AARC Authentication and Authorisation for Research and Collaboration

Policy and Best Practice Harmonisation (‘NA3’)

from the present to the future

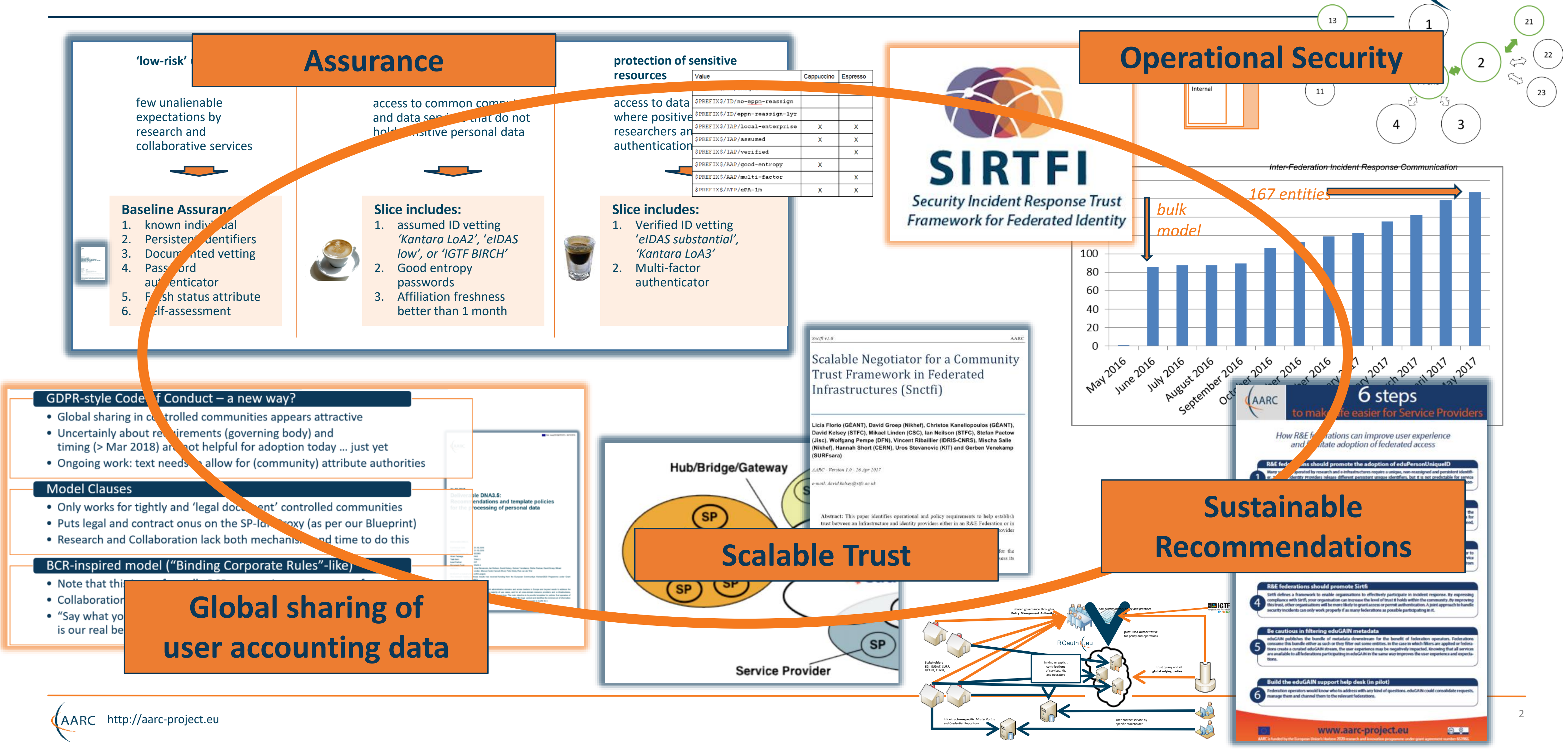
David Groep

NA3 activity coordinator

Nikhef

AARC2 Kick-Off meeting
6 – 8 June, 2017
Bad Herrenalb, Baden Württemberg, DE

From ‘the past’ …



Assurance

‘low-risk’

few unalienable expectations by research and collaborative services

Baseline Assuran

1. known indiv dual
2. Persisten identifiers
3. Docum nted vetting
4. Pass ord au enticator
5. F sh status attribute
6. elf-assessment

access to common comp and data ser that do not hold sitive 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 where positive researchers an authentication

Slice includes:

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

Value	Cappuccino	Espresso
[illegible]		
`$PREFIX$/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

Operational Security

SIRTFI

Security Incident Response Trust Framework for Federated Identity

Global sharing of user accounting data

GDPR-style Code f Conduct – a new way?

- Global sharing in c trolled communities appears attractive
- Uncertainly about re irements (governing body) and timing (> Mar 2018) ar ot helpful for adoption today … just yet
- Ongoing work: text needs allow for (community) attribute authorities

Model Clauses

- Only works for tightly and ‘legal doc ent’ controlled communities
- Puts legal and contract onus on the SP-Id oxy (as per our Blueprint)
- Research and Collaboration lack both mechanis nd time to do this

BCR-inspired model (“Binding Corporate Rules”-like)

- Note that thi
- Collaboratio
- “Say what yo is our real be

Delivera ble DNA3.5: Recomm endations and template policies for the p rocessing of personal data

Scalable Trust

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 rovider for the sess its

shared governance through a Policy Management Authority
non-discrimination and practices
IGTF
Joint PMA authoritative for policy and operations
RCauth.eu
Stakeholders EGI, EUDAT, SURF, GÉANT, ELIXIR, ...
in-kind or explicit contributions of services, kit, and operators
trust by any and all global relying parties
Infrastructure-specific Master Portals and Credential Repository
user contact service by specific stakeholder

Sustainable Recommendations

6 steps to mak fe easier for Service Providers

How R&E fe rations can improve user experience and f itate adoption of federated access

1. **R&E fed ns should promote the adoption of eduPersonUniqueID** — Many s perated by research and e-infrastructures require a unique, non-reassigned and persistent identifier. T identity Providers release different persistent unique identifiers, but it is not predictable for service
4. **R&E federations should promote Sirtfi** — Sirtfi defines a framework to enable organisations to effectively participate in incident response. By expressing compliance with Sirtfi, your organisation can increase the level of trust it holds within the community. By improving this trust, other organisations will be more likely to grant access or permit authentication. A joint approach to handle security incidents can only work properly if as many federations as possible participating in it.
5. **Be cautious in filtering eduGAIN metadata** — eduGAIN publishes the bundle of metadata downstream for the benefit of federation operators. Federations consume this bundle either as such or they filter out some entities. In the case in which filters are applied or federations create a curated eduGAIN stream, the user experience may be negatively impacted. Knowing that all services are available to all federations participating in eduGAIN in the same way improves the user experience and expectations.
6. **Build the eduGAIN support help desk (in pilot)** — Federation operators would know who to address with any kind of questions. eduGAIN could consolidate requests, manage them and channel them to the relevant federations.

www.aarc-project.eu

AARC is funded by the European Union's Horizon 2020 research and innovation programme under grant agreement number 653965.

