Leveraging the IGTF authentication fabric for research

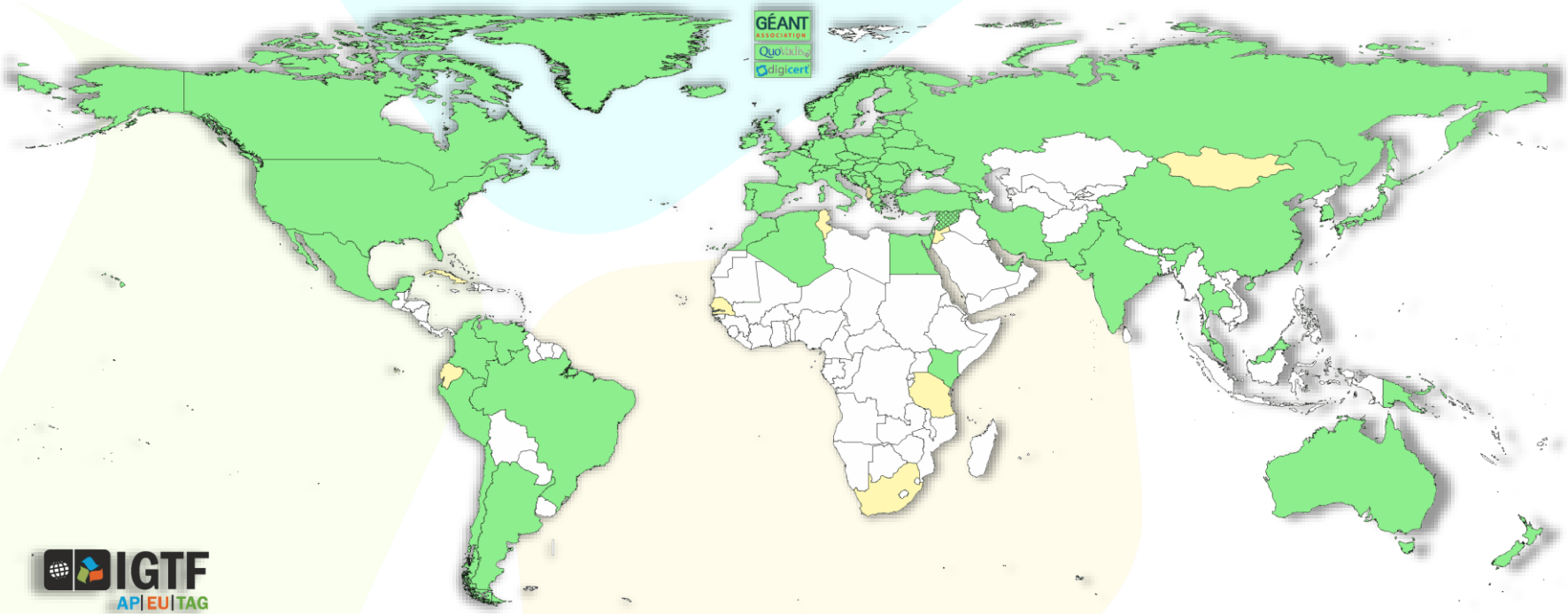
the IGTF-to-eduGAIN Bridge and the registration authority network

David Groep

Nikhef

co-supported by the Dutch National e-Infrastructure coordinated by SURF, and by EGI Core Services

