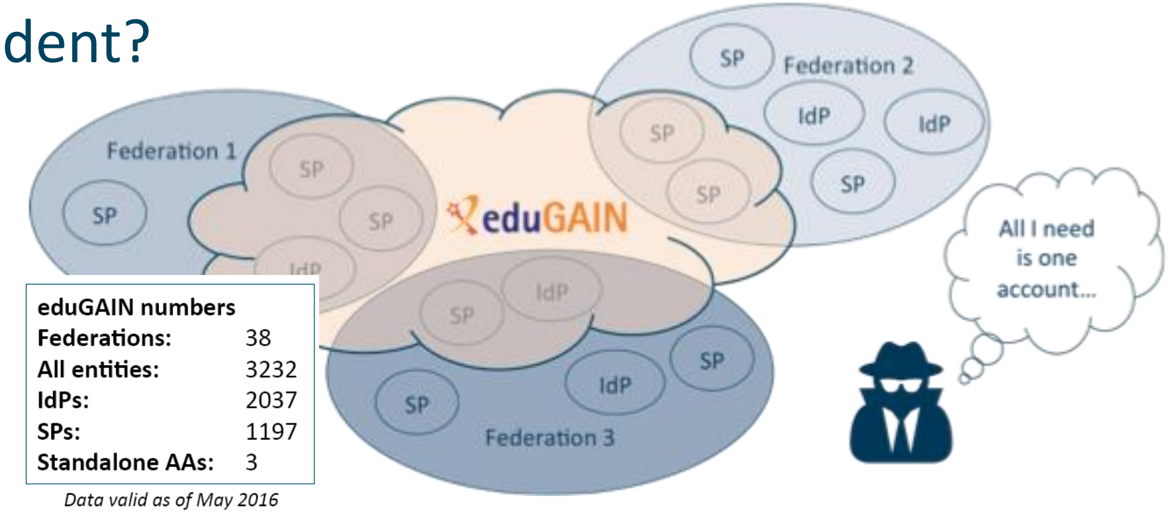
(Showstoppers for the AAI platform interoperability)

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



Security Incident Response in the Federated World

- 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

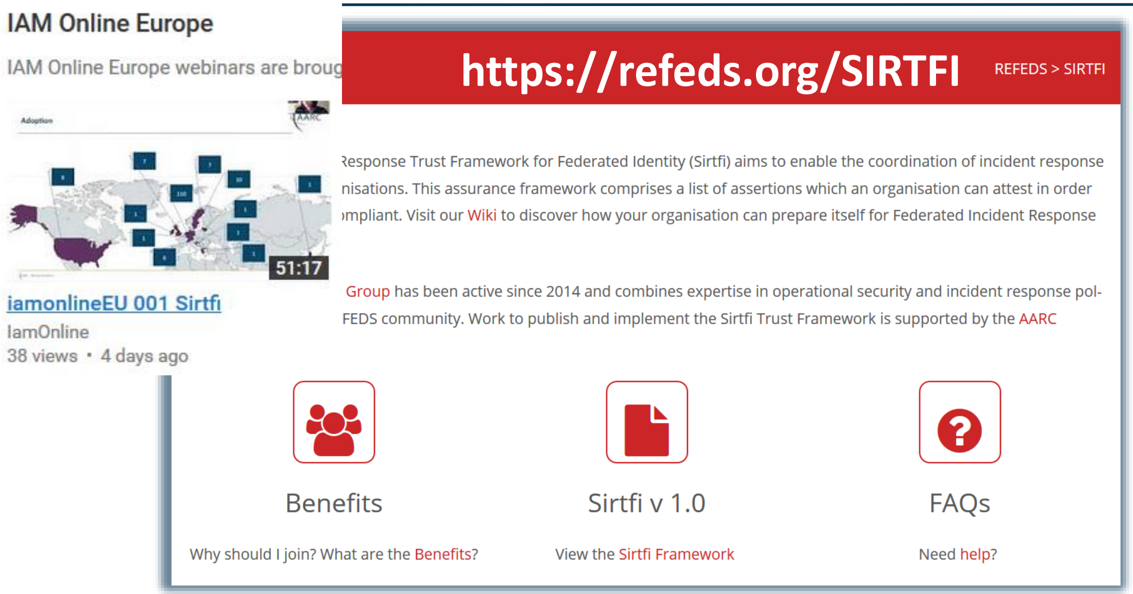
- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Sirtfi adoption by authentication providers and services



IAM Online Europe

IAM Online Europe webinars are broug

51:17

iamonlineEU 001 Sirtfi

IamOnline

38 views • 4 days ago

https://refeds.org/SIRTFI REFEDS > SIRTFI

Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response nisations. This assurance framework comprises a list of assertions which an organisation can attest in order ompliant. Visit our Wiki to discover how your organisation can prepare itself for Federated Incident Response

Group has been active since 2014 and combines expertise in operational security and incident response pol- FEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC

Benefits

Why should I join? What are the Benefits?