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

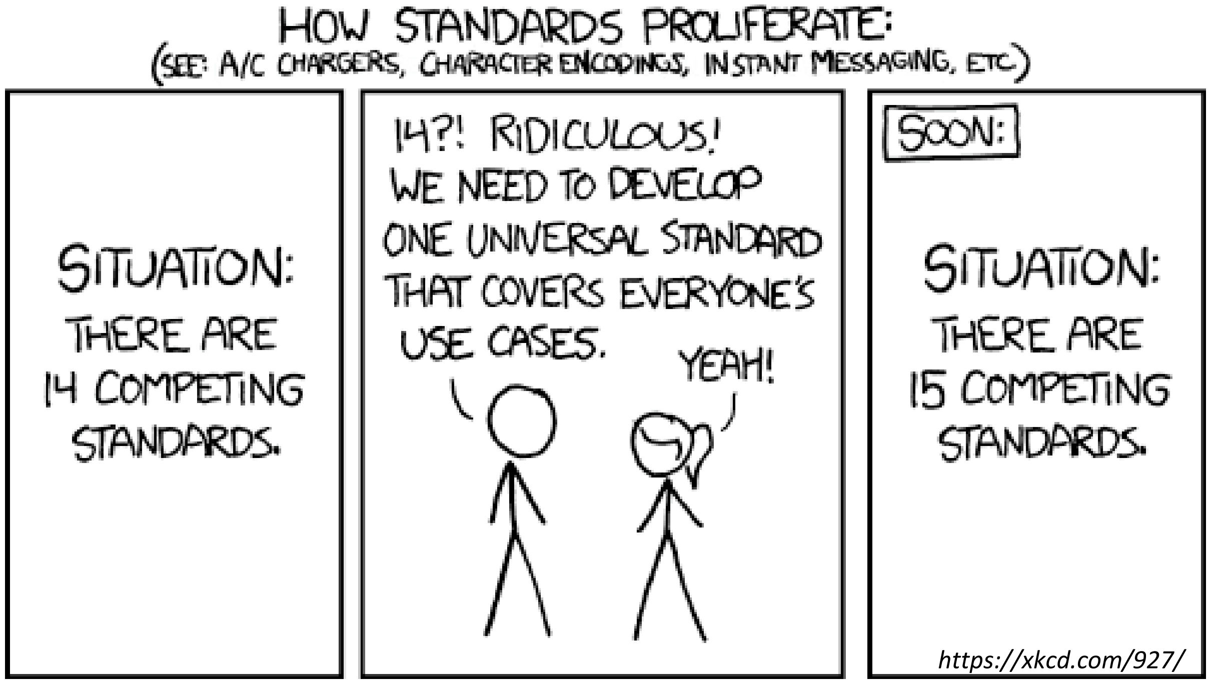
✓ Use **pre-existing groups and communities** to develop policies and harmonise practices and thus **avoid AARC becoming yet another island**

REFEDS

IGTF
Interoperable Global Trust Federation
AP | EU | TAG

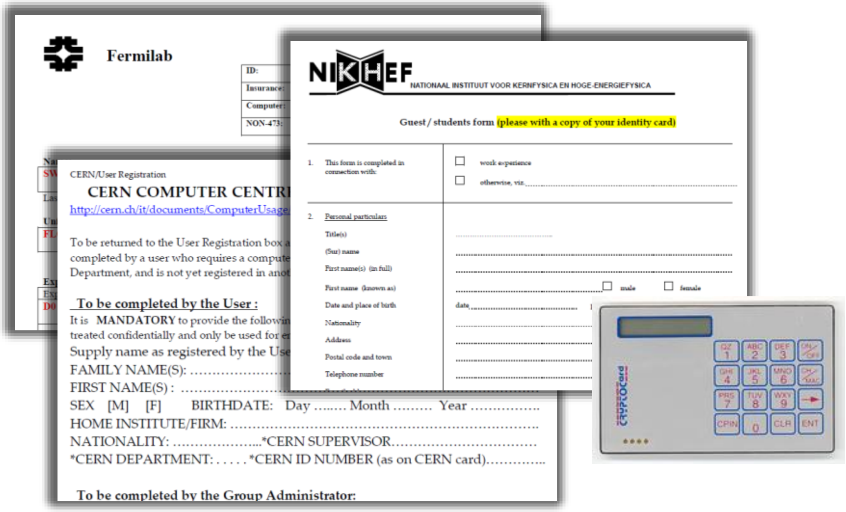
FIM$_4$R

WISE
COMMUNITY


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

https://xkcd.com/927/

Policy and Best Practices Harmonisation



Fermilab

ID:
Insurance:
Computer:
NON-473:

CERN/User Registration

CERN COMPUTER CENTR

http://cern.ch/it/documents/ComputerUsage

To be returned to the User Registration box a
completed by a user who requires a compute
Department, and is not yet registered in anot

To be completed by the User :

It is MANDATORY to provide the followin
treated confidentially and only be used for e
Supply name as registered by the Use
FAMILY NAME(S): ……………………
FIRST NAME(S) : ……………………
SEX [M] [F] BIRTHDATE: Day …..… Month ……… Year …………….
HOME INSTITUTE/FIRM: ……………………………………………………………
NATIONALITY: ………………..*CERN SUPERVISOR…………………………
*CERN DEPARTMENT: . . . . . *CERN ID NUMBER (as on CERN card)…………..

To be completed by the Group Administrator:

NIKHEF NATIONAAL INSTITUUT VOOR KERNFYSICA EN HOGE-ENERGIEFYSICA

Guest / students form (please with a copy of your identity card)

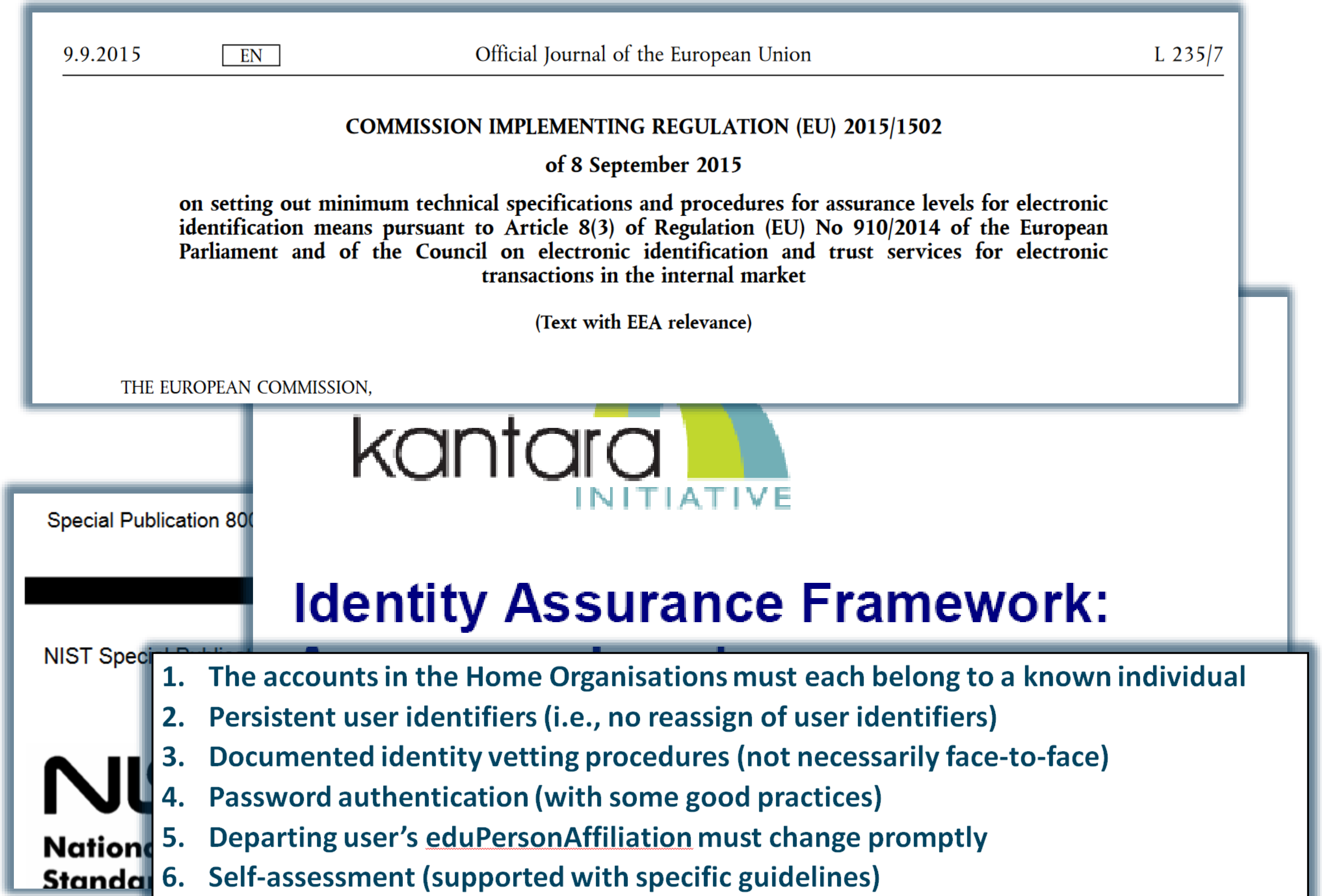
1. This form is completed in connection with: □ work experience
□ otherwise, viz. ……………………………

