AARC

Authentication and Authorisation for Research and Collaboration

WP3: Policy and Best Practice Harmonisation

addressing the research communities' requirements

David Groep

NA3 Activity Coordinator

Nikhef

AARC EC Review

27-28 June, 2017

Brussels

Agenda

- **Structure and administrative matters**
  - Team – tasks, task leaders, and partners
  - Resources – budget and effort utilisation
- **Objectives**
- **Achievements**
  - Differentiating Assurance Profiles for Research with Distinct Risk Levels
  - Trusted Security Incident Response for Federations
  - Sustainable Services: Models and Mechanisms
  - Enabling Infrastructures to Collaborate by Permitting Sharing of User Data
  - Building Agreements on Policy in a Scalable Fashion
- **Conclusions**

Activity Structure

Activity Lead	T1 Assurance Profiles	T2 Incident Response Trust	T3 Service Models & Sustainability	T4 Scalable Policy Mechanisms	T5 Accounting and Data Processing
					
David Groep Nikhef (FOM)	**Mikael Linden** CSC	**Hannah Short** CERN	**Peter Gietz** DAASI GmbH	**David Kelsey** STFC-RAL	**Uros Stevanovic** KIT

Partners

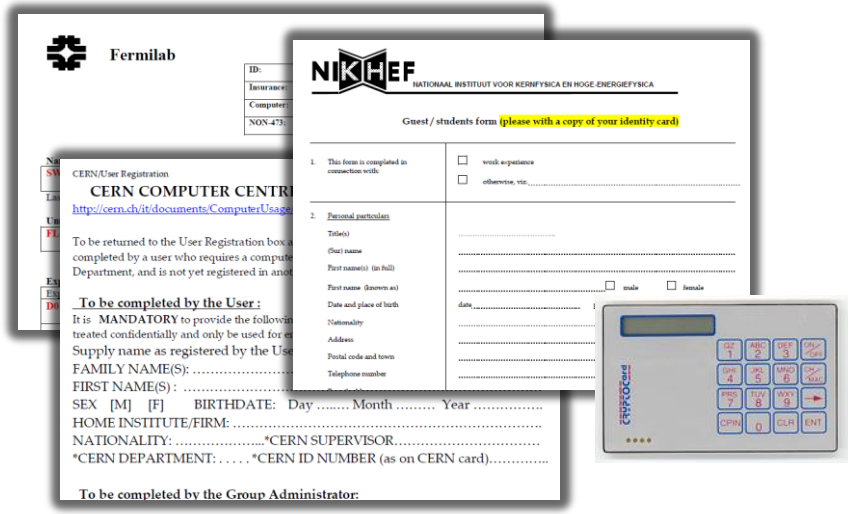
Nikhef
CSC – TIETEEN TIETOTEKNIIKAN KESKUS
DFN Deutsches Forschungsnetz
Science & Technology Facilities Council
CERN
DAASI International
Renater
grnet Networking Research and Education
LIBER
SURF SARA
KIT Karlsruhe Institute of Technology

Policy and best practice activity high-level objectives

- **Provide an assurance profile (LoA) framework** meeting the requirements of the resource providers (RIs and EIs) that is feasible to achieve by the identity providers in eduGAIN
- Identify a (distributed) approach to **handling security incidents** in a federated environment
- Investigate terms of for **delivering services – recommendations** and **sustainability models**
- Specify **scalable policy negotiation mechanisms** between identity providers, attribute providers and service providers to facilitate access to resource providers
- Develop guidelines to facilitate the **exchange of accounting and usage data** **

*** as defined in the work plan section 3.1 – was accidentally not reiterated in the NA3 WP objectives table*

Policy and Best Practices Harmonisation



Task 1

Development of best practices for Levels of Assurance

Assurance Profiles and 'differentiated' levels of assurance

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:

Special Publication 800

NIST Special Publication

National Standard

1. The accounts in the Home Organisations must each belong to a known individual
2. Persistent user identifiers (i.e., no reassign of user identifiers)
3. Documented identity vetting procedures (not necessarily face-to-face)
4. Password authentication (with some good practices)
5. Departing user's eduPersonAffiliation must change promptly
6. Self-assessment (supported with specific guidelines)

some of this seems obvious to any relying service provider, but
... since it was not the driving use case for eduGAIN, none of the above is currently present
... but the AARC joint voice gives critical mass for development at the IdPs!

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 there was in practice hardly any documented and agreed assurance level

Last year:
***baseline* assurance for research use cases**

Differentiated assurance from an Infrastructure viewpoint

‘low-risk’ use cases

few unalienable expectations by research and collaborative services

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

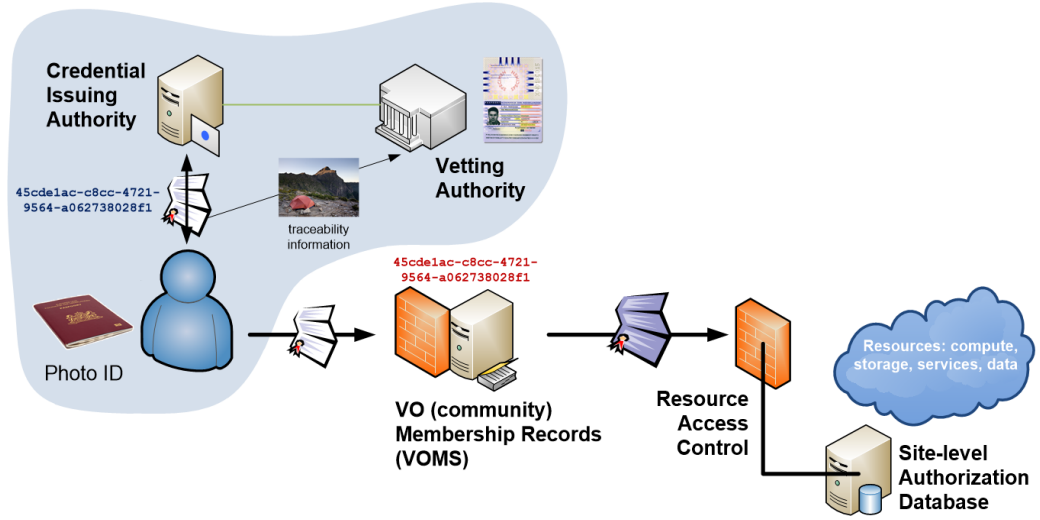
access to data of real people, where positive ID of researchers and 2-factor authentication is needed

Slice includes:

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

An example from EGI: beyond a single baseline with *differentiated assurance*?

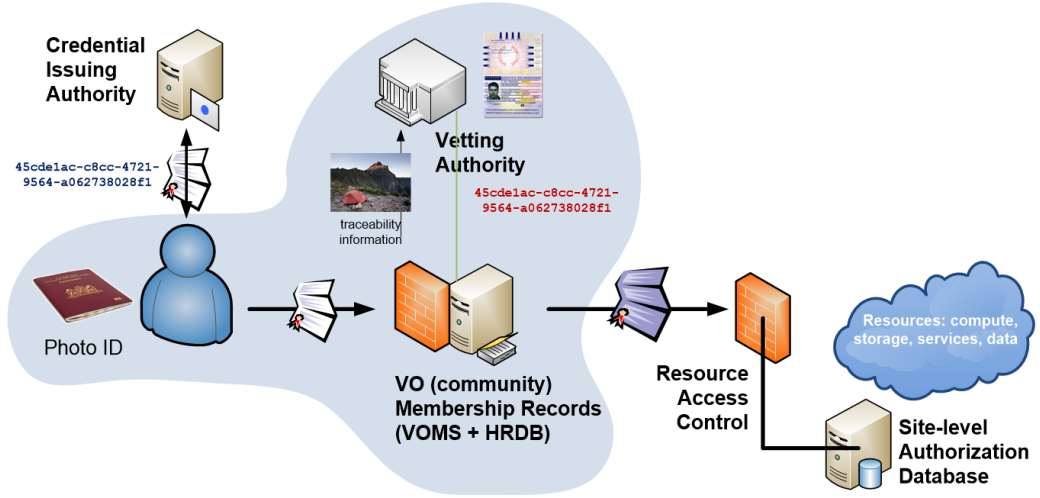
e-Infra example



- managed identity information
- real names, unique identifier
- user-level traceability through the IdP
- managed credential expiration or revocation

