



Authentication and Authorisation for Research and Collaboration

Policy and Best Practice Harmonisation *facilitating research and collaboration*

David Groep

NA3 Activity Lead



TNC2016 – AARC Workshop

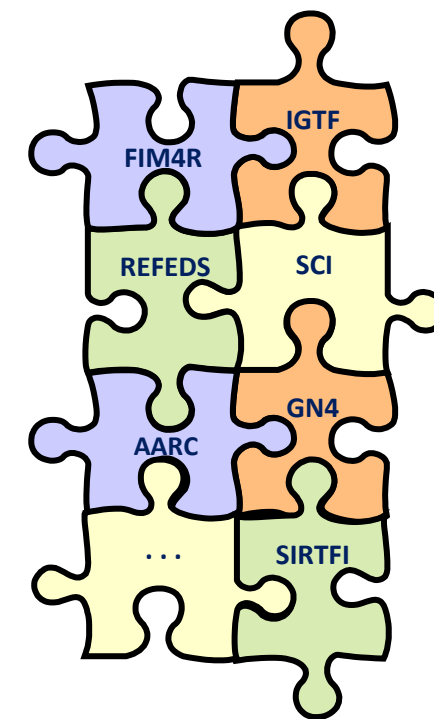
16 June, 2016

Prague

The Policy Puzzle

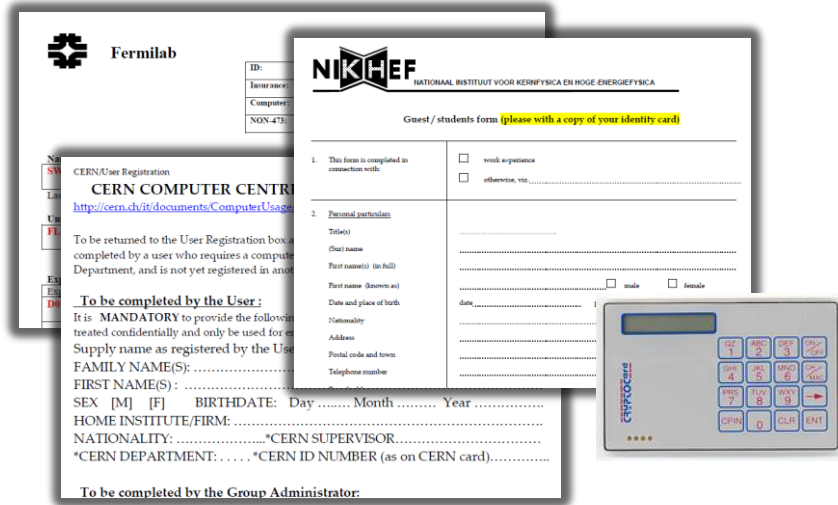
Many groups and (proposed) policies, but leaving many open issues

- AARC is tackling a sub-set of these
 - “Levels of Assurance” – a minimally-useful level and a differentiated set, for ID and attributes
 - “Incident Response” – encouraging ‘expression’ of engagement by (federation) partners and a common understanding on operational security
 - “Sustainability models and Guest IdPs” – how can a service be offered in the long run?
 - “Scalable policy negotiation” – beyond bilateral discussion
 - “Protection of (accounting) data privacy” – aggregation of personal data in operating collaborative infrastructures



Strategy is to support and extend established and emergent groups so as to leverage their support base (and ‘multiply’ the effect of policy investments from AARC)

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,

Special Publication 800-63-3
NIST Special Publication 800-63-3



Identity Assurance Framework: Assurance Levels



National Institute of Standards and Technology

Recommendations of the National Institute of Standards and Technology

Many layered models (3-4 layers)

but: specific levels don't match needs of Research- and e-Infrastructures:

- Specific combination ‘authenticator’ and ‘vetting’ assurance doesn't match research risk profiles
- Disregards existing trust model between federated R&E organisations
- Cannot accommodate distributed responsibilities

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

Assurance Profile development in AARC



European 'baseline' use case requirements ✓



REFEDS group on baseline assurance ✓

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)

R&E Feder
Assurance
Capabilities
GEANT4-1

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!

