Authentication and Authorisation for Research and Collaboration

Policy and Best Practices … the Story So Far

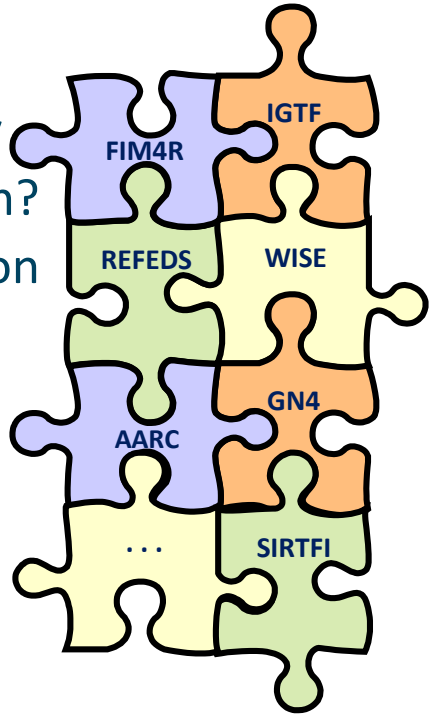
David Groep
P&BP activity lead
Nikhef, Amsterdam

AARC All Hands meeting Geneva
2016-11-29

Solving the Policy Puzzle

Pushing forward best practices and like policies across many participants

- "Levels of Assurance" – baseline and differentiated profiles, capabilities and grouping
- "Incident Response" – beyond Sirtfi: a common understanding on operational security
- "Sustainability, ops models & Guest IdPs" – how can a service be offered in the long run?
- "Scalable policy negotiation" – helping SPs move beyond bilateral discussion
- "Protection of (accounting) data privacy" – necessary aggregation without breaking the law too much



Strategy

to support and extend established and emergent groups

leverage their support base - and 'multiply' the effect of policy work from AARC

Baseline Assurance Profile – a widely supported set of qualities

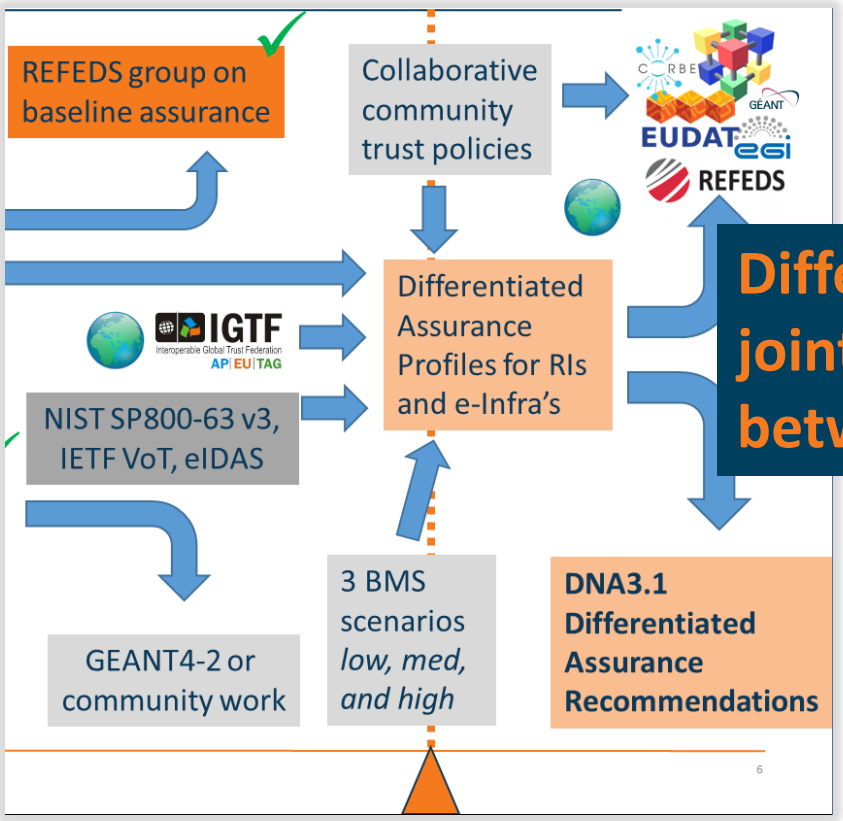
Minimum baseline is targeted to **concrete use cases** from currently running infrastructures