2. Personal particulars

Title(s) ……………
(Sur) name ……………………………
First name(s) (in full) ……………………………
First name (known as) …………………… □ male □ female
Date and place of birth date ……………………
Nationality ……………………
Address ……………………
Postal code and town ……………………
Telephone number ……………………

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

NI

Nation
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

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

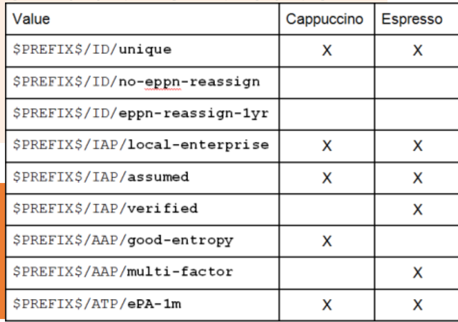
protection of sensitive resources

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

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



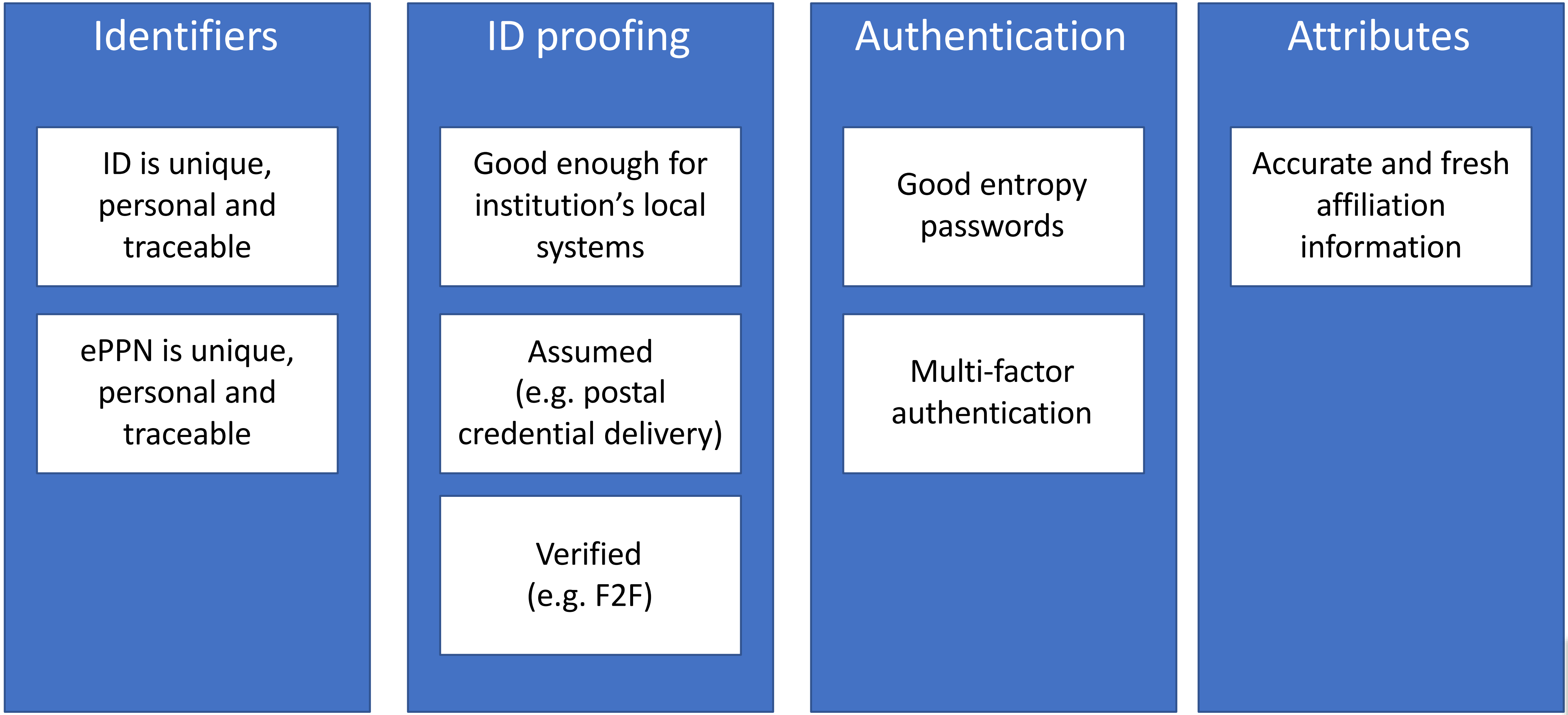
Value	Cappuccino	Espresso
$PREFIX$/ID/unique	X	X
$PREFIX$/ID/no-eppn-reassign		
$PREFIX$/ID/eppn-reassign-1yr		
$PREFIX$/IAP/local-enterprise	X	X
$PREFIX$/IAP/assumed	X	X
$PREFIX$/IAP/verified		X
$PREFIX$/AAP/good-entropy	X	
$PREFIX$/AAP/multi-factor		X
$PREFIX$/ATP/ePA-1m	X	X

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)