IGTF 'Birch' traditional assurance from IdP

Limited vetting requirements on community



- unique identifier based on some process
- not necessarily face-to-face
- credential expiration set at issuance only

IGTF 'Dogwood' identifier-only assurance from IdP

Traceability requirements added on community

https://documents.egi.eu/document/2930

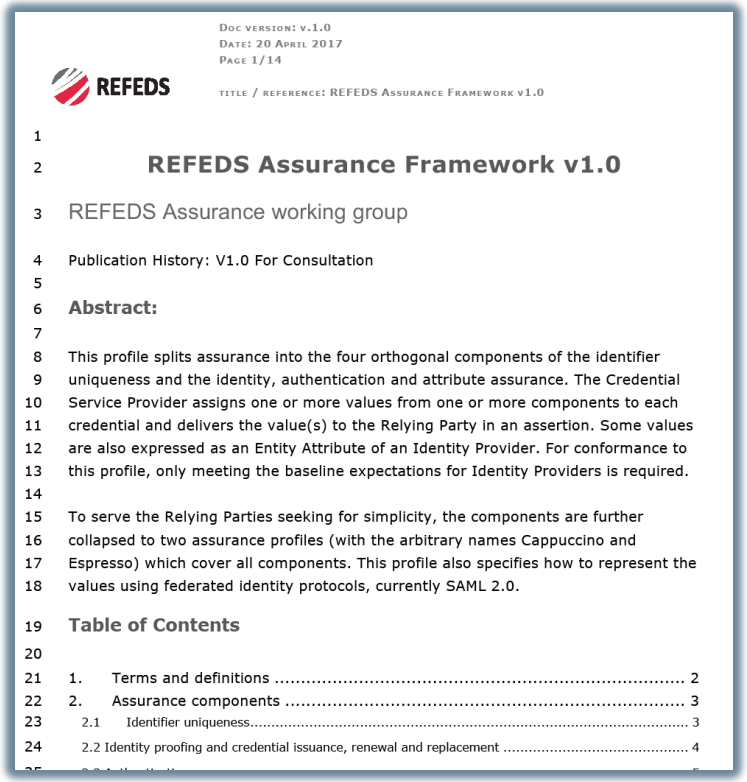
Gaining global adoption: REFEDS Assurance Framework

Why a REFEDS process?

- open forum – *AARC does not have all stakeholders inside*
- international forum – *a Europe-only approach not helpful*
- link to identity federations –
  adoption needs IdP to act and federations to communicate
- re-enforces complementary work – *on the REFEDS MFA profile*

Expression and technical adoption

- leads to new eduGAIN *metadata* and new *attributes* for IdPs
- Definite 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

Facilitate evaluation and peer review by kick-starting a self-assessment tool

Differentiated Assurance Profile – in eduGAIN, REFEDS, and beyond

Specific definitive guidance to IdPs and federations

- **Uniqueness** at least ePUID or ePTID/NameID
- **ID proofing**: 'local enterprise', 'assumed' (Kantara LoA2, IGTF BIRCH, eIDAS low), or 'verified (LoA3, eIDAS substantial)
- **Authenticator**: follow REFEDS MFA 'good-entropy' or 'multi-factor'
- **Freshness**: better than 1 month

Any and all assurance profiles
organisational-level authority, also used locally for 'real work', good security practices

Logical grouping and profiles for the Infrastructures

Value	Cappuccino	Espresso
$PREFIX$/ID/unique	X	X
$PREFIX$/ID/no-eppn-reassign		
$PREFIX$/ID/eppn-reassign-1yr		
$PREFIX$/IAP/local-enterprise	X	X
$PREFIX$/IAP/assumed	X	X
$PREFIX$/IAP/verified		X
$PREFIX$/AAP/good-entropy	X	
$PREFIX$/AAP/multi-factor		X
$PREFIX$/ATP/ePA-1m	X	X

… and simplicity for all – mandatory expression of profiles

https://wiki.refeds.org/display/CON/Consultation%3A+REFEDS+Assurance+Framework

Assurance with global impact
– LIGO Gravitational Waves Observatory response (REFEDS list, May 16th)

Re: [refeds] Consultation: REFEDS Assurance Framework • warren.anderson 18:30

From warren.anderson <warren.anderson@ligo.org>

Reply | Reply List | Forward | Redirect

Subject **Re: [refeds] Consultation: REFEDS Assurance Framework**

To refeds@lists.refeds.org

Dear All,

These profiles address some substantial issues with assurance currently experienced by LIGO and similar research VOs. LIGO believes that it will be a relatively straightforward process to have it's IdP satisfy Cappuccino requirements. In conjunction with Jim's proposal to accept Cappuccino for CILogon Silver, this will address a longstanding issue with LIGO using European Grid Infrastructure resources which has traditionally been an issue.

I endorse these profiles and look forward to their adoption.

Cheers,
Warren

+==========[WARRE
| LIGO Scientist, IAM Ma
| PO Box 413, Milwaukee,
+==========

but can struggle to meet the complete requirements at any given level. The REFEDS Assurance Framework and assurance profiles intend to meet known use-cases in a pragmatic and tailored way.

With thanks to AARC for supporting man-power to create this proposal.

Best wishes

Nicole

Main achievements in assurance profile development

Infrastructure interviews and FIM4R analysis	→	Baseline assurance requirements aligned with REFEDS R&S + Sirtfi
Analysis of assurance mechanisms IETF VoT and SP800-63v3 – balanced to relying party needs	→	Proposed Assurance *Profiles*, not *levels*, aligned with community needs
IdPs and federations need specific implementation guidance	→	Decomposition of assurance in 4 independently assessable components
Relying parties need actionable assertions	→	Profiles linked to concrete cases: baseline (IGTF identifier-only), 'cappuccino' (e-Infrastructures, IGTF Birch), and 'espresso' (biological, medical use cases)

