A history of the CACG, EUGridPMA, and the IGTF

(and some next steps)

First APGridPMA Face-to-Face Meeting Beijing

David Groep, 2005-11-29

A brief history …

From the CACG to EUGridPMA to IGTF …

- The EU DataGrid CACG
- The EUGridPMA: charter and growth
- IGTF Foundation on October 5th, 2005

The Federation: structure and documents

- Common guidelines
- Authentication Profiles
- Distribution and common naming
- Related bodies: GGF and TACAR

Current issues and new challenges

In the Beginning: the EU DataGrid CACG

The EU DataGrid in 2000 needed a PKI for the test bed

- Both end-user and service/host PKI
- CACG (actually David Kelsey) had the task of creating this PKI
  - for Grid Authentication only
  - no support for long-term encryption or digital signatures
- Single CA was not considered acceptable
  - Single point of attack or failure
- One CA per country, large region or international organization
  - CA must have strong relationship with RAs
  - Some pre-existing CAs
- A single hierarchy would have excluded existing CAs and was not convenient to support with existing software
- Coordinated group of peer CAs was most suitable choice

History

Five years of growth

December 2000:

First CA coordination meeting for the DataGrid project

March 2001:

First version of the minimum requirements

5 CAs: France (CNRS), Portugal (LIP), Netherlands (NIKHEF), CERN, Italy (INFN), UK (UK eScience)

December 2002:

Extension to other projects: EU-CrossGrid

…

History

‘Reasonable procedure … acceptable methods’

- Requirements and Best Practices for an “acceptable and trustworthy” Grid CA

```
Minimum requirements for RA - Testbed 1
---------------------------------------
An acceptable procedure for confirming the identity of the requestor and the right to ask
for a certificate e.g. by personal contact or some other rigorous method
The RA should be the appropriate person to make decisions on the right to ask for a
certificate and must follow the CP.

Communication between RA and CA
-------------------------------
Either by signed e-mail or some other acceptable method, e.g. personal (phone) contact with
known person

Minimum requirements for CA - Testbed 1
---------------------------------------
The issuing machine must be:
        a dedicated machine
        located in a secure environment
        be managed in an appropriately secure way by a trained person
        the private key (and copies) should be locked in a safe or other secure place
        the private keu must be encrypted with a pass phrase having at least 15 characters
        the pass phrase must only be known by the Certificate issuer(s)
        not be connected to any network

minimum length of user private keys must be 1024
min length of CA private key must be 2048
requests for machine certificates must be signed by personal certificates or verified by
other appropriate means
...
```

History

Building the initial trust fabric

- Identity only, no roles or authorization attributes (that's left for other mechanisms) – goal is a single common identity for every person

- PKI providers ('CAs') and Relying Parties ('sites') together shape the minimum requirements
  - Authorities testify compliance with these 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 CAs:
    - no audit statement needed by certified accountants ($$$)
    - but participation in the Federation does come with a price
  - Requires that the federation remains manageable in size
- Ultimate decision *always* remains with the RP

History

March 2003: The Tokyo Accord

- … meet at GGF conferences. …
- … 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

At The End of Data Grid …

In December 2003, the EU DataGrid project ended …

… and the Grid and CA arena had changed:

- the new EGEE project was just one of 3 *e*-Infrastructures
- the LHC Computing Grid turned into a production system
- TERENA TF-AACE had established TACAR

