IGTF
International Grid Trust Federation
AP | EU | TAG

The International Grid Trust Federation

enabling an interoperable global trust fabric

David Groep
EUGridPMA

eugridpma

also supported by EGI.eu EGI-InSPIRE RI-261323, and BiG Grid, the Dutch eScience Grid

egi

BiG Grid
the dutch e-science grid

The Need for a Global Trust Fabric

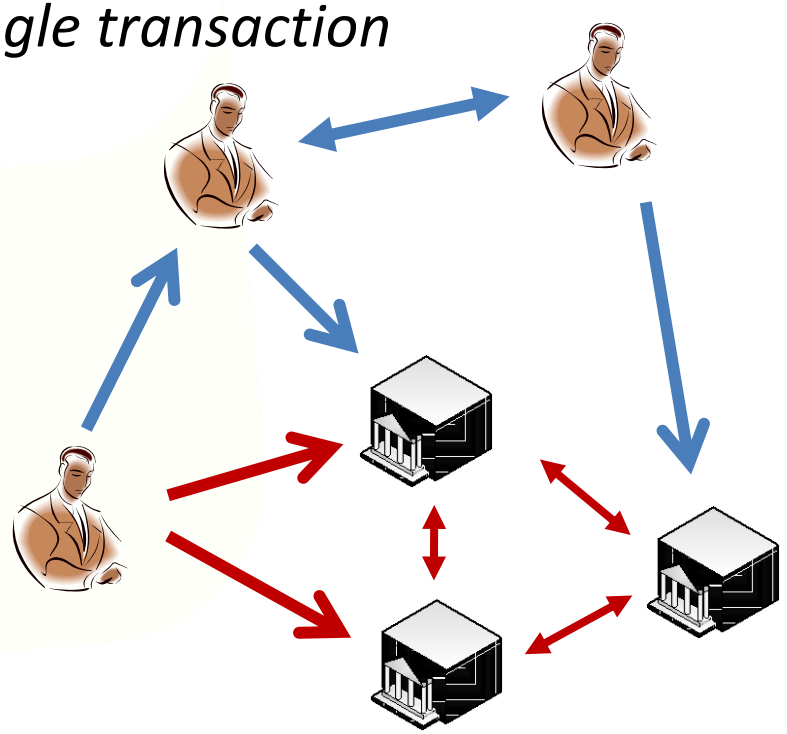
More than one administrative organisation

More than one service provider
participates in a single transaction

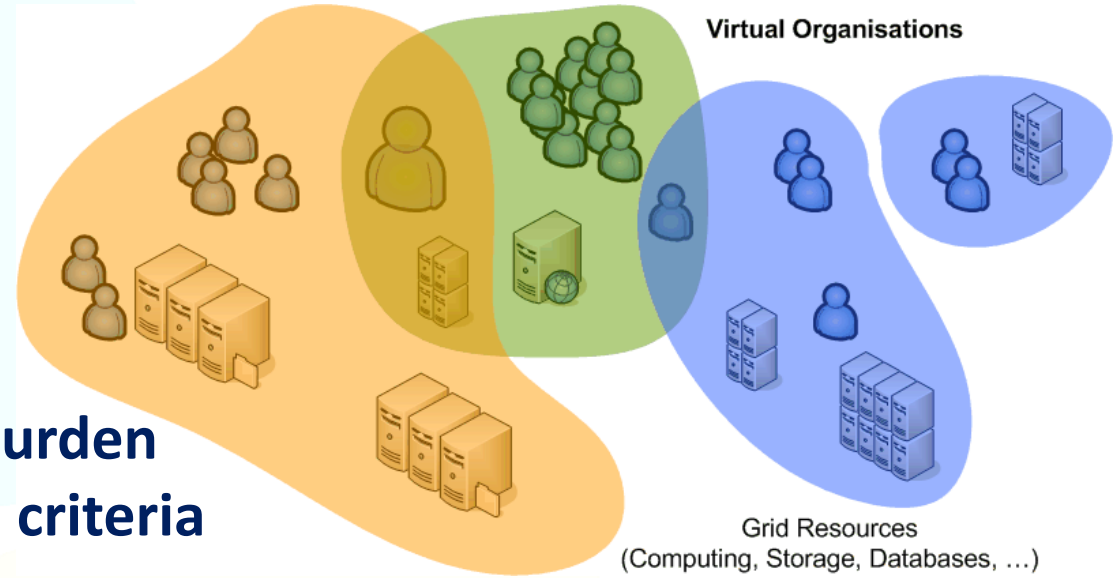
More than one user
in a single transaction