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 federation, it is not 'implicit',
and needs specific work on identifying authorities and eligible entities …

From Baseline to Differentiated Assurance

- REFEDS WG (mainly for IdPs) based on capabilities ('vectors')
- Grouping of capabilities with our SPs into profiles



Different profiles and joint alignment of assurance between e-Infras ongoing …

Assurance Profile (DRAFT)

REFEDS Assurance working group

Table of Contents:

Abstract

This profile splits assurance into five orthogonal components (a.k.a. vectors, dimensions). The Credential Service Provider assigns one or more values from one or more categories 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

@REFEDS: Assurance Components consultation early 2017 – simple structure

https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLl3UJbaOX5o9eLtsyBI

Security Operational Procedures

‘A Very Timely Activity’

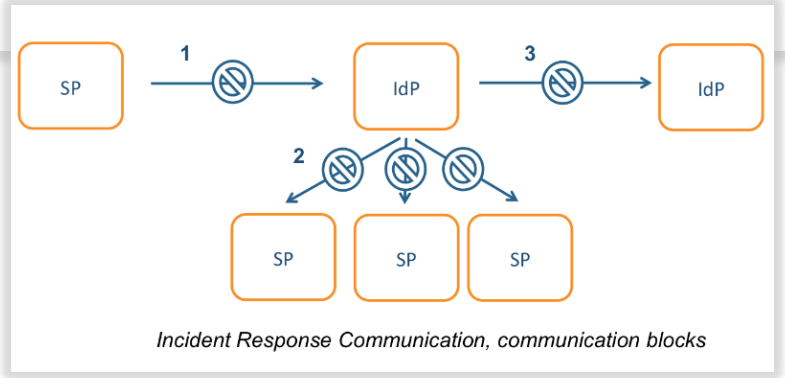
Incident response capabilities at IdPs and SPs:
Sirtfi v1 brings these to light

Beyond v1: proper channels, expectations,
and the operational capability are still missing

Need to establish homogeneous
Incident Response Procedure – **see the doc!**
– with a need for a central operational capability …

31-12-2016

Deliverable DNA3.2: DNA3.2 - Security Incident Response Procedure



Incident Response Communication, communication blocks

Read (quickly …) and comment – this affects you all

Link is on the AARC Wiki under Policy Coordination -> Incident Response

https://docs.google.com/document/d/1I3IhatjdP5sa6Sfji8SIT6yXo4CI1tf2kNOaccD9QCU

Sirtfi Training and Outreach

- REFEDS and federation focused FAQ
- Definition of the global Security Contact meta-data profile for use in eduGAIN
- Namespace for Sirtfi Assurance at IANA
- Used in cyber ops roleplay exercises
- Promoted at I2TechX, FIM4R, Kantara, and TF-CSIRT

- Ingredient to the 'CILogon pilot'
  combination of
  REFEDS "Research and Scholarship"
  and
  Sirfti v1.0

  meets **assurance requirements for RIs and EIs** according to the IGTF "assured identifier trust"