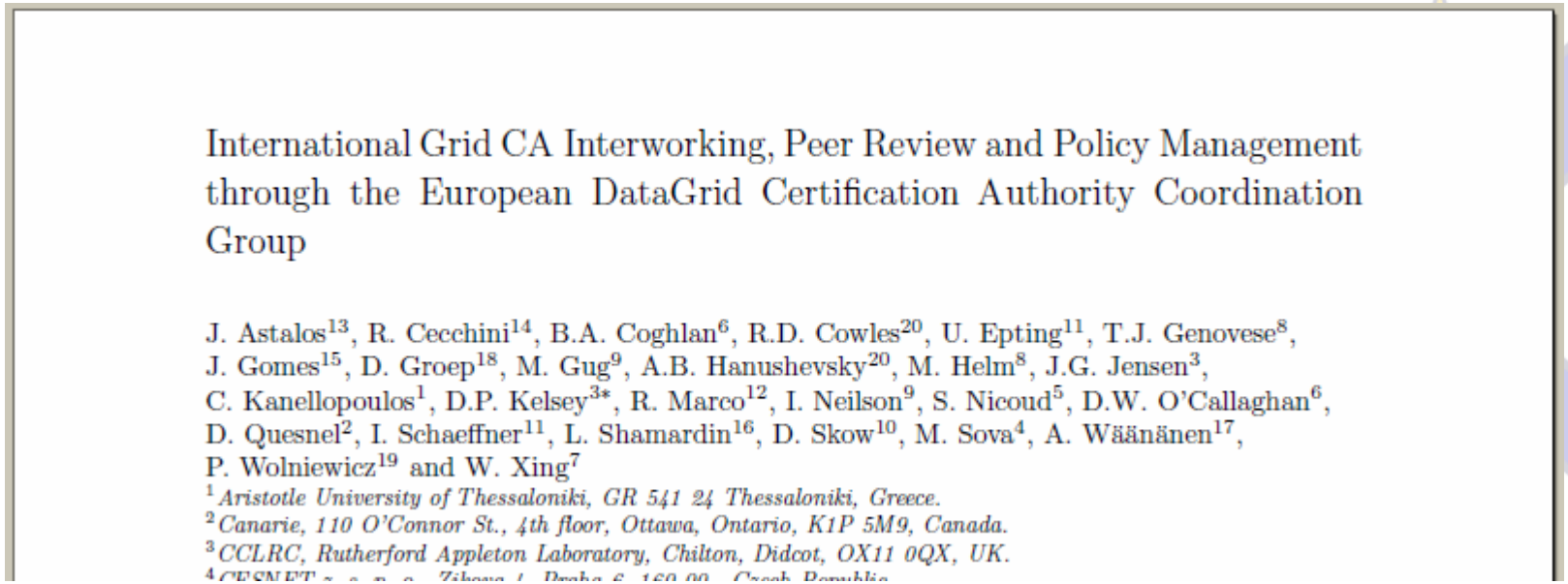
This called for a pan-European coordinated effort

- Encompassing all three e-Infrastructure projects
- To be recognized as a European coordination body
- With support from the new e-Infrastructure Reflection Group
- Fostered by the Irish EU Presidency in 2004

History

… we published and moved on to …

- Best practices of the CACG documented in the paper by David O'Callaghan *et al*.
  - *Lecture Notes in Computer Science* 3470 pp. 285-295



International Grid CA Interworking, Peer Review and Policy Management through the European DataGrid Certification Authority Coordination Group

J. Astalos[13], R. Cecchini[14], B.A. Coghlan[6], R.D. Cowles[20], U. Epting[11], T.J. Genovese[8], J. Gomes[15], D. Groep[18], M. Gug[9], A.B. Hanushevsky[20], M. Helm[8], J.G. Jensen[3], C. Kanellopoulos[1], D.P. Kelsey[3*], R. Marco[12], I. Neilson[9], S. Nicoud[5], D.W. O'Callaghan[6], D. Quesnel[2], I. Schaeffner[11], L. Shamardin[16], D. Skow[10], M. Sova[4], A. Wäänänen[17], P. Wolniewicz[19] and W. Xing[7]

[1] *Aristotle University of Thessaloniki, GR 541 24 Thessaloniki, Greece.*
[2] *Canarie, 110 O'Connor St., 4th floor, Ottawa, Ontario, K1P 5M9, Canada.*
[3] *CCLRC, Rutherford Appleton Laboratory, Chilton, Didcot, OX11 0QX, UK.*
[4] *CESNET z. s. p. o., Zikova 4, Praha 6, 160 00, Czech Republic*

History

The EUGridPMA "constitution"

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) CAs:

- A single Certification Authority (CA)
  - per country,
  - large region (e.g. the Nordic Countries), or
  - international treaty organization.
- The goal is to serve the largest possible community with a small number of stable CAs
- operated as a long-term commitment