More than one authority
influences effective policy

Single interoperating instance
at the global level



Overlapping Communities – Common Trust



Reduce over-all policy burden by adhering to common criteria

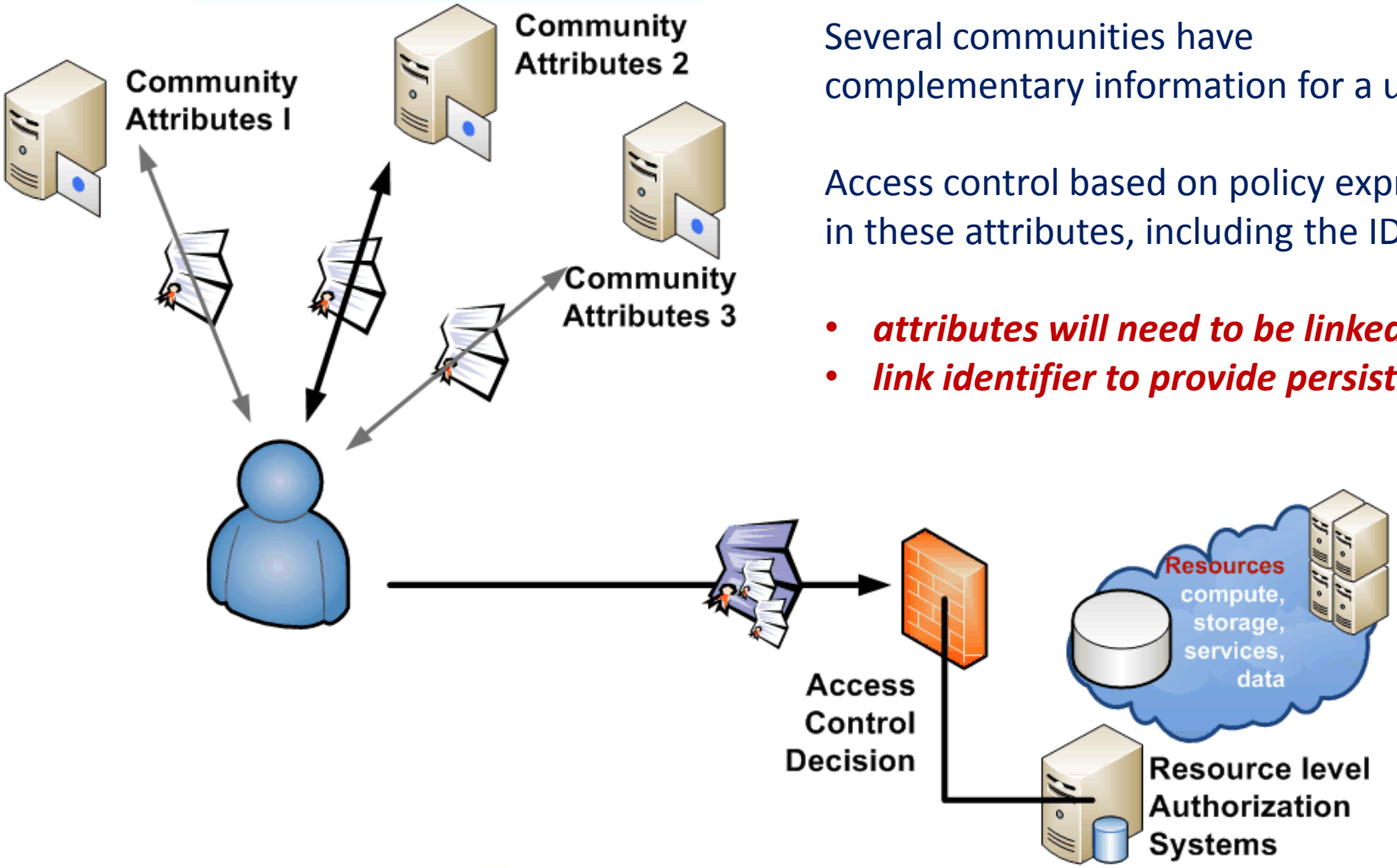
Goals

- allow multiple sources of authority: User, Institute, Community
- acknowledge both long- and short-term community structures
- enable security incident response and containment
- balance data protection and right to privacy