Nov 24th **114 IdPs ineduGAIN that support Sirtfi**

Operational models, federation and sustainability

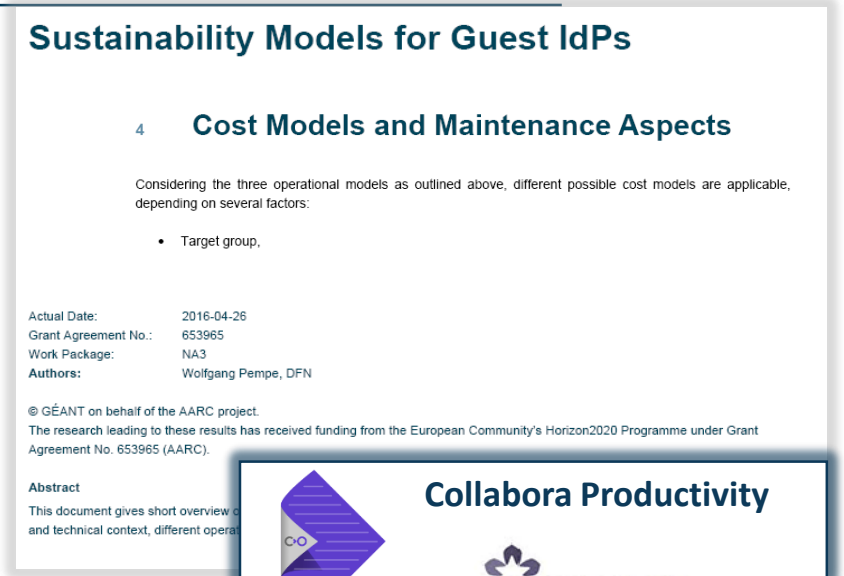
Sustainability models for guest IdPs

- Distribution of roles, costing model, maintenance, …

Operational mechanisms for federations and SPs and IdPs

- Governance, gaps in policy space, service operations for SPs, SP federations, … and Attribute Authorities (basis)
- Across both ESFRIs and global infrastructures

Dedicated 30’ slot tomorrow


Sustainability Models for Guest IdPs

4 Cost Models and Maintenance Aspects

Considering the three operational models as outlined above, different possible cost models are applicable, depending on several factors:

- Target group,

Actual Date: 2016-04-26
Grant Agreement No.: 653965
Work Package: NA3
Authors: Wolfgang Pempe, DFN

© 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

This document gives short overview c
and technical context, different operat

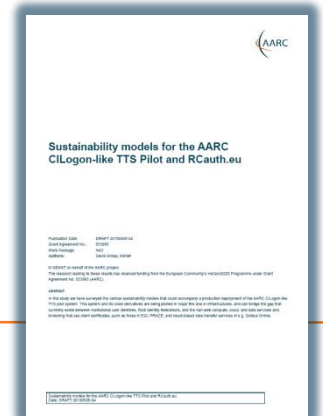

Collabora Productivity

DARIAH-EU

On-premise or SaaS trusted collaboration using LibreOffice Online and OwnCloud with integration of eduGAIN IdPs

Sustainability for the AARC pilots and their adoption by research and for collaborations

- Joint effort needed on making the SA1 pilots outlive their demo phase
- Case studies: collabra suite, CILogon/RCauth, … but we need this for all pilots
- There will be a *template* coming that will guide you in building such a plan


Sustainability models for the AARC CILogon-like TTS Pilot and RCauth.eu

https://docs.google.com/document/d/15v65wJvRwTSQKViep_gGuEvxLl3UJbaOX5o9eLtsyBI

E.g.: Federation operations – alignment recommendations for use in Pilots

Combined desk study (based on automated meta-data) and interviews (DFN AAI, SURFconext)

Differences	*care level offered to participants* *collective acceptance and provisioning of services*
	national funding model and adequacy, federation structure
Alignment	*acceptance policy for service providers and IdPs – intent is all the same*
	charging models: IdP connected without additional cost, SPs are 'free'
	entity categories for grouping 'alike' services and IdPs is supported
Alignment	*eduGAIN participation is still opt-in (needs convincing of each IdP)*

The report will also try to address attribute authority models – as a basis for AARC2

https://wiki.geant.org/display/AARC/Federations+Current+Policies+and+Practices

Full mesh policy negotiation does not scale – we cannot afford it!