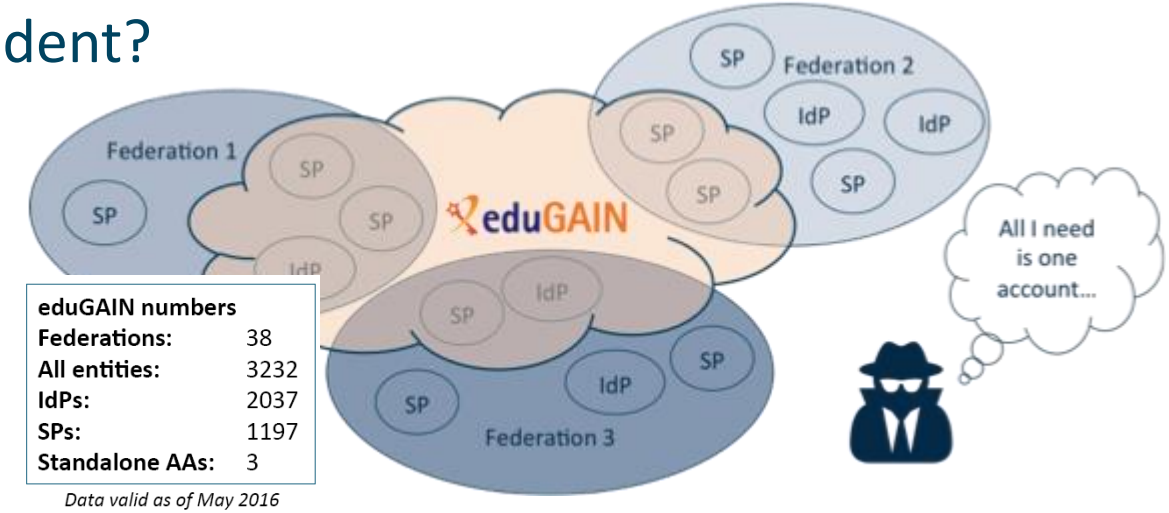
Policy and Best Practices Harmonisation

Task 2

Security Incident Response

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



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

Data valid as of May 2016

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

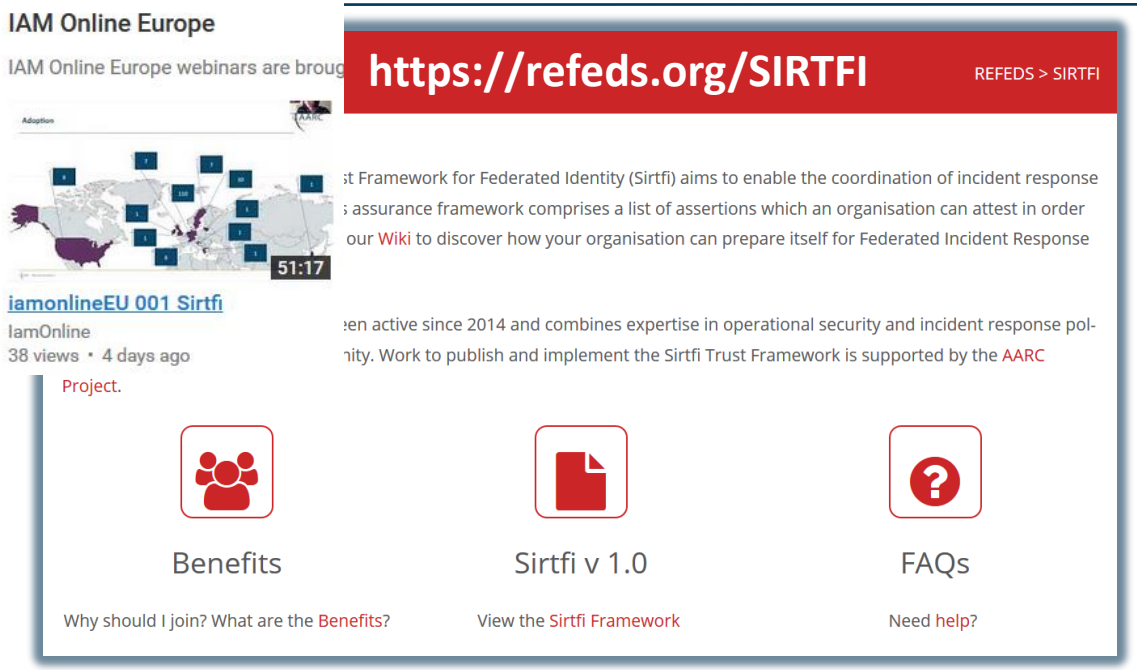
Traceability

- 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

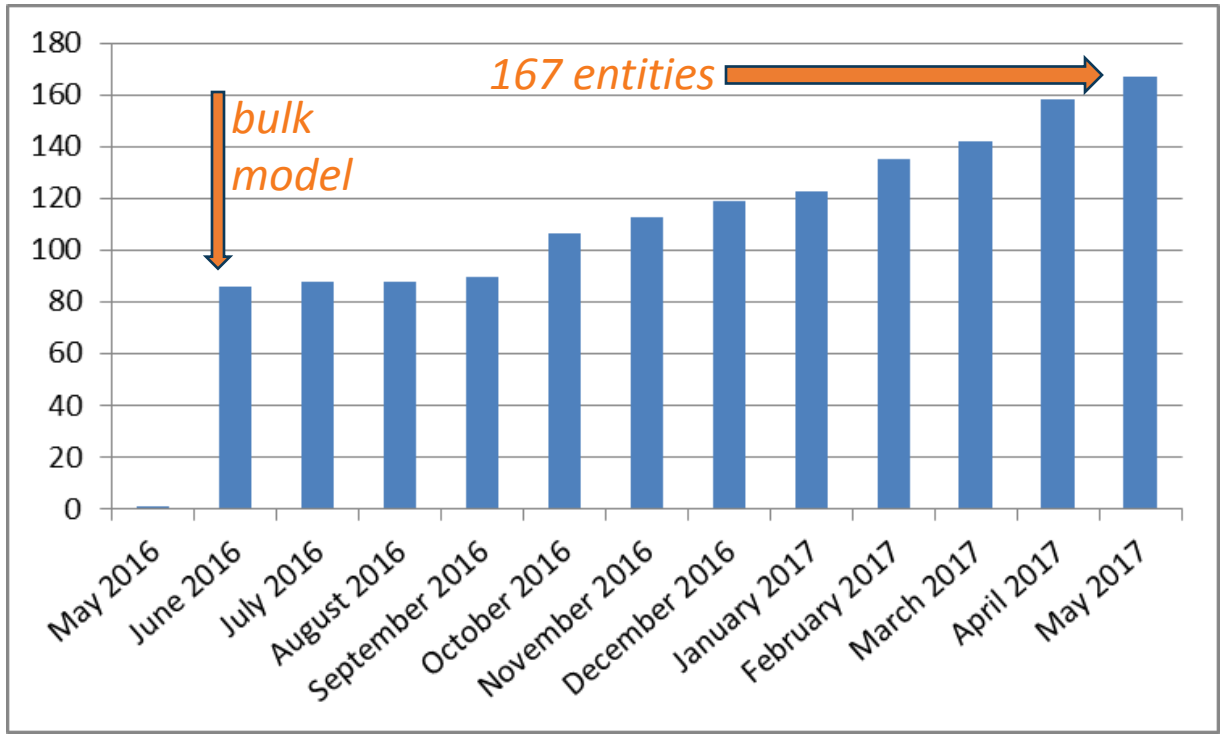
Sirtfi adoption in eduGAIN



- Adds security contact meta-data in eduGAIN
- namespace for Sirtfi Assurance at IANA
- with R&S specification:
  meets **baseline assurance requirements** and IGTF “assured identifier trust”

Promotional activities successful

- REFEDS, Internet2 TechX, ISGC Taipei, TNC, TF-CSIRT, FIM4R, Kantara webinars, …
- Used in CyberOps role play exercises

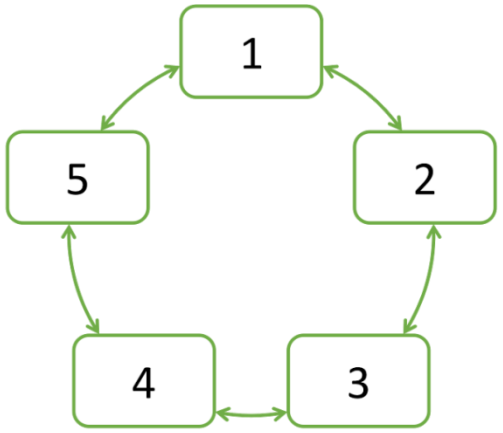


Compare: 376 REFEDS R&S after 3+ yrs

Beyond Sirtfi: streamlining the response process

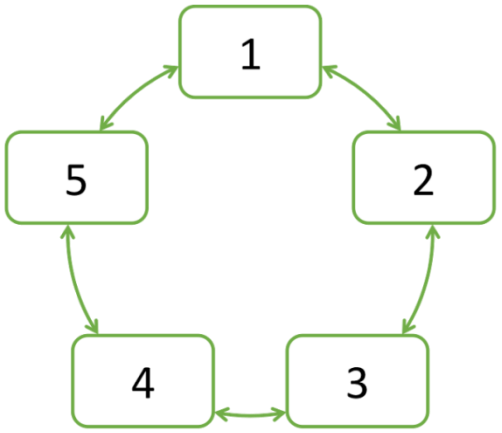
trust relationships: allow information to flow rapidly to all that need to know

