AARC Authentication and Authorisation for Research and Collaboration

LoA Policy Harmonisation and Best Practices

Developments in scalable negotiation and assurance

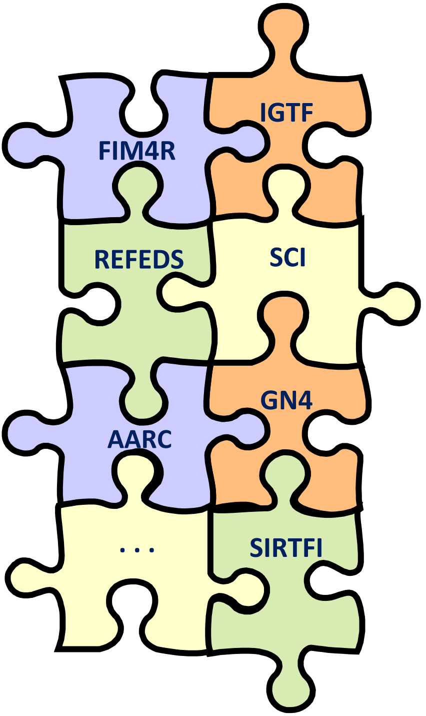
David Groep
AARC Policy & Best Practice Activity (NA3) Lead
Nikhef, Physics Data Processing Group
Nikhef

EGI Community Forum 2015, Bari, IT
12 November 2015

The Assurance Puzzle

- Many groups and many (proposed) policies, but they leave also many open issues
- via AARC Policy and Best Practice Harmonisation we try tackling a sub-set of these

  - “Levels of Assurance” – a minimally-useful profile and a differentiated set, for ID and attributes
  - “Sustainability models and Guest IdPs”– how can assurance be offered in the long run?
  - “Scalable policy negotiation” – beyond bilateral discussion
  - “Protection of (accounting) data privacy” – aggregation of PI-like data in collaborative infrastructures
  - “Incident Response” – encouraging ‘expression’ of engagement by (federation) partners and a common understanding https://wiki.refeds.org/display/GROUPS/SIRTFI



and thanks to all AARC folk for their work – esp. Mikael Linden, Dave Kelsey, Martin Haase, Peter Gietz; and to Daniela Pöhn of LRZ/GN4

I Assurance Level Landscape & activities

Plenty of definitions in commercial/gov space for identity providers

- NIST
- Kantara
- eIDAS (version now endorsed by EC comitology)
- VoT (new draft https://tools.ietf.org/html/draft-richer-vectors-of-trust-01)

…

In our R&E community

- Several (many) federation "identity management practice statements" + re-use of some of above
- e-Infrastructures trust: IGTF Generalised LoA* (with some 'differentiated responsibilities')

plus many community and national ones, see https://www.iana.org/assignments/loa-profiles/

PS: also Entity Categories ("R&S") and GEANT DP CoCo are akin to LoA definitions – but then 'reversed' to apply (mostly) to service providers

* www.igtf.net/ap/loa

eIDAS draft as of June 24th at CMTD(2015)0720

- ‘YALoAD’ - like NIST and Kantara mix of vetting assurance and authenticator qualities

eIDAS LoA	LoA=low	LoA=substantial	LoA=high
Application and registration	Applicant aware of terms, security precautions etc…	<- same	<-same
ID proofing and verification	Delivery to home address, exists in authorative registry	Perform a bank transaction etc	PhotoID face2face
AuthN means	Password	2 factor	2 factor + HSM
Issuance, delivery, activation	Mail	Secure delivery (Registered mail)	Secure delivery + activation
Suspension, revocation, reactivation	Timely by authorised person	<-same	<-same
Reneval, replacement	As initial delivery	<-same	<-same + verification from authorative registry
Authentication mechanism	Protection against guessing, etc.	Dynamic authentication	PKI…
Management, information security, audits	…		

Summary by Mikael Linden, CSC

See http://ec.europa.eu/transparency/regcomitology/index.cfm?do=search.documentdetail&jl9SmYIxaiPrPBeTK5Qyrmy+JAT8XSUYZ4c3fEwWtPjVqHZGdIwy2rS97ztb5t8b