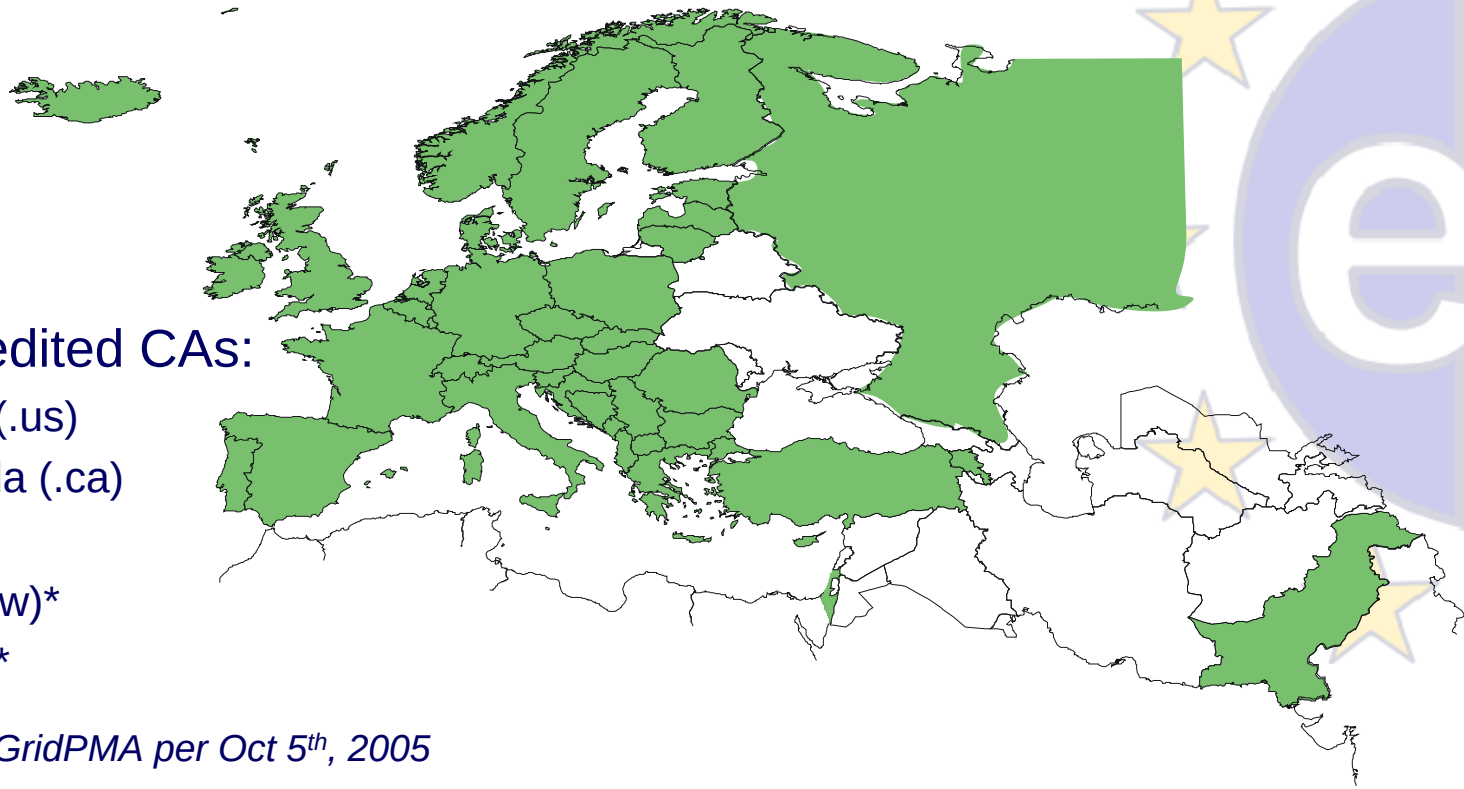
Many CAs are operated by the (national) NREN
(CESNET, ESnet, Belnet, NIIF, EEnet, SWITCH, DFN, …)

or by the e-Science programme/Science Foundation
(UK eScience, VL-e, CNRS, …)

Coverage of the EUGridPMA

Green: Countries with an accredited CA

- 23 of 25 EU member states (all 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*

The Catch-All CAs

Project-centric “catch all” Authorities

- For those left out of the rain in EGEE
  - CNRS “catch-all” (Sophie Nicoud)
  - coverage for all EGEE partners
- For the South-East European Region
  - regional catch-all CA
- For LCG world-wide
  - DoeGrids CA (Tony Genovese & Mike Helm, ESnet)
  - Registration Authorities through Ian Neilson