A look at the IGTF



IGTF capabilities

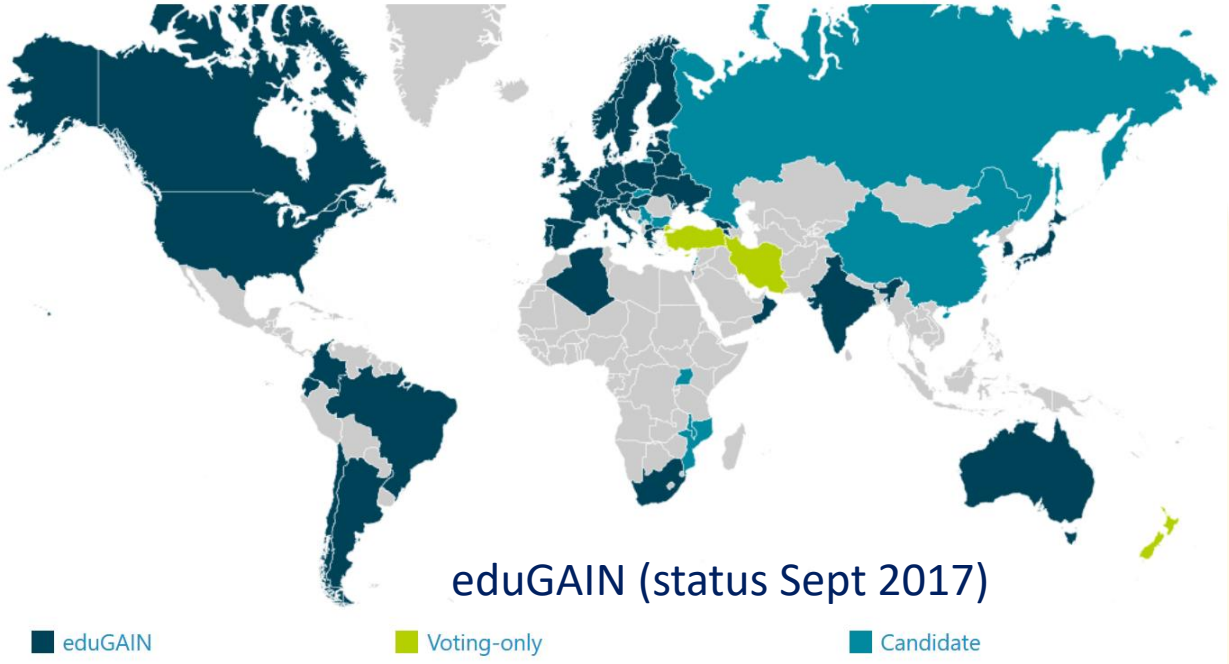
- AuthN fabric and identity availability (today)
- Assurance requirements and assessment for Infrastructures (tomorrow morning)
- Registry operational guidelines (tomorrow morning)
- Infrastructure policy harmonisation *Snctfi* (tomorrow)
- Registry and operational capabilities (tomorrow afternoon)

What we do (for authN services)

- *User-centric* authentication – across organisations
- Independent of user's home organization
- Inspired by and aligned with research communities and e-Infrastructures
- Differentiated assurance derived from a both solid and transparent assurance level
- Ability to transfer registrations across authorities and countries (with the Registration Practice Statement)

… and guidance around trust and trustworthy operations for AuthN and Attributes … and …

eduGAIN



- 40 NRENS (≈ countries)
- 4254 entities
  (of which 2533 IdPs, *i.e.*,
  authentication providers)

- organisation-centric, and with much national autonomy in policy & practice
- where it reaches the users *and* a 'link' is made, provides great ease of use
- in most organisations, research is not the primary use case (yet) for the 'IdP'