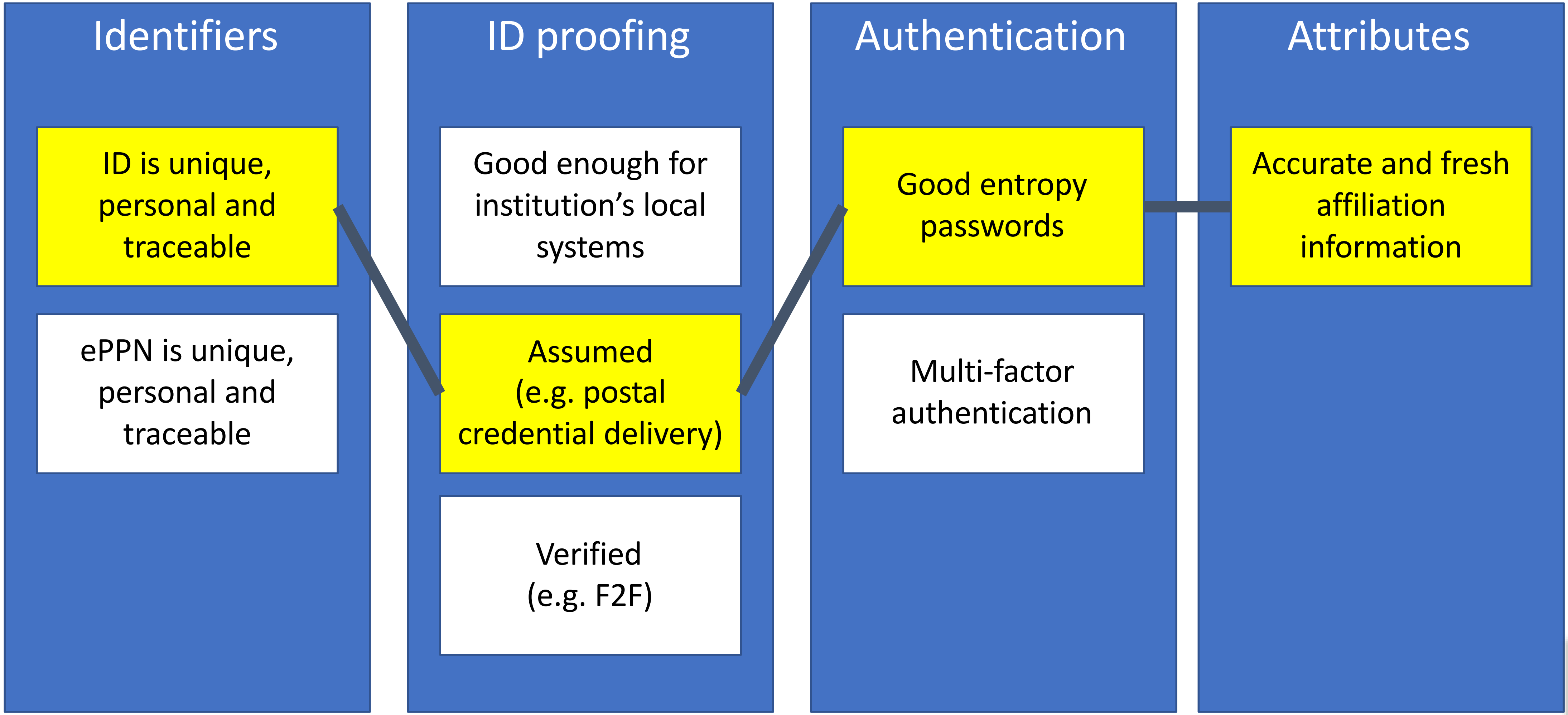
Authentication

- Good entropy passwords
- Multi-factor authentication

Attributes

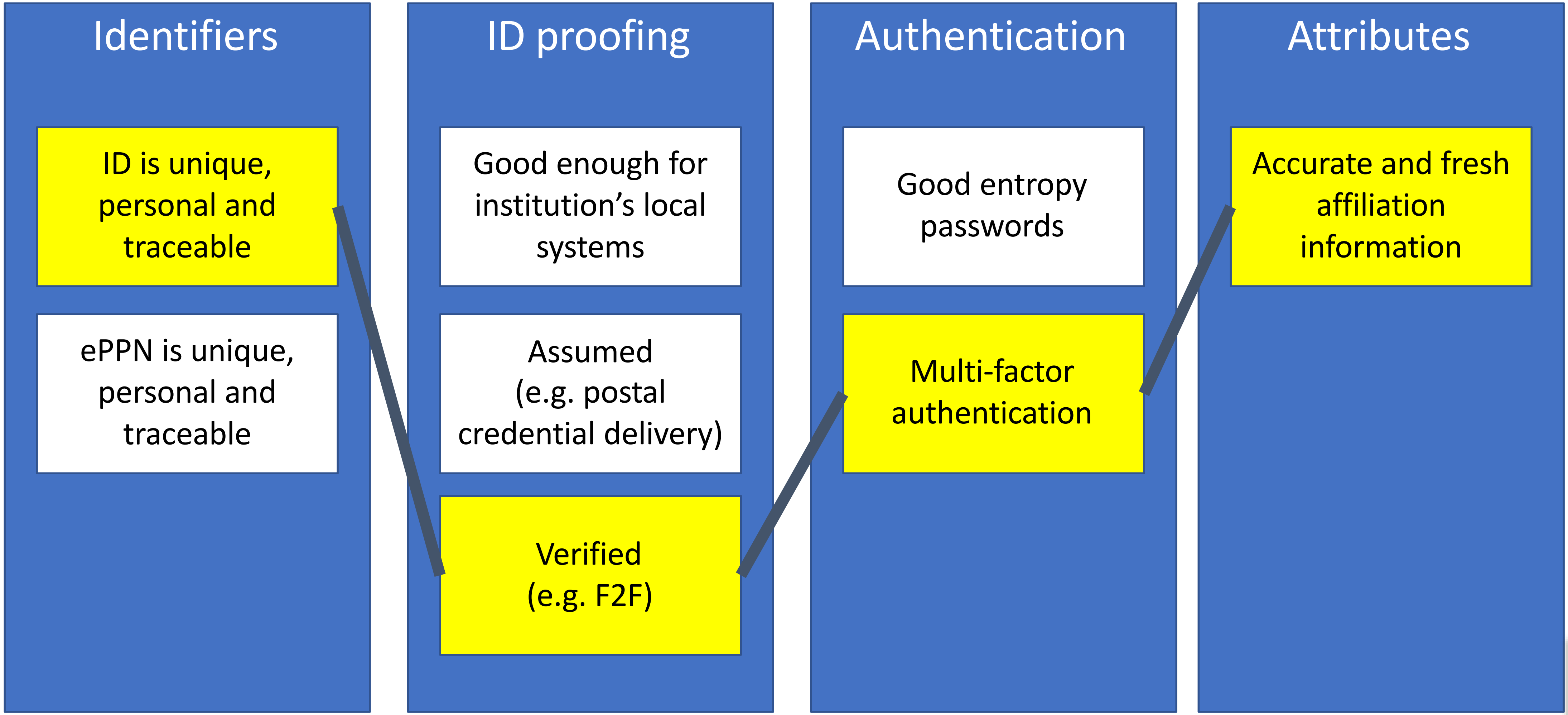
- Accurate and fresh affiliation information

”Cappuccino” profile for low risk use cases



Identifiers	ID proofing	Authentication	Attributes
ID is unique, personal and traceable	Good enough for institution’s local systems	Good entropy passwords	Accurate and fresh affiliation information
ePPN is unique, personal and traceable	Assumed (e.g. postal credential delivery)	Multi-factor authentication	
	Verified (e.g. F2F)		

”Espresso” profile for demanding use cases



Identifiers	ID proofing	Authentication	Attributes
ID is unique, personal and traceable	Good enough for institution’s local systems	Good entropy passwords	Accurate and fresh affiliation information
ePPN is unique, personal and traceable	Assumed (e.g. postal credential delivery)	Multi-factor authentication	
	Verified (e.g. F2F)		

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

Site 20 has 7 bots.

+1 bot at Site 21
Site 21 has 5 bots.

+1 bot at Site 22
Site 22 has 7 bots.

+1 bot at Site 33
Site 33 has 5 bots.

-2 bots at Site 1
Site 1 has 1 bot.

-2 bots at Site 3
Site 3 has 3 bots.

-2 bots at Site 4
Site 4 has 3 bots.

-1 bot at Site 5
Site 5 has 4 bots.

-1 bot at Site 7
Site 7 has 3 bots.

-1 bot at Site 10
Site 10 has 3 bots.

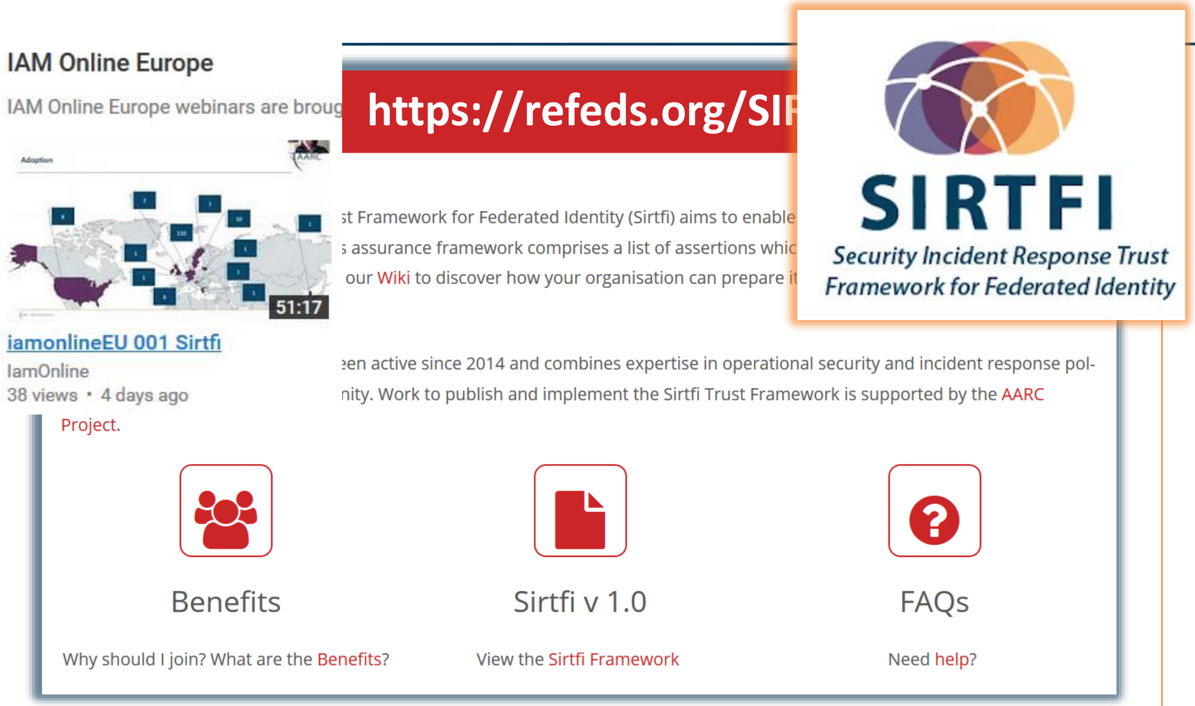
-1 bot at Site 12
Site 12 has 1 bot.

```
comment doe not go to the customers (sites) reply will also cc the site, lnlxon: right?
ti: I'm trying to follow the incident on RTIR, I don't like very much the emails in these cases
s Triantafyllidis: in RT (i guess the same applies for RTIR) Comment goes to owner + AdminCC while Reply goes to them + Requestor
thanks christos
sec5 pakiti: thanks a lot to Michal and Daniel
ti: Requestor = Correspondents ??
s Triantafyllidis: hm… yes
ti: ok, thanks
```

Command & Control service killed...

