



Authentication and Authorisation for Research and Collaboration

Bringing Harmonized Policy and Best Practice *from the present to the future*

David Groep
Activity Coordinator

Nikhef



TNC17

May 31, 2017

Linz, AT

From the present ...

Assurance

'low-risk'

few unalienable expectations by research and collaborative services

access to common components and data sets that do not hold sensitive personal data

protection of sensitive resources

access to data where positive researchers authentication

Value	Cappuccino	Espresso
\$PREFIX/ID/no-epgn-reassign		
\$PREFIX/ID/epgn-reassign-1yr		
\$PREFIX/ID/local-enterprise	X	X
\$PREFIX/ID/assumed	X	X
\$PREFIX/ID/verified		X
\$PREFIX/AD/good-entropy	X	
\$PREFIX/AD/multi-factor		X
\$PREFIX/ATP/eduA-1m	X	X

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

SIRTFI

Security Incident Response Trust Framework for Federated Identity

Operational Security

Internal

Inter-Federation Incident Response Communication

167 entities

bulk model

6 steps to make life easier for Service Providers

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

GDPR-style Code of Conduct – a new way?

- Global sharing in controlled communities appears attractive
- Uncertainty 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 mechanisms and time to do this

BCR-inspired model ("Binding Corporate Rules"-like)

- Note that this is a BCR model
- Collaboration
- "Say what you do" is our real best

Global sharing of user accounting data

Scalable Trust

Hub/Bridge/Gateway

Service Provider

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 a wider context.

Sustainable Recommendations

1. R&E federations should promote the adoption of eduPersonInquireID
2. R&E federations should promote the adoption of eduPersonInquireID
3. R&E federations should promote the adoption of eduPersonInquireID
4. R&E federations should promote the adoption of eduPersonInquireID
5. Be cautious in filtering eduGAIN metadata
6. Build the eduGAIN support help desk (in pilot)

www.aarc-project.eu

Why do we do it (and are maybe a bit pushy about it ...)

- ✓ Provide an assurance framework meeting that makes federated identities more valuable to large research and e-Infrastructures yet is feasible to implement by most home IdPs
- ✓ Expose existing security capabilities in federated organisations, and organise the flow of information through Sirtfi contact details and a tiered coordination function
- ✓ Recommendations for federations to make life easier for collaboration, and better models for sustainability for 'guest' identities and services in infrastructures
- ✓ Make it easier for communities to use federation by organizing in groups, and support the SP-IdP Proxies build a consistent view of their services with the Snctfi scheme
- ✓ Propose practical models to allow infrastructures to exchange per-user accounting data, globally and across organisations that limits compliance risks for personal data protection

Mechanisms for ensuring policies serve the community



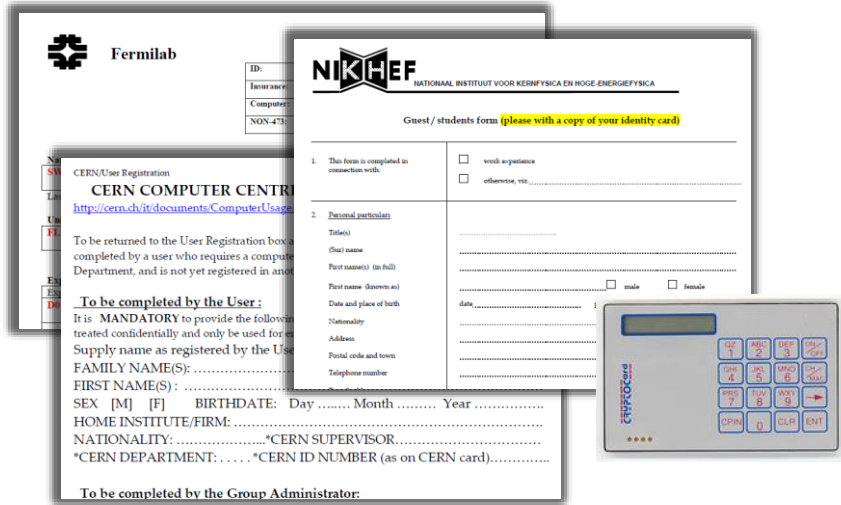
Use pre-existing groups and communities to develop policies and harmonise practices and thus avoid AARC becoming - yet another - island



HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)



Policy and Best Practices Harmonisation



Development of best practices for Assurance Profiles

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,



**Identity Assurance Framework:
Assurance Levels**

Special Publication 800-
██████████
NIST Special Publication



National Institute of Standards and Technology

Electronic Authentication
Guideline
*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

