Authentication and Authorisation for Research and Collaboration

Policy and Best Practice Harmonisation ('NA3')

from the present to the future

David Groep

NA3 activity coordinator

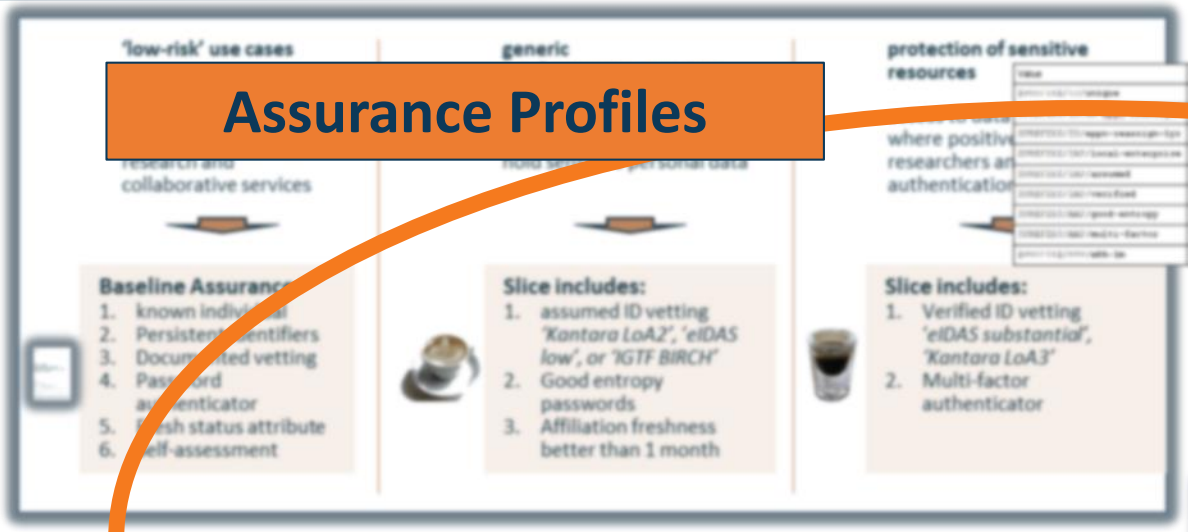
Nikhef

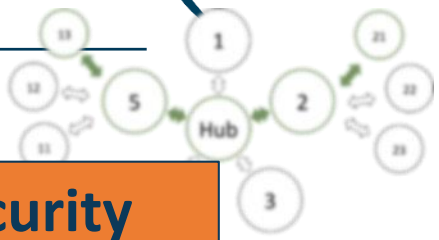
AARC2 Kick-Off meeting

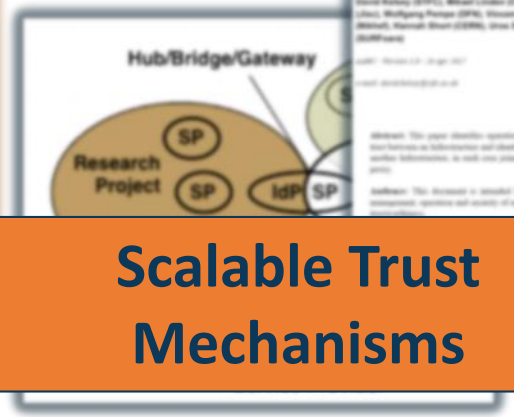
6 – 8 June, 2017

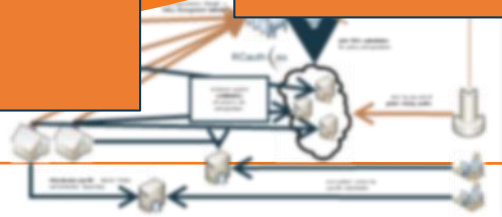
Bad Herrenalb, Baden Württemberg, DE

From the Past …









Assurance Profiles

Operational Security

Global sharing of usage & accounting data

Scalable Trust Mechanisms

Sustainable results & Recommendations

Yet what did we do it for?

Provide an **assurance** framework meeting to **make federated identities more valuable for** 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 & practices serve the community

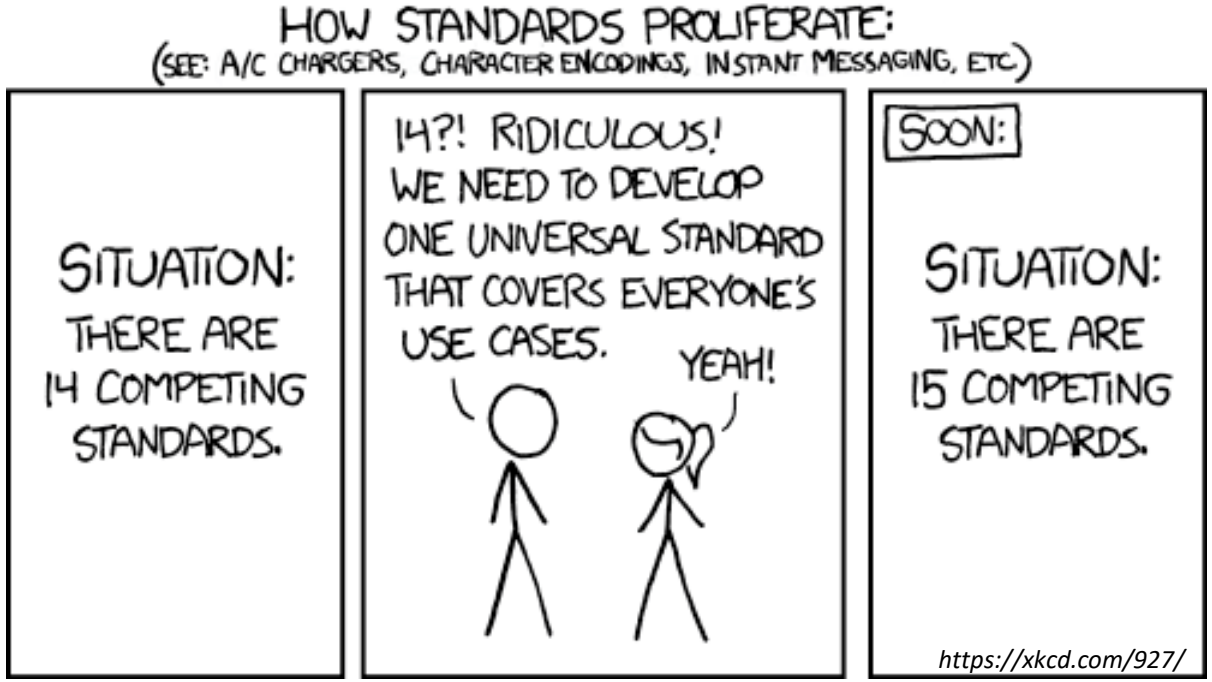
Use **pre-existing groups and communities** to develop policies and harmonise practices and thus **avoid AARC becoming yet another island**

