Authentication and Authorisation for Research and Collaboration

Frameworks for harmonized policies and practices

The Story So Far …

David Groep
Activity Coordinator
Dutch National Institute for sub-atomic Physics Nikhef

DI4R 2018
November 2017

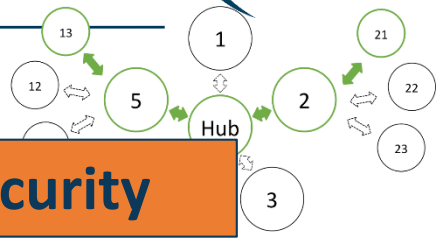
Touring the policy space in AARC

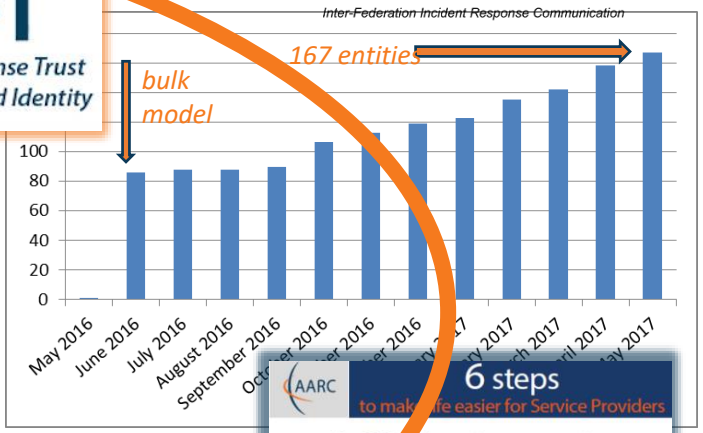
supporting Researcher Community Assurance

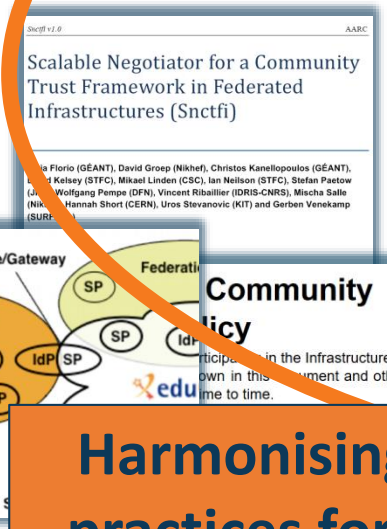
Operational Security

Harmonising support for practices for communties

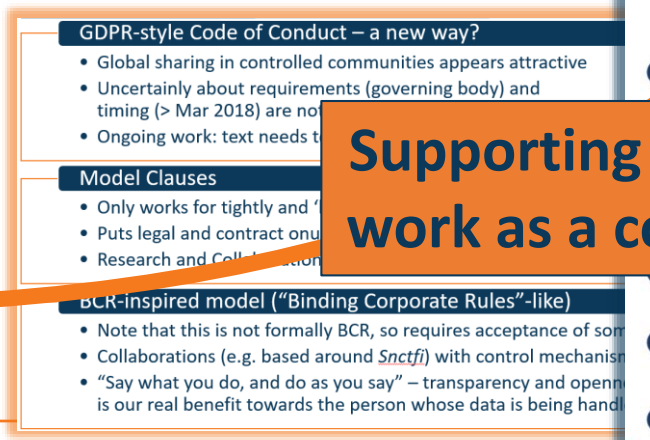
Supporting Infrastructures work as a coherent system