Infrastructure sharing model: PRACE, XSEDE, …



During Incident Response

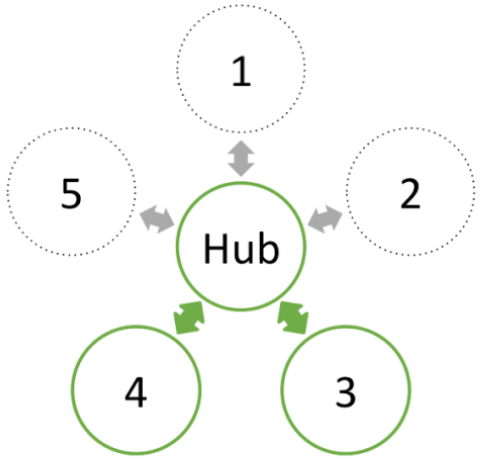
Information shared between all participants



Post-Incident-Report Sharing

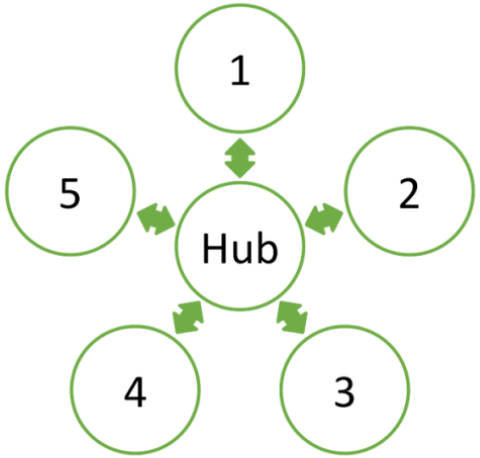
Information shared between all participants

Infrastructure sharing model: EGI, WLCG, …



During Incident Response

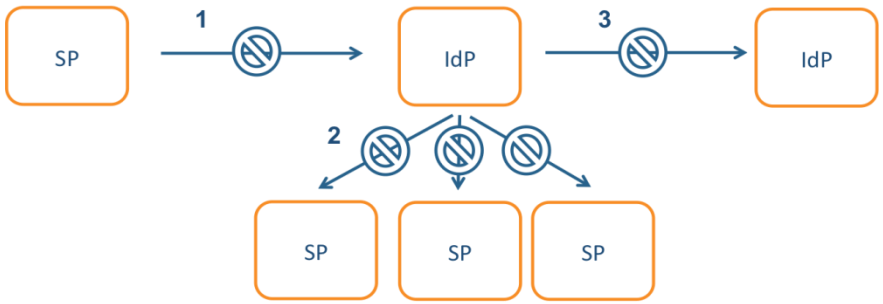
Information shared between affected participants



Post-Incident-Report Sharing

Information shared between all participants

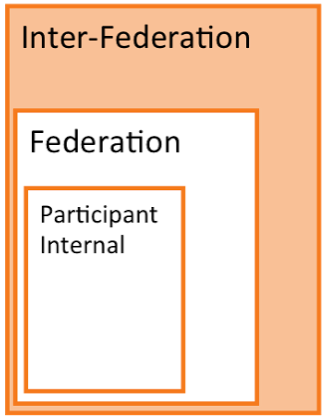
Incident response process evolution in federations



Incident Response Communication, communication blocks

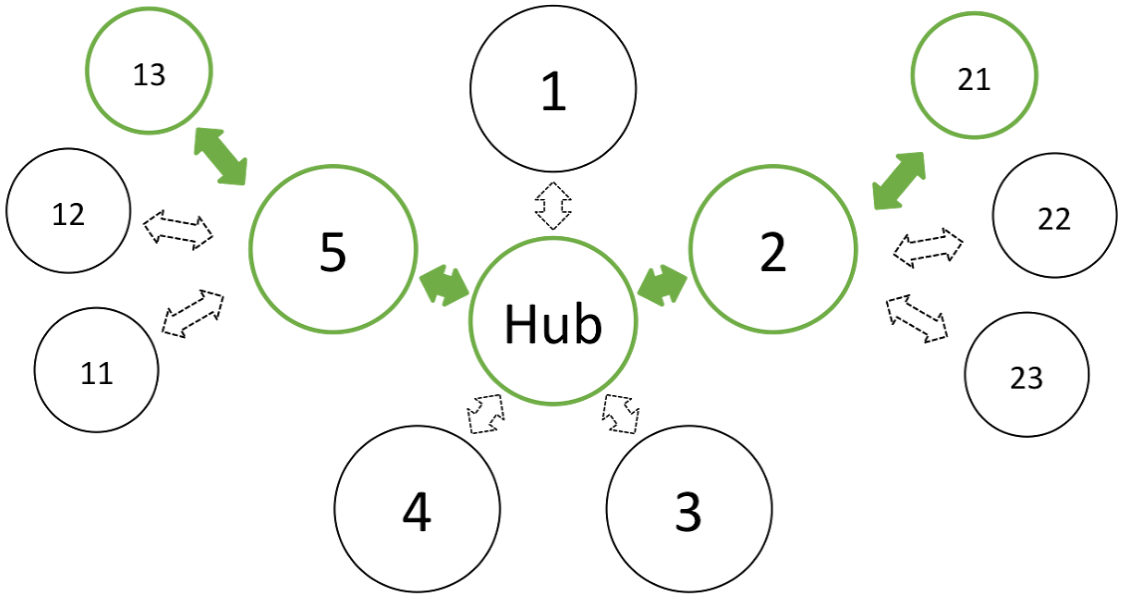
Challenges

- IdP appears outside the service' security mandate
- Lack of contact, or lack of trust in IdP which is an unknown party
- IdP fails to inform other affected SPs, for fear of leaking data or reputation
- No established channels of communication



Proposed solutions

- Stronger role for federation operators, as they are known to both SPs and IdPs
- Add hub capability centrally (@ eduGAIN)



Inter-Federation Incident Response Communication

Addressing Security Incidents – a Joint Effort

31-12-2016
Deliverable DNA3.2: DNA3.2 - Security Incident Response Procedure

AARC

Each federation should

- provide a federation security **contact point** which is well-known
- appoint a ***Security Coordinator*** when notified about a potential incident and help out

The eduGAIN inter-federation should

- **coordinate** the incident response process and communications **until it is resolved**
- produce and **share a report** of the incident **with all Sirtfi-compliant organisations**

Template procedure – in DNA3.2:

- Closely co-developed with GEANT "The Project" and eduGAIN
- the new eduGAIN support desk **will take on the coordination role** and act as last resort

✓

Infrastructures

- Appear as a single SP towards the federations (its SP-IdP Proxy)
- Leverage existing global trust relationships and detection capabilities and intelligence
- Now **also** interact with their federation partners

Main achievements in federated incident response

Sirtfi defined and achieved global consensus	→	Federation participants can identify trustworthy peers and self-assert compliance
Entity category defined in REFEDS	→	eduGAIN now carries contact data alongside R&S used in scalable access control
Multiple deployment models: both per-entity and per federation	→	> 167 IdPs in eduGAIN are Sirtfi'd today
Incident response procedure agreed	→	Prevent spreading of incidents and increase confidence within R&E federation
eduGAIN support pilot takes on security coordination	→	Information sharing between affected parties improved, reducing misunderstanding