REFEDS

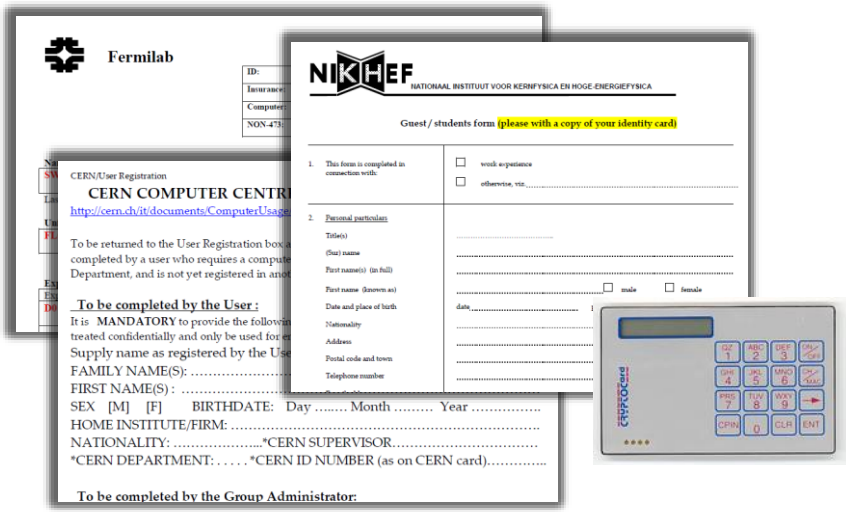
IGTF
Interoperable Global Trust Federation
AP | EU | TAG