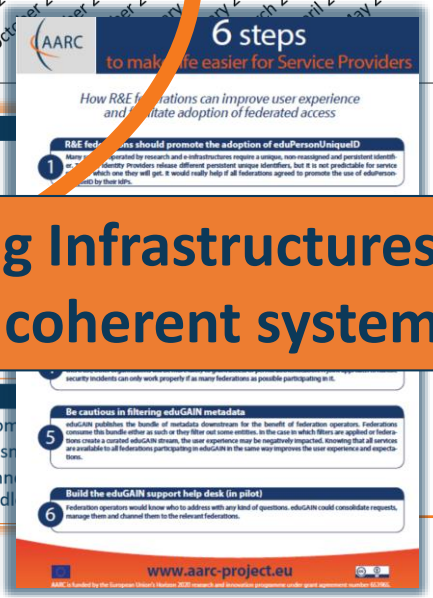






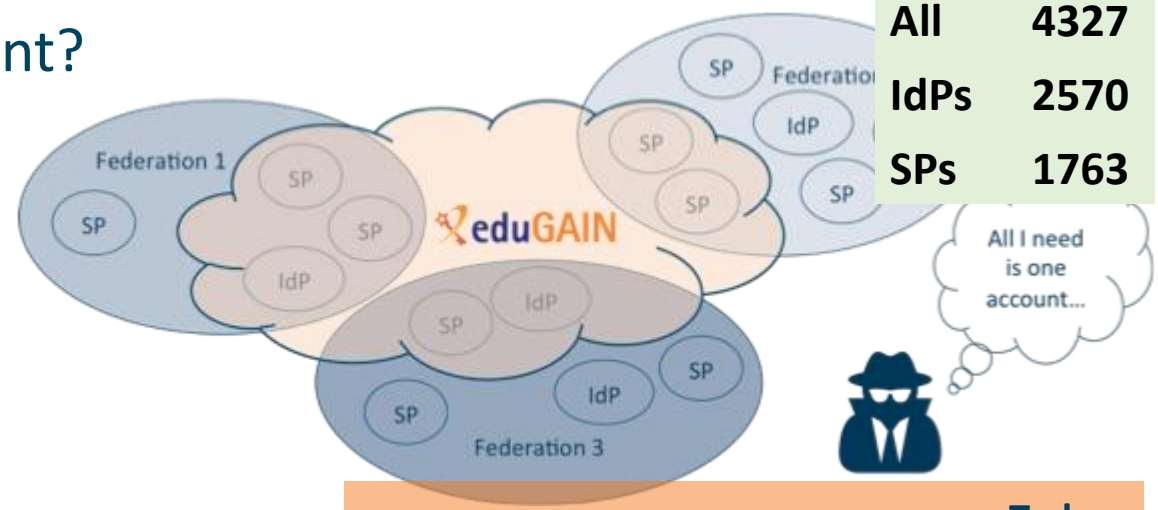
Sctfi





Security Incident Response in the Federated World

- How could we determine the scale of the incident?
  - Do useful logs exist? Could logs be shared?
- Taking responsibility for resolving an incident
- How could we alert the identity providers and service providers involved?
- Enable information to be shared confidentially



All	**4327**
IdPs	**2570**
SPs	**1763**

Today:
293 IdPs support **R&S**
188 IdPs from 18 feds support **Sirtfi**
63 IdPs (from 17 feds) support **both** …

Security Incident Response Trust Framework for Federated Identity

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

see **http://refeds.org/sirtfi**

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

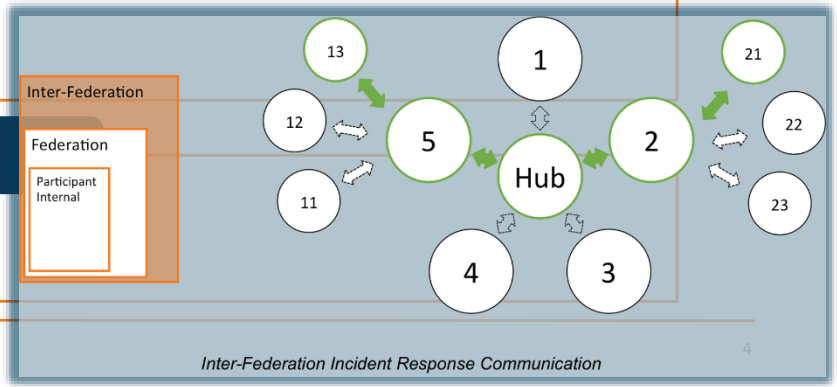
- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration

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



see http://refeds.org/sirtfi

Permissing usage accounting across collective services

Data collection necessary for ‘legitimate interests’ for Research and e-Infra

- Justification of **global** resource use, with infrastructures collecting data collaboratively
- Operational purposes: fault finding, researcher support, Incident response

Global view needed for accounting data

- exchange of personal data is imperative – both for EIs and Research Collaboration funding
- roles are defined to limit access to personally identifiable data

Policy coherency as enabler – model policies

- put in place policies on retention, permissible use, secure exchange, purpose limitation
- ‘binding’ - in the sense that a party can only remain in the club if it’s compliant
- policy suite identified by *Security for Collaborating Infrastructures* (SCI) group

Security Incident Response – data exchange

- add as permissible purpose, but leave its scope to Sirtfi and existing forums

Three community models – three Recommendations?