IETF VoT Vectors of Trust

Core Components*

- 2.1. Identity Proofing
- 2.2. Primary Credential Usage
- 2.3. Primary Credential Management
- 2.4. Assertion Presentation

“For example, the vector value "P1.C3.A2" translates to pseudonymous, proof of shared key, signed back-channel verified token in the context of this specification's definitions”

In SAML a VoT vector is communicated as an AuthenticationContextClassRef

OpenID Connect JSON: “{ "vtr": ["P1.C2.C3.A2", "C5.A2"] }”

Foreseen: to be used as ‘assurance profiles’ that define a surface in this space

* https://www.ietf.org/mailman/listinfo/vot

LoA requirements and 'achievability'

What do relying parties need, and what can IdPs provide?

- R&E federations and their IdPs looking at the 'service aspect' of **providing** assurance https://wiki.geant.org/display/gn41sa5/1.4+Service+Aspects+of+Assurance

- AARC (through surveys and FIM4R) looking at immediate and longer-term **need** by SPs and RPs https://wiki.geant.org/display/AARC/LoA+survey+for+SP+communities

- One important challenge is cost of operation, and who bears this cost
  - In some frameworks this has been partially side-stepped because of close coordination or (funding) links between the IdPs/CAs with the researcher user communities
  - 'open' generically provided IdPs tend to die sooner or later

- LoA capabilities are closely linked to a sustainability model …

II Sustainable models

Sustainable operating models

- **Who supports such a service?**
  Central national funding, the RPs using it,
  subscribers/user paying a subscription fee, community-centric funding, …
- Does it need specific promotion, and by whom? (to get subscriber/user buy-in for sustainable funding)

Over time, no generic - non-community-based - identity provider seems to survive…

- ProtectNetwork: now pay-per-use (SPs need to pay $ now), Feide OpenIdP: phase out by Jan 1st, 2016

Other open identity providers are sustained because they serve a dedicated community
– e.g. IGTF Identity Providers are (co)supported by national funding and by community groups

But homeless users exist (and need IdPs of Last Resort or “Guest IdPs”) with a defined assurance

- Policies for ‘homeless user’ accounts lifecycles
- Traceability and assignment of persistent non-reassigned identifiers
- Policies for translating social network identities into SAML federation users – effect on LoA?

‘Selling’ LoA – the very word may trigger allergic reactions …

Tradtitional identity providers who bear the costs have become weary of LoA …
… *especially if they are from a country where the Govt pushes rather firmly on formal LoA’s*

> *I'm assuming you are comparing "higher" to " existing broadly adopted levels" rather than "existing defined levels". So "higher than CoCo" but not necessarily "higher than InCommon Silver". From an advertising standpoint if nothing else I'd suggest avoiding the term "higher" when talking to US IdPOs. :)* – by Eric Goodman on the REFEDS list recently

… one option: take some ‘costly’ elements out in a - central or community - step-up LoA?

- but LoA is more than just 2FA, it is also ‘regular’ quality of attributes and their properties
- like having a persistent non-reassigned ID, and ‘reasonably verified’ attribute values
- and documenting and standing by described operating policies
- e.g. many of the e-Infrastructures are OK with a peer-reviewed self-assessment method, and don’t require formal audits for assertions coming from ‘trusted’ community providers!

III Scaling Policies and Assurance

Some existing ‘scalable’ policy mechanisms around now

- Coordinated ‘policy bridge’ trust anchor/meta-data distributions (e.g. IGTF trust fabric*)
- eduGAIN is policy-free, but there are Entity Categories (‘ECs’)

  Geant CoCo, iCoco, REFEDS R&S, and some evaluation of extent to which currently used

  - https://technical.edugain.org/entities.php
  - https://met.refeds.org/

Gaps or problems to be addressed

- Federations not exposing IdPs to eduGAIN, or lack of EC support (or willing IdPs with metadata got it re-written by their federation operator …)
- What about expressing SIRTFI trust compliance, should that be an EC?
- Should policies and ECs be single global definitions (like CoCo, R&S), or should we prepare for many ‘community trust marks’ - already some countries have scoped entity categories
- Remember TACAR* – where the registry is neutral but anchors can be ‘qualified’

Do service providers/RPs ‘on the ground’ actually understand LoA?