FIM4R

WISE COMMUNITY

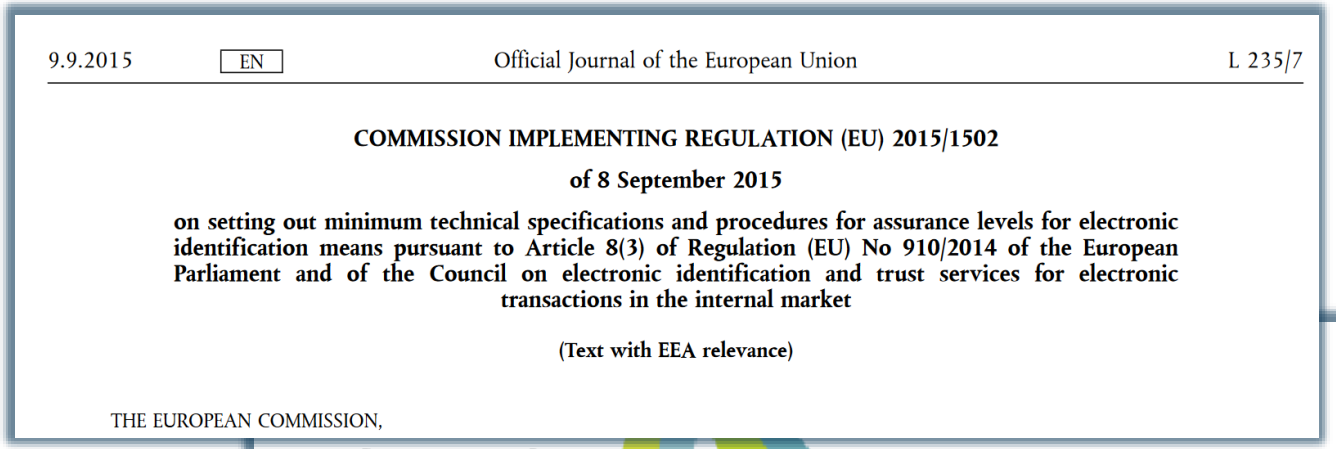


Policy and Best Practices Harmonisation



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

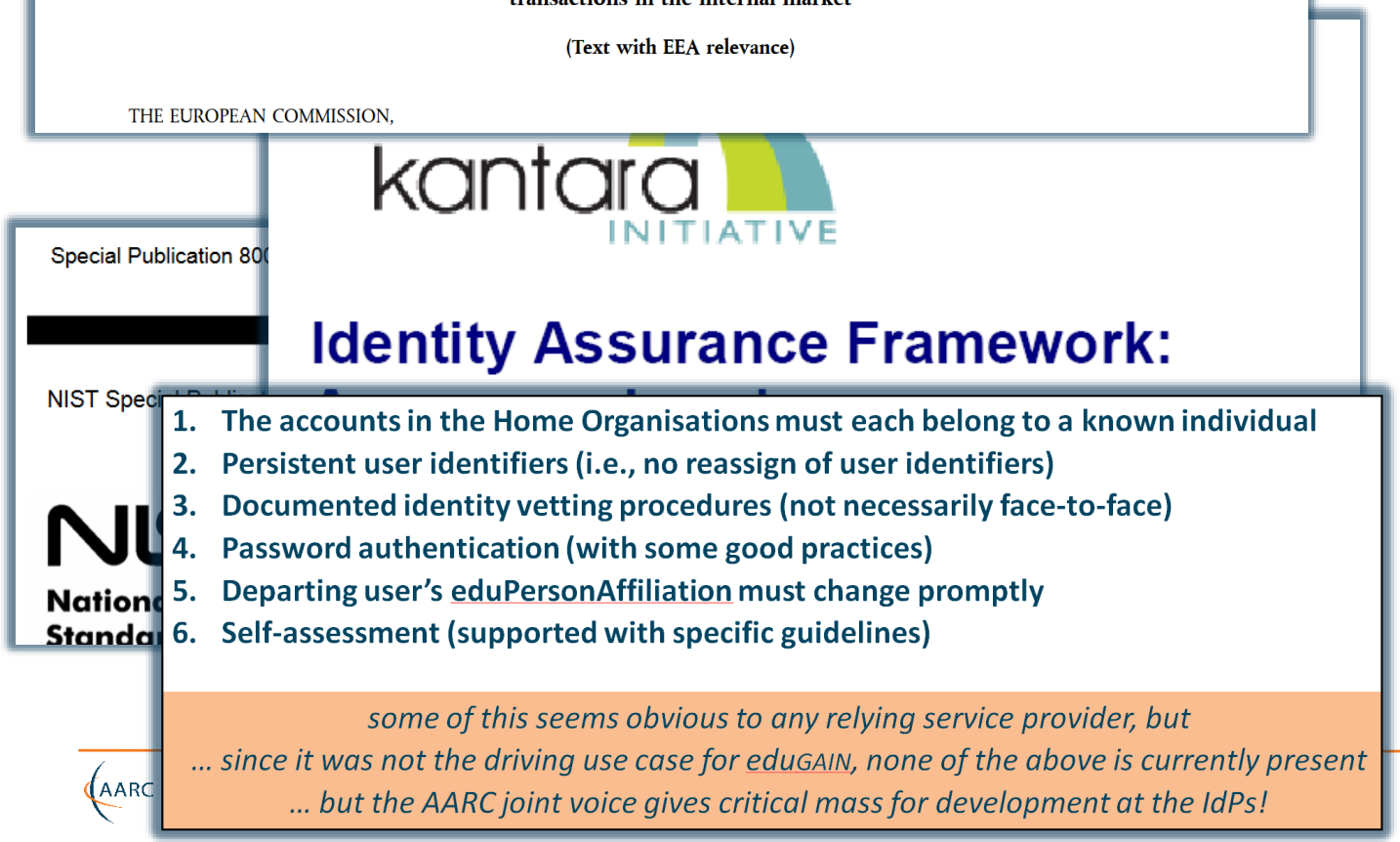
COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

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,



kantara INITIATIVE

Identity Assurance Framework:

Special Publication 80

NIST Speci

Nationa
Standa

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

generic e-Infrastructure services

access to common compute and data services that do not hold sensitive personal data

protection of sensitive resources

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

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

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

Mikael Linden’s work with the REFEDS Assurance WG, see also https://refeds.org/meetings/35th-meeting-may-2017

REFEDS assurance working group

- In 6/2016 REFEDS established the Assurance working group
  - Open to anyone to participate
  - Take AARC recommendation as input and extend it to a specification
  - International – participants from Europe&US
  - Cross-community – participants from federations & research communities

REFEDS Assurance Framework 1.0 draft
https://wiki.refeds.org/x/JwBYAQ
Exposed to a public consultation until 9th June 2017

REFEDS assurance fw: four dimensions of LoA

Identifiers

- ID is unique, personal and traceable
- ePPN is unique, personal and traceable

ID proofing

- Good enough for institution's local systems
- Assumed (e.g. postal credential delivery)
- Verified (e.g. F2F)