Collaborations by design have their services distributed

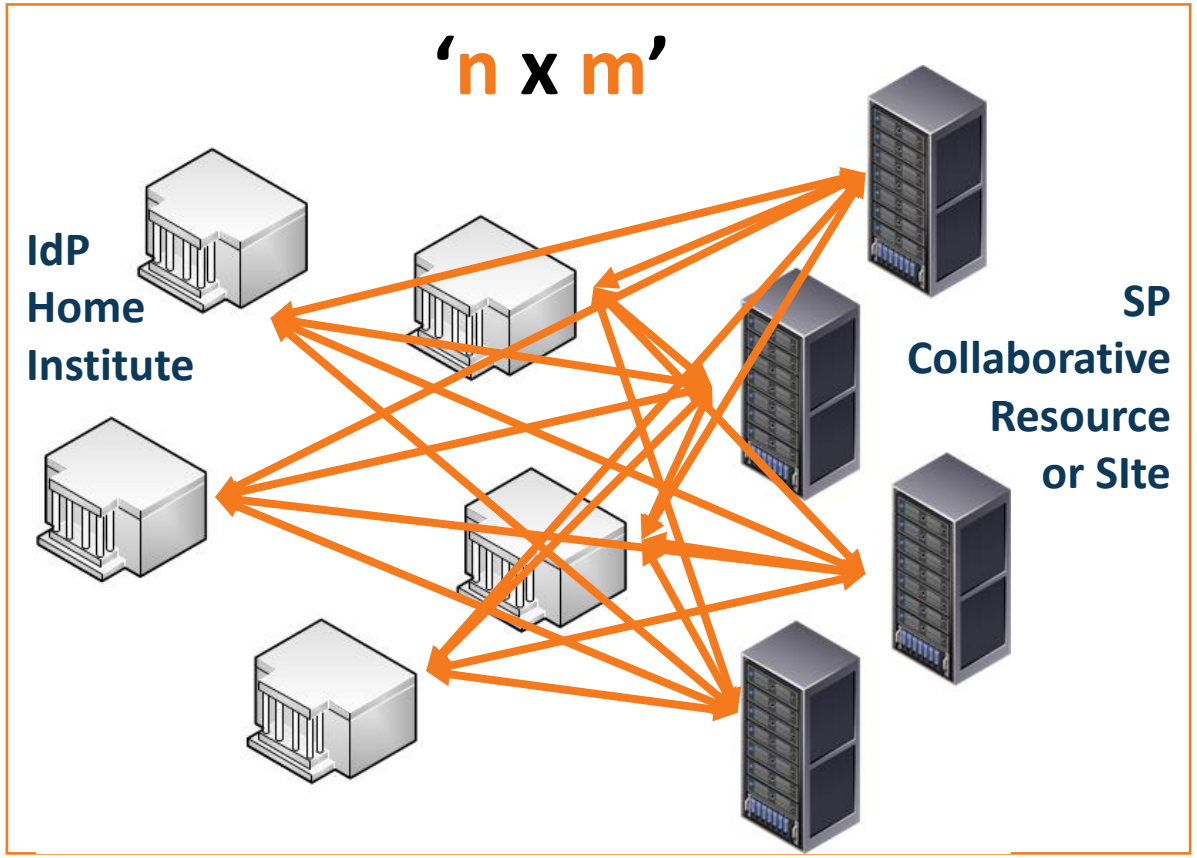
and

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

IdPs and Home Institutes

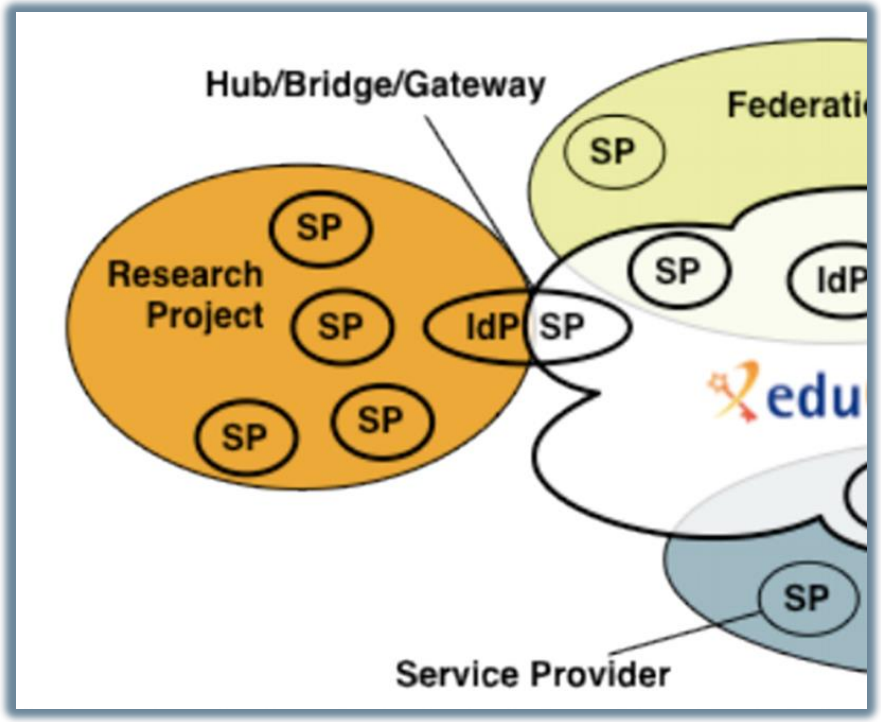
- do not have the effort to evaluate services that only impact a couple of their people
- are – in academia – in general very risk-averse

Group entities to easy negotiation process



Developing scalable policy models in light of the Blueprint: Snctfi!

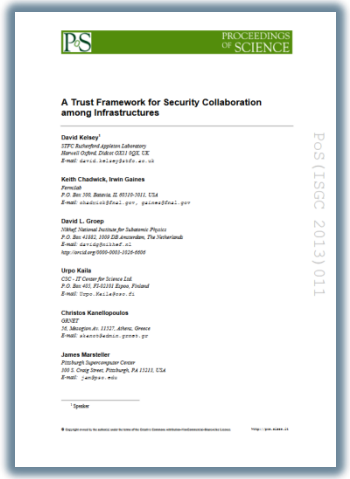
- ✓ allow proxy operators to assert ‘trust marks’ based on known SP properties
- ✓ Develop framework recommendations for RIs for **coherent policy sets**



evaluate with the SP-IdP-Proxies in pilots, based on the Blueprint (DNA3.4)

Collaborate in WISE & **FIM4R** to get global endorsement

Thursday morning Snctfi breakout


PROCEEDINGS OF SCIENCE

A Trust Framework for Security Collaboration among Infrastructures

PoS(ISGC 2013)011

Many SPs are alike

Policy frameworks for collective service providers Shared use of and collaboration on reputation services, together in FIM4R