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



Value	Cappuccino	Espresso
\$PREFIX\$/ID/unique	X	X
\$PREFIX\$/ID/no-eppn-reassign		
\$PREFIX\$/ID/eppn-reassign-lyr		
\$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

See Mikael Linden's presentation to the REFEDS Monday meeting
<https://refeds.org/meetings/35th-meeting-may-2017>

Policy and Best Practices Harmonisation

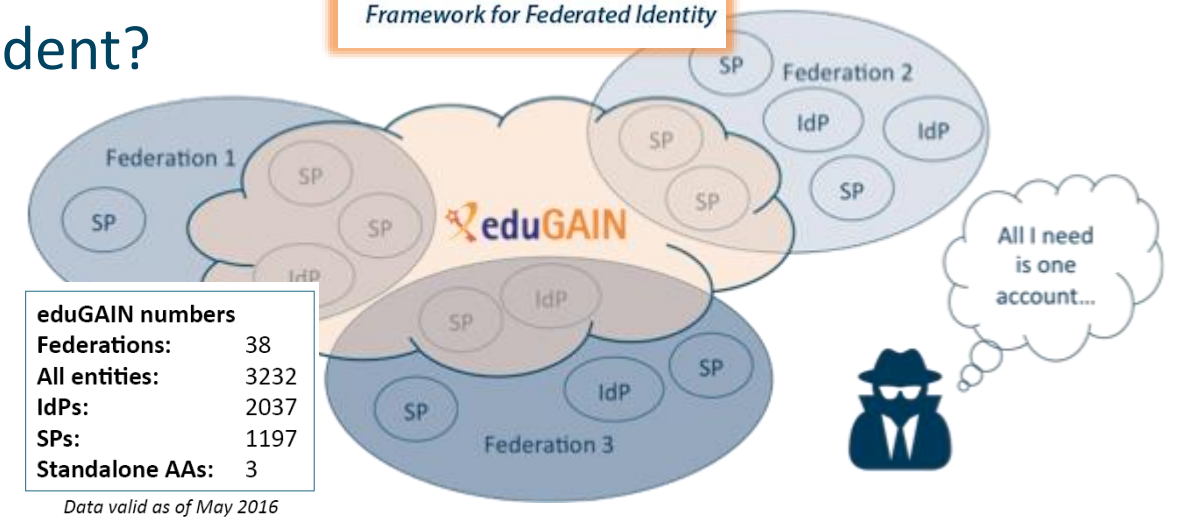


Security Incident Response

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?



Security Incident Response Trust Framework for Federated Identity

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

Sirtfi adoption in eduGAIN

IAM Online Europe

IAM Online Europe webinars are brought to you by AARC



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

You may – or should – have heard of this:

REFEDS Internet2 TechX, ISGC Taipei, TNC, Tara webinars, ...
 e play exercises

iamonlineEU 001 Sirtfi

IamOnline
 38 views · 4 days ago

st Framework for Federat
 s assurance framework c
 our Wiki to discover how

een active since 2014 and
 nity. Work to publish and

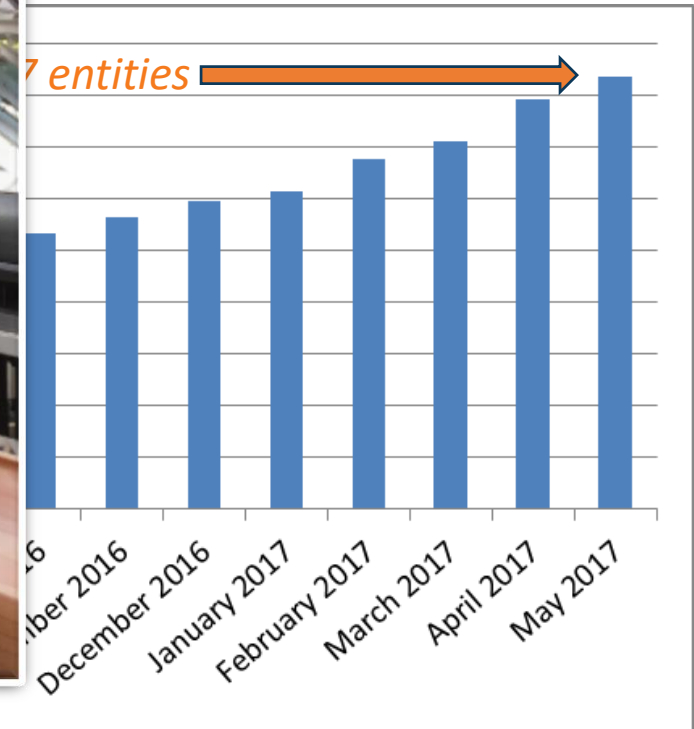
Project.