to

provide basis for access control decisions by resources and communities

Attributes and Access Control



Several communities have complementary information for a user

Access control based on policy expressed in these attributes, including the ID

- ***attributes will need to be linked***
- ***link identifier to provide persistency***

Requirements on a trusted source

Privacy and data protection

- important 'unalienable right' for research
- correlation of PII among service providers could allow profiling
- exchange of PII often fraught with issues

Access Control Attribute handle

- unique binding
- never re-assigned

Measurement and Accounting

- publication metrics
- usage metering, billing
- auditing and compliance monitoring

Incident Response

- long-term* traceable
- independent from short-lived community
- must be revocable
- correlate with other information sources
- banning and containment handle

A common ID must live in a policy ecosystem to protect participants and to limit its use to specific purposes

Elements of Trusted Identity

1. Vetting and assurance – for identity and attributes
   - vetting rules and data quality
   - expiration and renewal
   - revocation and incident containment
2. Operational requirements for identity providers
   - operating environment and site security
   - staff qualification and control
3. Publication and audits
   - openness of policy, practices and meta-data
   - review and auditing
4. Privacy and confidentiality guarantees
5. Compromise, disaster recovery and business continuity

Assurance levels

Trust in the assertions by resource and service providers is key

- Until now, our e-Infrastructure used a single ‘level’
  - there are well-known ‘government’ standards for LoA (US: OMB M-04-04 & NIST SP800-63)
  - but 95/46/EC and 1999/93/EC are not of much use to us and the Nice treaty states that identity is a national matter …
  - there is rough *but not 1:1* correspondence between balanced needs of the providers and users and the NIST LoA levels

IGTF Assurance Levels

Type and classification of e-Infrastructure services
drives the level of assurance required

- Security and assurance level set to be commensurate
  - not overly high for ‘commodity’ resources
  - not too low, as providers otherwise start implementing additional controls on top of and over the common criteria
  - defined *in collaboration with* resource providers
  - using transparency and a peer review processes
  - leveraging our own community organisation mechanisms