Graphics inset: Ann Harding, SWITCH

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**

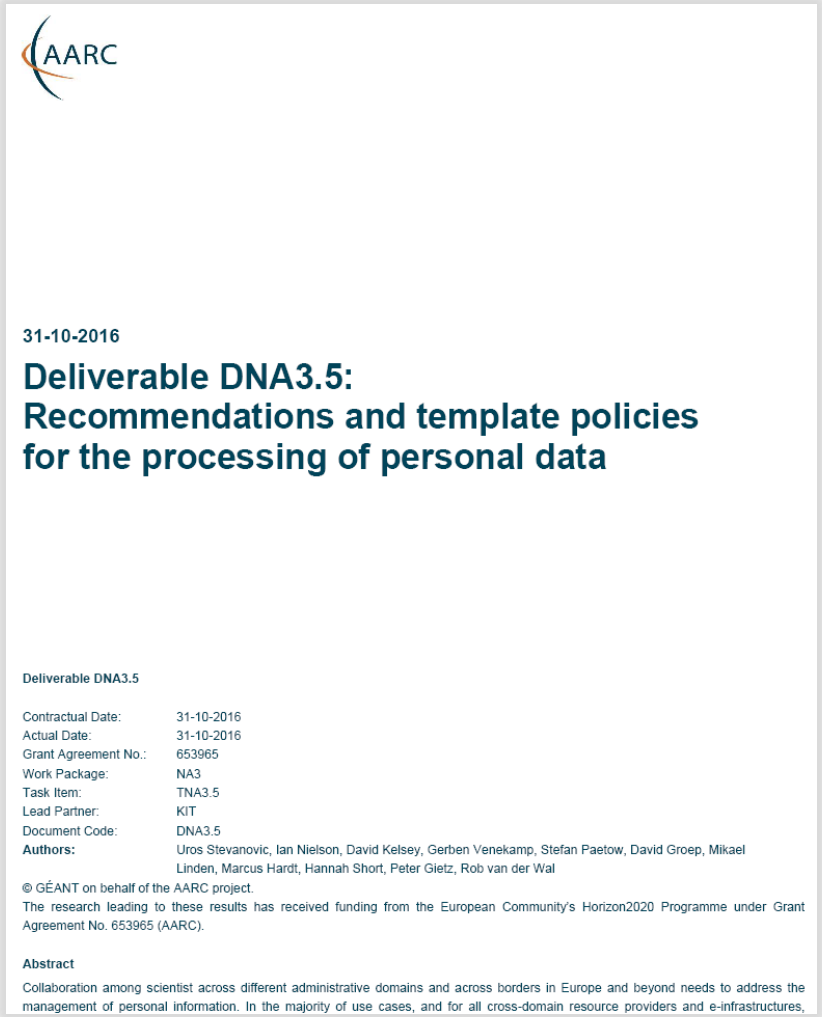
** GEANT Data Protection Code of Conduct – see http://geant3plus.archive.geant.net//uri/dataprotection-code-of-conduct/v1/Pages/default.aspx*

Data Protection Recommendation: the next step

How to work together without breaking too much the EU law?

- Accounting data exchange is needed:
  sustainable operating models, during incident response,
  and for meeting funding rules
- Yet the GDPR & current rules 'not always helpful' ☹
  for attribute release CoCo helps, but this is a different use case
- Novel use of existing policy frameworks
  that already bind RIs and e-Infra together
- Practical recommendations inspired by
  the 'Binding Corporate Rules' (BCR) mechanism
- Especially for collaborations that cannot rely on contracts
  but are willing to balance risk vs actual need …

Now: how to we share our experience with new communities?



AARC

31-10-2016

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

Deliverable DNA3.5

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

© 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

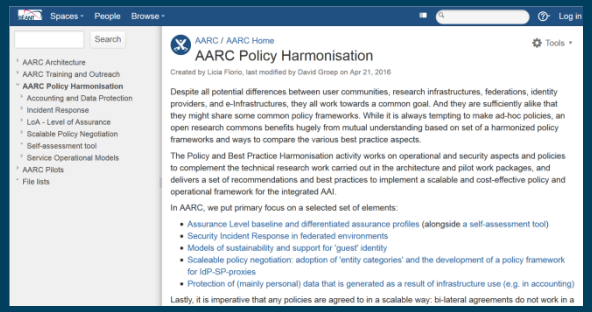
Collaboration among scientist across different administrative domains and across borders in Europe and beyond needs to address the management of personal information. In the majority of use cases, and for all cross-domain resource providers and e-infrastructures,

Inconsistency as our gravest risk? – towards AARC2

Reflected in updated AARC2 structure

- Operational security capabilities and Incident response in federations – beyond Sirtfi v1
- Service-centric policies: traceability & accounting, privacy, gateway operations & proxies
- e-Researcher-centric policies: alignment of AUPs and templates, authentication assurance, community attribute management models and provisioning

- Policy Engagement and Coordination: contributes to Community Engagement, provision of policy expertise to the Competence Centre, promotion of best practices globally (WISE, FIM4R, IGTF, REFEDS), easing **end-to-end coordination** across the chain



Thanks to all P&BP collaborators from CSC, CERN, DAASI, RAL/STFC, KIT, GRNET, DFN, SURFsara, LIBER, and the **community at large**!

Thank you

Any Questions?

davidg@nikhef.nl

https://aarc-project.eu

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