MNA3.1 "baseline LoA" document

TNA3.2 "Sirtfi"

GEANT4-2 or community work

PY2: Assurance Profile development in AARC

– collaborative and differentiated assurance



European 'baseline' use case requirements from RIs and EIs ✓

depth interviews

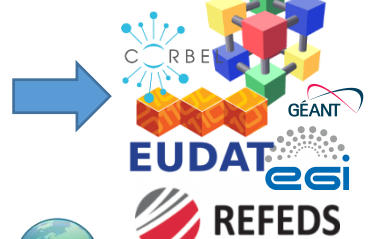
Baseline requirements for low-risk use cases



Global REFEDS consultation process

REFEDS group on baseline assurance ✓

Collaborative community trust policies



Differentiated Assurance Profiles for RIs and e-Infra's



NIST SP800-63 v3, IETF VoT, eIDAS

Self-assessment tool requirements ✓

R&E Federation Assurance Capabilities GEANT4-1

MNA3.1 "baseline LoA" document

TNA3.2 "Sirtfi"

GEANT4-2 or community work

3 BMS scenarios low, med, and high

DNA3.1 Differentiated Assurance Recommendations

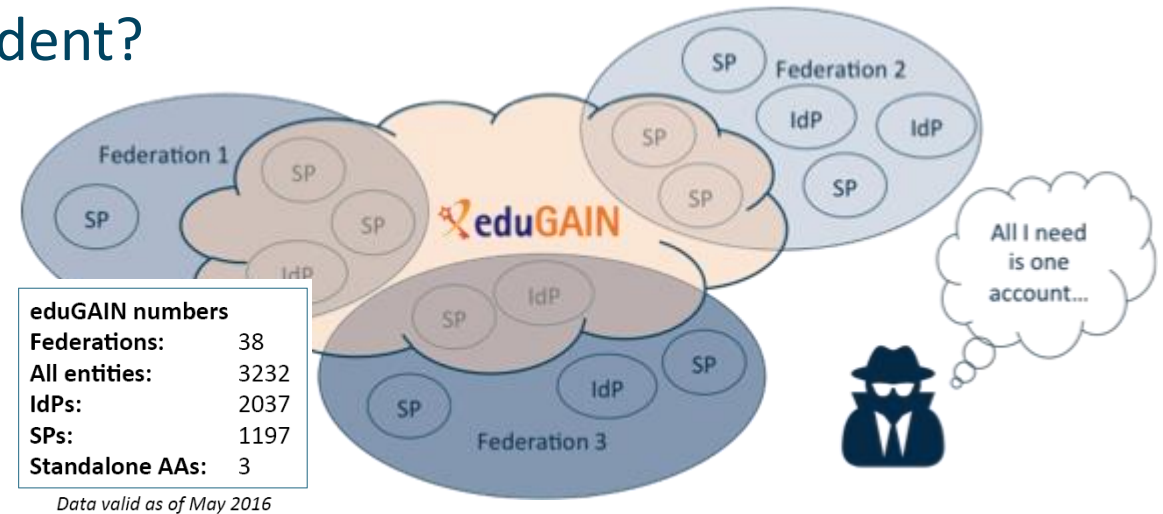
Policy and Best Practices Harmonisation



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?



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 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 Sirtfi v1.0*

meets assurance requirements for RIs and EIs according to the IGTF “assured identifier trust”

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


The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant. Visit our [Wiki](#) to discover how your organisation can prepare itself for Federated Incident Response with Sirtfi.

REFEDS' [Sirtfi Working Group](#) has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the [AARC Project](#).




Benefits

Why should I join? What are the [Benefits](#)?



Sirtfi v 1.0

View the [Sirtfi Framework](#)



FAQs

Need [help](#)?