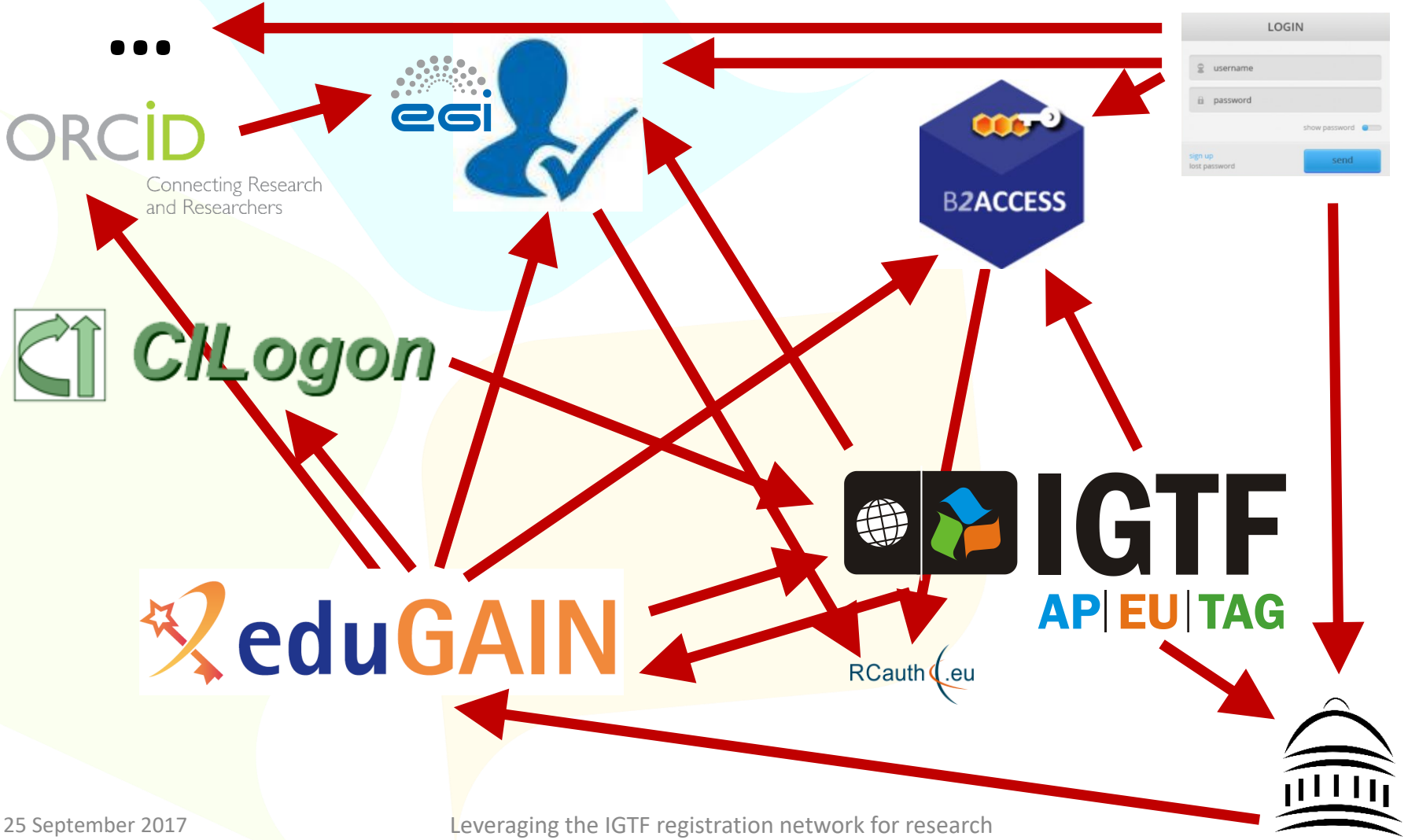
Infrastructure specific hubs

- EGI CheckIn
- B2ACCESS
- CILogon
- ORCID
- …

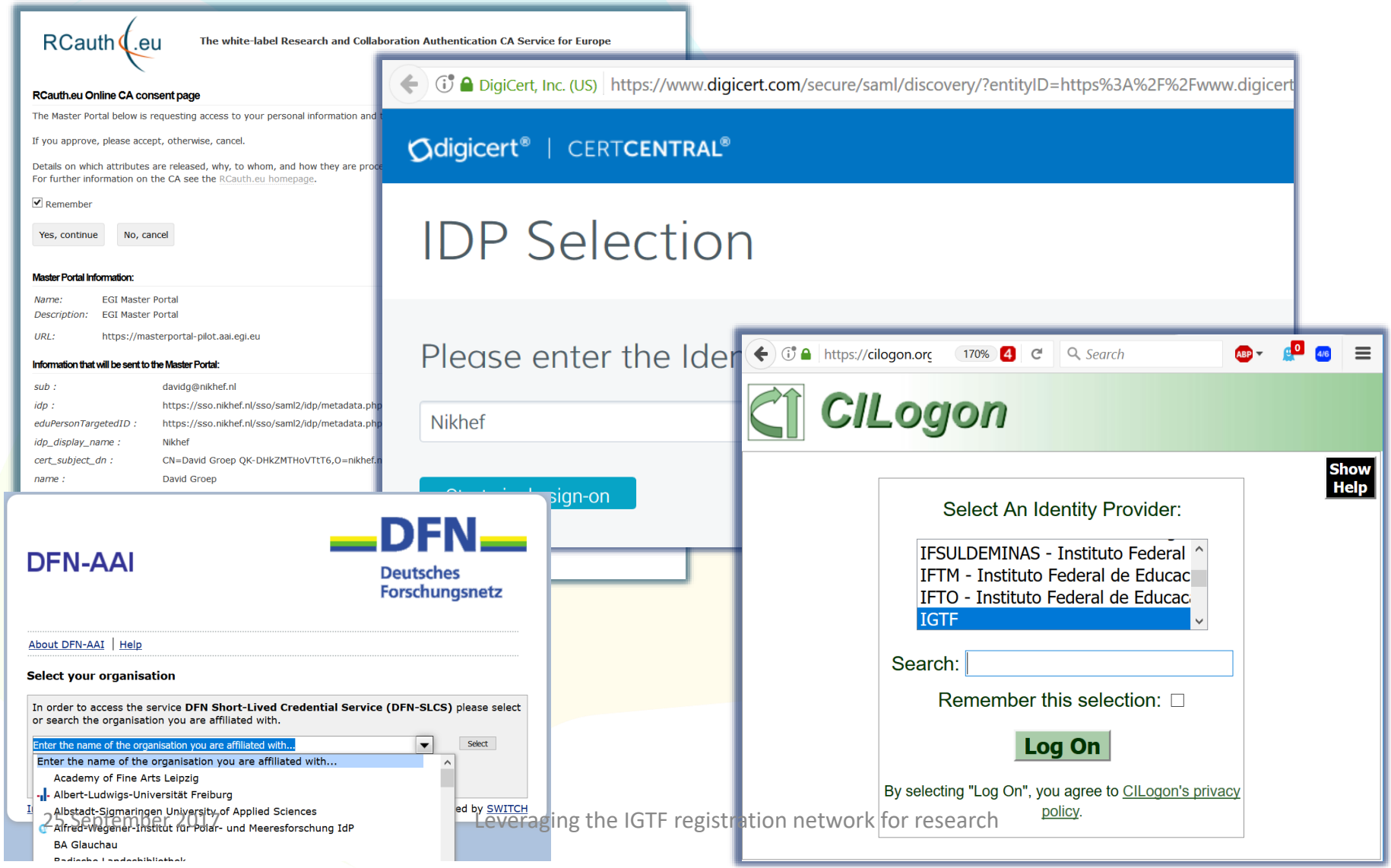
Service-bespoke solutions

- ~~Local log-in, mangled tokens, directory auth~~
  ‘golden’ portals ~~that accept your credentials,~~
  ‘golden’ portals assuming ownership of everything, …

