International Grid Trust Federation

towards worldwide interoperability in identity management

UK Presidency 2005 e-IRG Meeting

David L. Groep, IGTF and EUGridPMA Chair, 2005-12-13

Outline

Grid Security

- Authentication vs. Authorisation
- Grid Identity Management

Authentication Federation

- EUGridPMA
- International Grid Trust Federation
- Common Guidelines and Requirements

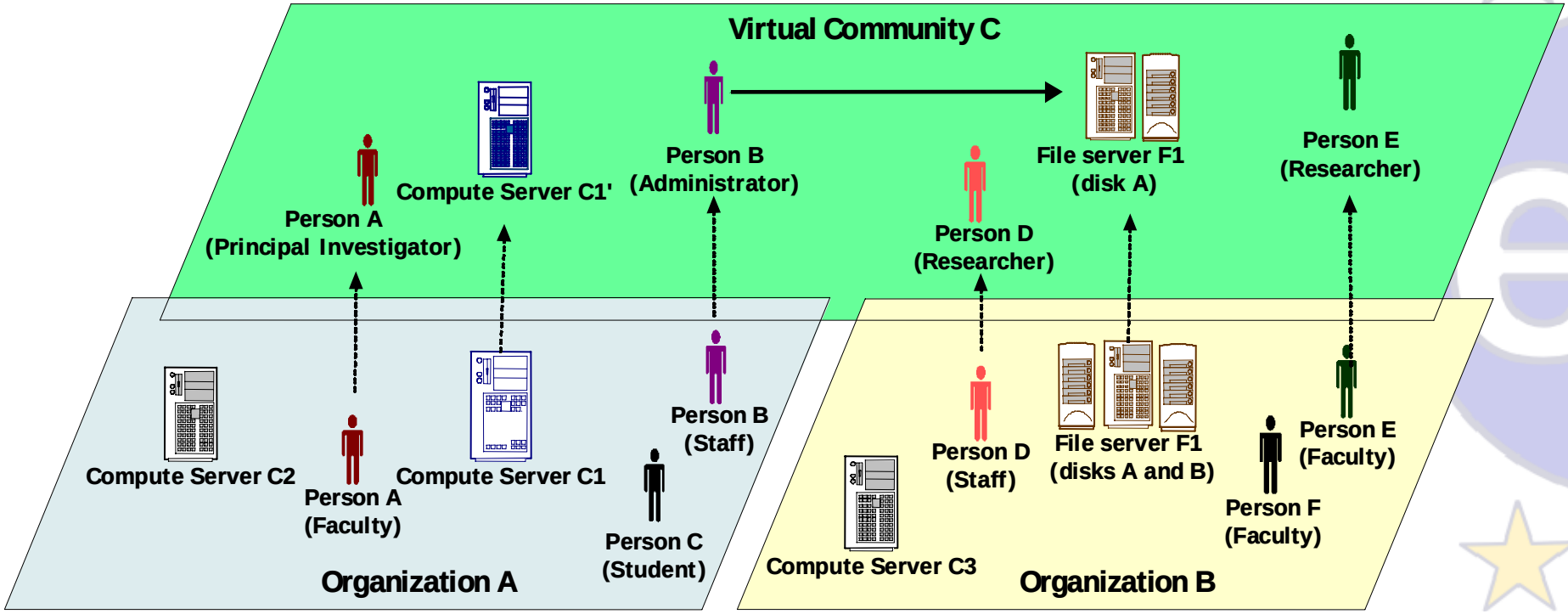
A roadmap for an integrated AAI

Essentials on Grid Security

- Access to shared services
  - cross-domain authentication, authorization, accounting, billing
  - common generic protocols for collective services
- Support multi-user collaborations
  - can contain individuals acting alone – their home organization administration may not know about their activities
  - organized in ‘Virtual Organisations’
- Enable ‘easy’ single sign-on
  - best security must be hidden from the user as far as possible
- Resource owner must always stay in control

Virtual vs. Organic structure

- Virtual communities (Virtual Organisations) are many
- A single person will typically be in many communities
  - Users want single sign-on across all these communities



Graphic from Frank Siebenlist, ANL & Globus Alliance
GGF OGSA Working Group

Stakeholders in Grid Security

Grid Security is user centric

- Conceptually, all members of a VO are equal
  - users can provide their own services
  - provider organisations may or may not have human members (or they actually only sell resources to a VO)
- There is no *a priori* trust relationship between members
  - VO lifetime can vary from hours to decades
  - VO not necessarily persistent (both long- and short-lived)
  - people and resources are members of many VOs
- … but a relationship is required
  - as a basis for authorising access
  - for traceability and liability, incident handling, and accounting