Security Incident Response

Sirtfi - supporting our federated respons to security incidents



IAM Online Europe

IAM Online Europe webinars are broug

51:17

iamonlineEU 001 Sirtfi

IamOnline

38 views • 4 days ago

https://refeds.org/SIR

SIRTFI

Security Incident Response Trust Framework for Federated Identity

st Framework for Federated Identity (Sirtfi) aims to enable s assurance framework comprises a list of assertions whic our Wiki to discover how your organisation can prepare it

een active since 2014 and combines expertise in operational security and incident response pol- nity. 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

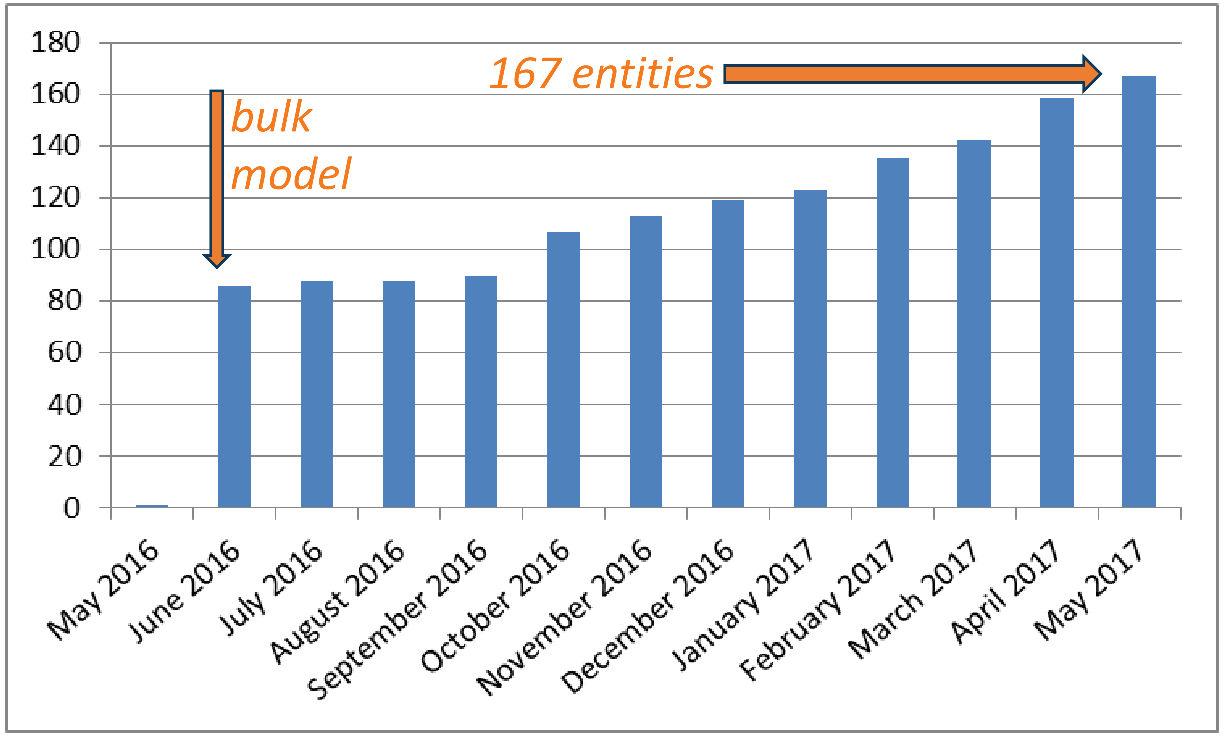
FAQs

Need help?

Security Incident Response Trust Framework for Federated Identity

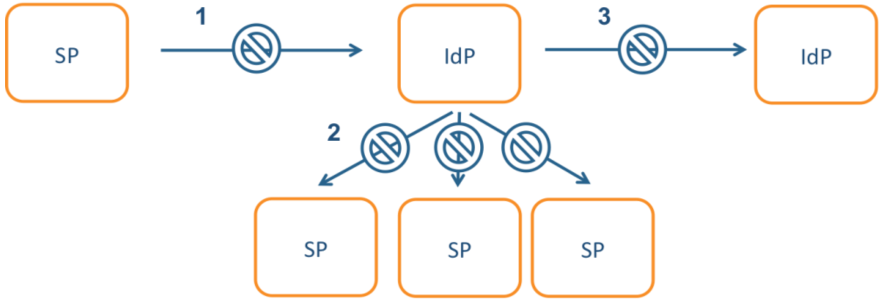
You cannot have missed it …

… even used in CyberOps role play exercises



- 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”

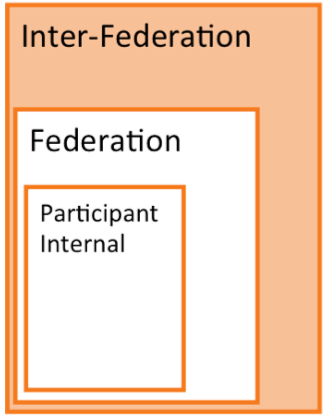
Incident response process evolution in federations



Incident Response Communication, communication blocks

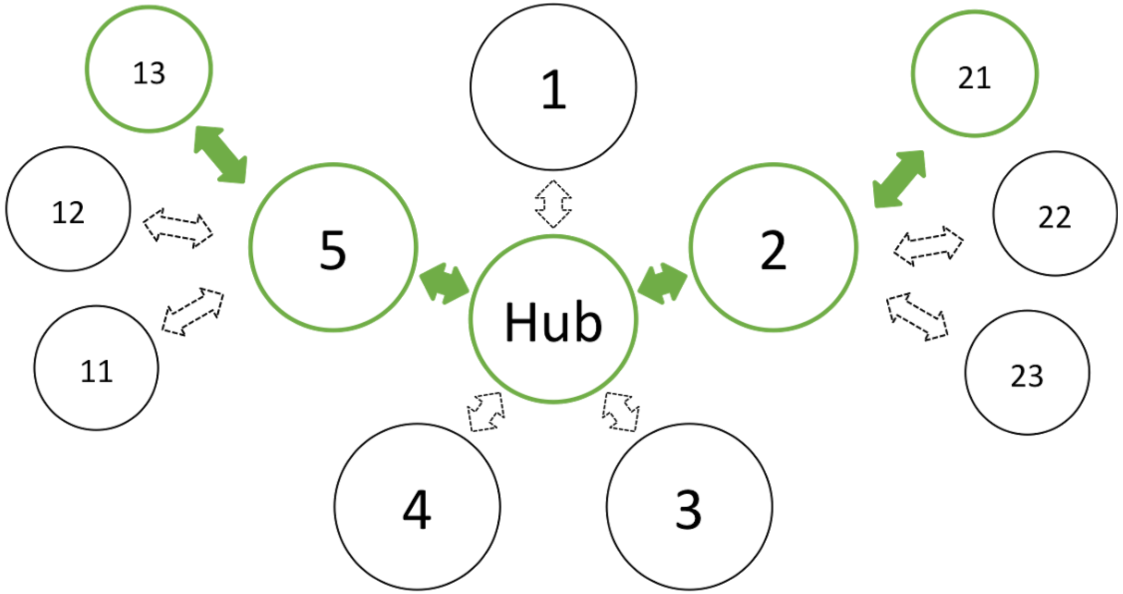
Challenges

- 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

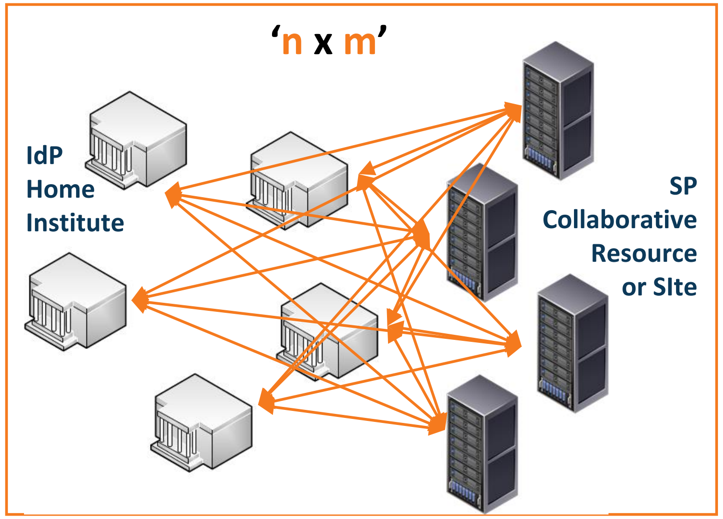
Develop policies models for SP-IdP Proxy – IdPs to SPs