GDPR-style Code of Conduct – a new way from May 2018

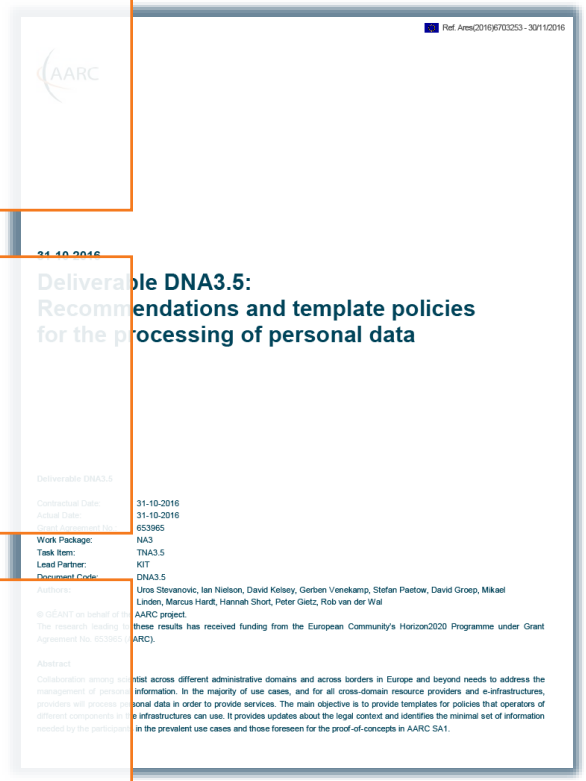
- Global sharing in controlled communities appears attractive
- Uncertainly about requirements (governing body) and timing (> Mar 2018) are not helpful for adoption today … just yet
- Ongoing work: text needs to allow for (community) attribute authorities

Model Clauses

- Only works for tightly and ‘legal document’ controlled communities
- Puts legal and contract onus on the SP-IdP Proxy (as per our Blueprint)
- Research and Collaboration lack both mechanism and time to do this

BCR-inspired model (“Binding Corporate Rules”-like)

- Note that this is not formally BCR, so requires acceptance of some risk
- Collaborations (e.g. based around *Snctfi*) with control mechanisms benefit
- “Say what you do, and do as you say” – transparency and openness is our real benefit towards the person whose data is being handled


Ref. Ares(2016)6703253 - 30/11/2016

Deliverable DNA3.5:
Recommendations and template policies for the processing of personal data

Contractual Date: 31-10-2016
Actual Date: 31-10-2016
Work Package: NA3
Task Item: TNA3.5
Lead Partner: KIT
Document Code: DNA3.5
Authors: Uros Stevanovic, Ian Nielson, David Kelsey, Gerben Venekamp, Stefan Paetow, David Groep, Mikael Linden, Marcus Hardt, Hannah Short, Peter Gietz, Rob van der Wal