Incident response – adoption process and impact



January 2016: Sirtfi document globally agreed (v1.0) and published
Description of incident response contact in eduGAIN

March, April 2016: extended adoption process to bulk-approve IdPs in 'tight' federations
May 2016: agreed adoption model with SURFconext and SWITCHaai,
interest from WAYF-DK, CSC/FUNET, DFN, and UK AMF



June 3rd: **87 IdP in eduGAIN that support Sirtfi**

Policy and Best Practices Harmonisation



Task 3

**Recommendation for service operational models
for enabling cross-domain sustainable services**

Sustainability models for 'guest' IdPs – serving users beyond academia

Guest IdPs are critical to almost all collaboration use cases

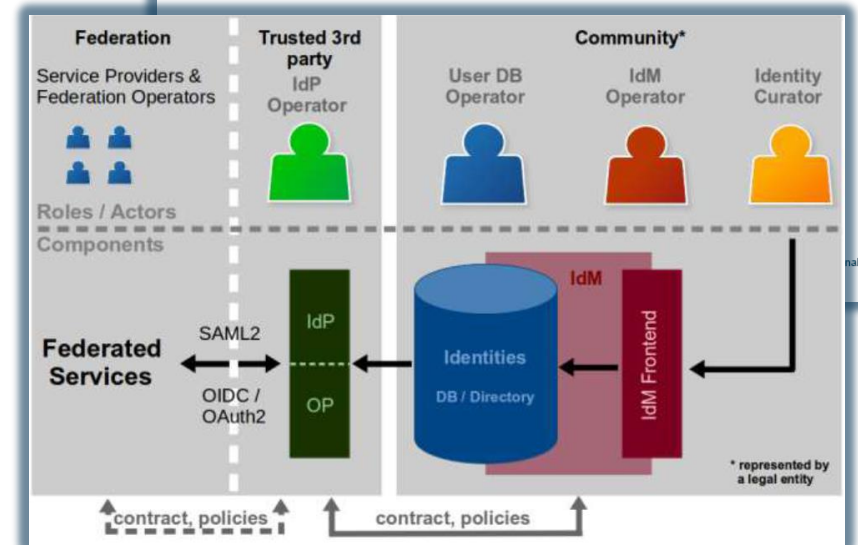
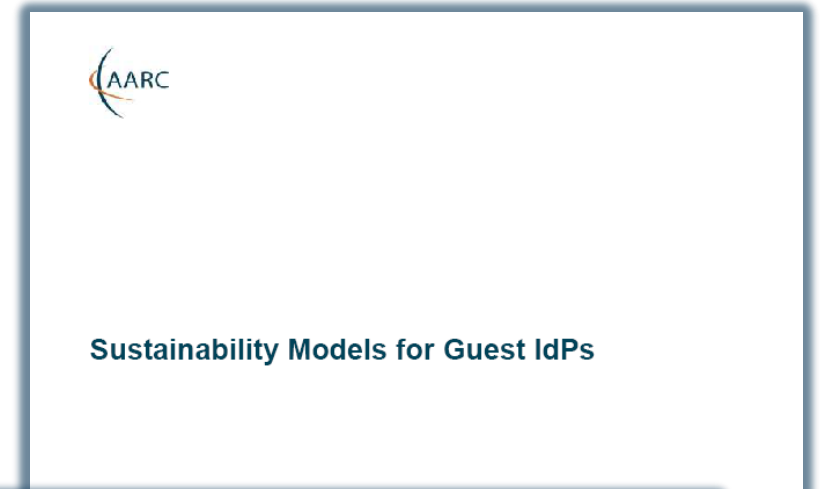
➤ Collaboration does not end at the door of the university !

PY1 work:

- Model study – too often 'guest' IdPs have faded or become less usable for research collaborations
- Identify sustainable IdP models based on experience

PY2 plans:

- based on use of guest IdPs in the Blueprint
- Leverage work of GEANT4 on COPaaS
- Review feasibility of 'paid' & 'external' IdPs services *which may or may not be free at point of use*



