eResearchers Requirements

the IGTF model of interoperable global trust and with a view towards FIM4R

AAI Workshop

Presenter: David Groep, Nikhef

IGTF
Interoperable Global Trust Federation
AP | EU | TAG

eugridpma

NIKHEF
SURF SARA

egi
e-infrastructure

IGTF – *Interoperable Global Trust Federation*

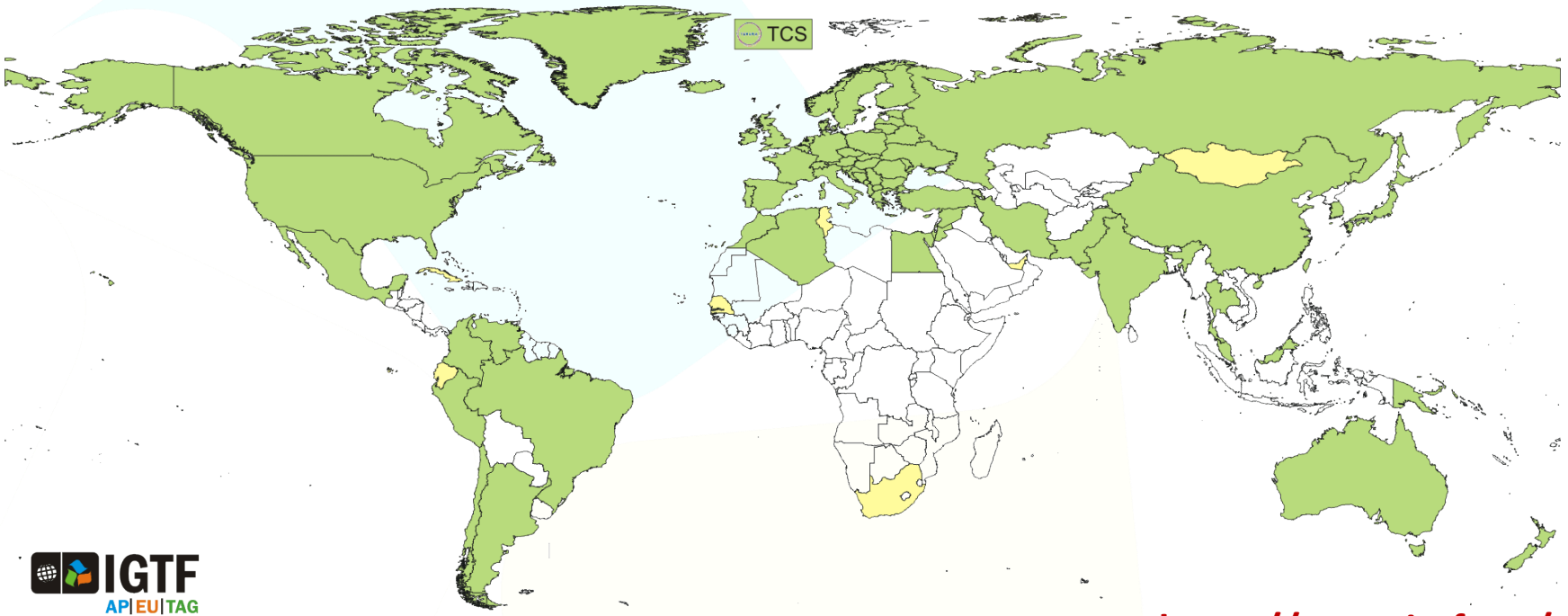
supporting distributed IT infrastructures for research

- IGTF brings together
  - e-Infrastructure resource providers, user communities and identity authorities

  to agree on
  - global, shared minimum requirements and assurance levels
  - inspired and coordinated by the needs of relying parties

- Trust is technology-agnostic
  - focus on global, coordinated identity across communities and across service providers for *cooperative services*
  - define ‘best practices’ for assurance levels, attribute authority operations, credential management, auditing and reviewing

Coverage: users and providers



https://www.igtf.net/

- ~100 000 users and resources
- 89 national and regional identity authorities: R&E and commercial
- >1000 different user communities: small and large, national and global
- Major relying parties: EGI, PRACE, XSEDE, Open Science Grid, HPCI, wLCG, OGF, …

IGTF is a coordinating body, and not a legal entity in itself – although its members may be