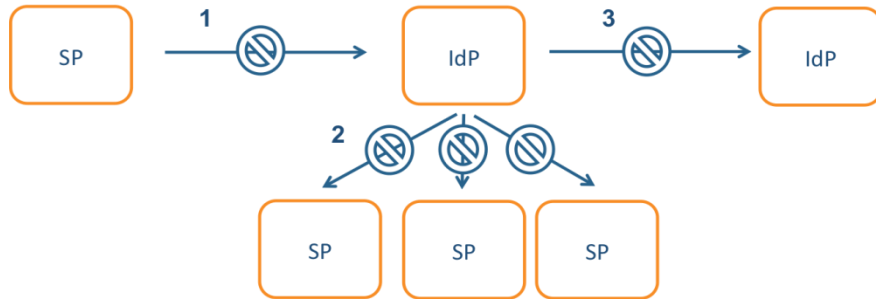
Benefits

Why should I join? What are the Benefits?

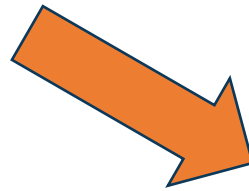
- Adds security conta
- namespace for Sirtfi
- with R&S specificati
 meets **baseline assu**
 and IGTF “assured id



Incident response process evolution in federations

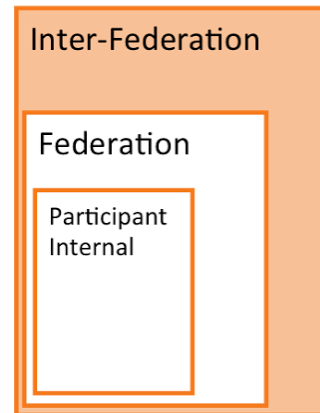


Incident Response Communication, communication blocks



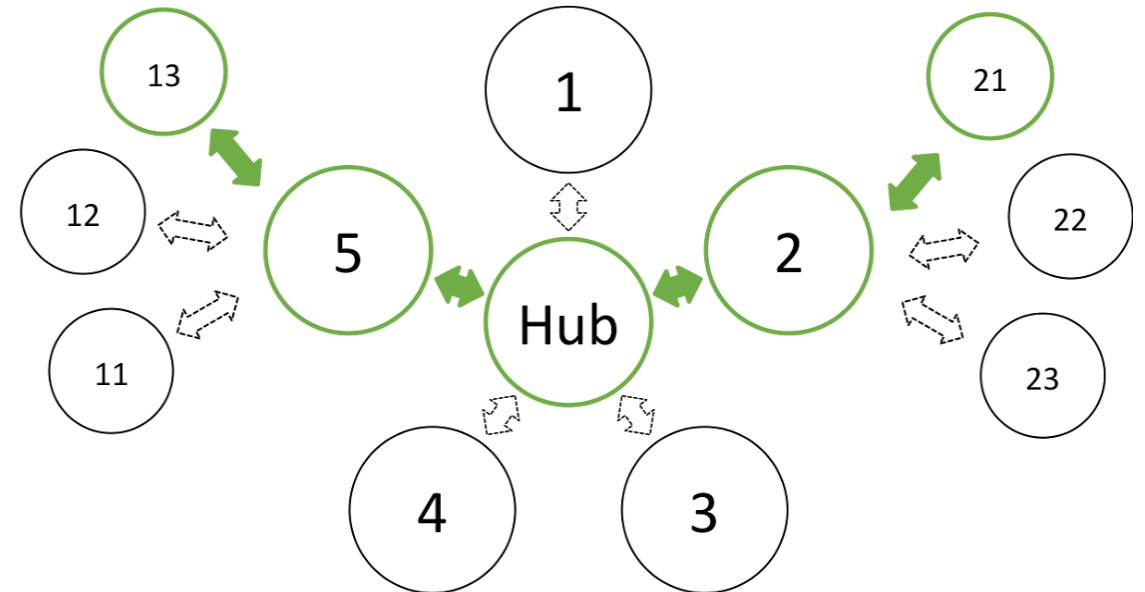
Challenges

- 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



Solution

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



Inter-Federation Incident Response Communication

Policy and Best Practices Harmonisation



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

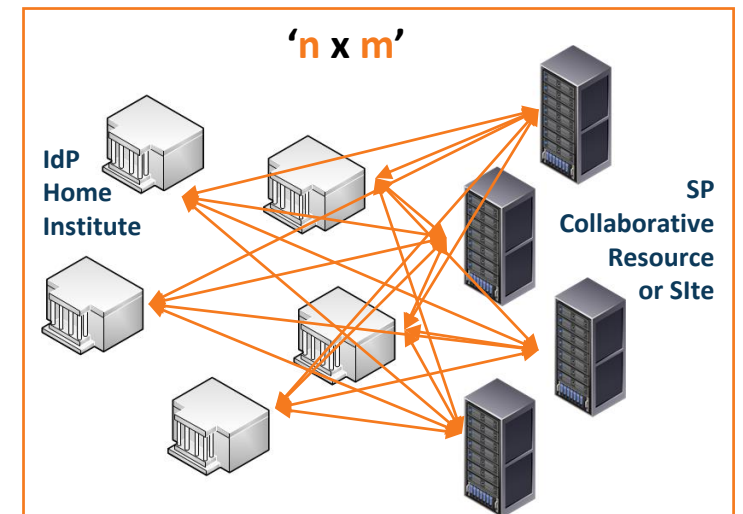