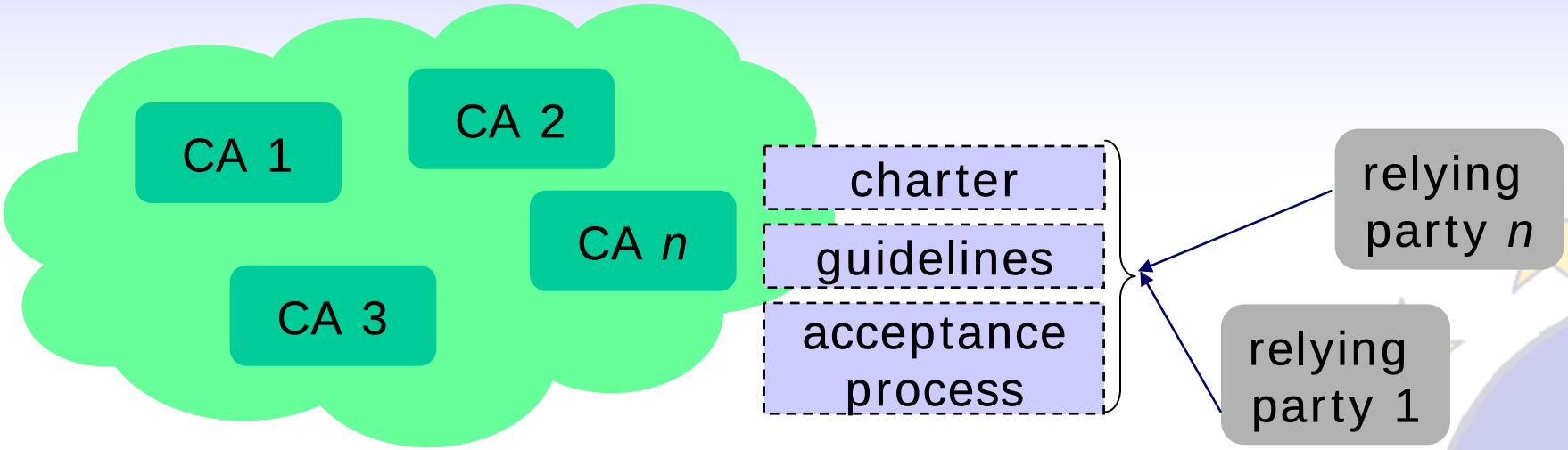
Separating *Authentication* and *Authorization*

- Single Authentication token (“passport”)
  - issued by a party trusted by all,
  - recognised by many resource providers, users, and VOs
  - satisfy traceability and persistency requirement
  - in itself does not grant any access, but provides a unique binding between an identifier and the subject
- Per-VO Authorisations (“visa”)
  - granted to a person/service via a virtual organisation
  - based on the ‘passport’ name
  - acknowledged by the resource owners
  - providers can obtain lists of authorised users per VO, but can still ban individual users

Authentication … academia, industry, and …

- National PKI
  - in generally uptake of 1999/93/EC and e-Identification is slow
  - where available, a national PKI can be leveraged
- Various commercial providers
  - Main commercial drive: secure web servers based on PKI
  - Entrust, Global Sign, Thawte, Verisign, SwissSign, …
  - primary market is *server* authentication, not end-user identities
  - usually expensive but don't actually subsume liability …
  - are implicitly (but maybe unduly) trusted by many, since web browsers pre-install the roots of trust
  - use of commercial CAs solves the 'pop-up' problem ... so for (web) servers a pop-up free service is still needed
- Academic PKI
  - generally a task of the NREN or national e-science project
  - got better attention only after the advance of grid computing

Federation Model for Grid Authentication



- A Federation of many independent CAs
  - common minimum requirements
  - trust domain as required by users and relying parties
  - well-defined and peer-reviewed acceptance process
- No strict hierarchy with a single top
  - spread of reliability, and failure containment (resilience)
  - maximum leverage of national efforts and complementarities

Relying parties in Grid Security

- In Europe
  - Enabling Grid for E-sciencE (EGEE) (222 sites)
  - Distributed European Infrastructure for Supercomputer Applications (DEISA) (~11 sites)
  - South Eastern Europe: SEE-GRID (10 countries)
  - *many national projects (VL-e, UK e-Science, Grid.IT, IRISgrid, …)*
- In the Americas
  - EELA: E-infrastructure Europe and Latin America (24 partners)
  - WestGrid (6 sites), GridCanada, …
  - Open Science Grid (OSG) (54 sites)
  - TeraGrid (9 sites)
  - *and also many others …*
- In the Asia-Pacific
  - AP Grid (~10 countries and regions participating)
  - Pacific Rim Applications and Grid Middleware Assembly (~15 sites)
  - …

~400

data as per December 8th, 2005

Relying Party issues to be addressed

Common Relying Party requests on the Authorities

1. standard accreditation profiles sufficient to assure **approximate parity** in CAs
2. monitor [signing namespaces for **name overlaps**
3. a **forum** [to] participate and raise issues
4. [operation of] a **secure collection point** for information about CAs which you accredit
5. **common practices** where possible

[list courtesy of the Open Science Grid]

Building the federation

- PKI providers ('CAs') and Relying Parties ('sites') together shape the common requirements
  - Several *profiles* for different identity management models
  - Authorities testify to compliance with profile guidelines
  - Peer-review process within the federation to (re) evaluate members on entry & periodically
  - Reduce effort on the relying parties
    - single document to review and assess for all CAs
  - Reduce cost on the authorities
    - no audit statement needed by certified accountants
    - but participation in the federation comes with a price
    - requires that the federation remains manageable in size
- Ultimate decision *always* remains with the RP

The EUGridPMA

EUGridPMA founded April 2004 as a successor to the CACG

The European Policy Management Authority for Grid Authentication in e-Science (hereafter called EUGridPMA) is a body

- *to establish requirements and best practices for grid identity providers*
- *to enable a common trust domain applicable to authentication of end-entities in inter-organisational access to distributed resources.*

As its main activity the EUGridPMA

- *coordinates a Public Key Infrastructure (PKI) for use with Grid authentication middleware.*

The EUGridPMA itself does not provide identity assertions, but instead asserts that - within the scope of this charter – the certificates issued by the Accredited Authorities meet or exceed the relevant guidelines.