Federation operations – alignment recommendations for use in Pilots



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

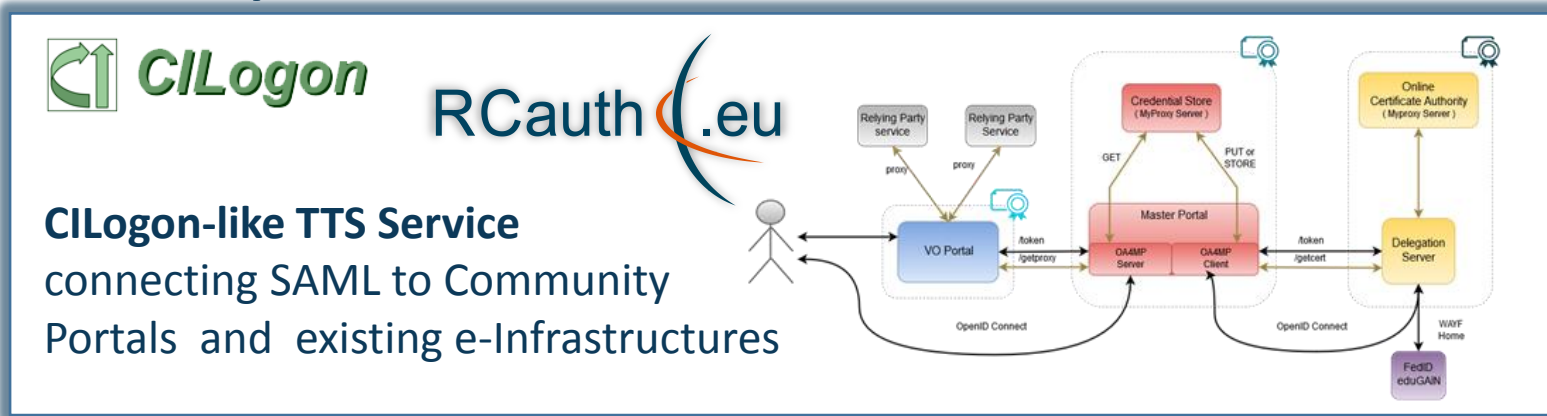
Differences	<i>care level offered to participants</i> <i>collective acceptance and provisioning of services</i>
	<i>national funding model and adequacy, federation structure</i>
Alignment	<i>acceptance policy for service providers and IdPs – intent is all the same</i>
	<i>charging models: IdP connected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

In PY2 focus on obvious differences, such as:

- support for catch-all ‘guest’ IdPs in all federations
- support of attribute authorities: is either complicated or easy depending on federation structure

AARC Pilot sustainability

PY1 completed:

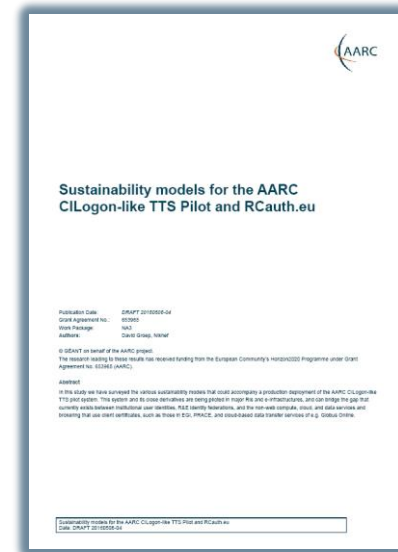


Sustainability models
Integration with EIs/RIs
Funding schemes
Transition negotiations
Intentionally 'white label'

PY2 schedule:



Develop business model and demonstrate feasibility



Policy and Best Practices Harmonisation



Task 4

Development of scalable policy negotiation mechanisms

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

Collaborations by design have their services distributed

and

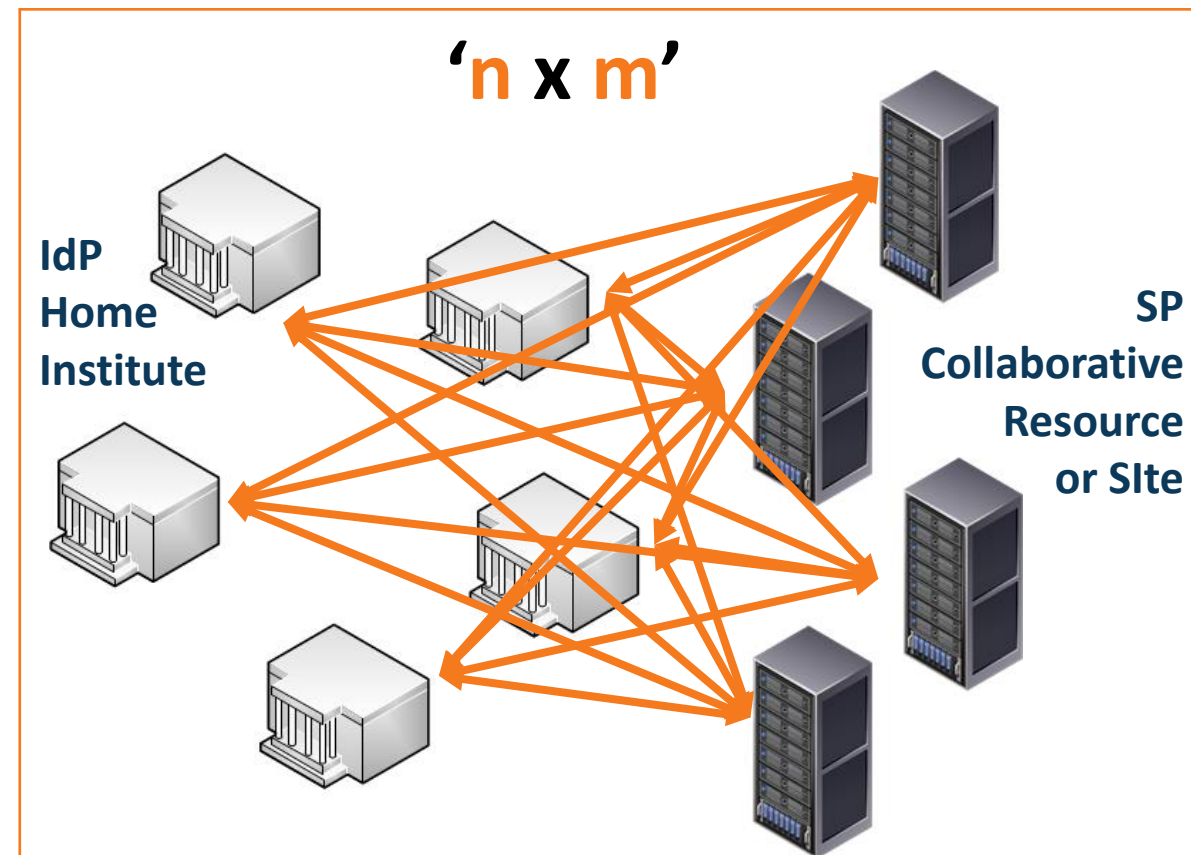
- not that many collaborations are a legal entity
- or are not ‘authoritative’ for constituent services

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



Grouping of entities – PY1 results

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’, ...

Evolving results: AARC Wiki*

Entity Category Experiment using Sirtfi

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

Unexpectedly rapid adoption:

- *87 Sirtfi entities in **4 month***
- *R&S: 284 in ~ **3 yr***
- *CoCo: 157 in ~ **2 yr***

Conclude: time is ‘ripe’ for it

Use of proxy bridging components

- *how much of eduGAIN can we connect to **current** EI resources*
- *based on entity categories*
- *leverage Sirtfi and ‘R&S’*
- *proxying is bi-directional*

Use ‘CILogon-like TTS’ pilot

- *can we get the back-end CA accredited⁺ to the IGTF*
- *and thus have instant global acceptance for some ECs?*

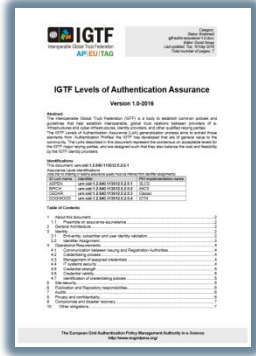
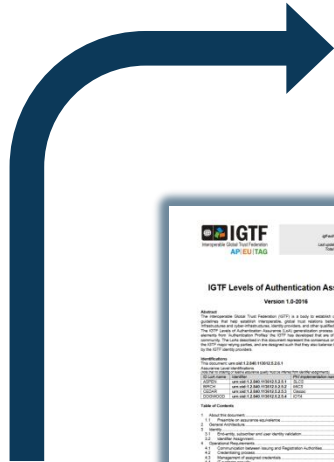
RCauth.eu – supporting the CILogon Token Translation Pilot