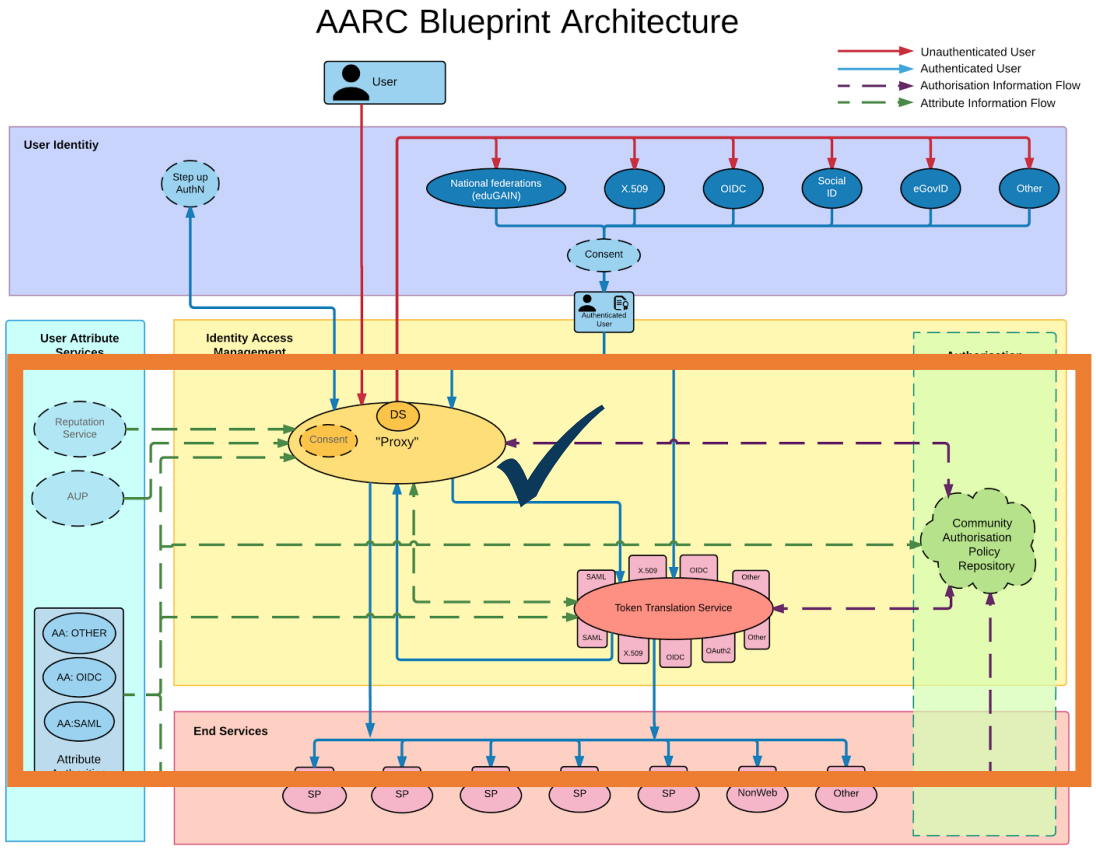
© GÉANT on behalf of the AARC project.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Abstract

Collaboration among scientist across different administrative domains and across borders in Europe and beyond needs to address the management of personal information. In the majority of use cases, and for all cross-domain resource providers and e-infrastructures, providers will process personal data in order to provide services. The main objective is to provide templates for policies that operators of different components in the infrastructures can use. It provides updates about the legal context and identifies the minimal set of information needed by the participants in the prevalent use cases and those foreseen for the proof-of-concepts in AARC SA1.

Proxying not just AAI flow, but policy & practice as well



- ✓ allow SPIdP Proxies to assert ‘qualities’, categories, based on assessable common trust
- ✓ Develop recommendations and framework for a infrastructure coherent policy set

Snctfi

Scalable Negotiator for a Community Trust Framework in Federated Infrastructures

- Derived from SCI, the framework on *Security for Collaboration among Infrastructures*
- Infrastructures would assert *existing* categories to IdPs: REFEDS R&S, Sirtfi, DPCoCo, …

see http://igtf.net/snctfi

Ease the flow across infrastructures – targeting users & communities!

Identify and support commonality between acceptable use policies (AUPs)
So that a user that signed one of them need not be bothered again – and still move across silos

- Generic e-Infrastructures have a similar, but slightly diverged, AUP based on the Taipei Accord
- Realign the Taipei Accord concepts, and add a layered approach to support communities