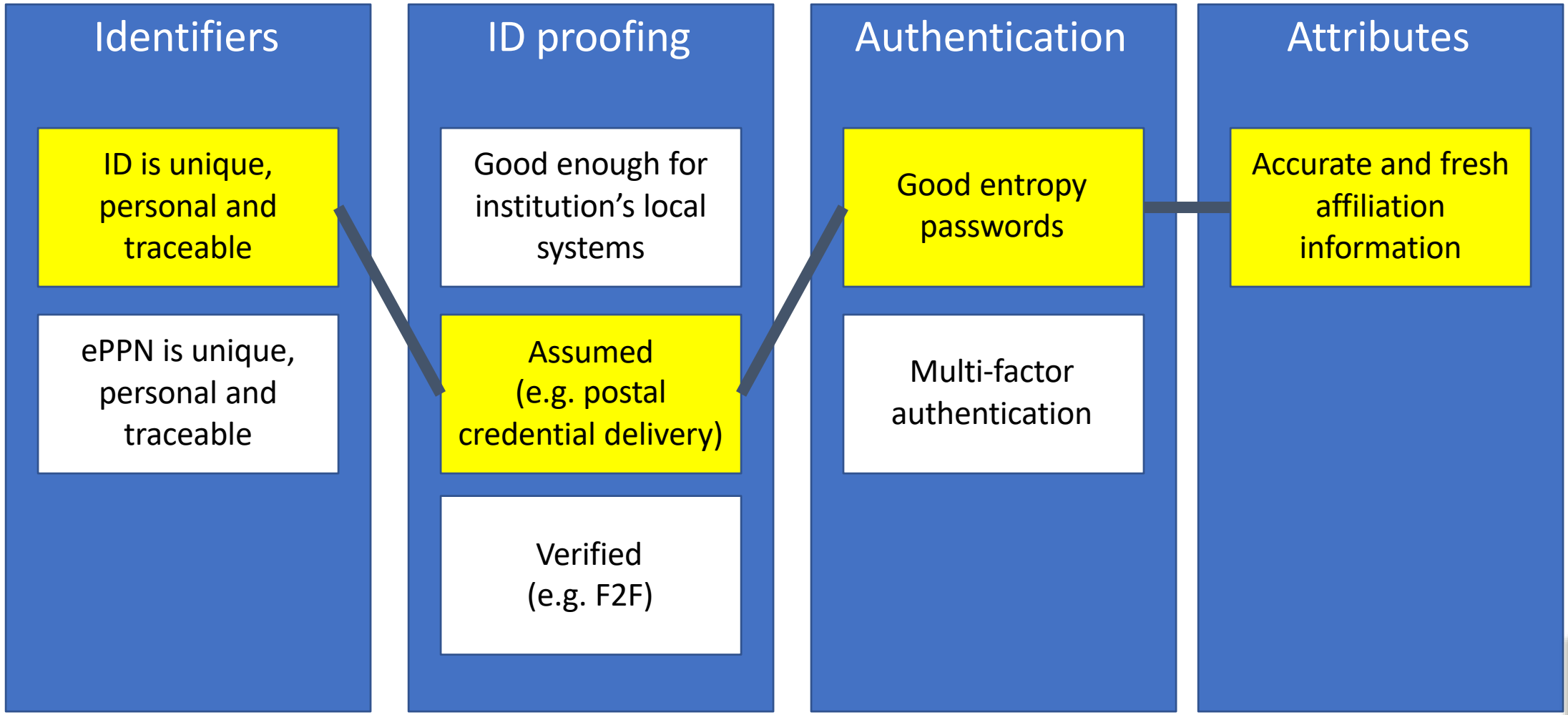
Authentication

- Good entropy passwords
- Multi-factor authentication

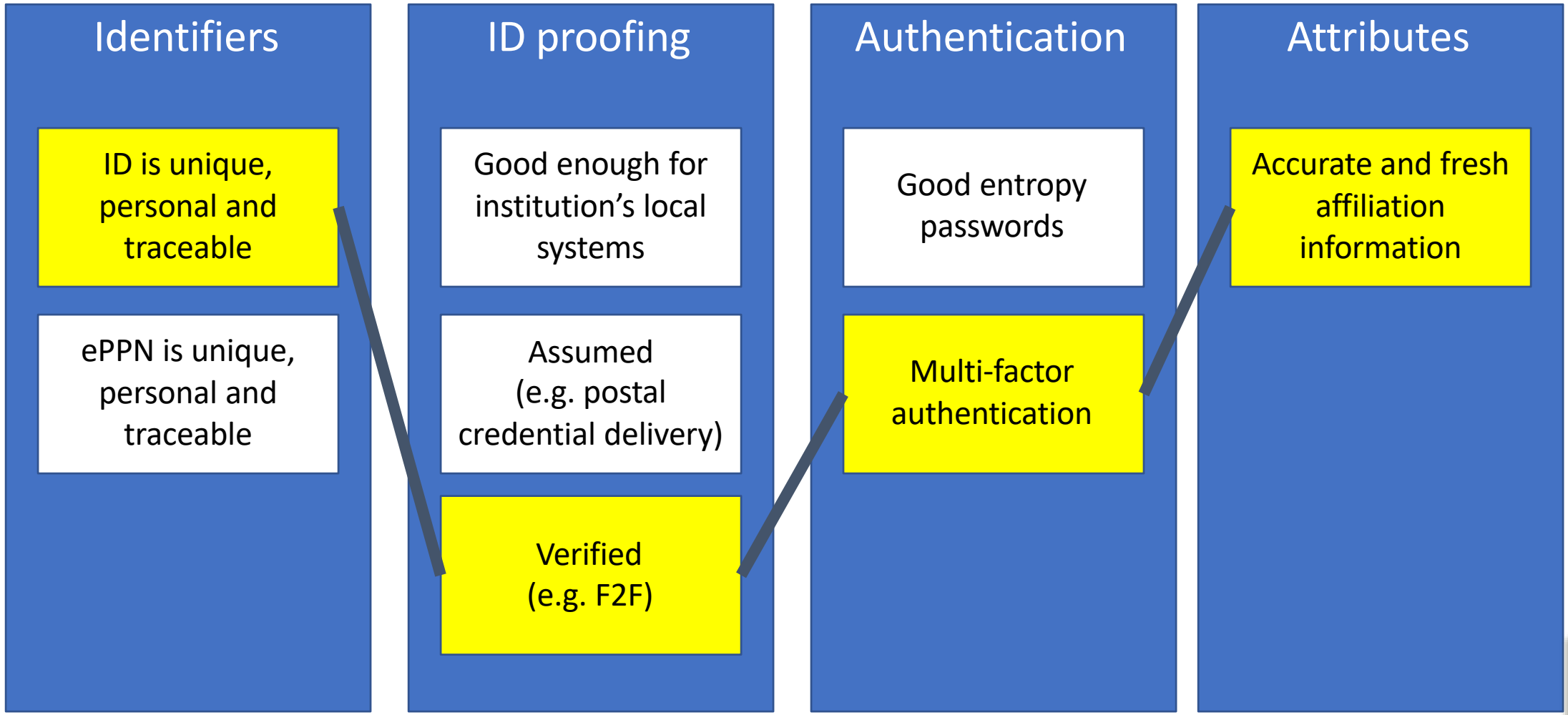
Attributes

- Accurate and fresh affiliation information

”Cappuccino” profile for low risk use cases



”Espresso” profile for demanding use cases



Representing the assurance profile on SAML 2.0

Value	eduPersonAssurance	AuthenticationContextClassRef	Metadata entity attribute
$PREFIX$			X
$PREFIX$/ID/unique	X		
$PREFIX$/ID/no-eppn-reassign	X		
$PREFIX$/ID/eppn-reassign-1y	X		
$PREFIX$/IAP/local-enterprise	X		
$PREFIX$/IAP/assumed	X		
$PREFIX$/IAP/verified	X		
$PREFIX$/AAP/good-entropy		X	
https://refeds.org/profile/mfa		X	
$PREFIX$/ATP/ePA-1m	X		
$PREFIX$/profile/cappuccino	X		X