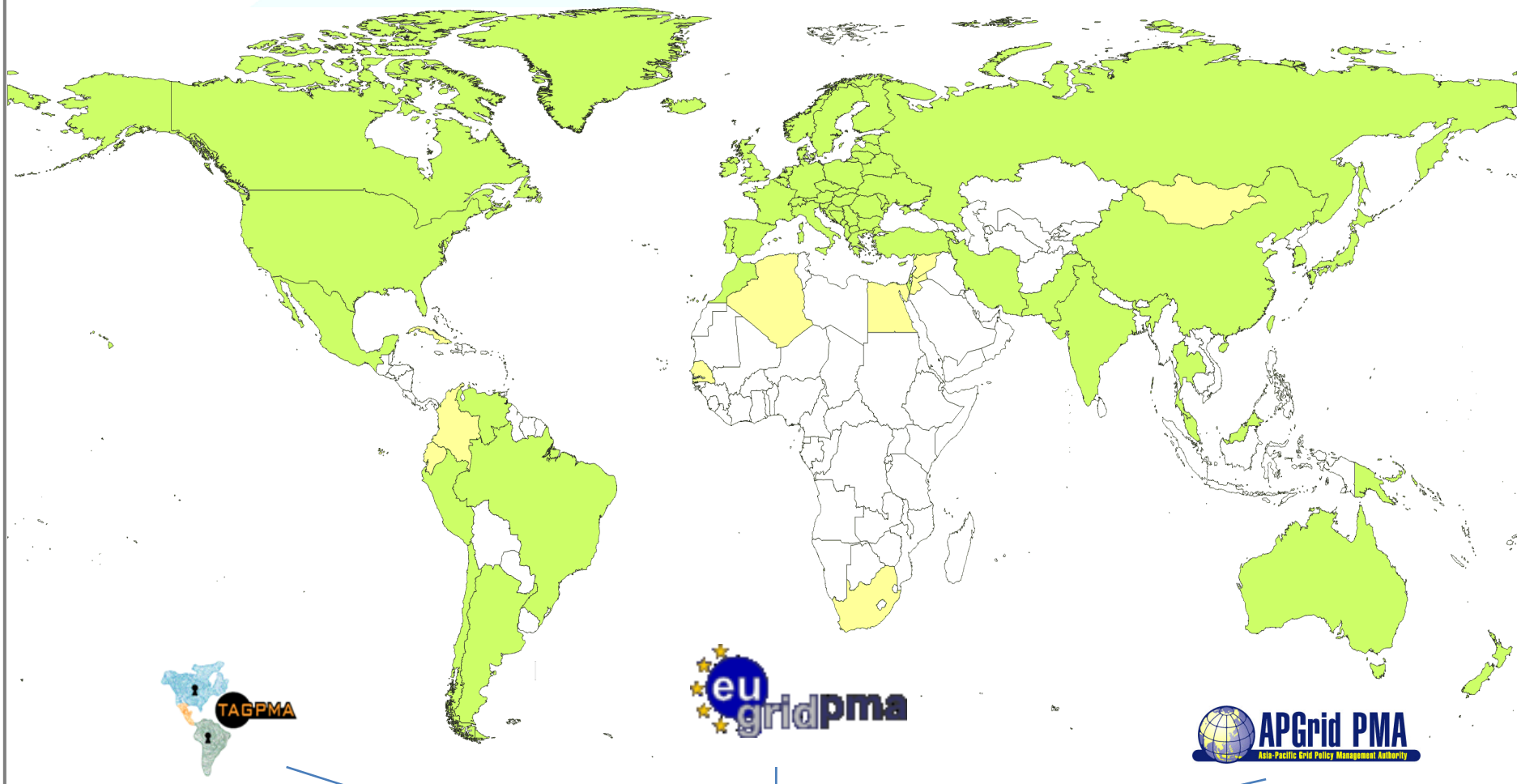
Establishing the IGTF – EU AP TAG

- EU DataGrid established Coordination Group in 2000
- Global need resulted in the 2003 Tokyo Accord

- With start of production e-Infrastructures
  - EUGridPMA established with DEISA, EGEE, SEE-GRID, and TERENA (TACAR) as relying parties and national identity providers in 2004, with e-IRG endorsement
  - APGrid and PRAGMA establish the APGridPMA
  - Canada, EELA-countries and USA IdPs establish TAGPMA