- 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)

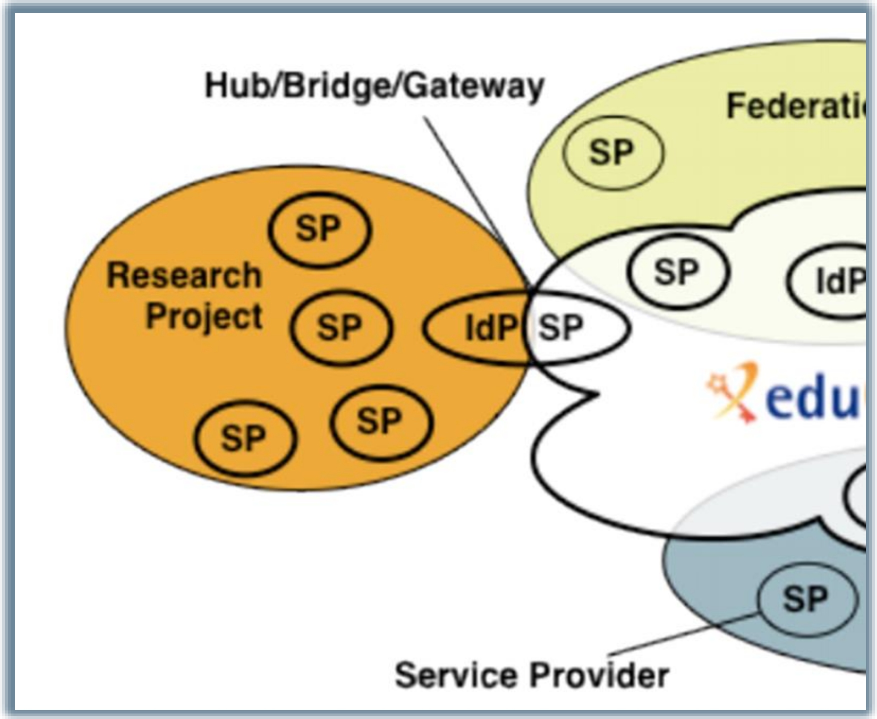
Licia Florio (GÉANT), David Groep (Nikhef), Christos Kanellopoulos (GÉANT), David Kelsey (STFC), Mikael Linden (CSC), Ian Neilson (STFC), Stefan Paetow (Jisc), Wolfgang Pempe (DFN), Vincent Ribaillier (IDRIS-CNRS), Mischa Salle (Nikhef), Hannah Short (CERN), Uros Stevanovic (KIT) and Gerben Venekamp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

RCauth.eu

RCAUTH Home

RCAUTH Pilot ICA

Policy

Privacy Statement

Comments to [illegible]

Website hosted by Nikhef

Last updated May 6, 2016

News as of 5 June, 2016

version 0.07 of policy accredited by IGTF

Sustainability model study

The white-label Research and Collaboration Authentication CA Service for Europe

The RCauth Pilot ICA G1 CA issues certificates to end-entities based on a successful authentication to a Federated Identity Management System (FIMS) operated by an eligible Registration Authority - typically a FIMS Identity Provider (IdP) operated by an academic or research organisation. The certificates issued by the RCauth Pilot ICA G1 CA are valid for a period of at most 13 months, but may be as short as 1Ms.

The certificates for use in science, research, and innovation, specifically for the purpose of (cross-organisational) distributed resource access, solely in the context of academic and research and similar, not-commercially competitive, applications.

The RCauth Pilot ICA G1 certificates are primarily intended for the practitioners of scientific research that are supported enabled by or work in collaboration with the EC co-funded project on Authentication and Authorisation for Research and Collaboration AARC, and its successor, ancillary, collaborating, and affiliated projects, infrastructures, communities and endeavours, appropriately taking into account the global nature of research and collaboration.

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
Previous policies		

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

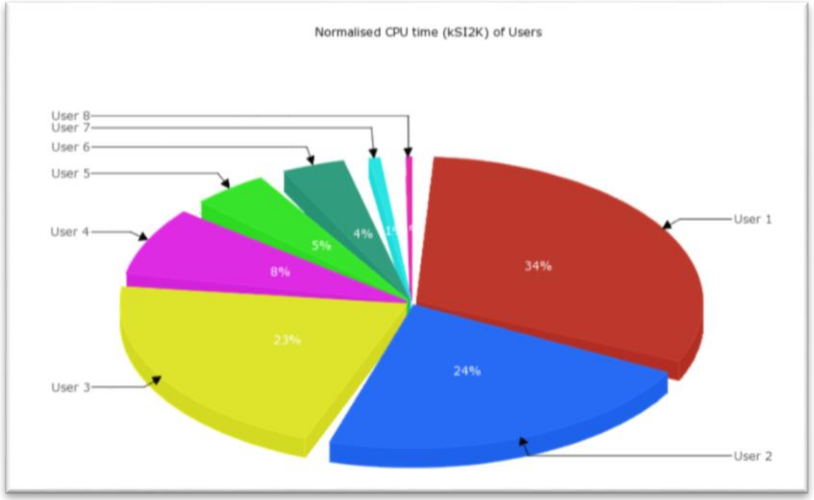
- For cross-infrastructure services, peer review and accreditation significantly helps adoption

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



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

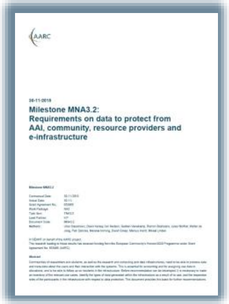
Personal data processing in accounting & collaboration

- *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 (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



30-11-2018

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

[illegible]

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?

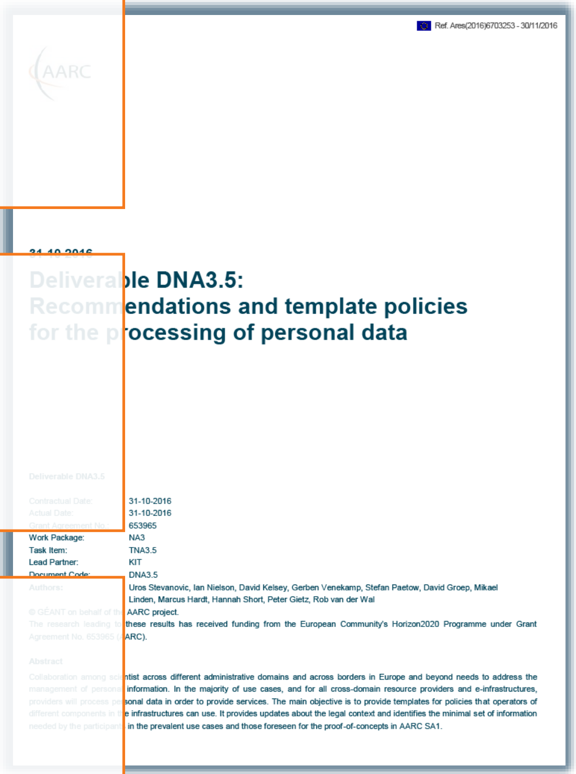
- Global sharing in controlled communities appears attractive
- Uncertainly about requirements (governing body) and timing (> Mar 2018) are not helpful for adoption today … just yet
- Ongoing work: text needs to allow for (community) attribute authorities

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

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, 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