Sirtfi v 1.0

View the Sirtfi Framework

FAQs

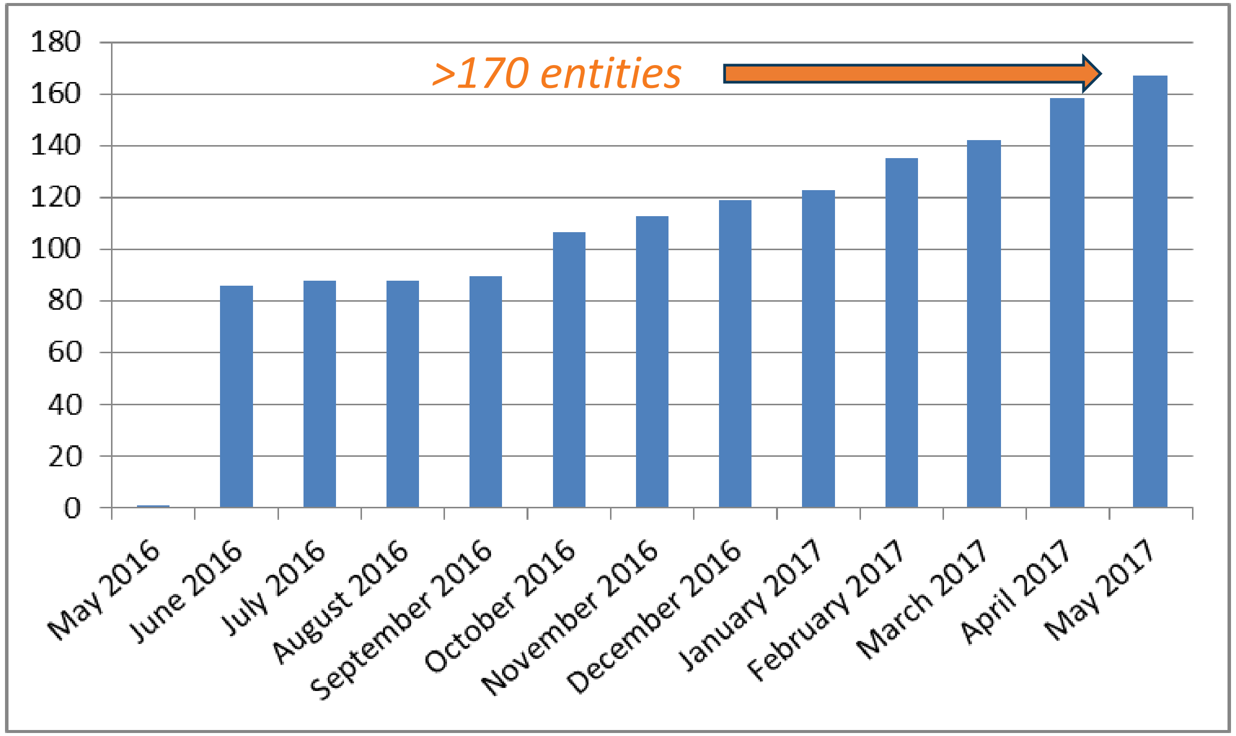
Need help?