Minimum Requirements

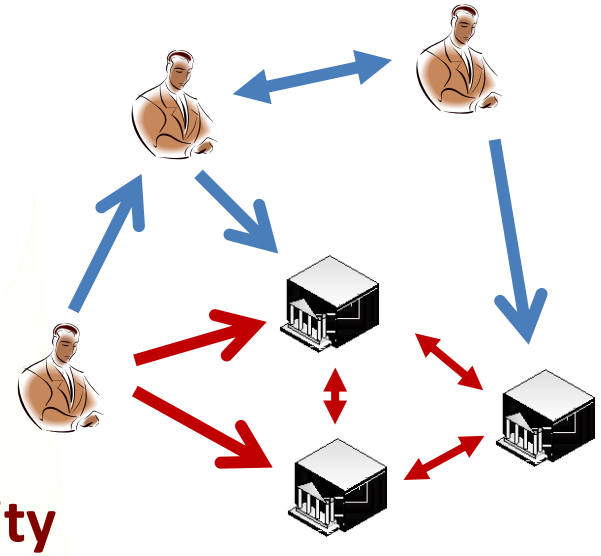
- Federation imposes *minimum requirements* on identity provider participants
  - Reflect operational and security needs of resource providers
  - Differentiated LoA support
    - classic user-based subscriber services: serve all users
    - identity services leveraging (R&E) federations with ID vetting
    - 'LoA1+' Identifier-Only Trust Assurance
      – if relying party has other ways to vet its users, allow for lower-assurance identifiers, thus enabling more ID federations

    } *'LoA2-'*

  - **Research-inspired verification process**: self-audits, peer-review, transparent open policies and processes
  - 'meet or exceed' required minimum standards

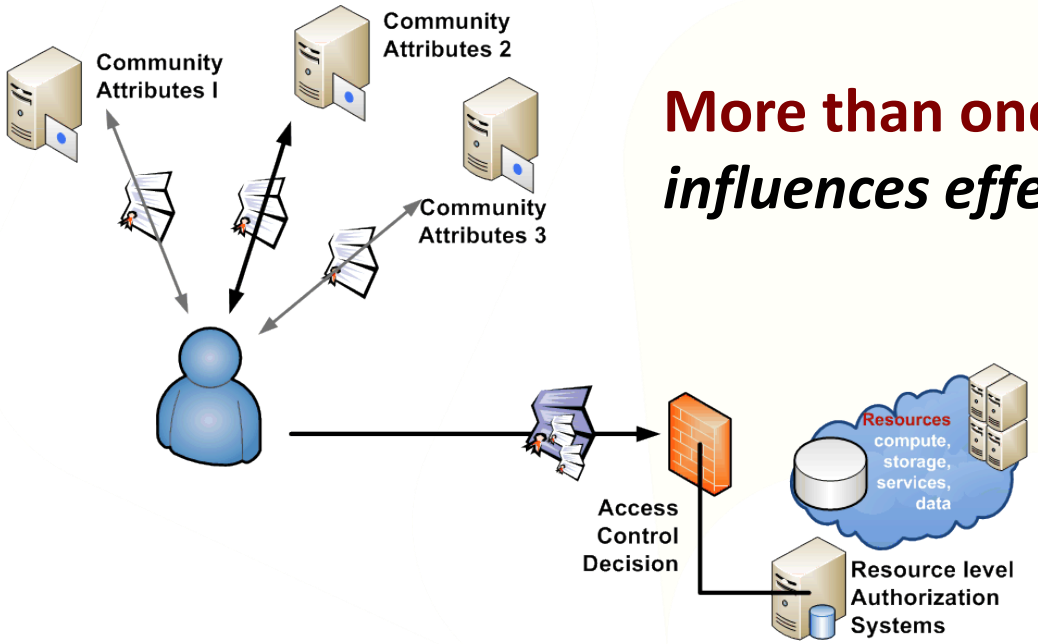
Community characteristics

More than one administrative organisation



More than one service provider
participates in a single transaction

More than one user
in a single transaction



More than one authority
influences effective policy

Single interoperating instance
at a global level

AAI requirements

FIM4R captures the key requirements

- different Levels of Assurance with provenance
- authorisation under community and/or facility control
- browser & non-browser federated access
- attributes must be able to cross national borders

and we **also need**

- federations and IdPs to work in a collaborative security and policy framework, addressing the areas identified in e.g. SCI
- support for individual researchers
  communities are widely distributed and although large as a whole may be only a one or a few per institution
- global scope: scientific collaborations extend *beyond Europe*

FIM4R: **https://cdsweb.cern.ch/record/1442597/files/CERN-OPEN-2012-006.pdf**
SCI – Security for Collaboration among Infrastructures: **https://www.igtf.net/sci**

Are the Requirements Met?

NO

- security trust and operational issues
- differentiated LoA: reviewed and/or audited
- support for community and facility control, set by themselves and propagated to the SPs
- both browser and non-browser access
- attributes to cross national borders

Each of these may have been solved in some federations – but what we need is a coherent European/global view, where these requirements are addressed ubiquitously!

Are the Requirements Met?

YES

- Much of the technology is there for
  community attributes, facility control, non-web-access
  – we 'just' need to bridge it to together,
  and make sure the technology is deployed uniquitously
  there may even be 'too much' technology, in that we now need to bridge for interoperability – bridges, proxies, and credential stores will a part (likely supported by the RPs, communities and facilities)
- attributes to cross borders: DPCoC is a great step
  - now can we do the same for IdPs please?
    the GEANT eduGAIN Federation Template looks like going this way …
  - the model of 'minimum requirements' and open processes worked well in the IGTF and is 'natural' to a research environment

www.igtf.net

Interoperable Global Trust Federation