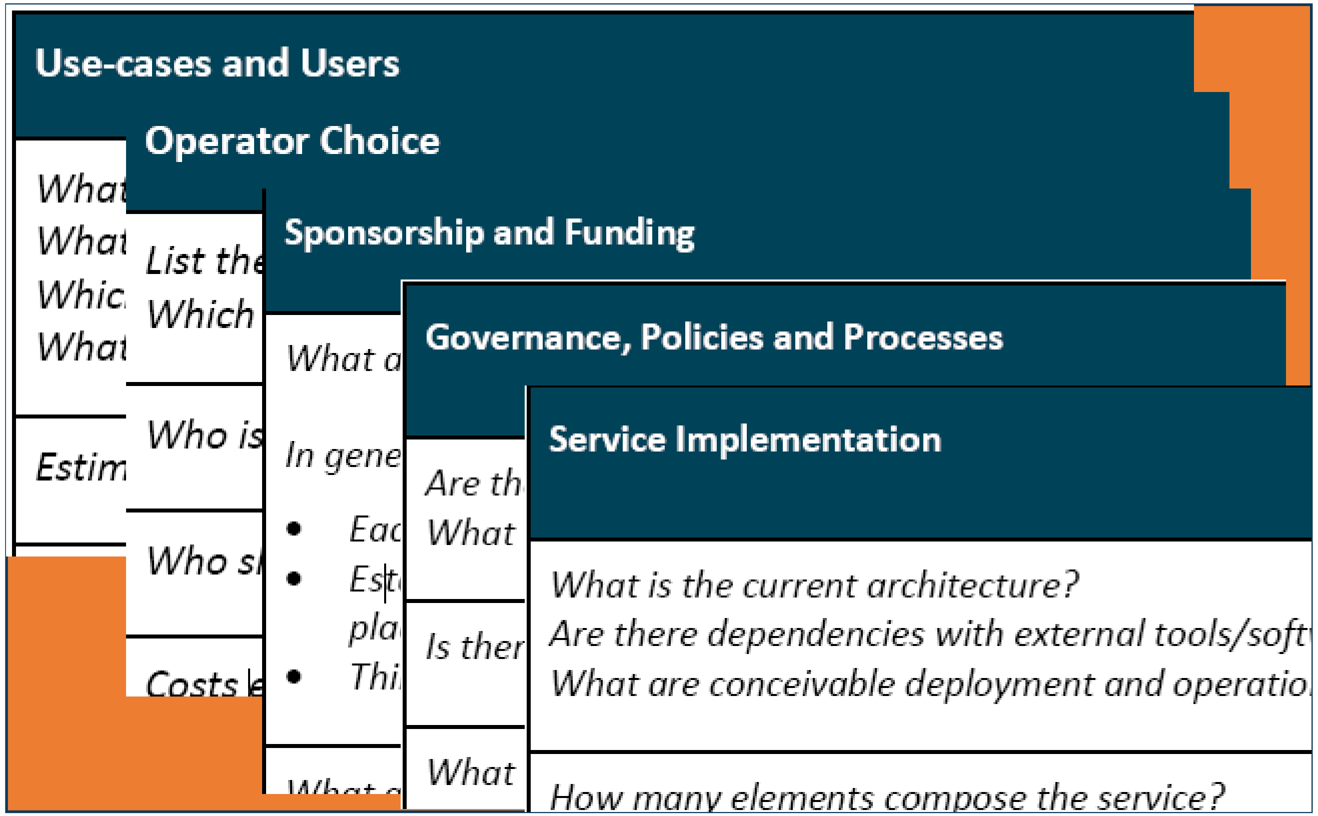
'Investigate terms of (AAI) usage for delivering services'

> 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



Use-cases and Users

What
What
Whic
What
Estim

Operator Choice

List the
Which
Who is
Who sl
Costs l

Sponsorship and Funding

What a
In gene
- Eac
- Est
pla
- Thi

What a

Governance, Policies and Processes

Are th
What
Is ther
What

Service Implementation

What is the current architecture?
Are there dependencies with external tools/soft
What are conceivable deployment and operatio

How many elements compose the service?

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

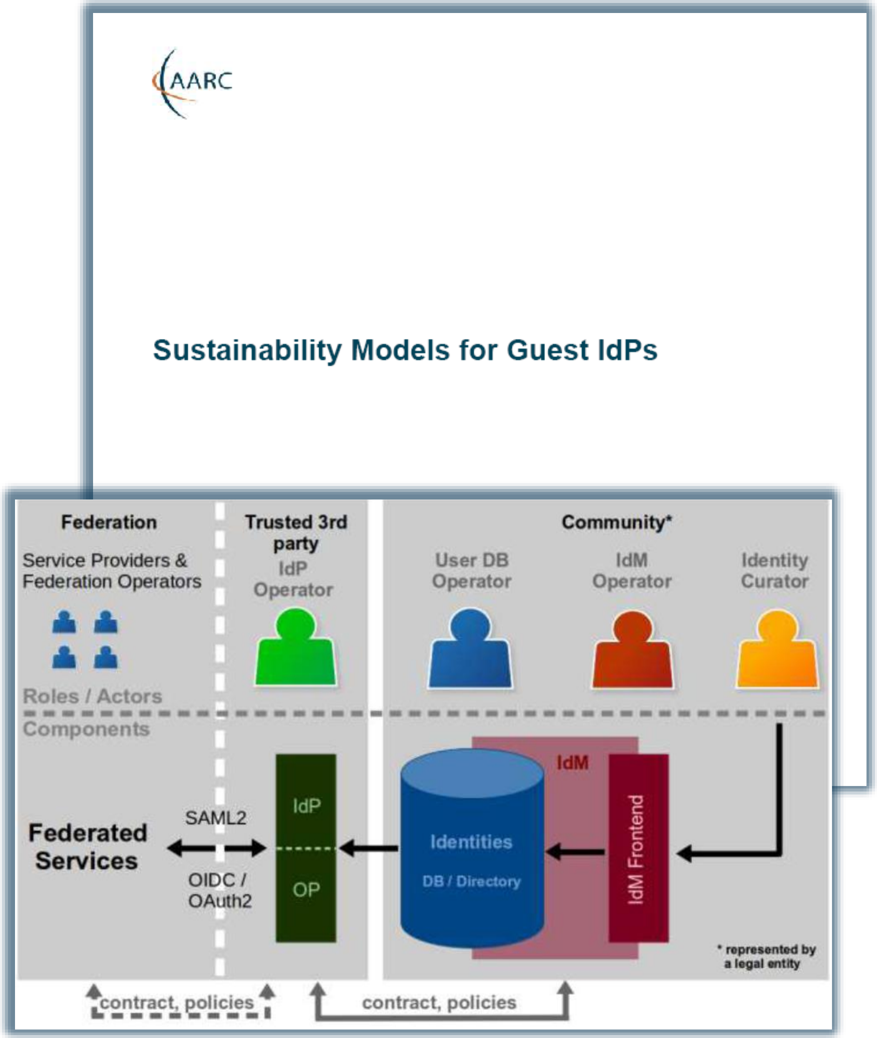
Guest IdPs are critical to almost all collaboration use cases

➢ *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*



Sustainability Models for Guest IdPs

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**

We want AARC t[wo]o!

Moving on from here …

… yet there's a lot to do still!

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 CoCo models for sharing necessary information, and meet policy needs for SP-IdP Proxies, repositories and translators

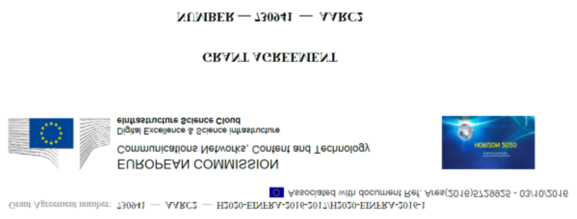
e-Researcher-Centric Policies

- 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

Our high-level (programme) objectives



Development of a pan-European identity federation, interoperable at global level

- Leverage eduGAIN plus Infrastructures – using global mechanisms (WISE, IGTF, FIM4R, REFEDS)

Stimulate … to manage and share their resources

- Ease movement of users and data across infrastructures
  that's why we want to align best practices across so many domains

Deliver an integrated identity management infrastructure that responds to cybersecurity and community assurance requirements.