$PREFIX$/profile/espresso	X		X

Public consultation

REFEDS Assurance Framework 1.0 draft
https://wiki.refeds.org/x/JwBYAQ
Exposed to a public consultation until 9th June 2017

For more information

- See the REFEDS assurance framework infoshare 24 May: goo.gl/HFNyXd

Policy and Best Practices Harmonisation

Security Incident Response

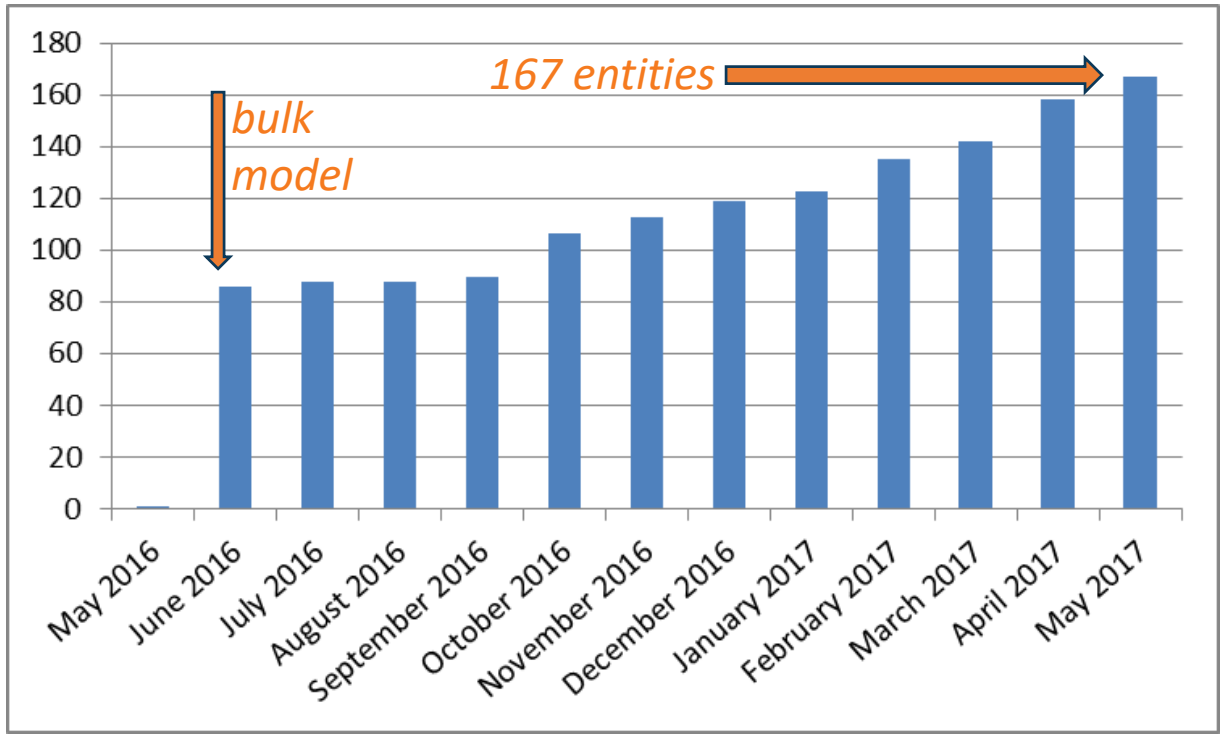
Sirtfi - supporting our federated respons to security incidents

SIRTFI
Security Incident Response Trust Framework for Federated Identity

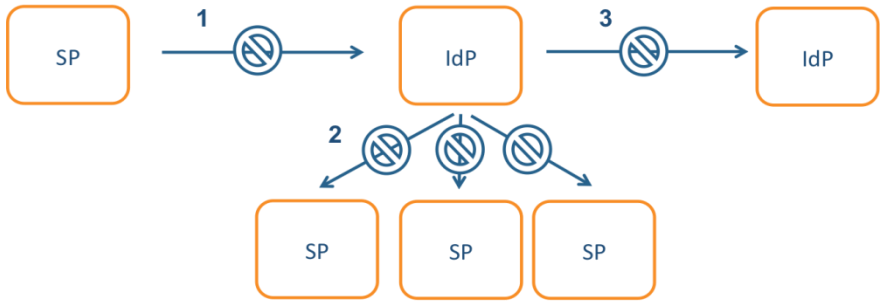
- Adds security contact meta-data in eduGAIN
- namespace for Sirtfi Assurance at IANA
- with R&S specification:
  meets **baseline assurance requirements**
  and IGTF “assured identifier trust”