* www.igtf.net, * www.tacar.org

Beyond identity-only

How do we extend scalable policy agreement to general Attribute Authorities and others?

- Need to identify entities to be classified (non-IdP AAs, credential translators, others)
- What codes of conduct are required? Classify an Attribute Authorities with a (single) LoA?
- Other operational best practices (how to AA *operations** affect LoA)?

Now every country is different, and there's no current best practice for communities

*e.g. igtf.net/guidelines/aaops/

Levels of Assurance convergence – a survey based process

‘Towards a useful basic assurance level that’s both feasible and useful for research and schorlarly collaboration as a consensus first step’

- Identity management services and providers (Daniela)
- Federation operators (Daniela)
- Relying parties and service providers (Mikael)

Differentiated LoA recommendations – a *limited* set of consensus levels. “to reflect the options for distribution of responsibilities amongst the three identified participant roles: researchers and research communities, resource and e-infrastructure providers, and identity federations and their constituent IdPs”

- This needs experience from actual responsibility distribution experiments
- Based on pilots and the AAI architecture models

Current status to be collected

- IdP survey https://wiki.geant.org/display/gn41sa5/IdP+survey
- Federation survey https://wiki.geant.org/display/gn41sa5/Federation+survey
- SP survey https://wiki.geant.org/display/AARC/Level+of+Assurance+survey+for+SP+communities

SP responses – an example

- Track progress of the interviews at
  https://wiki.geant.org/display/AARC/LoA+-+Level+of+Assurance
- Contribute answers based on the survey to Mikael Linden
- We already know about the FIM4R requirements

Explicit communities

- EGI, wLCG, PRACE
- DARIAH, CLARIN, ELIXIR, Photon/Neutron/Umbrella
- Libraries
- Commercial (‘cloud’) services for research
- *find some more RIs from FIM4R community*

Early findings - to be published end of November 2015

“Recommendation on minimal assurance level relevant for low-risk research use cases” (document: AARC MNA3.1)

- Accounts belong to a known individual (i.e. no shared accounts)
- Persistent identifiers (i.e. are not re-assigned)
- Documented identity vetting (not necessarily F2F)
- Password authN (with some good practices)
- Departing user’s account closes/ePA changes promptly
- Self-assessment (supported with specific guidelines)

For a later iteration – so as not to overload and cause delays at the IdP side – adoption of the incident response framework for federations (SiRTFi) – which in itself has a phased approach

Also more complex assurance profiles are recommendations for a future version (end 2016)