Policy guidance	Technical information	Operational information
Pilot ICA G1 policy	ICA Certificates RCAUTH Pilot G1 Certificate (DER) RCAUTH Pilot G1 Certificate (PEM)	Research and Collaboration Authentication Pilot CA - RCAUTH Superior CA DCA Root G1

Head side of the coin

Entity categories to identify qualifying IdPs, so that the collaborative services can trust what comes out of the federated Identity Providers

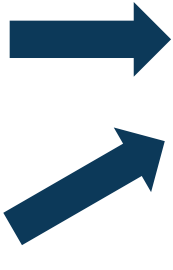
Privacy Policy, Data Protection, CP/CPS



RCauth.eu

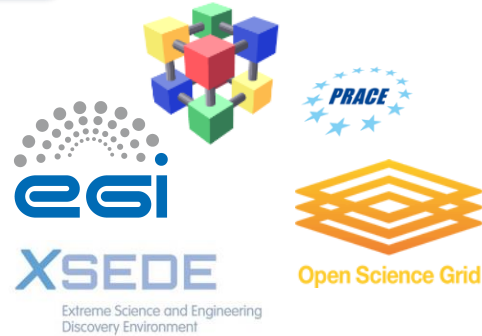
REFEDS R&S 'section 6' – non-reassigned identifiers for users

Sirtfi incident response – traceability for users at time of issuance



meets IGTF 'Identifier Trust Assurance' requirements profile

SP-based heuristic resolution of Federated IdP inconsistencies

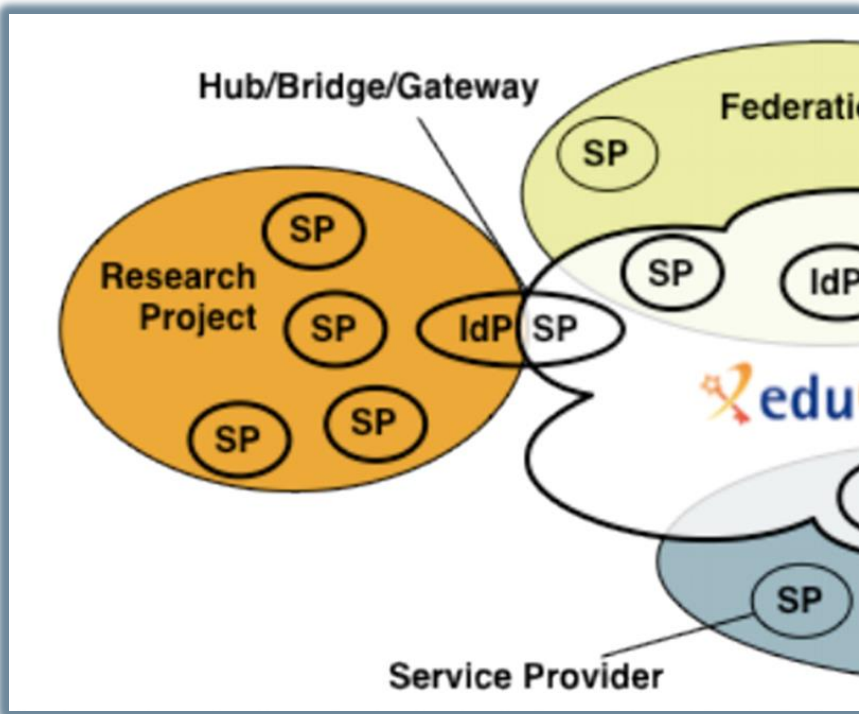


PY2: Developing scalable policy models in light of the Blueprint

- ✓ allow proxy operators to assert CoCo and R&S based on known SP properties
- ✓ Develop framework recommendations for RIs for coherent policy sets