Develop policies models for SP-IdP Proxy – IdPs to SPs

- 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



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)

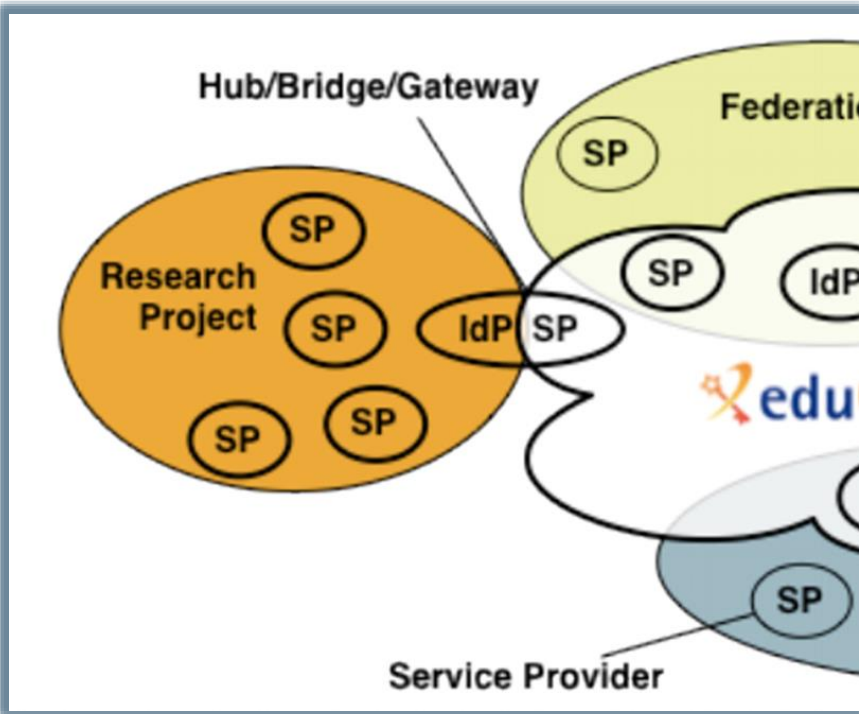
Licia Florio (GEANT), David Groep (Nihel), Christos Kanellopoulos (GEANT), David Kelsey (STFC), Mikael Lindén (CSC), Ian Neilson (STFC), Stefan Praetow (Jisc), Wolfgang Pamppe (DFN), Vincent Ribailier (IDRIS-CNRS), Mischa Sallé (Nihel), Hannah Short (GEM), Uros Stevanovic (KIT) and Gerben Venekamp (SURFsara)

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, ...

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?



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

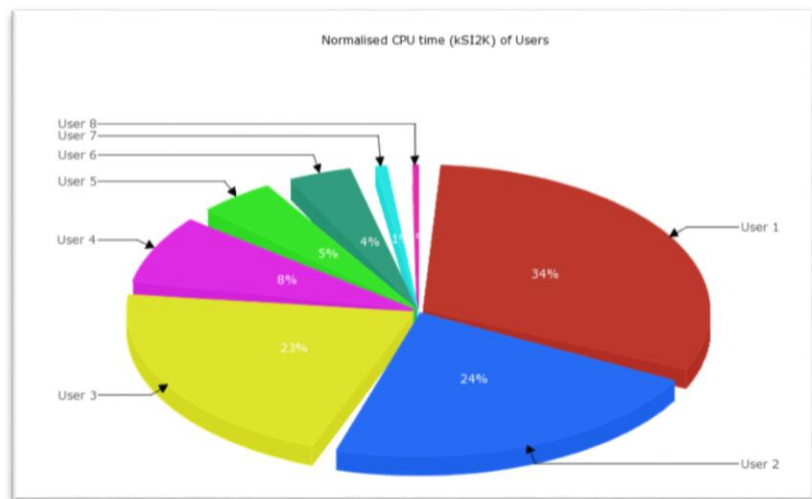
Leverage entity categories and assurance profiles