EUGridPMA Membership

EUGridPMA membership for (classic) Authorities

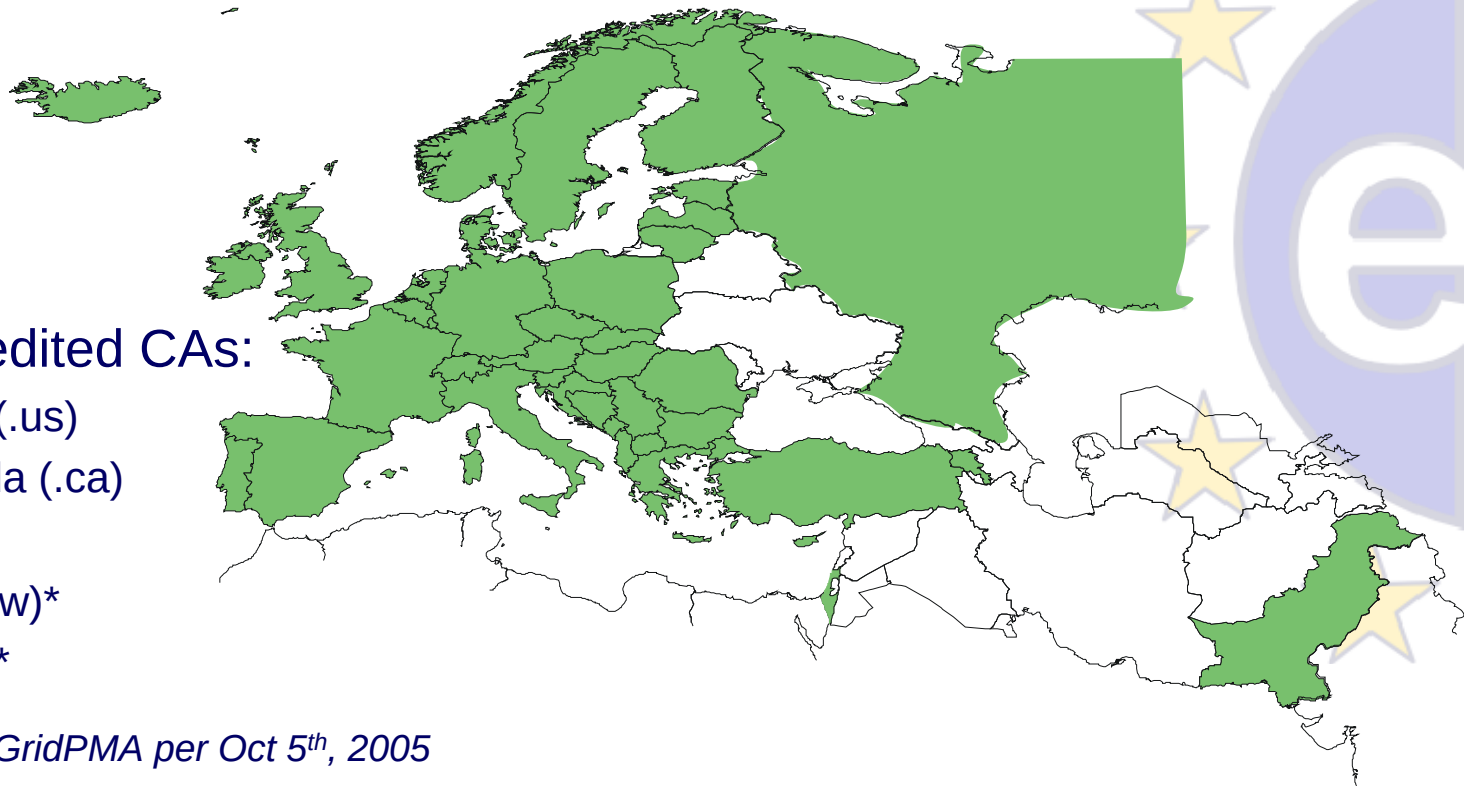
- a single Authority per
  - country,
  - large region (e.g. the Nordic Countries), or
  - international treaty organization.
- ‘serve the largest possible community with a small number of stable CAs’
- operated as a long-term commitment
  - many CAs are operated by the (national) NREN (CESNET, ESnet, Belnet, NIIF, EEnet, SWITCH, DFN, …)
  - or by the e-Science programme/science foundation (UK eScience, VL-e, CNRS, …)

Relying Parties: DEISA, EGEE, SEE-GRID, TERENA, …

Coverage of the EUGridPMA

Green: Countries with an accredited CA

- The EU member states (except LU, MT)
- + AM, CH, IL, IS, NO, PK, RU, TR, “SEE-catch-all”