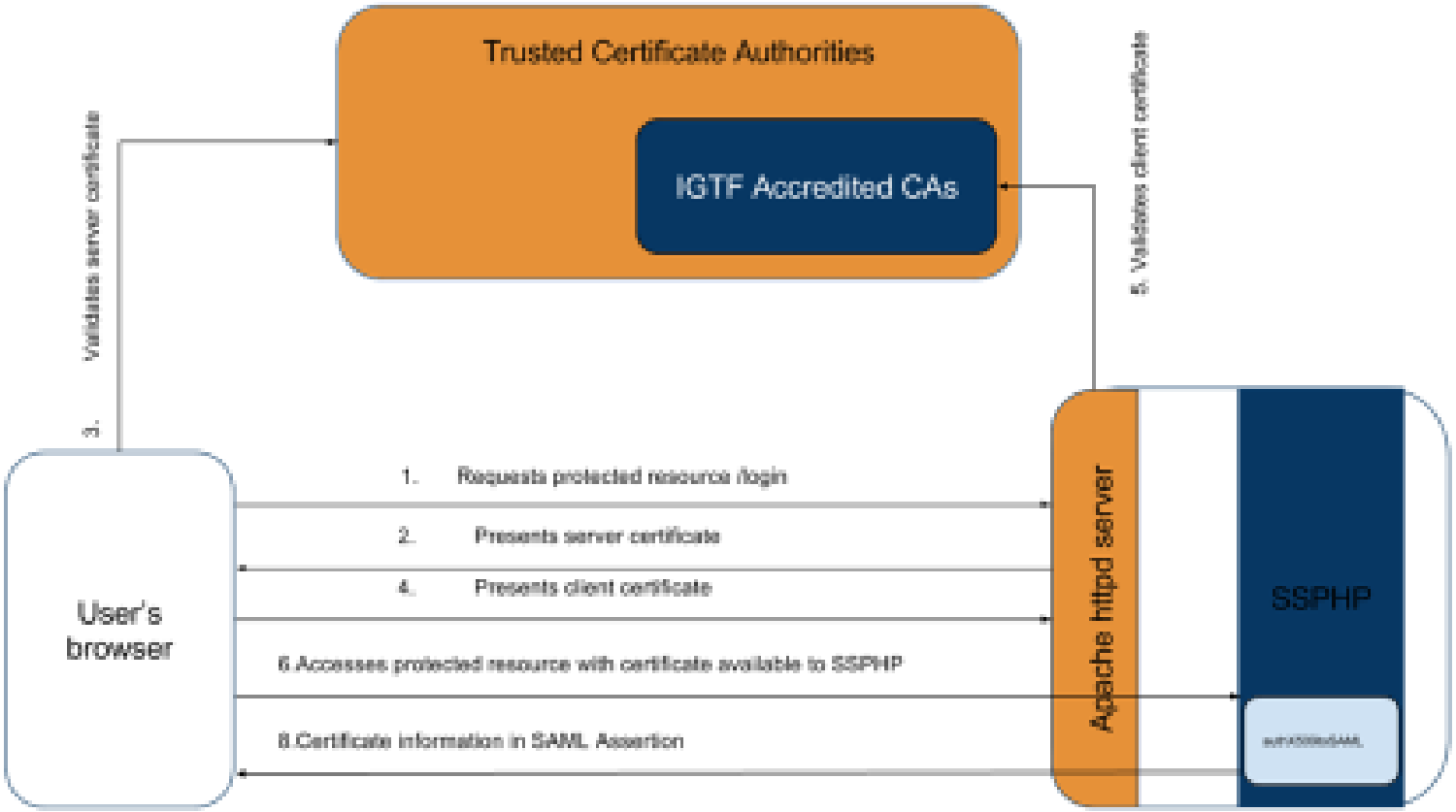
Turtles all the way down … and up!