- 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

Policy and Best Practices Harmonisation



Accounting and the processing of data

Scope of the AARC Accounting and Processing of Data task

Protection of personal data in research data

- *patient records*
- *survey data collation*
- *big data analytics*
- *research data combination*

Research Infrastructures

Institutional

Ethical Committees

ESFRI Cluster Projects

User attribute release by federated organisations

- *institutional IdP attributes*
- *GEANT DP CoCo**
- *minimal release in eduGAIN*
- *REFEDS*
Research & Scholarship

REFEDS, GEANT4

- *community management*

Joint RIs, EIs and AARC work

Personal data processing in accounting & collaboration

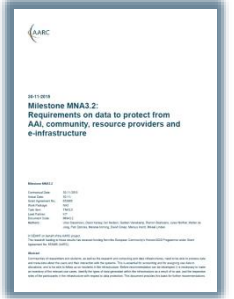
- *collection of usage data in RIs and e-Infrastructures*
- *correlating resource usage to people and groups*
- *collate usage data across countries and continents*
- *personal data used for incident response*

AARC targeted work item

We must share – that’s what collaboration and joint services are about

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?

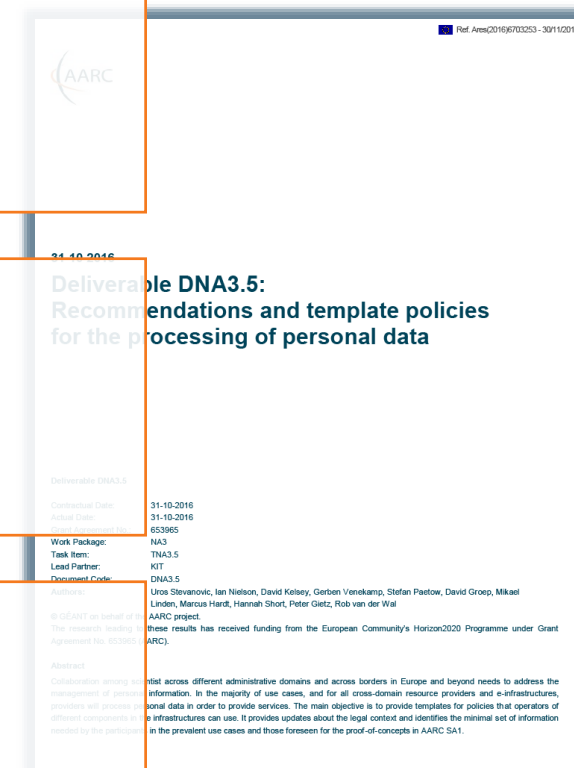
- Global sharing in controlled communities appears attractive
- Uncertainty about requirements (governing body) and timing (> Mar 2018) are not helpful for adoption today ... just yet
- Ongoing work: text needs to allow for (community) attribute authorities

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)

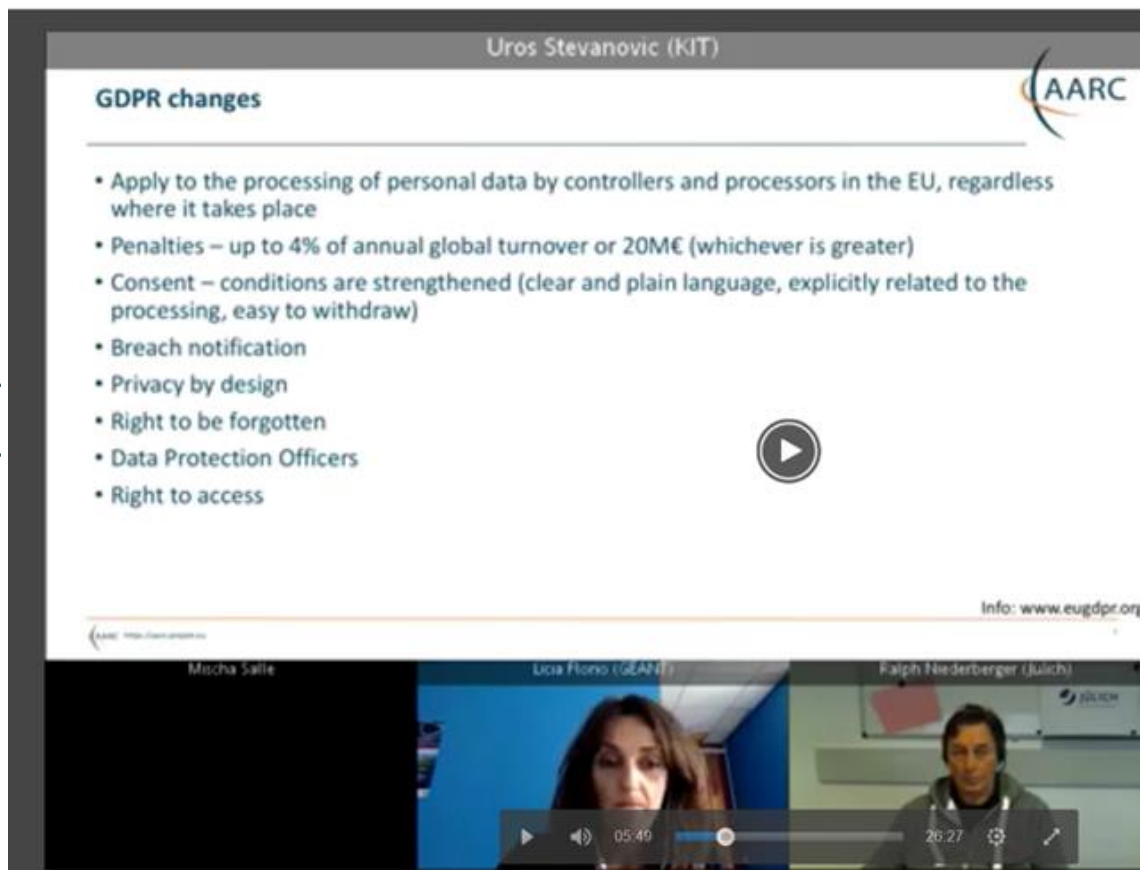
- Note that this is not formally BCR, so requires acceptance of some risk
- Collaborations (e.g. based around *Snctfi*) with control mechanisms benefit
- “Say what you do, and do as you say” – transparency and openness is our real benefit towards the person whose data is being handled