- 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

Snctfi v1.0 AARC

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

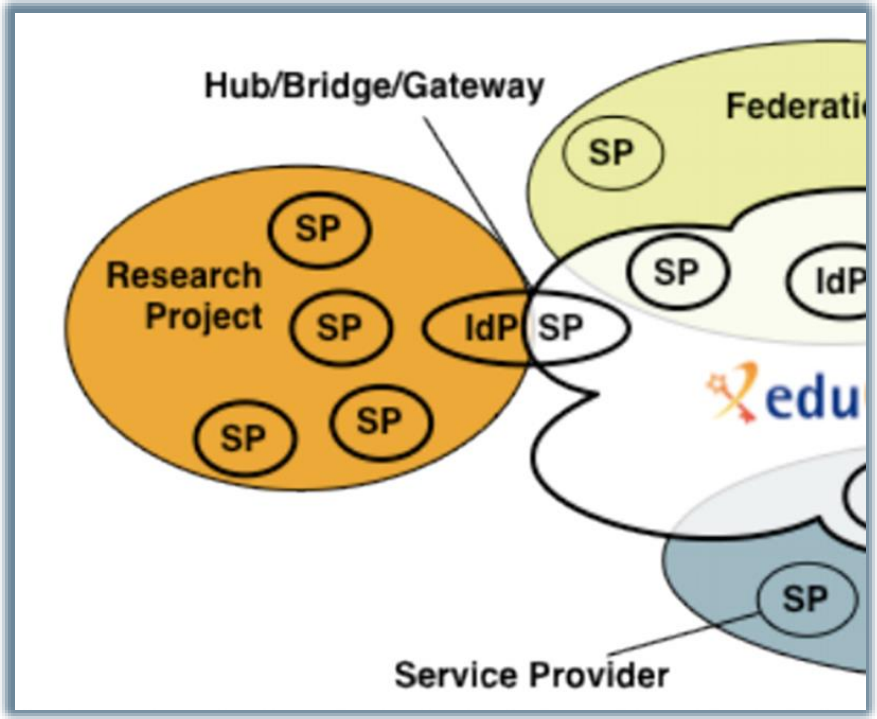
Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp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

E-INFRASTRUCTURES: MAKING EUROPE THE BEST PLACE FOR RESEARCH AND INNOVATION

- 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

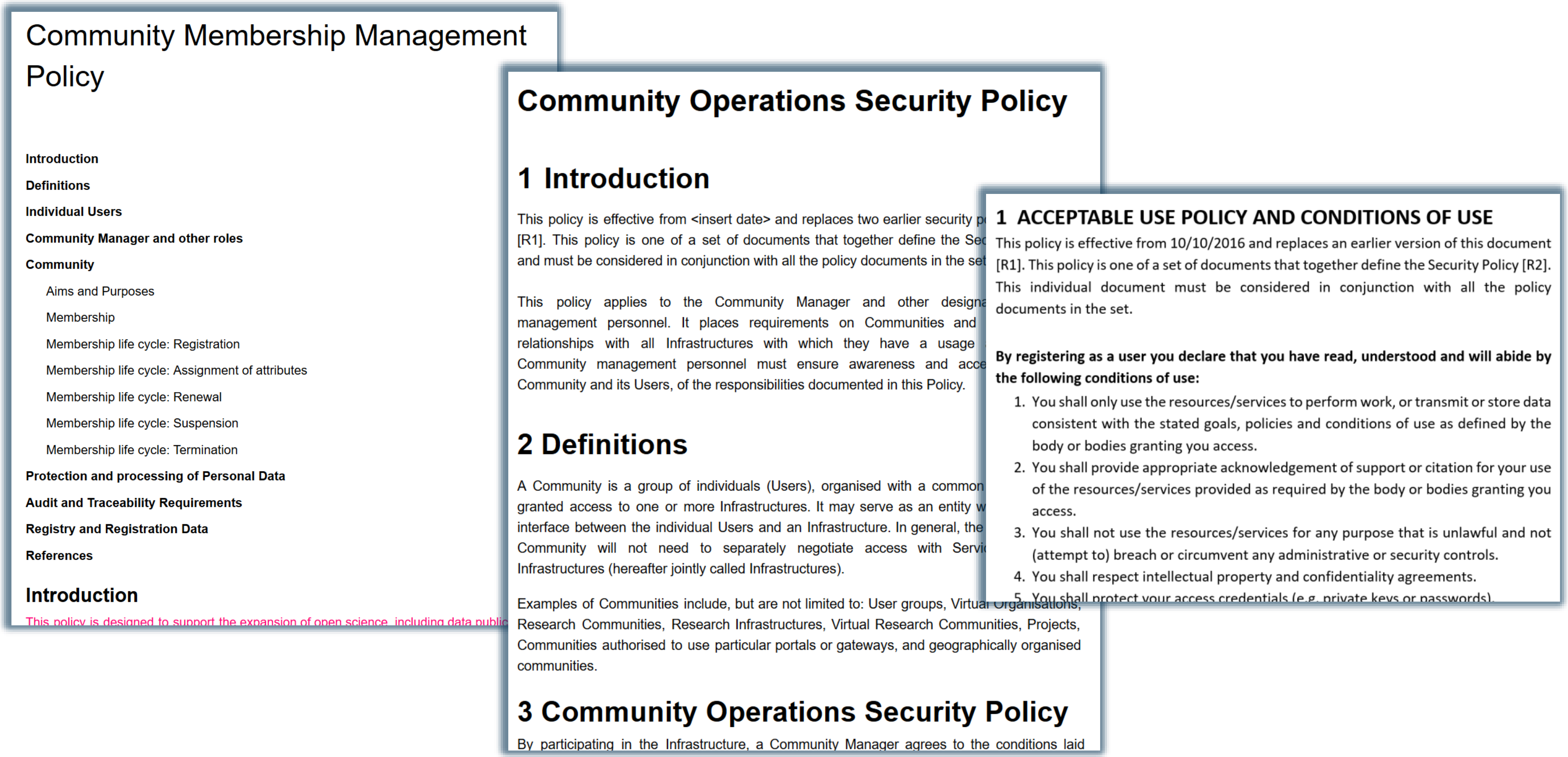
- Awareness: users and communities need to know there are policies
- Have an AUP covering the usual
- Community registration and membership should be managed
- Have a way of identifying both individuals and communities
- Define the common aims and purposes *(that really helps for data protection …)*