- Consistent guidelines and service provider involvement

Global Trust

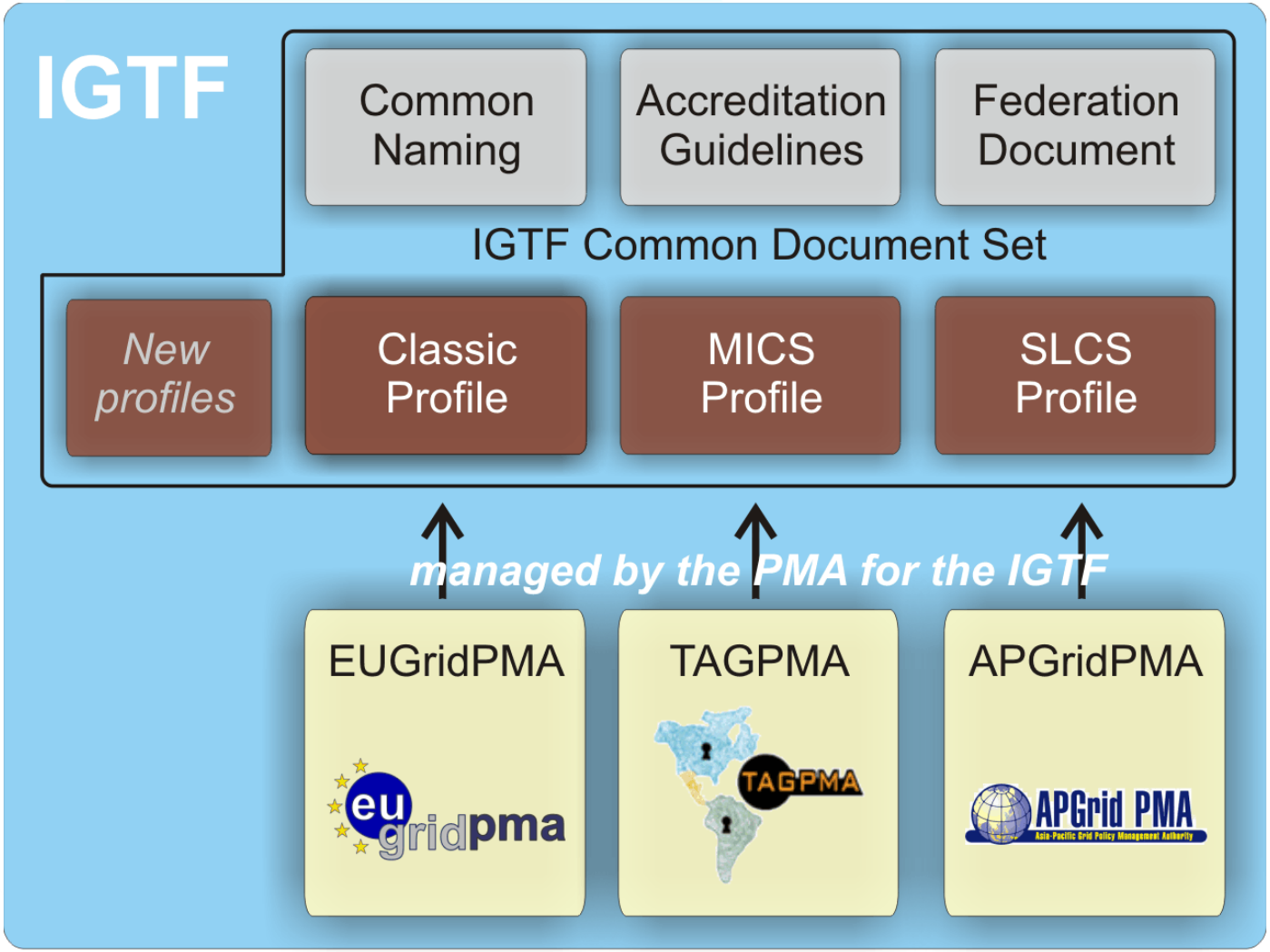


86 accredited authorities from 53 countries and economic regions

Structure of Trust

- Common criteria and model
  - globally unique and persistent identifier provisioning
  - not fully normative, but based on **minimum requirements**
- Trust is technology agnostic
  - technology and assurance 'profiles' in the same trust fabric
  - 'classic' traditional public key infrastructure
  - 'MICS' dynamic ID provisioning leveraging federations
  - 'SLCS' on-demand short-lived token generation
    a basis for 'arbitrary token' services
  - *new profiles*

IGTF Common Criteria



IGTF
International Grid Trust Federation
AP | EU | TAG

Assurance levels in the IGTF

Technical and operational controls

- Authorities come in two basic flavours
  - **off-line** (only used in 'traditional' PKI): human controls and air-gap security provide protection against attacks
  - **on-line infrastructure** (federation-backed, SLCS and classic): valuable security material is network connected need compensatory controls:
    - secure hardware, compliant to FIPS 140-2 level 3
    - additional layered network security
- *Technical* requirements apply to any attribute source
  - such as community registries like 'VOMS'

Vetting Assurance Levels

Identity controls and vetting

- long-term traceable assurance (classic, MICS)
  - based on in-person checking of (nationally defined) official identity documents
  - recorded identity persists beyond the moment of issuance
  - assertions can live for a long time (over a year) to facilitate long-term use
  - but compromise may happen, so is revocable
- momentary assurance (SLCS)
  - traceability to a physical person for at least one year
  - may use any vetting mechanism that assures that traceability
  - but assertions are limited in time to 24 hours (unless revocable, in which case: 11 days)