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



Uros Stevanovic (KIT)

GDPR changes

- Apply to the processing of personal data by controllers and processors in the EU, regardless where it takes place
- Penalties – up to 4% of annual global turnover or 20ME (whichever is greater)
- Consent – conditions are strengthened (clear and plain language, explicitly related to the processing, easy to withdraw)
- Breach notification
- Privacy by design
- Right to be forgotten
- Data Protection Officers
- Right to access

Info: www.eugdpr.org

Mocha Salle

Lisa Florio (GLAN)

Faigh Nierderberger (Julich)

05:49 / 26:27



Recommendation for sustainable services and models

Recommendations for Research and e-Infrastructures to Build Sustainable Services

Even AARC will have an end ...

... we need the results taken up by others!



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 starting a guest identity provider

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

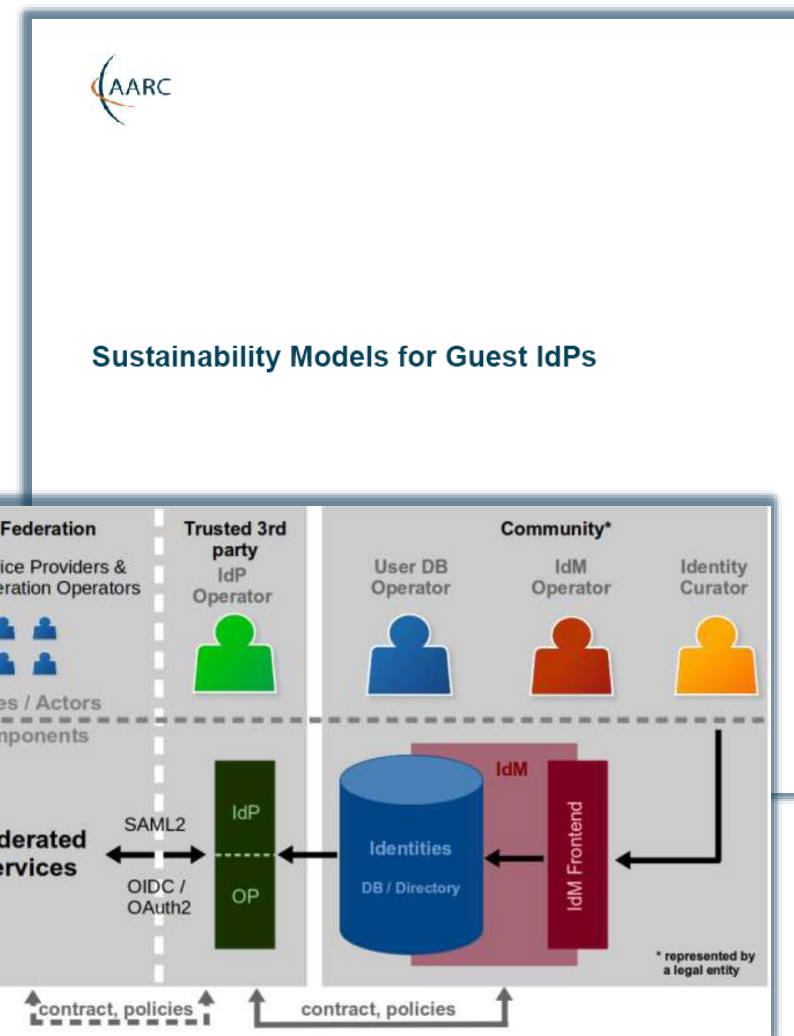
Guest IdPs are critical to almost all collaboration use cases