Post (ISGC 2013) 011



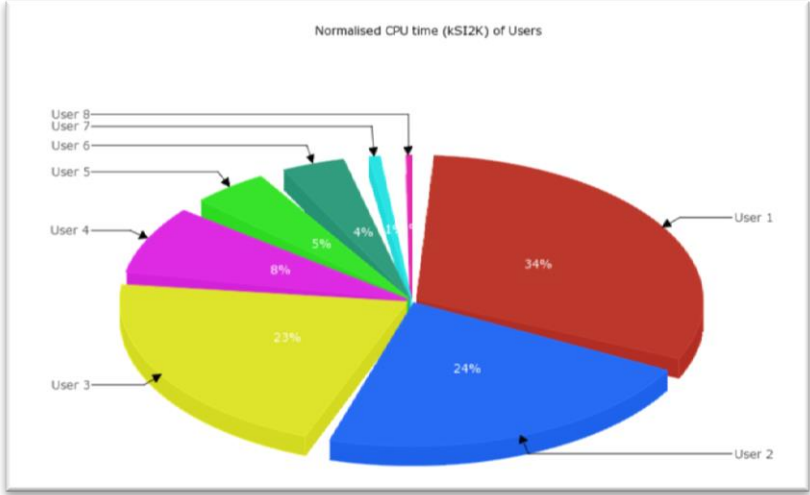
evaluate with the SP-IdP-Proxies in pilots, based on the Blueprint (DNA3.4)

Collaborate in WISE & FIM4R to gain global endorsement

Tail side of the coin

Policy frameworks for collective service providers, so they can – via Entity Categories – convince IdPs of their joint compliance

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

- *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 “TNA3.5” – this task

What data needs to be protected, and who has a role in it?

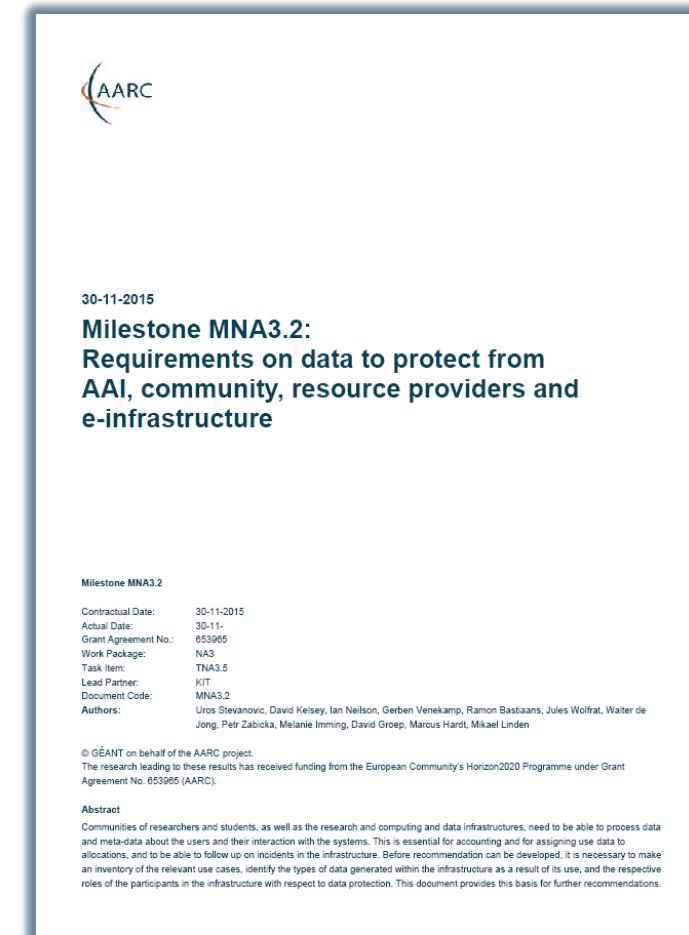
Survey of distinct cross-national infrastructure use-cases: **EGI, PRACE, and DARIAH**

Data collection necessary for ‘legitimate interests’

- Accounting and justification of **global** resource use: personal data (name, unique ID, roles, attributes, rights, ...) kept for up to 18 months after use because of yearly reporting cycle
- Operational purposes: fault finding, researcher support
- Incident response and security operations

MNA3.2 drafted under challenging conditions

- at delivery in November 2015 the GDPR was still an (advanced) draft
- full implementation of the GDPR will outlive the AARC project
- different organisational awareness of EU-US data transfers
... even if Safe Harbour never worked for research anyway ...