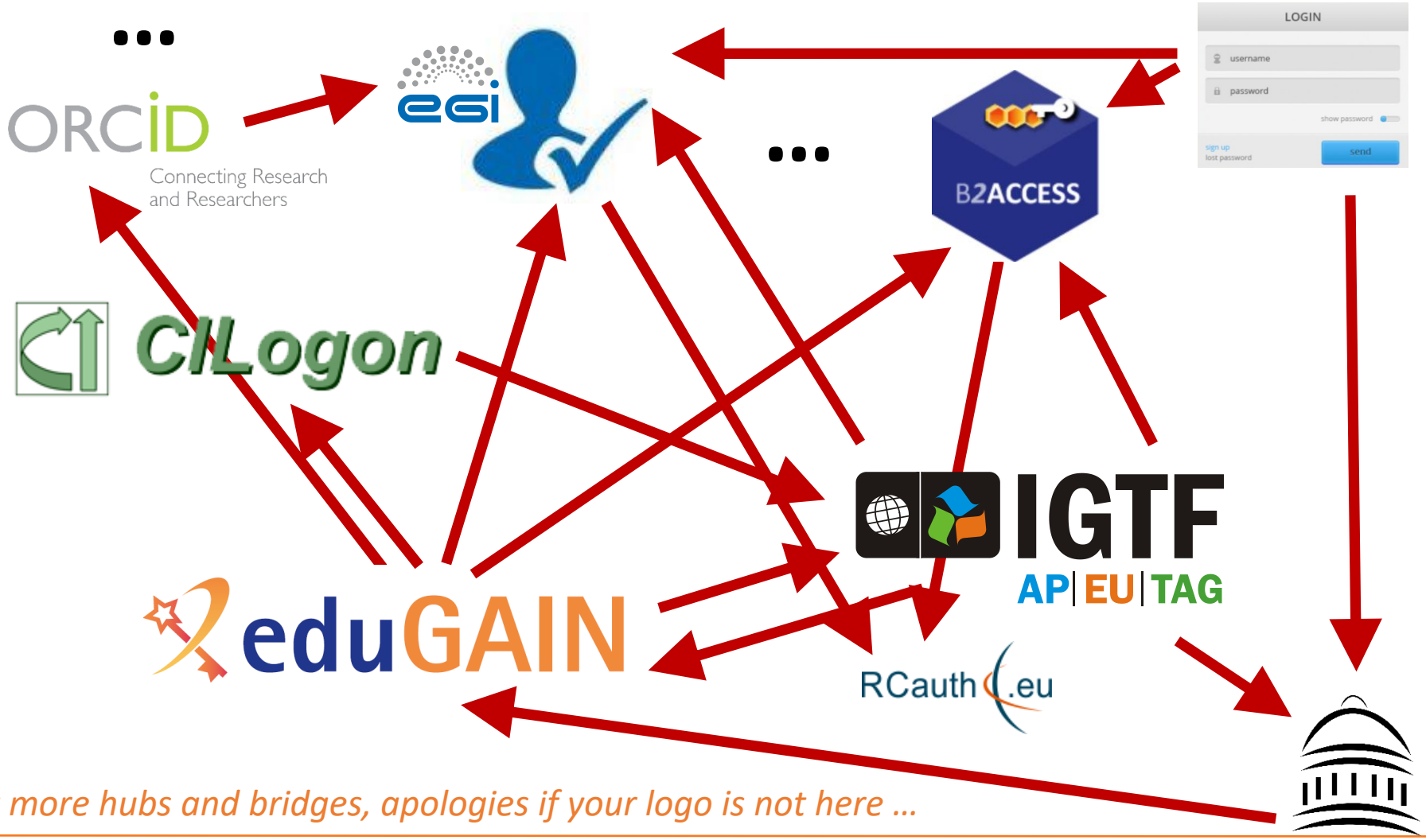
Support user communities implementing the gaps in Snctfi
Reference practices for communities setting up their AAI

- With the central role of the community, you gain control and responsibilities

Commonly agreed suite of Authentication Assurance Profiles
Common Profiles accepted and deployed for all target groups

- Making the baseline a real baseline, and Cappuccino a common occurrence
- Align assurance between the generic e-Infrastructures to permit use to flow
- Stronger assurance for access to biomedical and human-related data