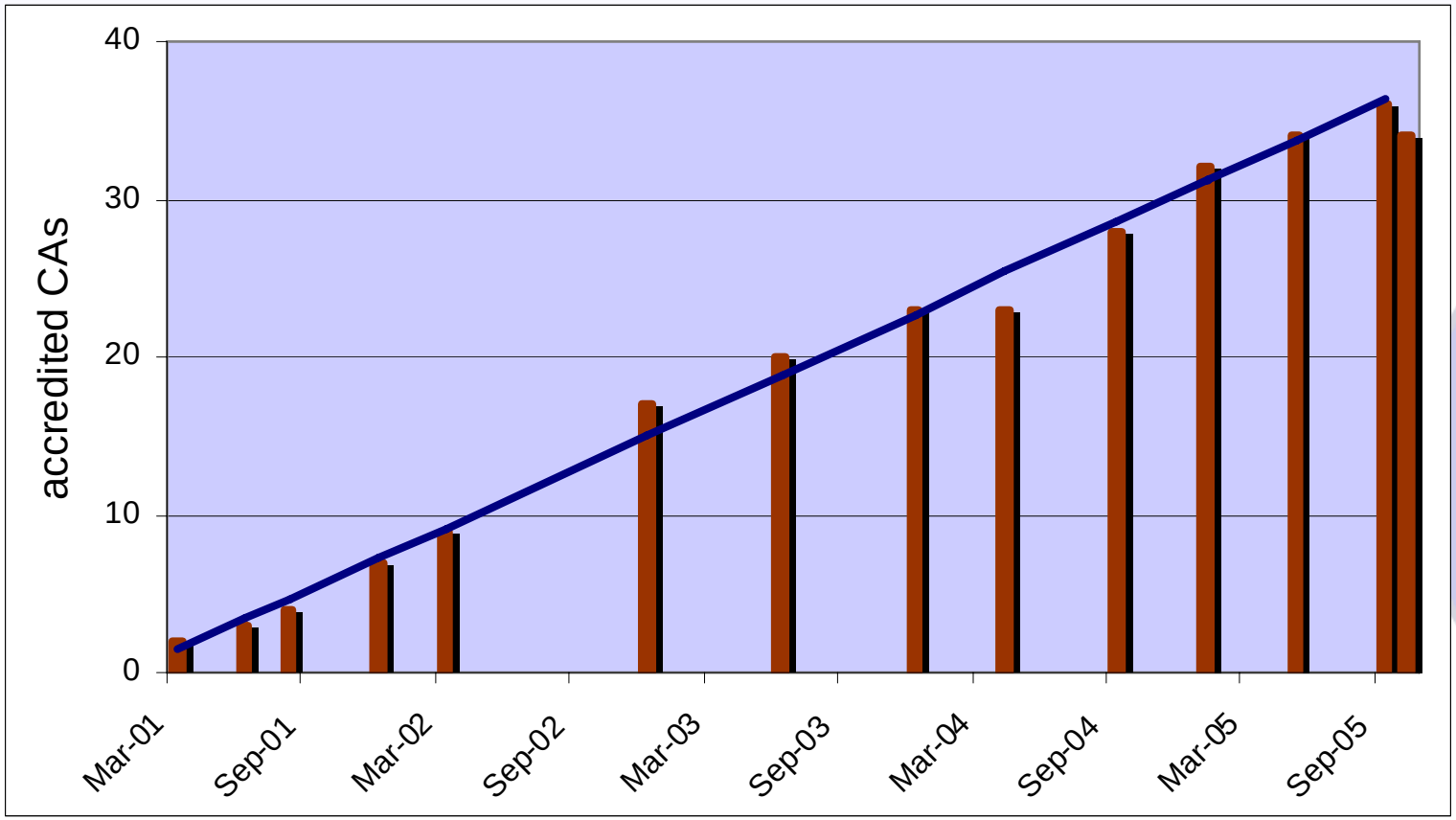


Other Accredited CAs:

- DoEGrids (.us)
- GridCanada (.ca)
- CERN
- ASGCC (.tw)*
- IHEP (.cn)*

** Migrated to APGridPMA per Oct 5th, 2005*

Growth of the EDG CACG and EUGridPMA



History

Five years of growth

December 2000:

First CA coordination meeting for the FP5 DataGrid project

March 2003:

Tokyo Accord (GGF7)

April 2004:

Foundation of the EUGridPMA

June 2004:

Foundation of the APGridPMA

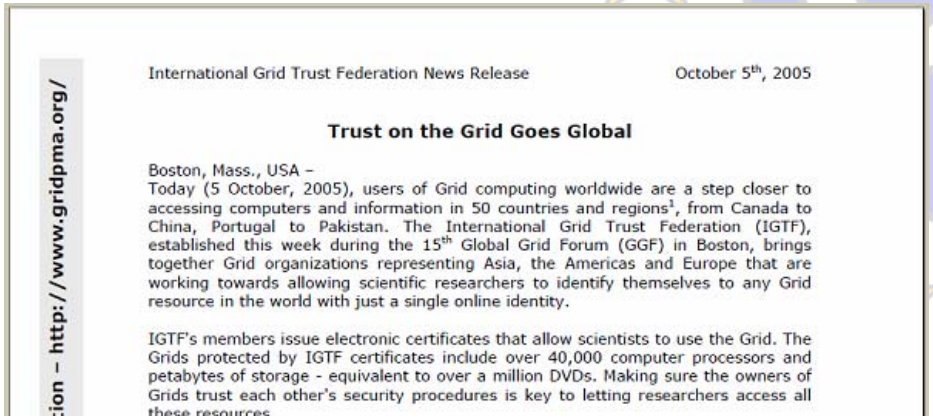
June 2005:

Foundation of TAGPMA (GGF14)

5 October 2005:

Establishment of the International Grid Trust Federation IGTF

…



ion – http://www.gridpma.org/

International Grid Trust Federation News Release October 5th, 2005

Trust on the Grid Goes Global

Boston, Mass., USA –
Today (5 October, 2005), users of Grid computing worldwide are a step closer to accessing computers and information in 50 countries and regions[1], from Canada to China, Portugal to Pakistan. The International Grid Trust Federation (IGTF), established this week during the 15th Global Grid Forum (GGF) in Boston, brings together Grid organizations representing Asia, the Americas and Europe that are working towards allowing scientific researchers to identify themselves to any Grid resource in the world with just a single online identity.

IGTF's members issue electronic certificates that allow scientists to use the Grid. The Grids protected by IGTF certificates include over 40,000 computer processors and petabytes of storage - equivalent to over a million DVDs. Making sure the owners of Grids trust each other's security procedures is key to letting researchers access all these resources

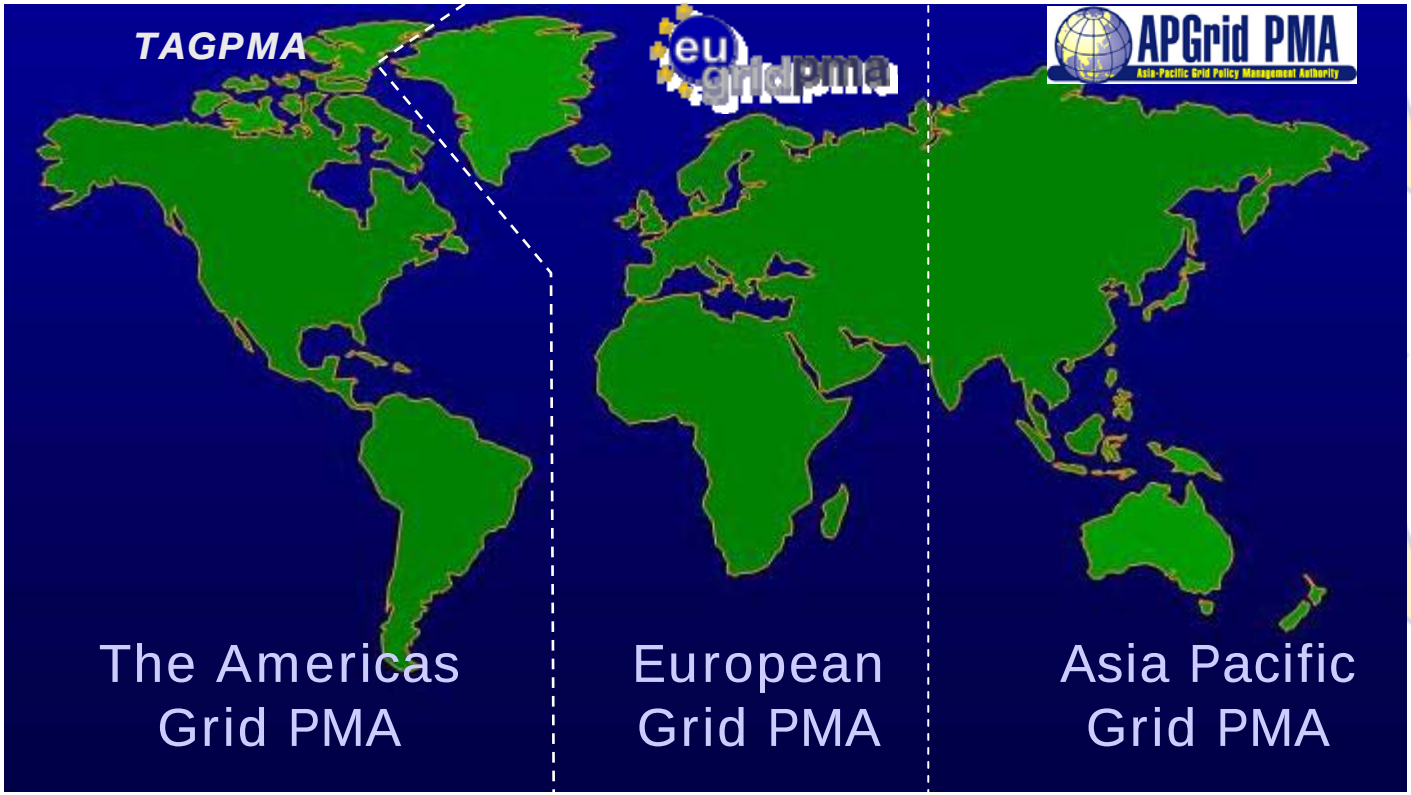
March 2003: the Tokyo Accord

- … meet at GGF conferences to …
- … work on … Grid Policy Management Authority: GRIDPMA.org
- develop Minimum requirements – based on EDG work
- develop a Grid Policy Management Authority Charter
- [with] representatives from major Grid PMAs:
  - European Data Grid and Cross Grid PMA:
    16 countries, 19 organizations
  - NCSA Alliance
  - Grid Canada
  - DOEGrids PMA
  - NASA Information Power Grid
  - TERENA
  - Asian Pacific PMA:
    AIST, Japan; SDSC, USA; KISTI, Korea;
    BII, Singapore; Kasetsart Univ., Thailand; CAS, China