Security Incident Response Trust Framework for Federated Identity

You cannot have missed it …
… even used in CyberOps role play exercises



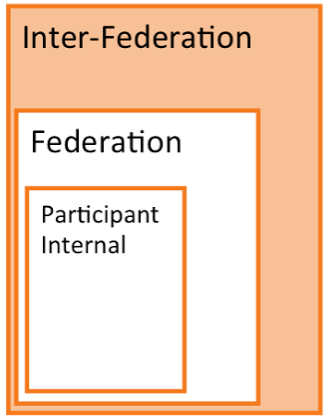
Incident response process evolution in federations



Incident Response Communication, communication blocks

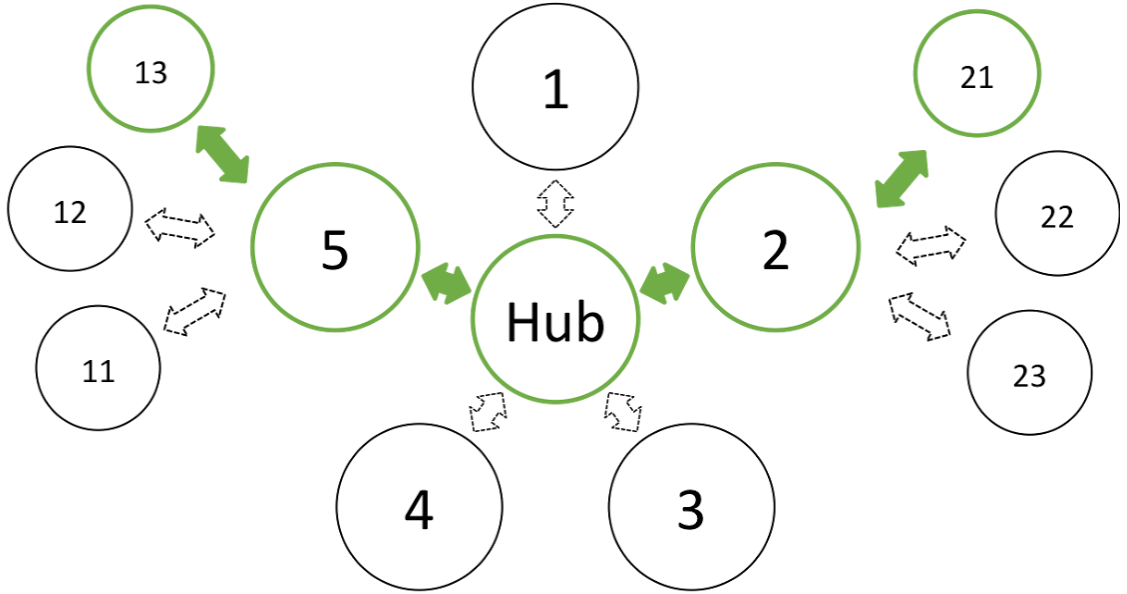
Challenges

- 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

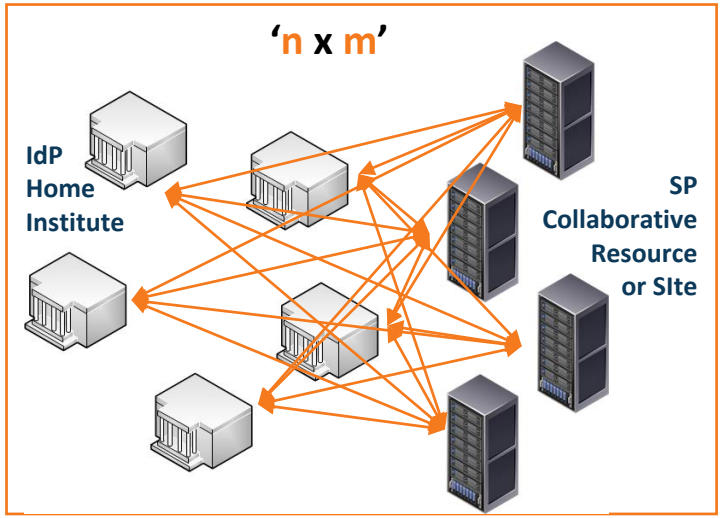
Develop policies models for SP-IdP Proxy – IdPs to SPs

- 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

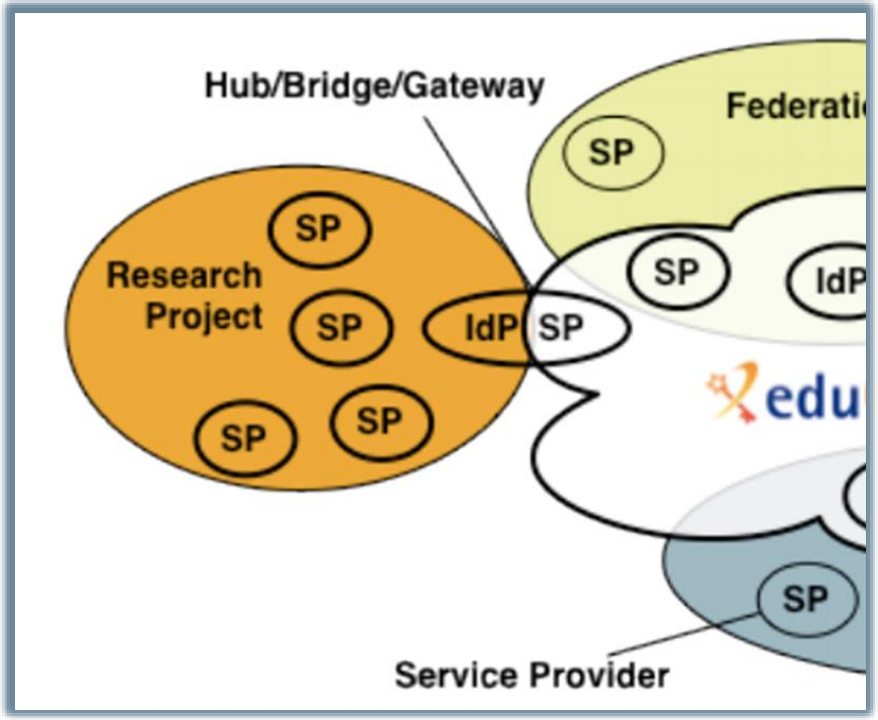
and

- 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 (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