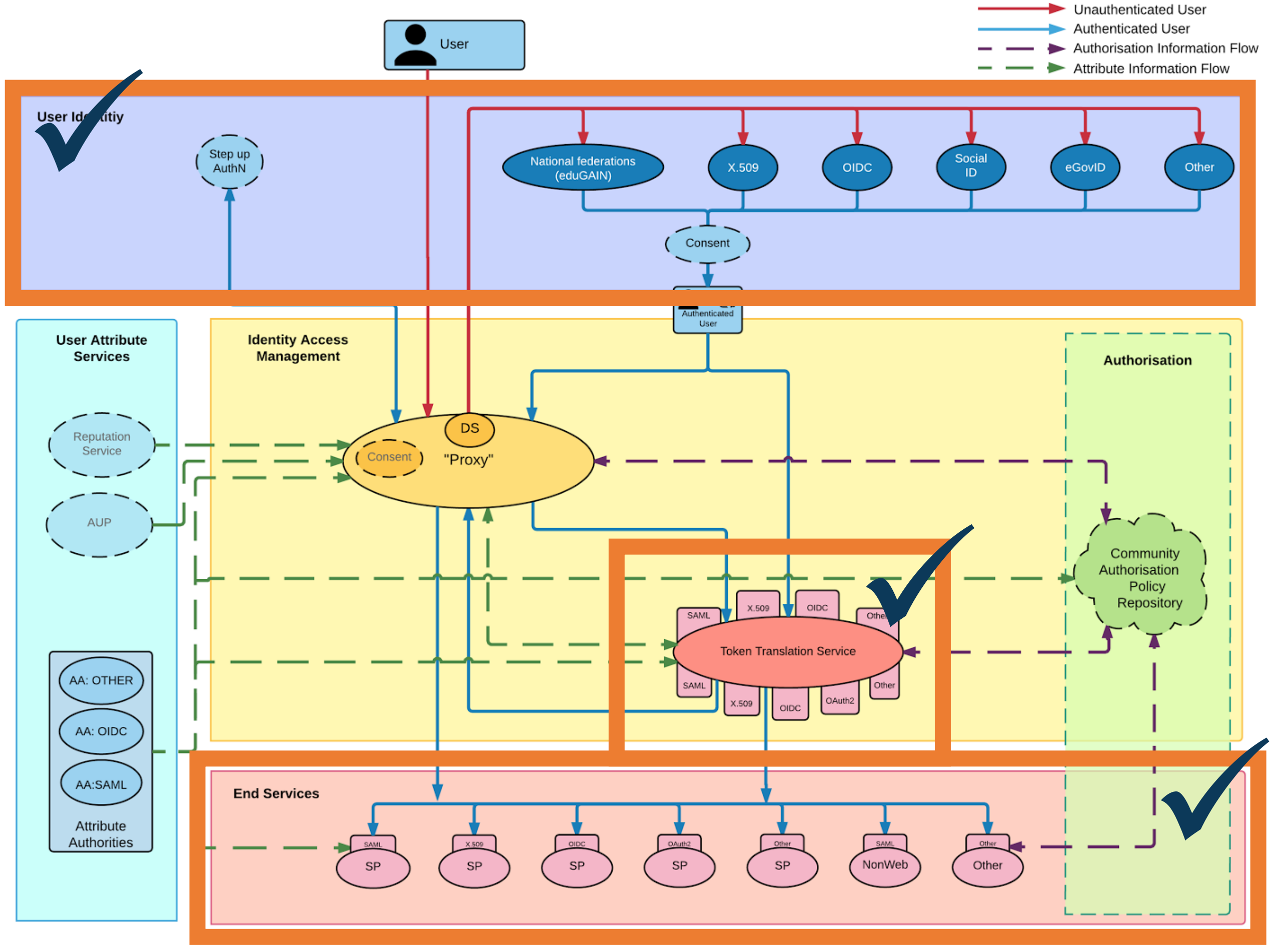
- Getting the Assurance Profiles deployed, esp. the ones needed by new research use cases
- Security incident response, through trust groups, WISE, and REFEDS

User-driven design and prototyping

- Practices must apply beyond just the project, we need *wide* consultation

Operational Security – we're all in it together!

AARC Blueprint Architecture

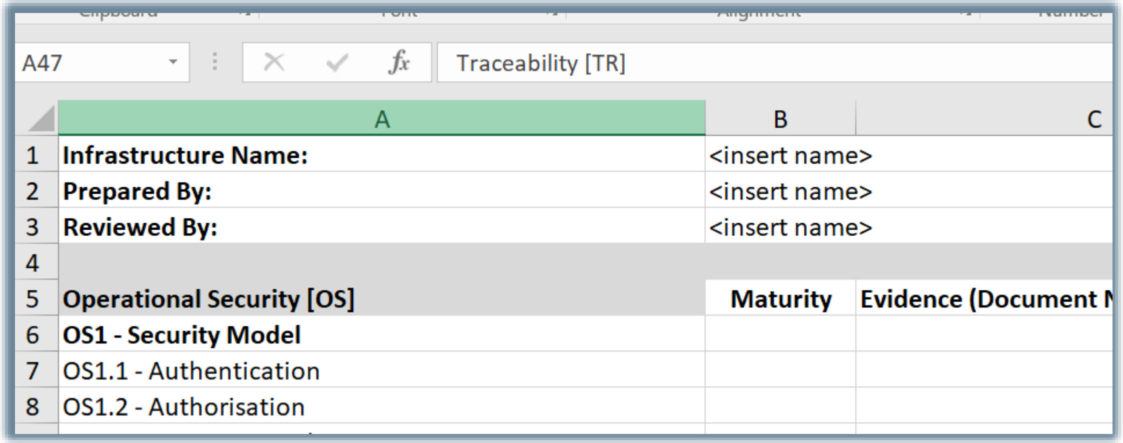


In the past 2 years, we managed to address security coordination for the federations, IdPs, and the e-Infrastructure collective services …
… but everyone needs to be involved, globally!

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



A47 | 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 N**
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

Engagement and global alignment

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*
- *Trusted Credential Mngt & Attribute Authy Ops*
- *Self-assessment and peer review methods*

AARC Engagement

help us progress by adopting results

Meanwhile, we do have to produce these reports as well

2 (phased) reports on service-centric practices

- DNA3.1 - Report on the coordination of accounting data sharing amongst Infrastructures (initial phase) - (M12)
- DNA3.3 –Accounting and Traceability in Multi-Domain Service Provider Environments (M23)

Security incident response

- DNA3.2 – Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios (M22)

Assurance and researcher-centric policies

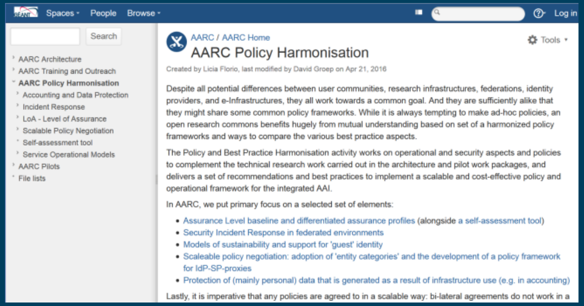
- DNA3.4 – Recommendations for e-Researcher-Centric Policies and Assurance (M24)

Obligatory Lord Kitchener Poster

<u>Substantial discussions on</u>
wise@lists.wise-community.org
sciv2-wg@lists.wise-community.org
igtf-general@igtf.net
sirtfi@lists.refeds.org
assurance@lists.refeds.org
refeds@lists.refeds.org
federatedIdentity-members@cern.ch
fim4r-editors@cern.ch

<u>Project deliverables welcome on</u>
aarc-na3@geant.org

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



AARC Policy Harmonisation

Created by Licia Florio, last modified by David Groep on Apr 21, 2016

Despite all potential differences between user communities, research infrastructures, federations, identity providers, and e-Infrastructures, they all work towards a common goal. And they are sufficiently alike that they might share some common policy frameworks. While it is always tempting to make ad-hoc policies, an open research commons benefits hugely from mutual understanding based on set of a harmonized policy frameworks and ways to compare the various best practice aspects.

The Policy and Best Practice Harmonisation activity works on operational and security aspects and policies to complement the technical research work carried out in the architecture and pilot work packages, and delivers a set of recommendations and best practices to implement a scalable and cost-effective policy and operational framework for the integrated AAI.

In AARC, we put primary focus on a selected set of elements:

- Assurance Level baseline and differentiated assurance profiles (alongside a self-assessment tool)
- Security Incident Response in federated environments
- Models of sustainability and support for 'guest' identity
- Scaleable policy negotiation: adoption of 'entity categories' and the development of a policy framework for IdP-SP-proxies
- Protection of (mainly personal) data that is generated as a result of infrastructure use (e.g. in accounting)

Lastly, it is imperative that any policies are agreed to in a scalable way: bi-lateral agreements do not work in a

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. 730941 (AARC2).