History

2005: Extending Trust – the International Grid Trust Federation

- common, global best practices for trust establishment
- better manageability of the PMAs



APGridPMA

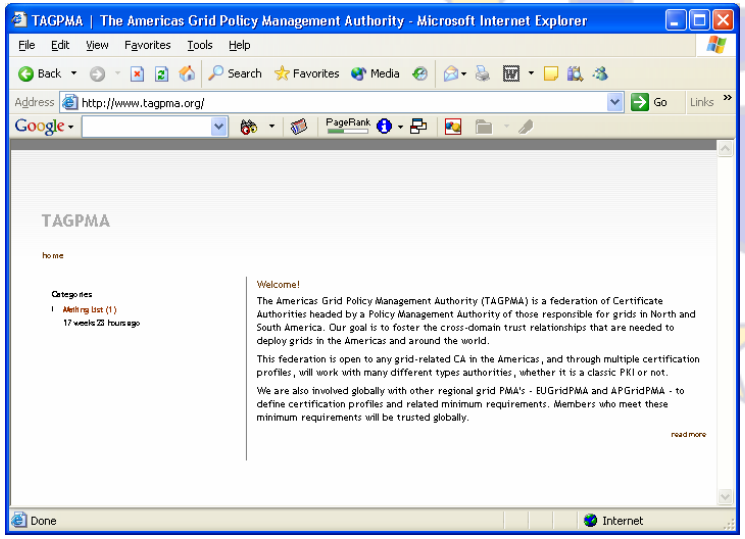
- 13 members from the Asia-Pacific Region,

  - AIST (.jp)
  - APAC (.au)
  - BMG (.sg)
  - CMSD (.in)
  - HKU CS SRG (.hk)
  - KISTI (.kr)
  - NCHC (.tw)
  - NPACI (.us)
  - Osaka U. (.jp)
  - SDG (.cn)
  - USM (.my)
  - IHEP Beijing (.cn)
  - ASGCC (.tw)

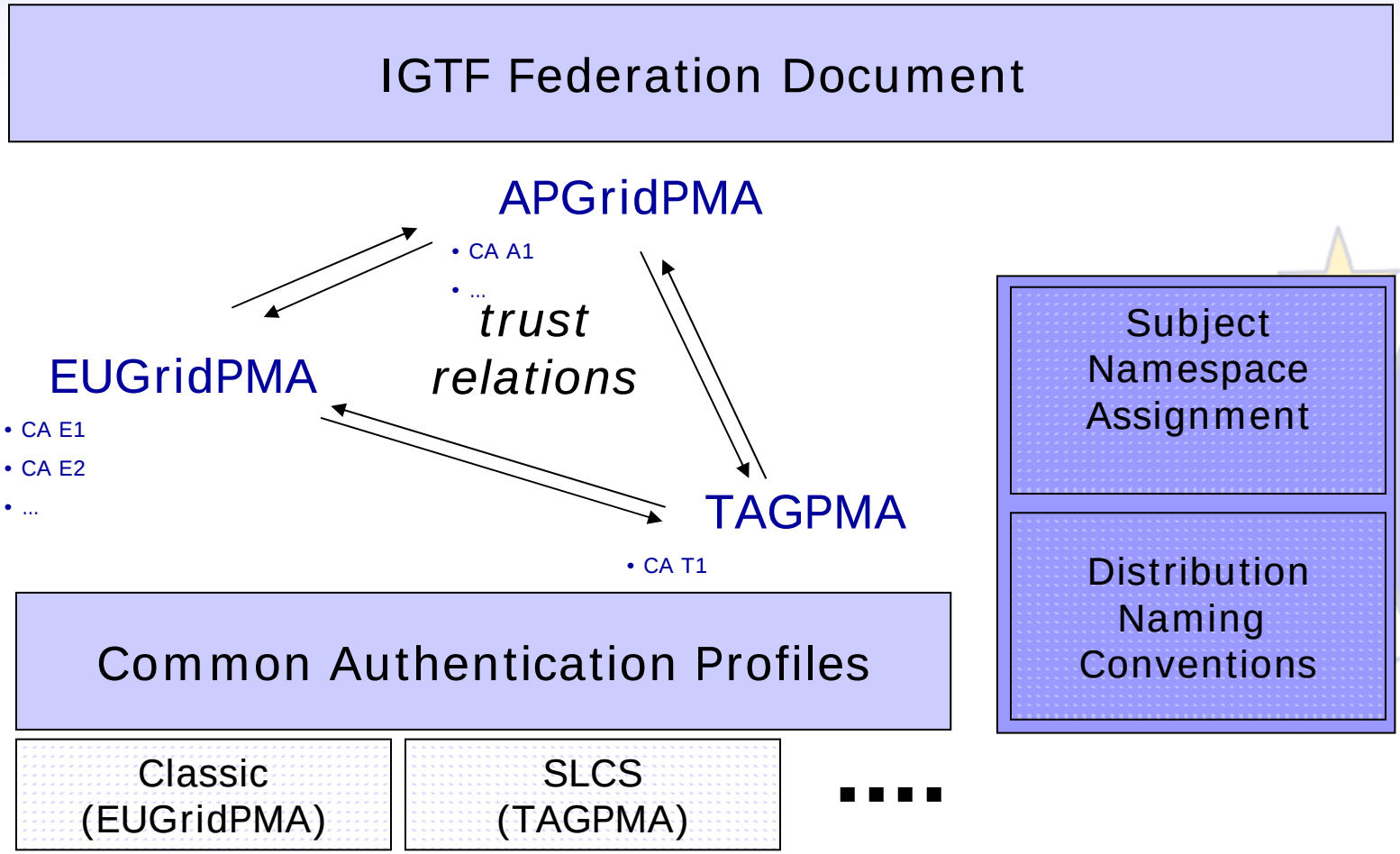
- Launched June 1st, 2004, chaired by Yoshio Tanaka
- Minimum Requirements taken from EUGridPMA
- First face-to-face meeting on Nov 29th, 2005
- Today 6 ‘production-quality’ authorities in operation