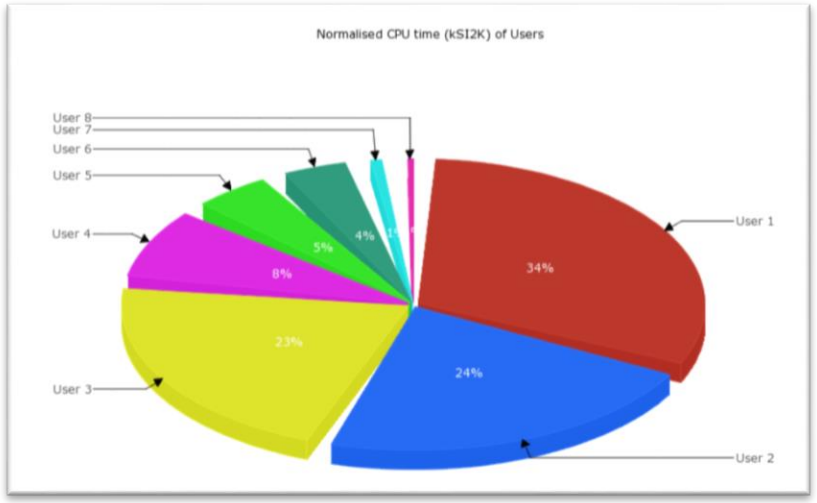
Leverage entity categories and assurance profiles

- 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

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	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 (1)'s work**

** 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 – identify need and the parties involved

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


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

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?

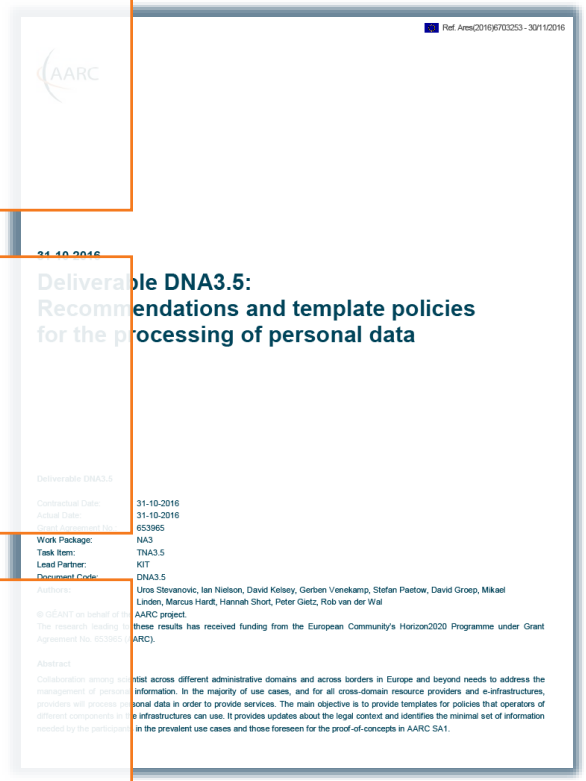
- Global sharing in controlled communities appears attractive
- Uncertainly about requirements (governing body) and timing (> Mar 2018) are not helpful for adoption today … just yet
- Ongoing work: text needs to allow for (community) attribute authorities

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

© GÉANT on behalf of the AARC project.

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

Abstract

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

Policy and Best Practices Harmonisation

Recommendation for sustainable services and models

Recommendations for Research and e-Infrastructures to Build Sustainable Services

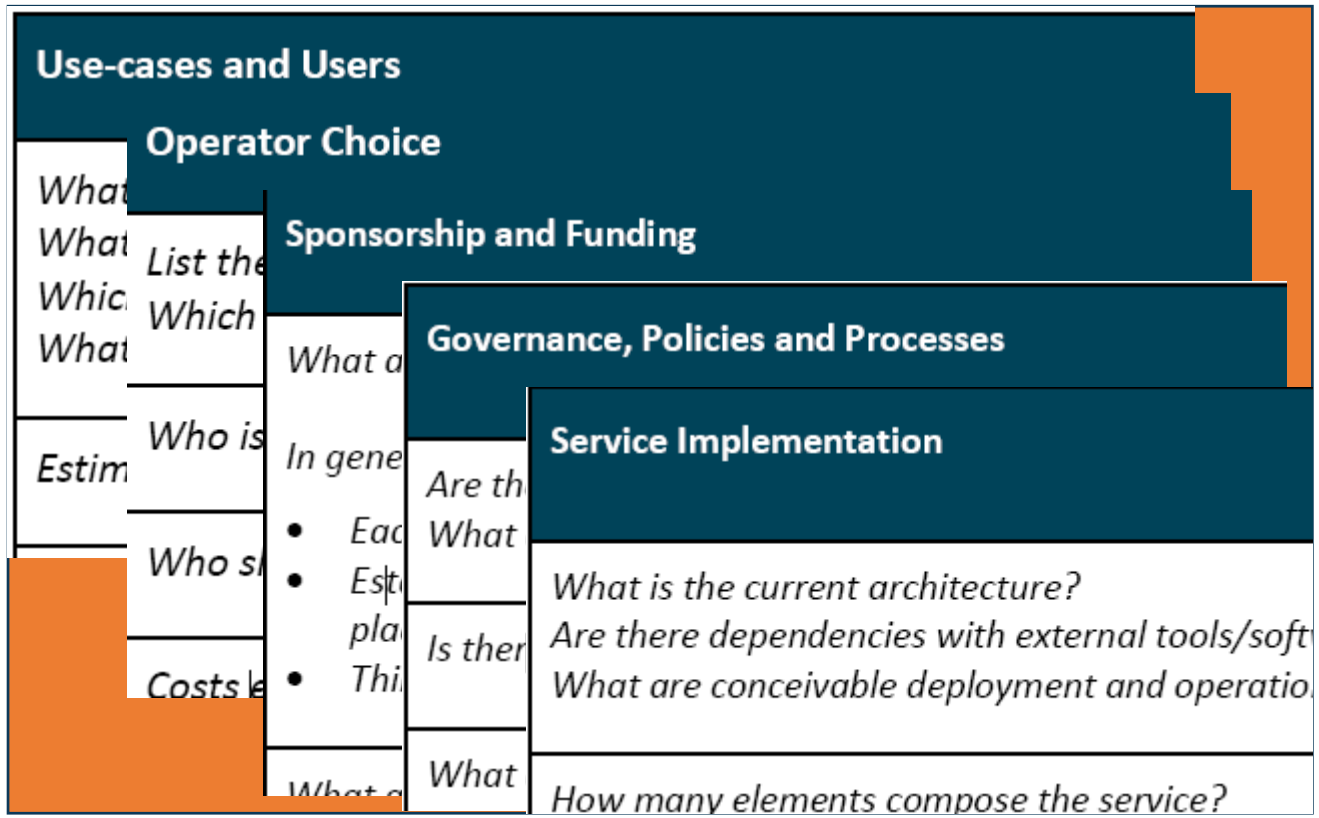
'Investigate terms of (AAI) usage for delivering services'