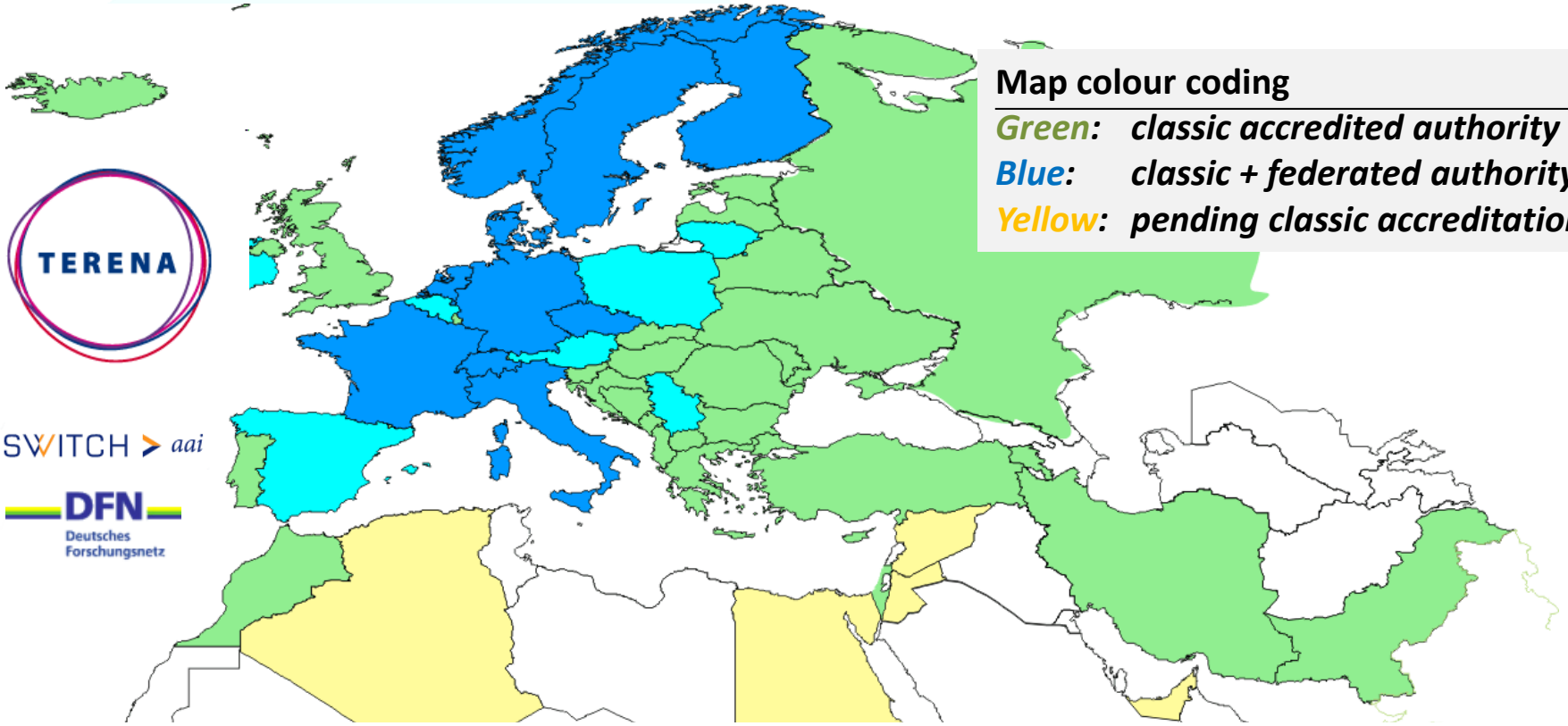
https://www.eugridpma.org/guidelines/{classic,mics,slcs}

Building trust – an exercise in scaling

- Accreditation process
  - Extensively documented *public* practices (CP/CPS, RFC3647)
  - Interviewing and scrutiny by peer group (the PMA)
  - Assessment against the Authentication Profiles
  - Technical compliance checks (RFC5280 and GFD.125)
- Periodic, peer-reviewed, self-audits
  - Based on Authentication Profiles, standard reference: GFD.169
  - OGF & IGTF, inspired by NIST SP800-53/ISO:IEC 27002
- Federated assessment methodology by region (IGTF)

https://www.eugridpma.org/guidelines/accreditation

Federated Identity in Europe Today



Federated 'translating' authorities: *integrity requirements propagate to all data sources*
***e.g.* TERENA Certificate Service qualifying Federations IdPs meet all IGTF requirements and TCS provides instant access to globally trusted identities**