TCS – CILogon – DFN SLCS – RCauth.eu



Bridging IGTF to eduGAIN
authX509toSAML



Work by Ioannis Kakavas and Nicolas Liampotis (GRNET) for the AARC project

Guidance we have and use

Assurance Profile

- https://www.igtf.net/ap/

Assessment support

- http://wiki.eugridpma.org/Main/AssuranceAssessment

‘Back-office’ template practices

- https://www.eugridpma.org/documentation/rps/

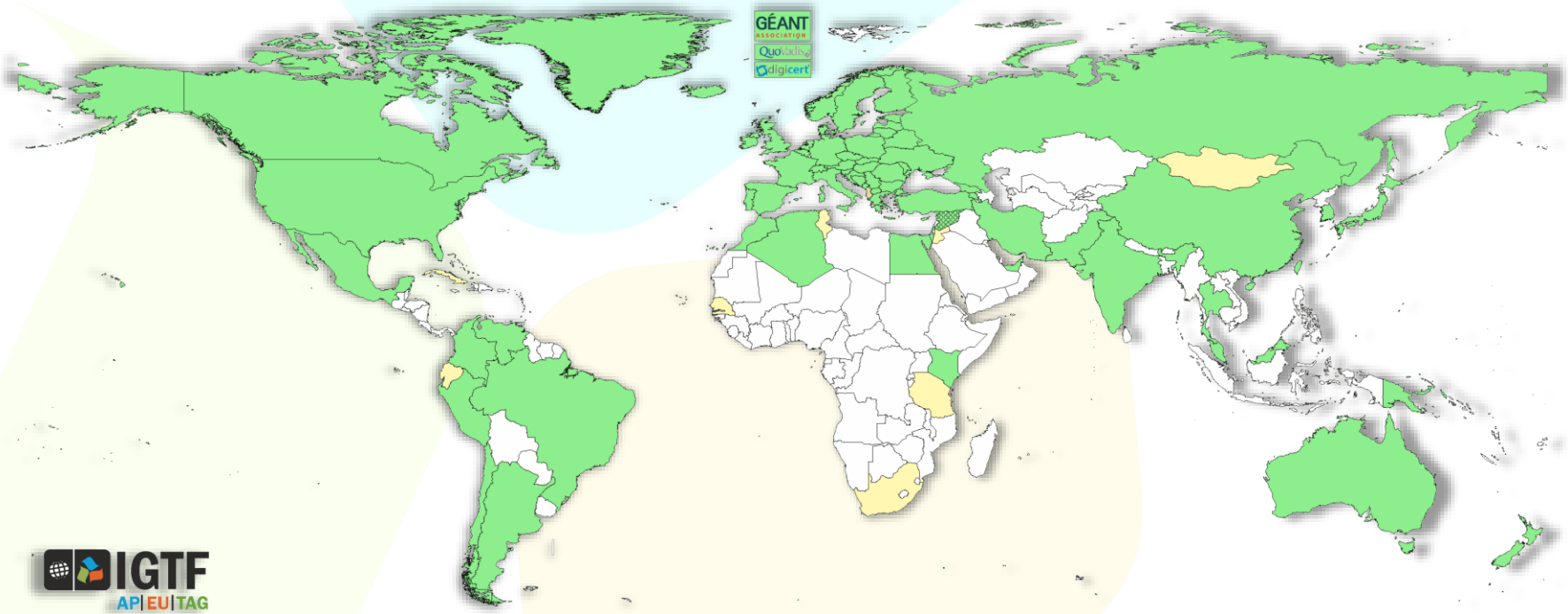
Registration Networks

Although the process is labour-intensive and relatively slow, for some user categories the prevalent 'user-held' credential is the only one that 'works':

- non-academic users (SMEs, industrial R&S)
- users in a place without an eduGAIN federation
- users in a place that does not do unique ID
- users in an organization that does not release attributes
- users in an organization that does not provide assurance
- …

A ‘high-quality IdP of last resort’?

- Most useful asset is our RA network!



Ideas …

- Promote the use of (existing) bridges
- Support other credential types and/or interfaces?
- In places without an existing federation
  - Promote its establishment, as now eduGAIN is more open than before …
  - join eduGAIN yourself – as a ‘trivial hub&spoke’ using the bridge IdP technology?
- Where a federation exists
  - Establish direct links – there’s an opportunity in ‘long-tail’ support and IdP-of-last-resort services ☺?
  - Push for a federation policy aligned with global (researcher) needs?
- Expose differentiated assurance model to subscribers?
- User-held credentials avoid much of the privacy issues?

Discussion!

BUILDING A GLOBAL TRUST FABRIC