Everything meshed together … look for your favourite loop …



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

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

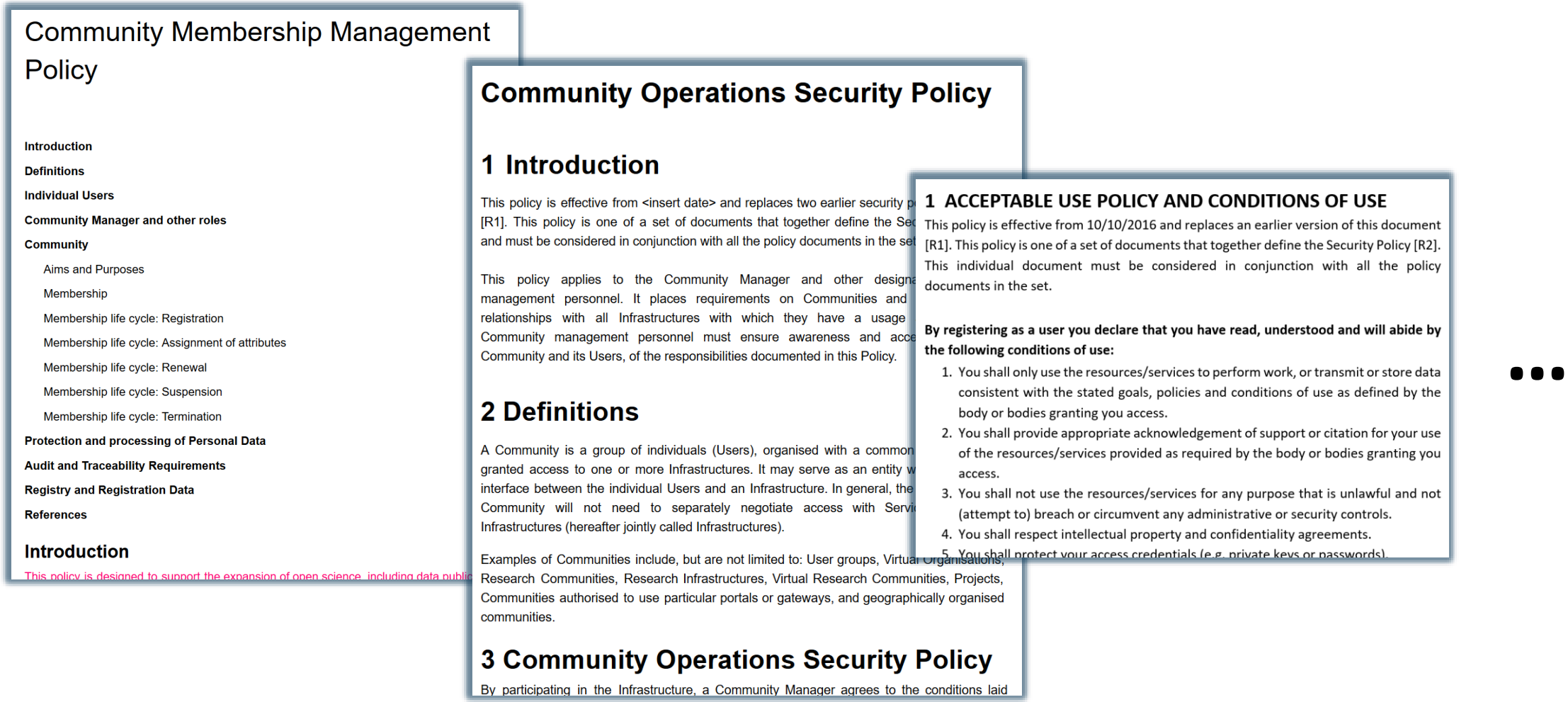
User Responsibilities

- 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

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.

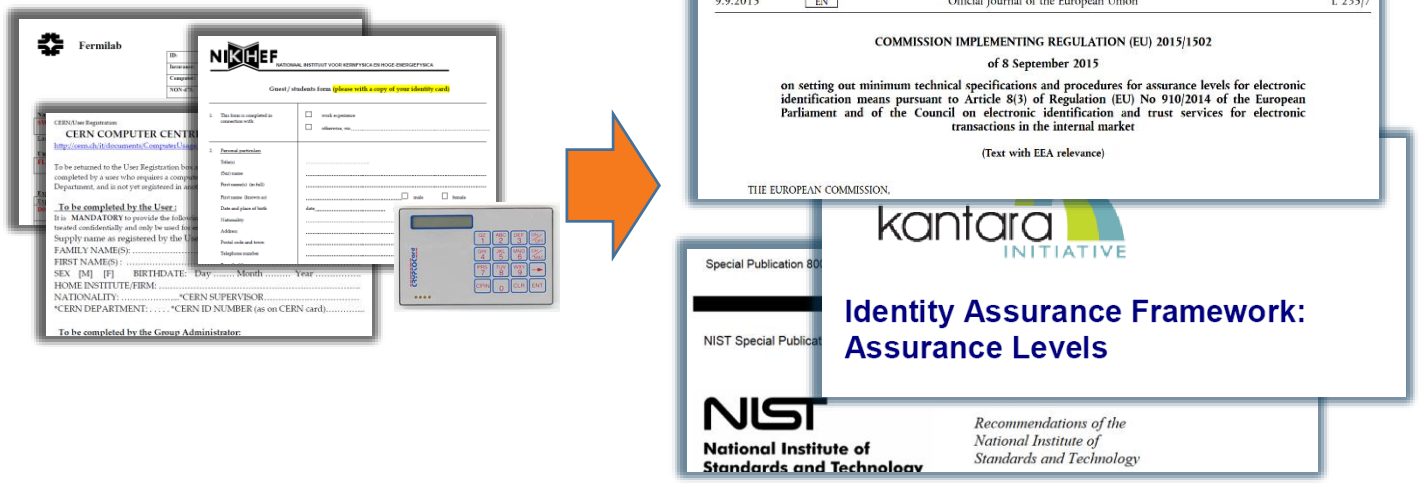
By registering as a user you declare that you have read, understood and will abide by the following conditions of use:

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

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

As a result, in R&E federation there was in practice hardly any documented and agreed assurance level

Beyond uncontrolled identifiers:

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

Differentiated assurance from an 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

Minimal 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

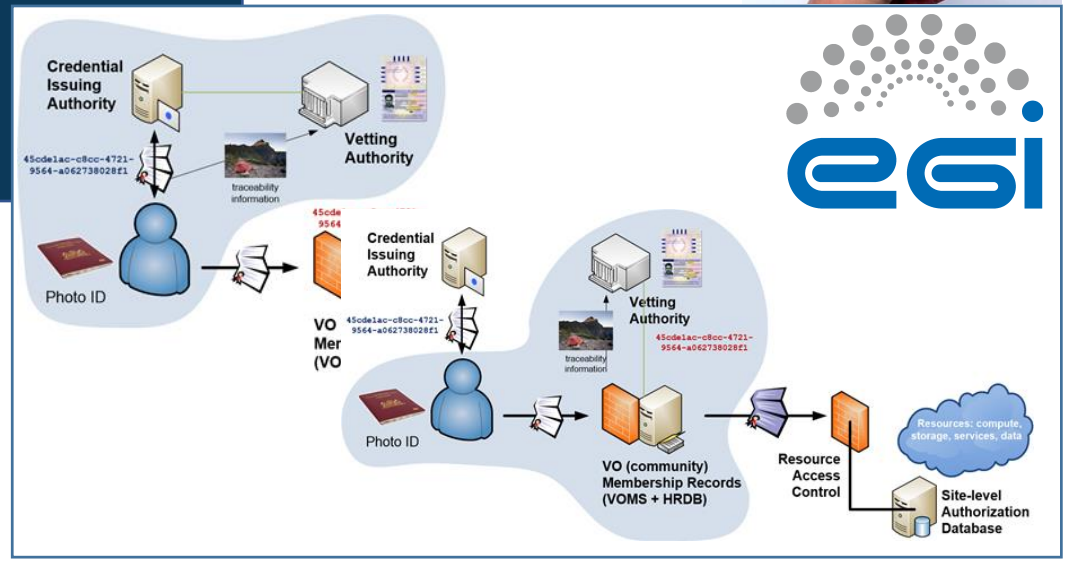
Slice includes:

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

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

Using Assurance in practice: mixing your favourite drink

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/collabative assurance by identifier source and vetting attributes
See also the JRA1.1A Guidelines

see also http://igtf.net/ap/loa and https://www.iana.org/assignments/loa-profiles

Engagement and global alignment

Use **pre-existing groups and communities** to develop policies and harmonise practices and thus **avoid each infrastructure becoming yet another island**

Develop

Through

- *WISE and SCI*
- *REFEDS*
- *IGTF*
- *(FIM4R)*
- *… and all willing policy & CSIRT groups*

work with us
by collaborating in these groups

Adopt

In your Infrastructure, IdP, and Federation

- *Persistent, non-reassigned identifiers*
- *Incident Response capabilities & Sirtfi NG*
- *Protected personal data sharing*
- *Snctfi conformant policy models*
- *Self-assessment and peer review methods*

help collaboration progress
by adopting results

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941 (AARC2).