➤ *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*



Policy and Best Practices Harmonisation



... but we need more ...

... towards the future!

Operational Security and Incident Response

- Security capabilities and response for community attribute authorities and services
- Promote trust groups and reference templates and models to be used throughout eduGAIN

Service-centric policies

- Harmonize traceability, accounting, and attribute policies in infrastructures based on SCI model
- Explore GDPR and Code of Conduct models for sharing necessary information, and meet policy needs for SP-IdP Proxies, repositories and translators

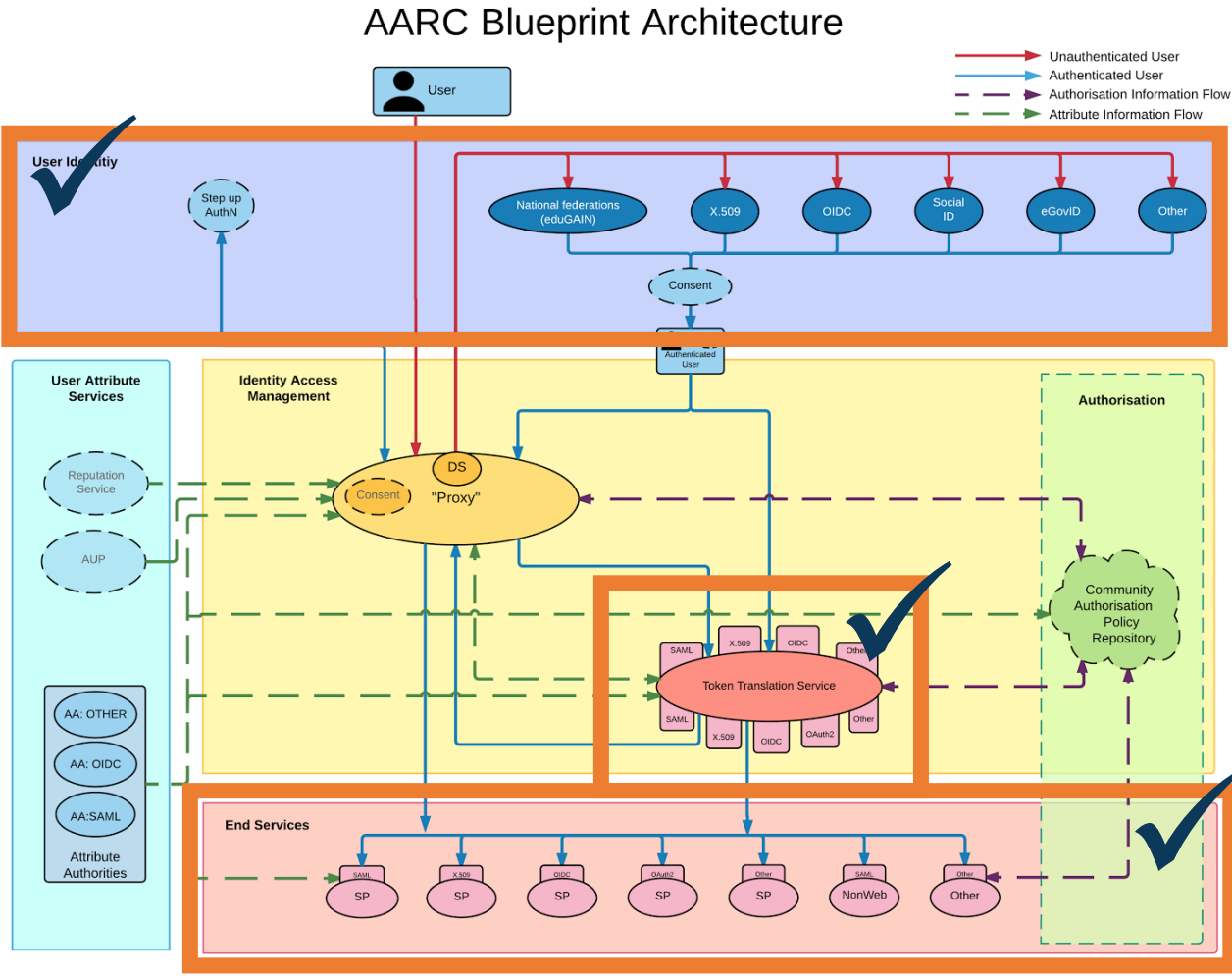
e-Researcher-centric Policies

- Aligning AUPs and assurance profiles to ease cross-infrastructure sharing beyond the silo
- Align models for community attribute management & provisioning (e.g. ease risk assessment)

Policy Development Engagement and Coordination

- Work with the communities to promote alignment across research and generic Infrastructures

Operational Security – we’re all in it together!