Task 3

Recommendation for sustainable services and models

Recommendations for Research and e-Infrastructures to Build Sustainable Services

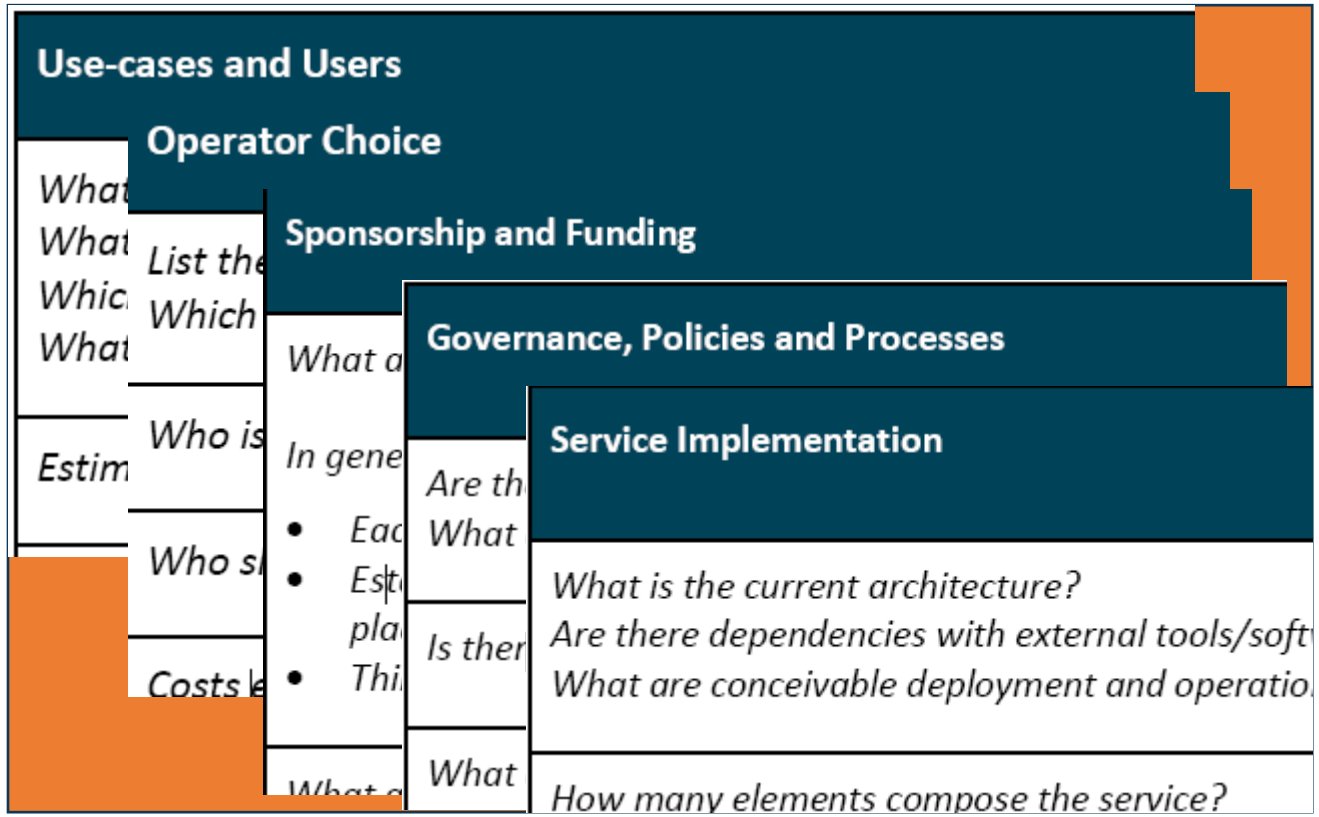
'Investigate terms of (AAI) usage for delivering services'

> Making services sustainable – beyond funding cycles and across domains
> *Guidelines, templates, and how to apply them to the AARC pilots*

> Mitigating heterogeneity in Infrastructure and Federation policies and practices
> *Recommendations for future federation development in line with FIM4R*

> Identity providers 'of last resort', by the Infrastructure or the community
> *Strategies and risks in staring a guest identity provider*

Promoting sustainability through recommended templates



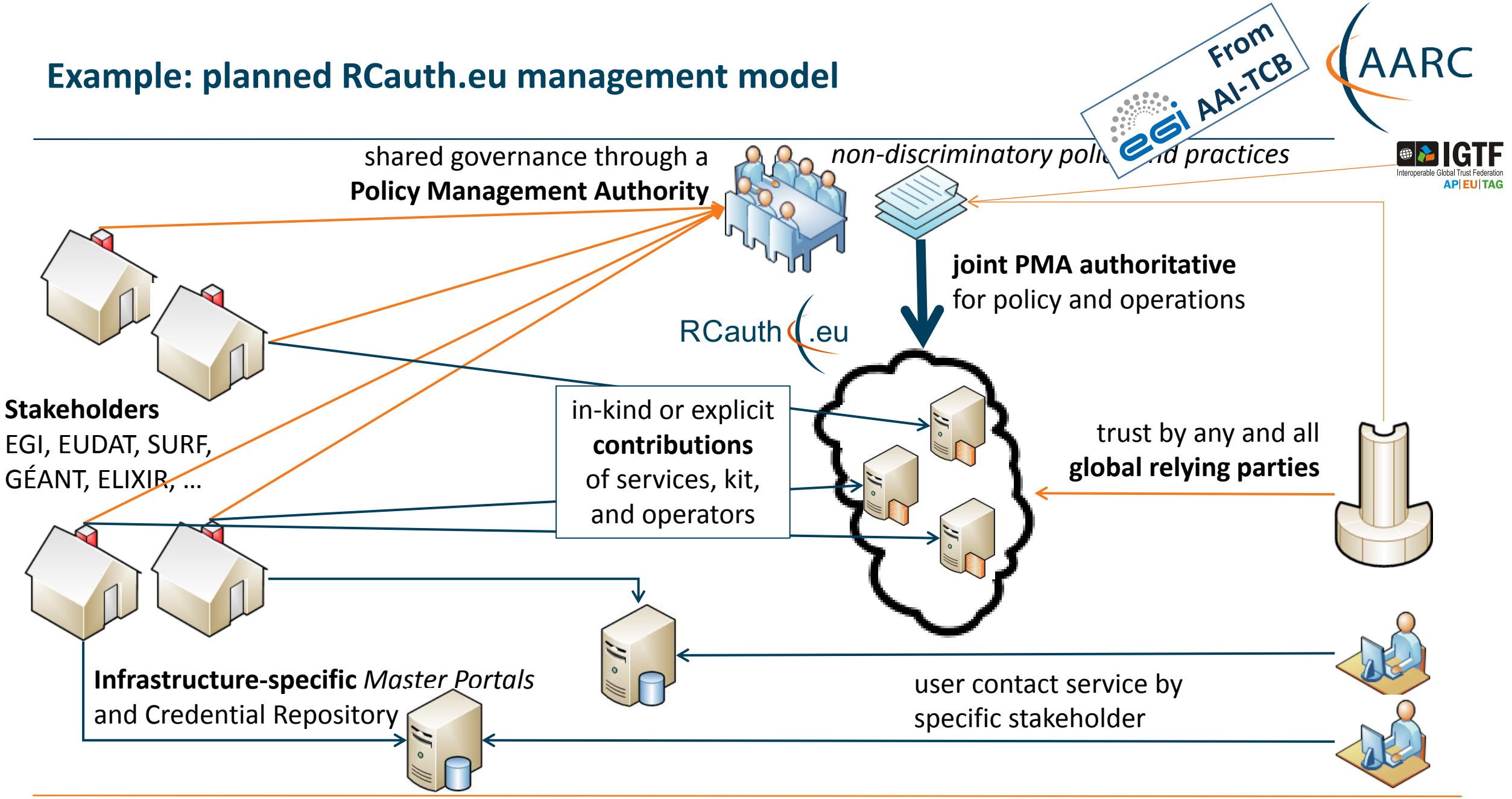
Common analysis

- Initial focus usually on 'use cases' and 'service implementation'
  this misses the long-term sustainability
- Only few pilots have yet addressed full set
- Template approach encourages focus ☺

AARC SA1 Pilots with a sustainability plan

- RCauth.eu*
- DARIAH Guest IdP
- Social IDs to SAML
- WaTTS

Example: planned RCauth.eu management model



Planned RCauth.eu: operator distribution and support plans

From AAI-TCB

Beyond just the 'Nikhef Best Effort™' service

- what is 'the service' in this context: Delegation Service & WAYF
- can be anywhere between a few kEur to well over 100+kEur cost per year …

Recuperation model

- Credential Management services from other (non-RCauth) sources, per-Infrastructure
- Delegation Service and RCauth.eu: free at point of use
- funded via in-kind contributions by the major e-Infrastructures
- distributed H/A setup, leveraging existing capabilities and some additional person effort

EOSC Hub Consortium picked middle ground

- contribute effort and some hardware resources to the joint pan-European pool
- help steer the development through joint, independent, management body (PMA)
- partners with existing security operations expertise: GRNET, STFC, FZJ + SURF/Nikhef