Identified needs and structure – now towards PY2 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

PY2 plans

Recommendations for RIs, EIs & proxies based on developing **coherent and binding** policy set: in open, transparent, yet creative way interpret principles of **Binding Corporate Rules**

Policy and Best Practices Harmonisation



Integrated approach – an example:
RCauth.eu Token Service and the ‘European CILogon’

CILogon-for-Europe TTS in PY1: 'of the Pilot, the Blueprint, and the Policy'

Global Collaboration

Joint work+coordination with CTSC and CILogon

Operational guarantee for RCauth.eu by Dutch National e-Infrastructure (SURF) at Nikhef as long as needed



JRA1 - Blueprint Architecture

Demonstrates the use of credential translation to connect infrastructures

Task 4 – scalable policy

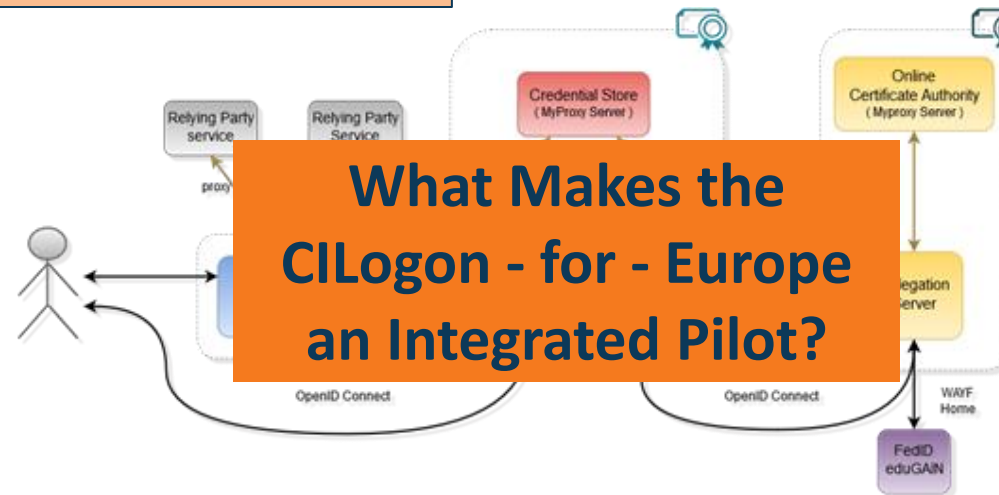
Use of ECs in IdP-SP-proxy to bridge policy domains

Task 3 – sustainability

Sustainability model study to enable EGI, ELIXIR, etc, to decide business model

Task 4 – scalable policy

Accreditation to the IGTF pilots sufficiency of Sirtfi and R&S entity categories



What Makes the CILogon - for - Europe an Integrated Pilot?

Task 2 – Incident Response

Reference implementation of traceable non-reassigned identifiers using R&S + Sirtfi

SA1 - Pilots with communities

*Enabled the SA1 Pilot to demonstrate with ELIXIR on production EGI infra**

Task 1 – assurance levels

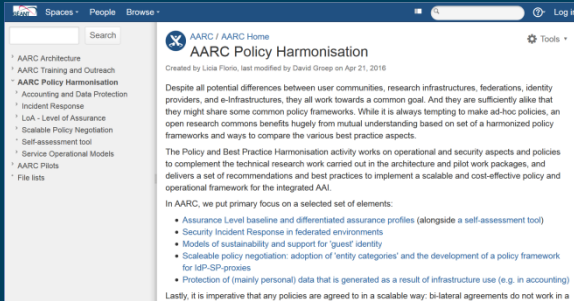
Implements the Baseline; Introduces collaborative assurance basis for federated identity in EIs

Conclusions

- Baseline Assurance Profile set *and moved to REFEDS for implementation*
- Sirtfi v1.0 approved and already implemented by 87 IdPs in eduGAIN
- Joint Sirtfi and Assurance self-assessment tool requirements set
- Alignment of federation operations shows improvement
- Sustainability model study for CILogon-for-Europe TTS picked up by EGI, ELIXIR and others to adopt the service for production use
- RCauth.eu – backend to CILogon – accredited for use in RIs and EIs
- Accounting data exchange found viable route option by binding to “BCR-like” infrastructure policy sets

But now for an exciting second year ... with ... You!

<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



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