TAGPMA

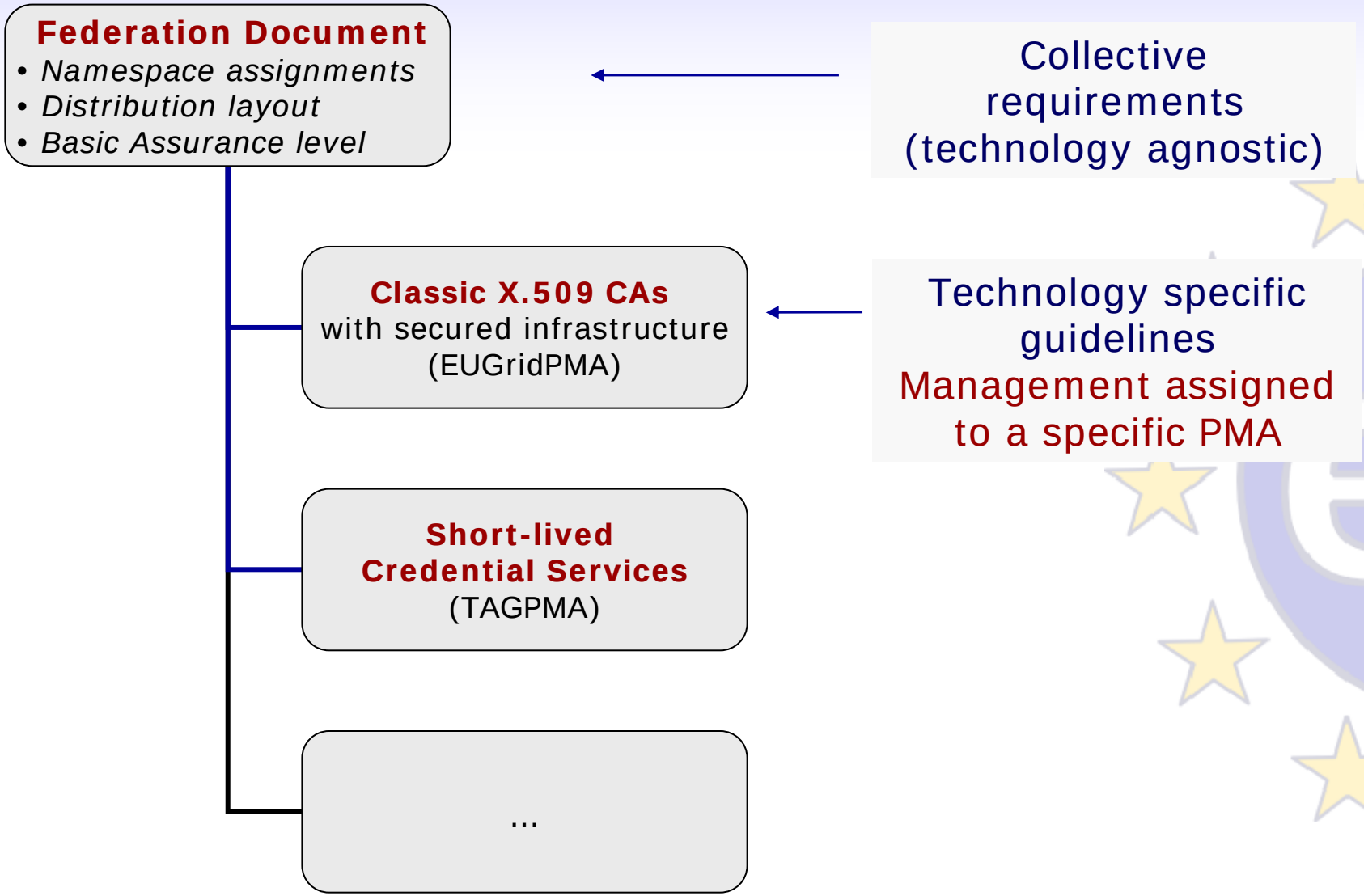
- To cover all of the Americas
- 8 members to date
  - Canarie (.ca)
  - OSG (.us)
  - TERAGRID (.us)
  - Texas H.E. Grid (.us)
  - DOEGrids (.us)
  - SDSC (.us)
  - FNAL (.us)
  - Dartmouth (.us)
  - Brazil (pending)
- Launched June 28th, 2005 chaired by
  Darcy Quesnel, CANARIE