Also in Australia: ARCS SLCS, in USA: CILogon

Beyond identity

- Many attributes come in to an authorization decision
  - identity, community, group membership, roles, position, ...
  - the 'other attributes' are important for contextual control *and thus of importance beyond only resource providers*

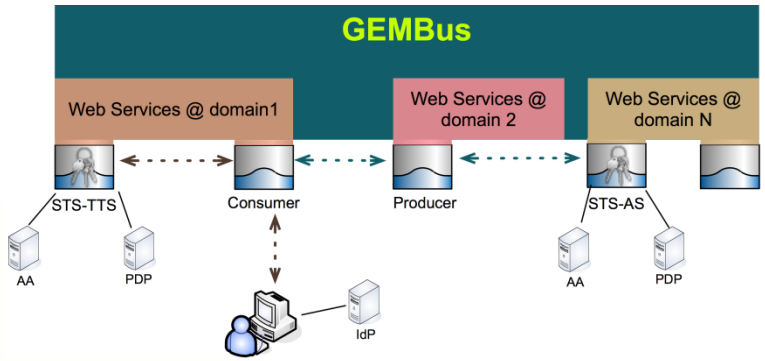
- **Operational** requirements
  translate easily to any kind of attribute source
- **Operational and assurance** requirements
  apply where assertions are bridged such as in the *STS*

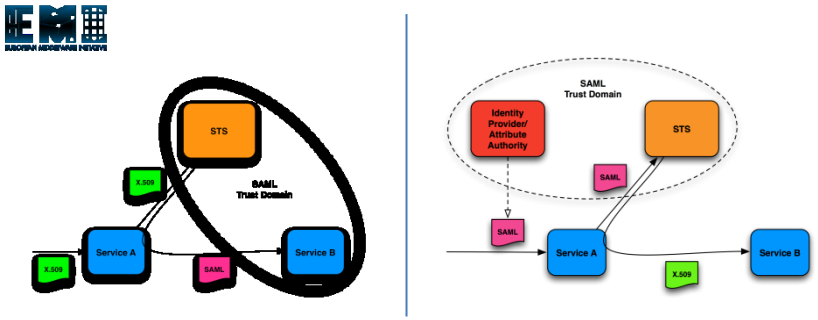
Carrying assertions across domains

Service access crosses technology and domain boundaries and may need translating in a Security Token Service (STS)

- trust relationship
- operational requirements

STS examples: GEMBus, EMI-STS, ...





Requirements on

- assurance level
- operational security
- auditing, data protection

and transparency of process all remain

GEMBus image by Diego Lopez, RedIRIS and GEANT, 22nd EUGridPMA meeting
EMI STS image by Christoph Witzig, SWITCH and EMI, 22nd EUGridPMA meeting

Common Criteria and Diversity

- Up till now ...
  - providers of compute and storage services in e-Infra able to agree single ‘least common denominator’
  - many content-only (web site) providers could live with lower assurance and asked no real LoA requirements

... but this may be changing

- more diverse content and services being offered – via many mechanisms, both web and non-web
  - may need diversifying not only technology, but also LoA

So why IGTF?

- **Trust is technology independent**

- **Agreeing on common minimum requirements on global scale**
  - facilitates interoperation across infrastructures
  - significantly reduces potential for failures and obstacles for interop

- **Participative model, including major relying parties and national representatives, ensures commensurate security level**
  - the single assurance level is convenient, but the world *will* likely diversify
  - the IGTF assurance levels will follow and adapt as a result
  - as well as expand to address changing technologies

Defining assurance requirements need strong involvement by relying parties, resource providers and users

International Grid Trust Federation –
http://www.igtf.net/

EUGridPMA
European Policy Management Authority for grid authentication in e-Science –
https://www.eugridpma.org/