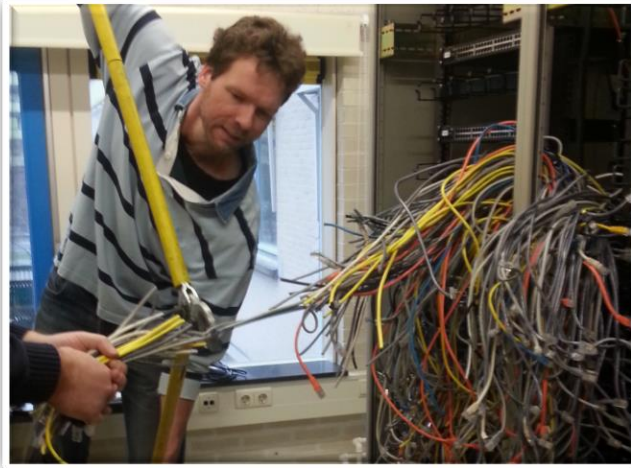


In the past 2 years, we managed to address security coordination for the federations, IdPs, and the e-Infrastructure collective services ... but everyone needs to be involved, globally!

*User Attribute Service operations security
Integrity and trust for the SP-IdP-Proxies
Link security hubs (eduGAIN Support Desk, eInfra CSIRTs) to community capabilities*

- **Promote trust groups and their expansion to effectively cover the eduGAIN network**
- **Define reference templates on how incident notifications should be conveyed**
- **Encourage endorsement by global standards bodies and communities**

Helping out the providers – with service-centric harmonisation



Traceability [TR]			
	A	B	C
1	Infrastructure Name:	<insert name>	
2	Prepared By:	<insert name>	
3	Reviewed By:	<insert name>	
4			
5	Operational Security [OS]	Maturity	Evidence (Document M
6	OS1 - Security Model		
7	OS1.1 - Authentication		
8	OS1.2 - Authorisation		



Traceability and accounting policy framework

Compare models for comparing and considering equivalency of policies for traceability, accounting aggregation, and registration records retention in interfederation



Explore the GDPR (2018) options for sharing of data on, and for, infrastructure usage

Infrastructures need to share data, globally, but a scalable model will be community dependent



Recommendations for Blueprint Architecture Elements

Create the reference templates for SP-IdP-proxies, gateways, targeted credential repositories, &c

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

- Remember the Taipei Accord: WLCG, EGI, PRACE, OSG, XSEDE share an understanding
- and accept each other's AUP as sufficient



Enhance the Authentication Assurance Profiles

Get the new Profiles accepted and deployed for all target groups

- Authenticating for access to biomedical and human-related data
- Implementing verified identity vetting in the GDPR era
- Making the baseline a real baseline, and Cappuccino a common occurrence



Define a model for community attribute management and provisioning

Reference practices for communities setting up their membership and attribute services

- So that the community is always in control, and the services can rely on that

We need you to work with us

Develop

Through

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



AARC 'Competence Centre'

work with us by collaborating in these groups

Adopt

In your Infrastructure, Federation, and FIM4R

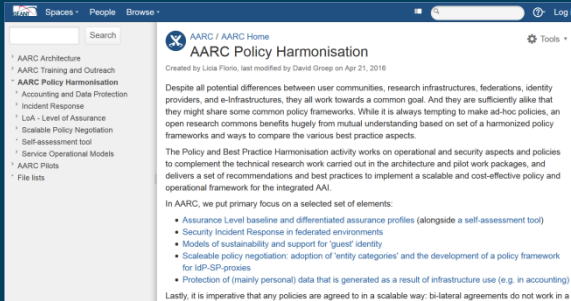
- *Persistent, non-reassigned identifiers*
- *Incident Response capabilities*
- *Sirtfi NG*
- *Snctfi*
- *Self-assessment and peer review methods*



AARC Engagement

help us progress by adopting results

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



Thank you Any Questions?

davidg@nikhef.nl



<http://aarc-project.eu/>



© GEANT on behalf of the AARC project.

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).