Collect Recommendations in one place – for Infrastructures & Federations

For Research and generic e-Infrastructures

- Following the AARC BluePrint and the intent of the FIM4R group – make it easier for users
- Support GEANT DP CoCo when possible + R&S – ease the liability on IdPs to give you data
- Joint Sirtfi – and help the R&E security stance
- Apply homogeneous policy mapping frameworks inside your Infrastructure: '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

Models for ‘guest’ IdPs – serving users beyond academia

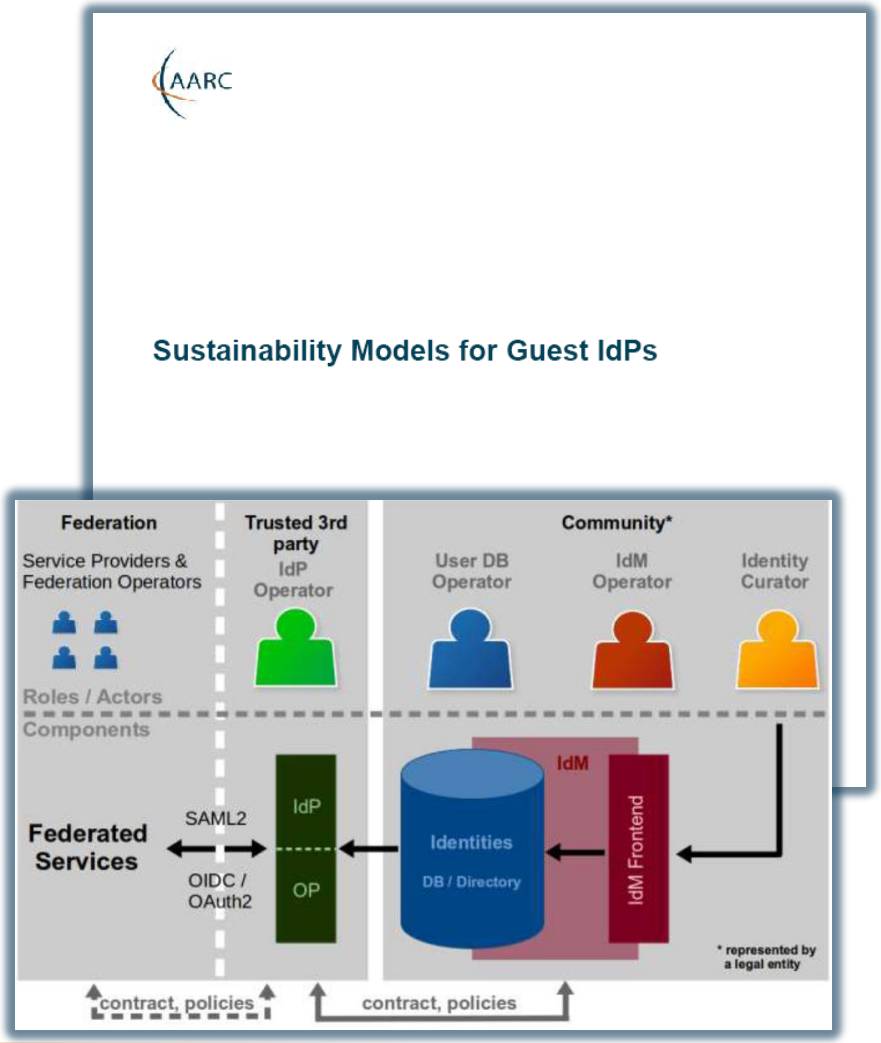
Guest IdPs are critical to almost all collaboration use cases

➢ *Collaboration does not end at the door of the university!*

Model study: too often ‘guest’ IdPs have faded – sustainable elements extracted:

- Use established, long-lived, institutional partners
- Ensure funding beyond projects
- Framework needed for ‘non-trivial’ communities

*As collaboration moves to meeting at least **baseline assurance**, cheap-and-cheerful guest IdPs will fail*



https://wiki.geant.org/display/AARC/Sustainability+models+for+Guest+IdPs

Main achievements in sustainability development

Template for sustainability analysis	→	Concrete future plans for SA1 pilot results
RCauth sustainability model	→	Adoption as baseline service by major Research and e-Infrastructures
Recommendations for Infrastructures	→	Better attribute release by federations and increased usability by researchers
Recommendations for federations	→	Increased adoption of R&S and Sirtfi allows research SPs like CERN and EGI to join
Model study for guest IdPs	→	Improve planning and expectations of 'cheap-and-cheerful' project-based IdPs

Policy and Best Practices Harmonisation

Task 4

Development of scalable policy negotiation mechanisms

Getting agreements in a distributed world: scalable policy mechanisms

Group entities to ease agreements with federations

- Aim: improve attribute release by IdPs & Federations
- Entity Category mechanism: ‘R&S’, DP CoCo, Sirtfi, …

Define trust framework for Infrastructures – SPs-to-IdPs

- Framework for Infrastructures to assess back-end SPs
- Permit Gateway to assert entity categories with confidence
- Readiness survey for services evaluated with HNSciCloud PCP

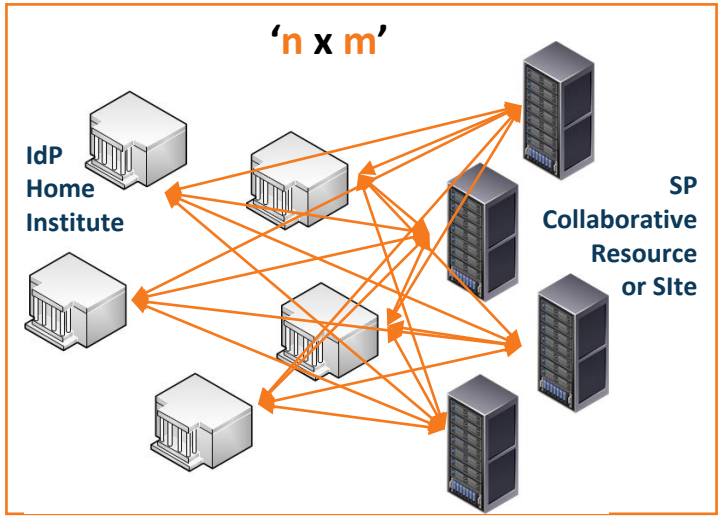
Develop policies models for SP-IdP Proxy – IdPs to SPs

- Model for service providers that ‘hide’ complexity of all R&E
- Through concrete (RCauth.eu) use case & with global review

Collaborations by design have their services distributed

and

- not that many collaborations are a legal entity
- or are not ‘authoritative’ for constituent services



Entity Category adoption – R&S and Sirtfi

eduGAIN 'SAML' Entity Categories Review

- *adoption survey*
- *granularity of categories*
- *traditionally pushed by IdPs, with requirements on SPs, but that is changing!*

'REFEDS R&S**'**, 'DP CoCo',
but also
'CLARIN', 'SWAMID AL1', …

Entity Category Experiment using Sirtfi

- *Sirtfi compliance via ECs*
- *self-assessment facilitates adoption – but does it show in eduGAIN publication?*

Continuous monitoring

GEANT and eduGAIN

- *technical.edugain.org*

Unexpectedly rapid adoption:

- *Sirtfi*: 167 entities / ~1 yr
- *R&S:* 284 → 646 entities/1yr
- ***Both grow together now!***

Thus: time is 'ripe' for EC ☺

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)