> 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

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

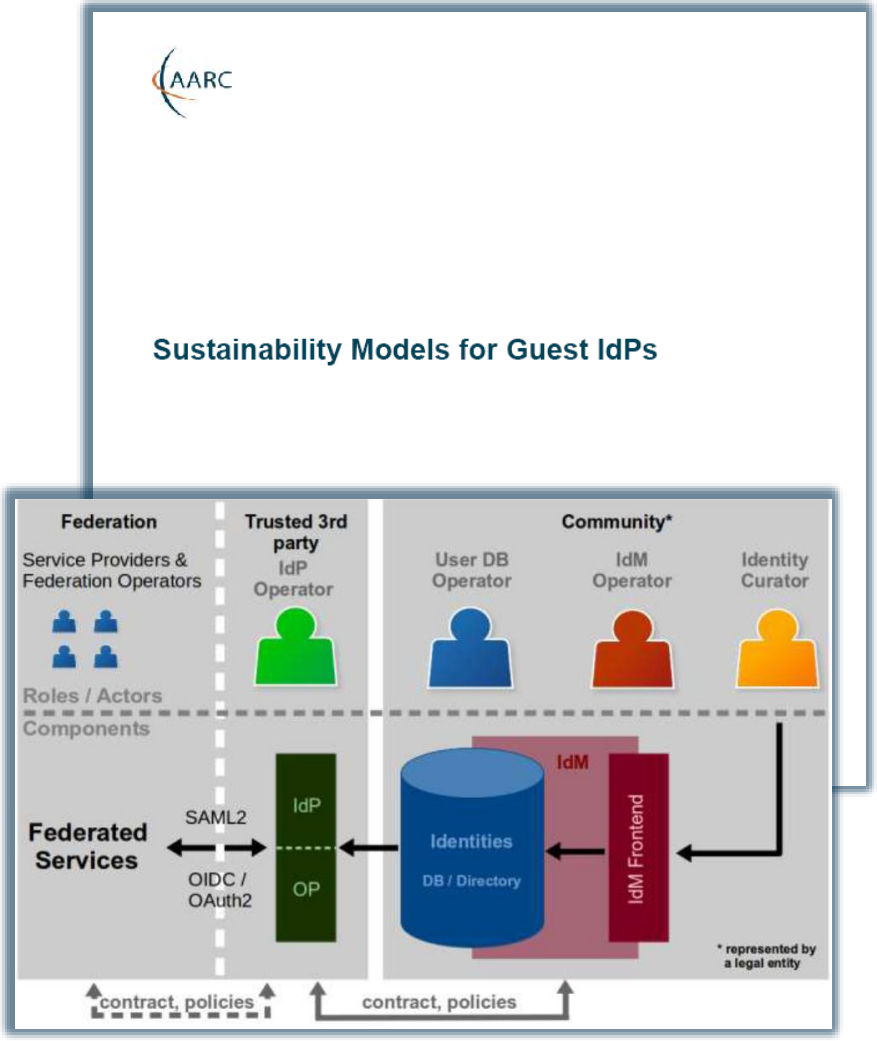
Guest IdPs are critical to almost all collaboration use cases

➢ *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

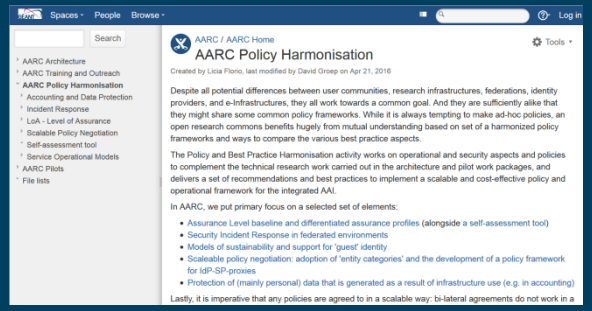
Policy and Best Practices Harmonisation

Pulling it all together

So where are we now?

- 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**

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



Thank you

Any Questions?

davidg@nikhef.nl

AARC

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. 730941 (AARC2).