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 Sec
and must be considered in conjunction with all the policy documents in the set

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.

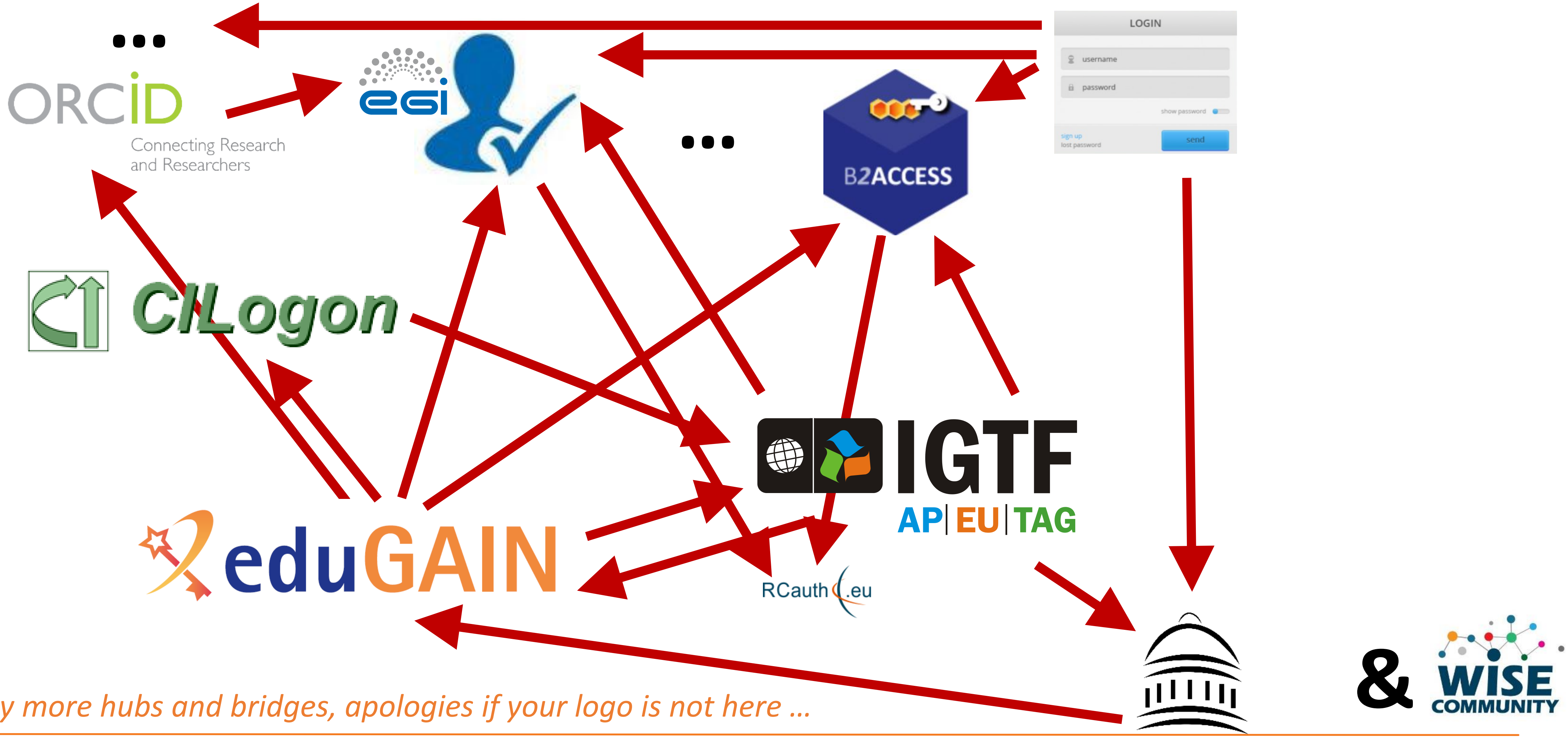
By registering as a user you declare that you have read, understood and will abide by the following conditions of use:

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 …

Collect Recommendations – both for Infrastructures & Federations

For your Research and generic e-Infrastructures

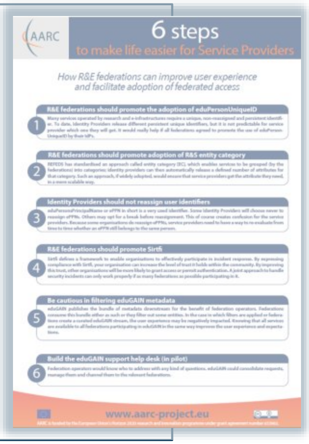
- Following AARC Blue Print Architecture and the recommendations – makes it easier for you
- Support Personal Data Protection (EU) + tag R&S – IdPs could giving you useable identifiers
- Assess if Sirtfi + R&S is sufficient for access. Or add a REFEDS Assurance Profile.
- Apply policy frameworks inside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



AARC

6 steps
to make life easier for Service Providers

How R&E federations can improve user experience and facilitate adoption of federated access

1. **R&E federations should promote the adoption of eduPersonUniqueID**
Many services operated by research and e-infrastructures require a unique, non-reassigned and persistent identifier. To date, Identity Providers release different persistent unique identifiers, but it is not predictable for service provider which one they will get. It would really help if all federations agreed to promote the use of eduPersonUniqueID by their IdPs.

2. **R&E federations should promote adoption of R&S entity category**
REFEDS has standardised an approach called entity category (EC), which enables services to be grouped (by the federations) into categories; identity providers can then automatically release a defined number of attributes for that category. Such an approach, if widely adopted, would ensure that service providers get the attribute they need, in a more scalable way.

3. **Identity Providers should not reassign user identifiers**
eduPersonPrincipalName or ePPN in short is a very used identifier. Some Identity Providers will choose never to reassign ePPNs. Others may opt for a break before reassignment. This of course creates confusion for the service providers. Because some organisations do reassign ePPNs, service providers need to have a way to re-evaluate from time to time whether an ePPN still belongs to the same person.

4. **R&E federations should promote Sirtfi**
Sirtfi defines a framework to enable organisations to effectively participate in incident response. By expressing compliance with Sirtfi, your organisation can increase the level of trust it holds within the community. By improving this trust, other organisations will be more likely to grant access or permit authentication. A joint approach to handle security incidents can only work properly if as many federations as possible participating in it.

5. **Be cautious in filtering eduGAIN metadata**
eduGAIN publishes the bundle of metadata downstream for the benefit of federation operators. Federations consume this bundle either as such or they filter out some entities. In the case in which filters are applied or federations create a curated eduGAIN stream, the user experience may be negatively impacted. Knowing that all services are available to all federations participating in eduGAIN in the same way improves the user experience and expectations.

6. **Build the eduGAIN support help desk (in pilot)**
Federation operators would know who to address with any kind of questions. eduGAIN could consolidate requests, manage them and channel them to the relevant federations.

www.aarc-project.eu

AARC is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement number 653965.

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

CEF
COMMUNITY
ENGAGEMENT
FORUM

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

Thank you

Any Questions?

davidg@nikhef.nl

AARC

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).