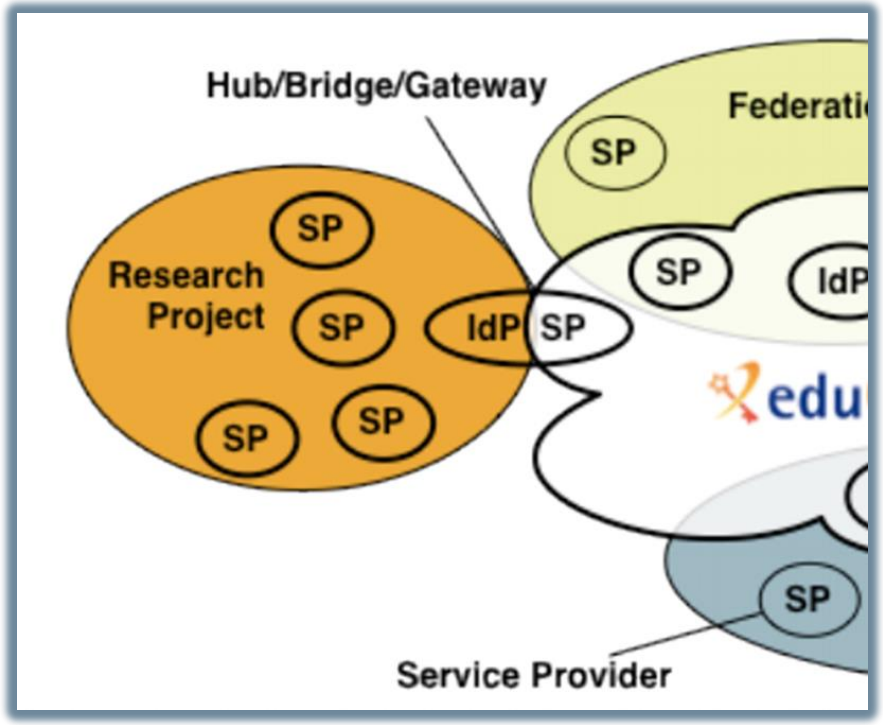
Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp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

- 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, …

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

Model scalable policies for SP-IdP Proxies – the RCauth.eu example

- **How can a SP-IdP proxy leverage federation policies?**
- **What are useful design criteria for a scalable service?**

RCauth.eu

Focus on permitting individual access, engaging both federations and Infrastructures

- Avoid an opt-in model, or a scheme where specific countries can opt-out or block access
- Allow infrastructures explicitly to operate an IdP of last resort, and recognise its qualities

Meet your (target) infrastructure needs

- For cross-infrastructure services, peer review and accreditation significantly helps adoption

Leverage entity categories and assurance profiles

- Don’t ask IdPs to do something special just for your gateway

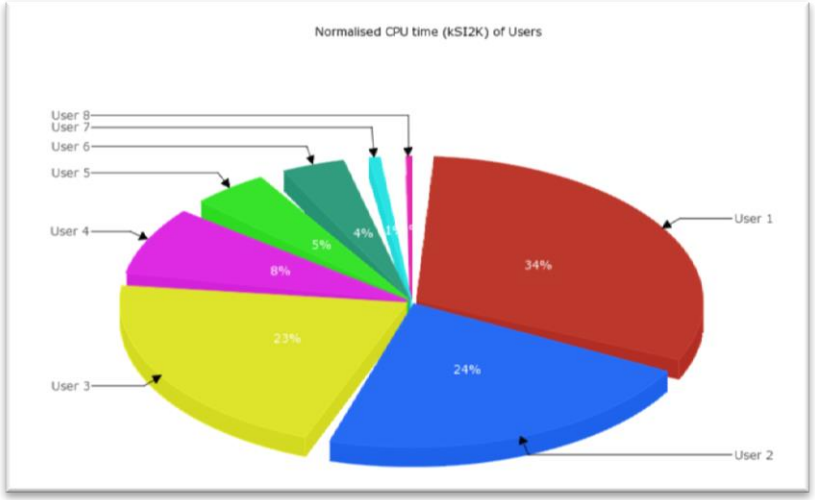
Be ready to deal with a complex, multi-national, and multi-federation reality

- Incidental non-compliance needs to be mitigated in your service – use Sirtfi & eduGAIN support

Main achievements in scalable policy models

Status of Entity Category adoption in eduGAIN	➔	Identifying entities speeds adoption *done very successfully for Sirtfi*
Snctfi policy coherency for Infrastructures	➔	Document endorsed by infrastructure reps will be homed long-term by IGTF (or FIM4R)
RCauth.eu policy reference implementation	➔	Accredited gateway service with global reach enabling federated access to resources in EGI, OSG, XSEDE, ELIXIR, and others
HelixNebula Science Cloud recommendations	➔	Easy checklist to push to new (commercial) providers that we want to be federated

Policy and Best Practices Harmonisation



Task 5

Accounting and the processing of data

Scope of the AARC Accounting and Processing of Data task

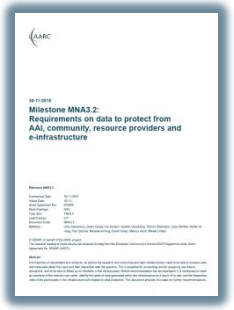
Protection of personal data in research data	User attribute release by federated organisations	Personal data processing in accounting & collaboration
• *patient records* • *survey data collation* • *big data analytics* • *research data combination* **Research Infrastructures** **Institutional Ethical Committees** **ESFRI Cluster Projects**	• *institutional IdP attributes* • *GEANT DP CoCo** • *minimal release in eduGAIN* • *REFEDS Research & Scholarship* **REFEDS, GEANT4** • *community management* **Joint RIs, EIs and AARC work**	• *collection of usage data in RIs and e-Infrastructures* • *correlating resource usage to people and groups* • *collate usage data across countries and continents* • *personal data used for incident response* **AARC "TNA3.5" – this task**

** GEANT Data Protection Code of Conduct – see http://geant3plus.archive.geant.net//uri/dataprotection-code-of-conduct/v1/Pages/default.aspx*

Identified needs and structure – MNA3.2 as basis for recommendations

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


AARC

26-11-2019

Milestone MNA3.2:
Requirements on data to protect from AAI, community, resource providers and e-infrastructure

Milestone MNA3.2

Contractual Date: 30-11-2019
Actual Date: 30-11-2019
Grant Agreement No.: 730941
Work Package: WP3
Task Item: TNA3.2
Lead Beneficiary: GÉANT
Document Code: MNA3.2
Authors: Mario Reale (GÉANT), Dave Kelsey (for Nikos), Stefan Venekotter, Marco Malavolti, Linda Mellor, Adam Lewis, Paul Dekkers, Nicolas Liampotis, David Groep, Marcus Hardt, Mikael Linden

AARC is funded by the EU under grant:
"The research leading to these results has received funding from the European Community's Horizon 2020 Programme under Grant Agreement No. 730941 (AARC)."

Abstract

Federations in stakeholders and citizens, as well as the research and connecting and data infrastructures, need to be able to access data and manipulate data that was put into the system with the purpose. This is essential for connecting and for keeping one's data. Alternatives, and to be able to delete and be included in the infrastructure. Within interoperability, we are attempting to make the data available to the infrastructure, and to be able to delete and be included in the infrastructure. Within interoperability, we are attempting to make the data available to the infrastructure, and to be able to delete and be included in the infrastructure. This document provides the basis for further recommendations, and a first prototype. It is independent of IT-support or data protection. This document provides the basis for further recommendations.

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?