slide partially by: Mikael Linden, AARC AHM Milano

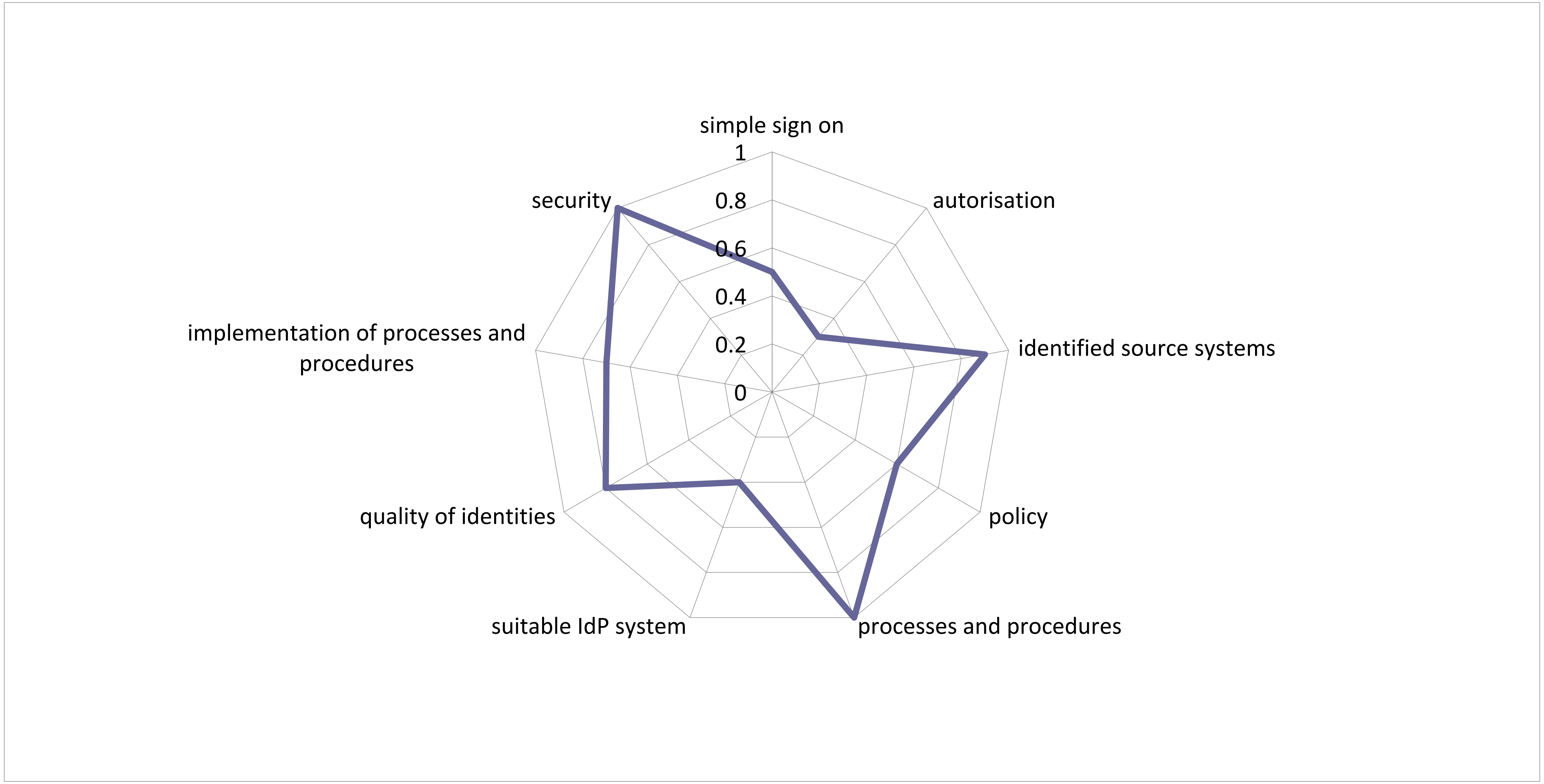
Idea: How to assist IdPs to do the LoA self-assessment

AARC policy development pilot option is open to develop and pilot a tool which

- is itself an eduGAIN SP to which any eduGAIN IdP admin can log in
- Presents structured self-assessment questions to the IdP/IdM admin
  - Quantitive: (”do accounts belong to an individual”)
  - Qualitative: (”explain how you ensure accounts belong to an individual”)
- Publishes the results for anyone to read
- Evaluates if the LoA minimum is fulfilled
- Spits an Entity Category tag to eduGAIN metadata for the IdP
  - Can we do that centrally?
- Asks the IdP admin to re-evaluate every year
- Can assist in the LoA peer-review
  - If peer review becomes a requirement e.g. for a higher LoA level

slide: Mikael Linden, AARC AHM Milano

c.f. SURFnet's IdM maturity scan for Dutch Home Organisations



slide: Mikael Linden, AARC AHM Milano

You can still contribute to AARC and GN4 SP and Relying Party Questionnaire

In-depth interviews based on structures questionnaires

https://wiki.geant.org/display/AARC/Level+of+Assurance+survey+for+SP+communities

https://wiki.geant.org/display/gn41sa5/IdP+survey

https://wiki.geant.org/display/gn41sa5/Federation+survey

Thanks to all AARC folk whose slides and work I used in here – esp. Mikael Linden, Dave Kelsey, Martin Haase, Peter Gietz and to Daniela Pöhn of LRZ/GN4

Thank you

Any Questions?

davidg@nikhef.nl

AARC

https://aarc-project.eu

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).