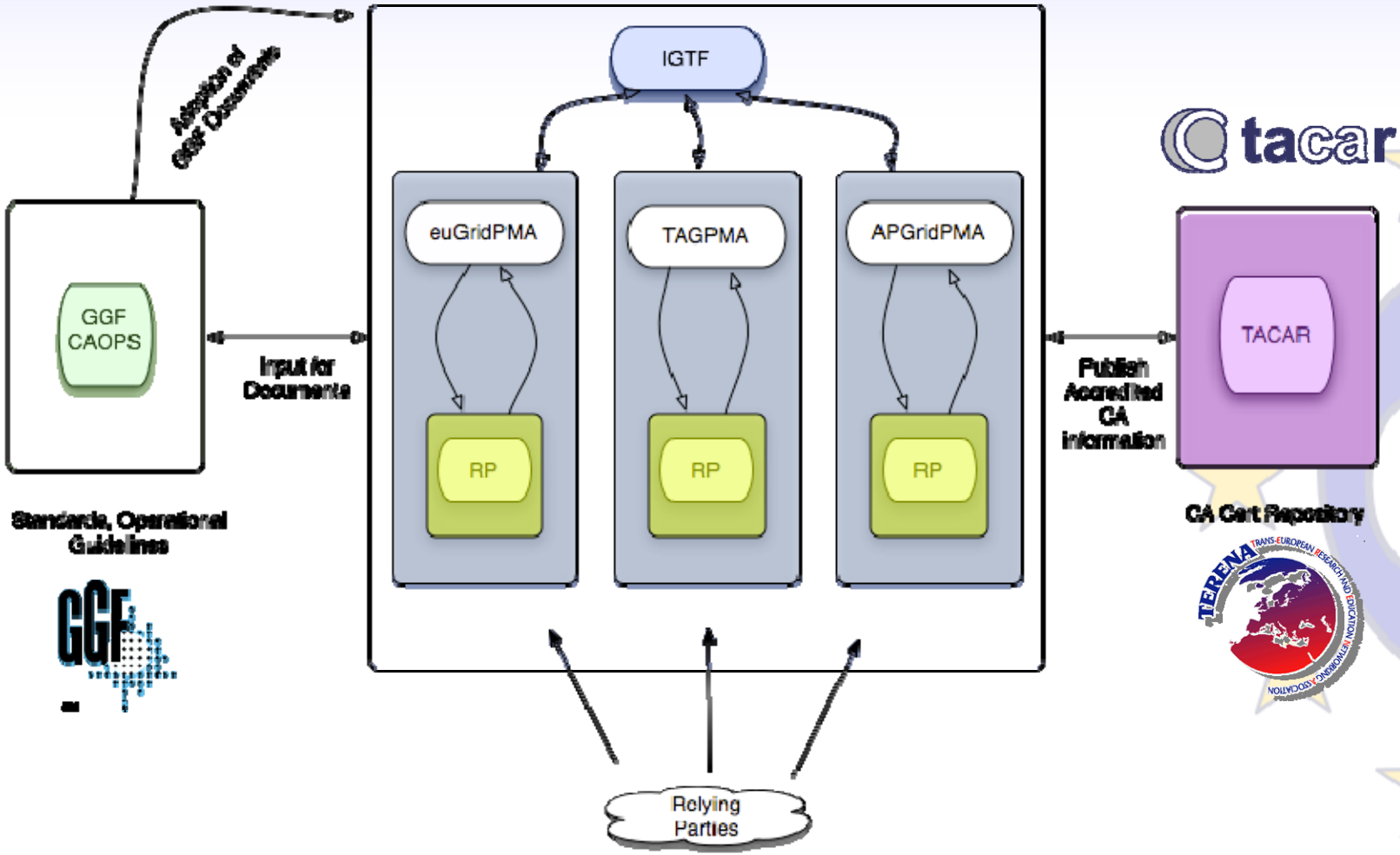
IGTF Federation Structure



Common Guidelines for all of the IGTF



Relationships: IGTF, PMAs, TACAR and GGF



Grid Authorization today

Leverages authentication provided by a *PKI (the 'passport')*

- Identity management decoupled from access control
- Creation of short-lived 'tokens' ('proxy' certificates) for single sign-on based on these identities

Status today

- Variety of mechanisms
  - Per-resource list of authorized users
  - Directories of authorized users
  - Embedded assertions
- Variety of sources of authority
  - Semantics to describe roles and rights differs
  - No common namespace
- Integration with other AA mechanisms still in progress…

Recent developments in AAI

- from the EUGridPMA side
  - Extending PMA and the IGTF actively to more countries and regions, and to more mechanisms
- from TERENA
  - NRENs-GRID workshop series
  - TF-EMC2 / TF-Mobility
  - possible TACAR extensions
- REFEDS – Research and Education Federations
  - broad AAI scope
  - IGTF, eduroam, A-Select, PAPI, SWITCH-AAI, InCommon, HAKA, FEIDE/Moria
  - See **http://www.terena.nl/tech/refeds/**

EUGridPMA – http://www.eugridpma.org/

IGTF – http://www.gridpma.org/