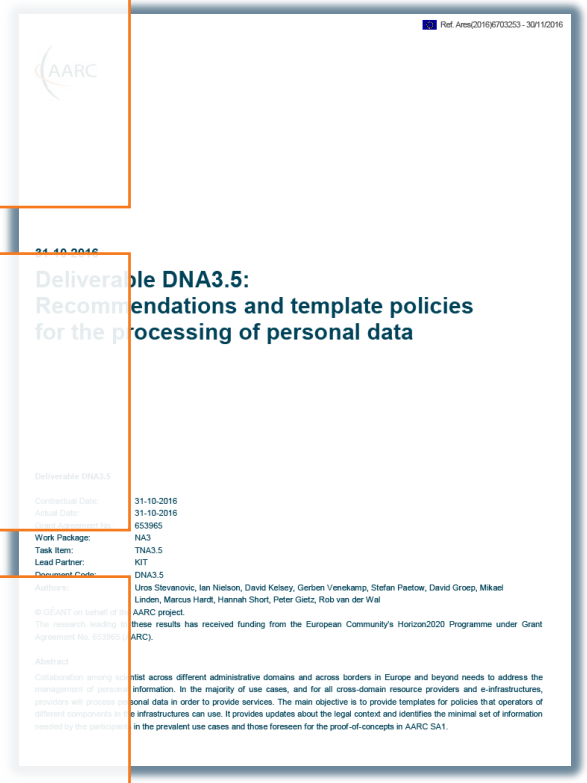
- Global sharing in controlled communities appears attractive
- Uncertainly about requirements (governing body) and timing (> Mar 2018) are not helpful for adoption today … just yet
- Ongoing work: text needs to allow for (community) attribute authorities

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

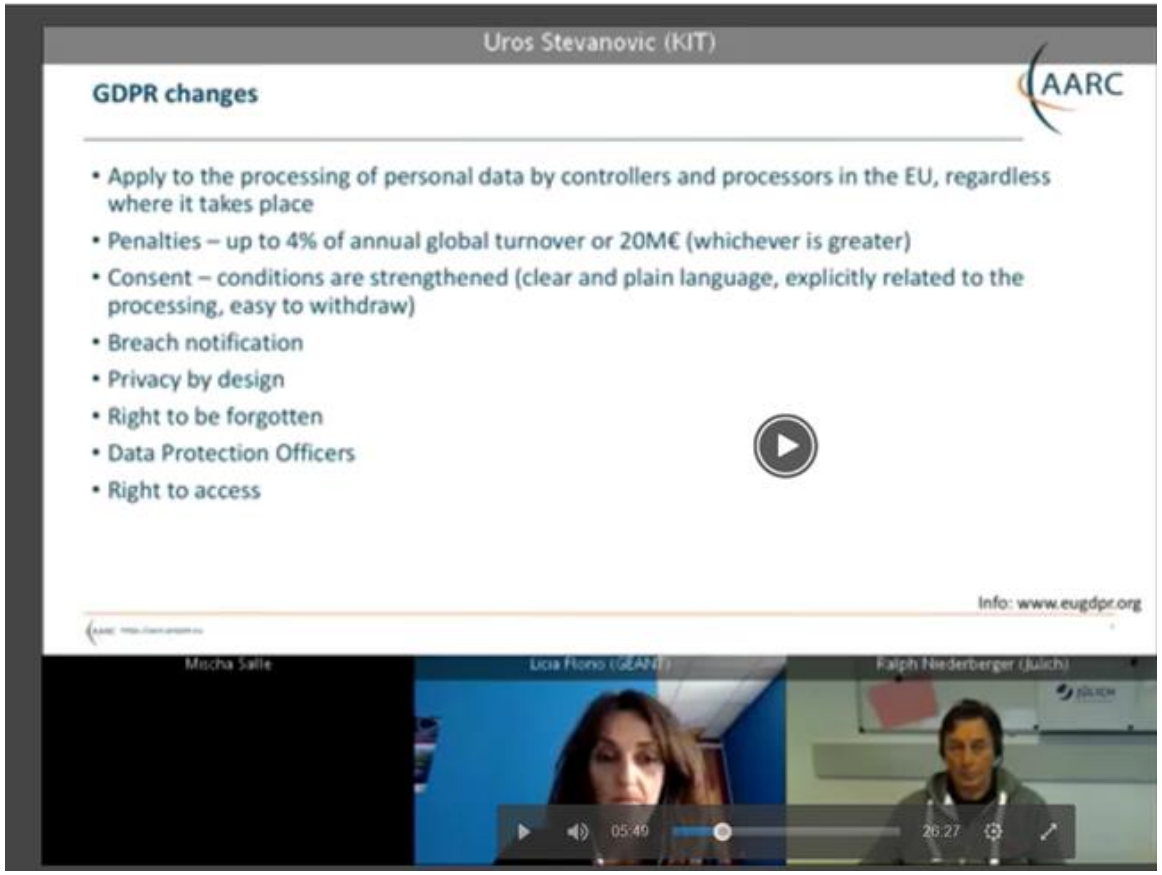
Contractual Date: 31-10-2016
Actual Date: 31-10-2016
Grant Agreement No.: 653965
Work Package: NA3
Task Item: TNA3.5
Lead Partner: KIT
Document Code: DNA3.5
Authors: Uros Stevanovic, Ian Nielson, David Kelsey, Gerben Venekamp, Stefan Paetow, David Groep, Mikael Linden, Marcus Hardt, Hannah Short, Peter Gietz, Rob van der Wal

Abstract

AARC InfoShare on data related to accounting, monitoring and logging

Talk and present the accounting data protection recommendations everywhere!
Especially since most researchers actually don't care about this
(and frankly don't understand the fuss we make about their personal data …)

Uros Stevanovic (KIT), March 2017



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

Main achievements in infrastructure & accounting data protection

Survey of requirements for AAI data protection	➔	Infrastructures collect similar kinds of data, and do not need sensitive personal data for accounting: common guidance is realistic
	➔	Global exchange of this data is essential
Review of GDPR changes	➔	Identified BCR-like model as basis for data processing in Infrastructures
	➔	GDPR-style Codes of Conduct attractive, but uncertainty about need governing body
	➔	No straightforward legal basis exists for scalable global research collaboration ☹

Policy and Best Practices Harmonisation

Pulling it all together

Our Achievements

- Bridged need for specific guidance and actionable assurance with **infrastructure-driven profiles**
- Developed via REFEDS to get **global adoption** and federation acceptance
- **Sirtfi** approved and rapidly implemented: **strong growth** in eduGAIN with already 167 entities
- Practical **process for addressing global incidents**, in close collaboration with eduGAIN Support
- Concrete **recommendations for Infrastructures and Federation** to drive FIM4R and eduGAIN
- Ensure the result will live: **sustainability** templates lead to successful long-lived services
- Snctfi aids **Infrastructures presenting coherent qualities** towards federations with confidence
- Accounting Data Protection recommendations **help Infrastructures provide services jointly**

Primary Open Challenges – for AARC2 and the Community

Snctfi is 'just a framework' – now apply it to interoperate

- Provide best practices and give recommendations to infrastructures on how to address responsibilities, security, and trust mechanisms to enable interoperation
- 'Cross-silo' trust between Research Infrastructures, and with generic e-Infrastructures
- Encourage joint trust in acceptable use policies, attribute management, and identity assurance

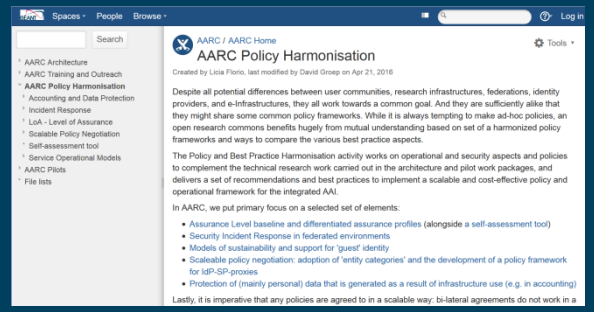
Policy baselines – beyond mapping to harmonisation

- Extend the Assurance Baseline and differentiated Profiles to other areas: traceability and logging, differentiates views on accounting and user data, evolution of the GDPR,
- Create – through the AARC2 Competence Centre – a global consensus: IGTF, FIM4R, &c

Security Incident Response

- Communities and research infrastructures hold the key to mitigating user-centric incidents: involve attribute authorities and involve SP-IdP Proxies in the mitigation process
- Promote organisational & individual trust groups within the eduGAIN constituency: WISE, eduGAIN
- Standards for sharing incident response notifications and reports

https://aarc-project.eu/workpackages/policy-harmonisation/
https://wiki.geant.org/display/AARC/AARC+Policy+Harmonisation



Thanks to all P&BP collaborators from CSC, CERN, DAASI, RAL/STFC, KIT, GRNET, DFN, Renater, SURFsara, LIBER, and Nikhef, and to Jim Basney of NCSA, CTSC and CILogon

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).