New CAs: the Accreditation Process

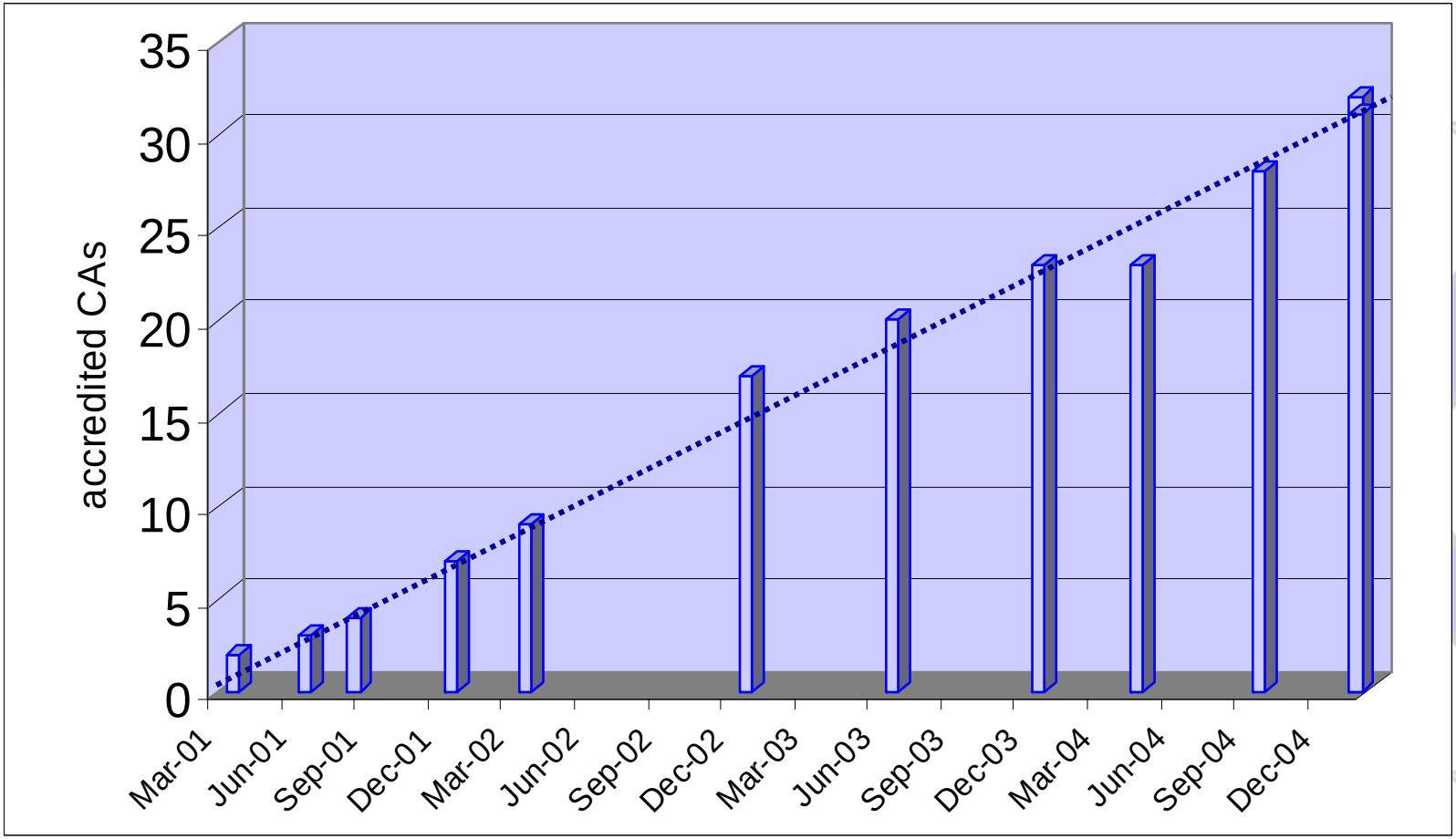
Accreditation Guidelines for EUGridPMA

Key elements:

- Codification of procedures in a CP(S) for each CA
  - *de facto* lots of copy/paste, except for vetting sections
- Peer-review process for evaluation
  - comments welcomed from all PMA members
  - two assigned referees
- In-person appearance during the review meeting

- Accreditation model for other PMAs typically embedded in their charter …
- Peer-auditing and periodic re-evaluation are needed

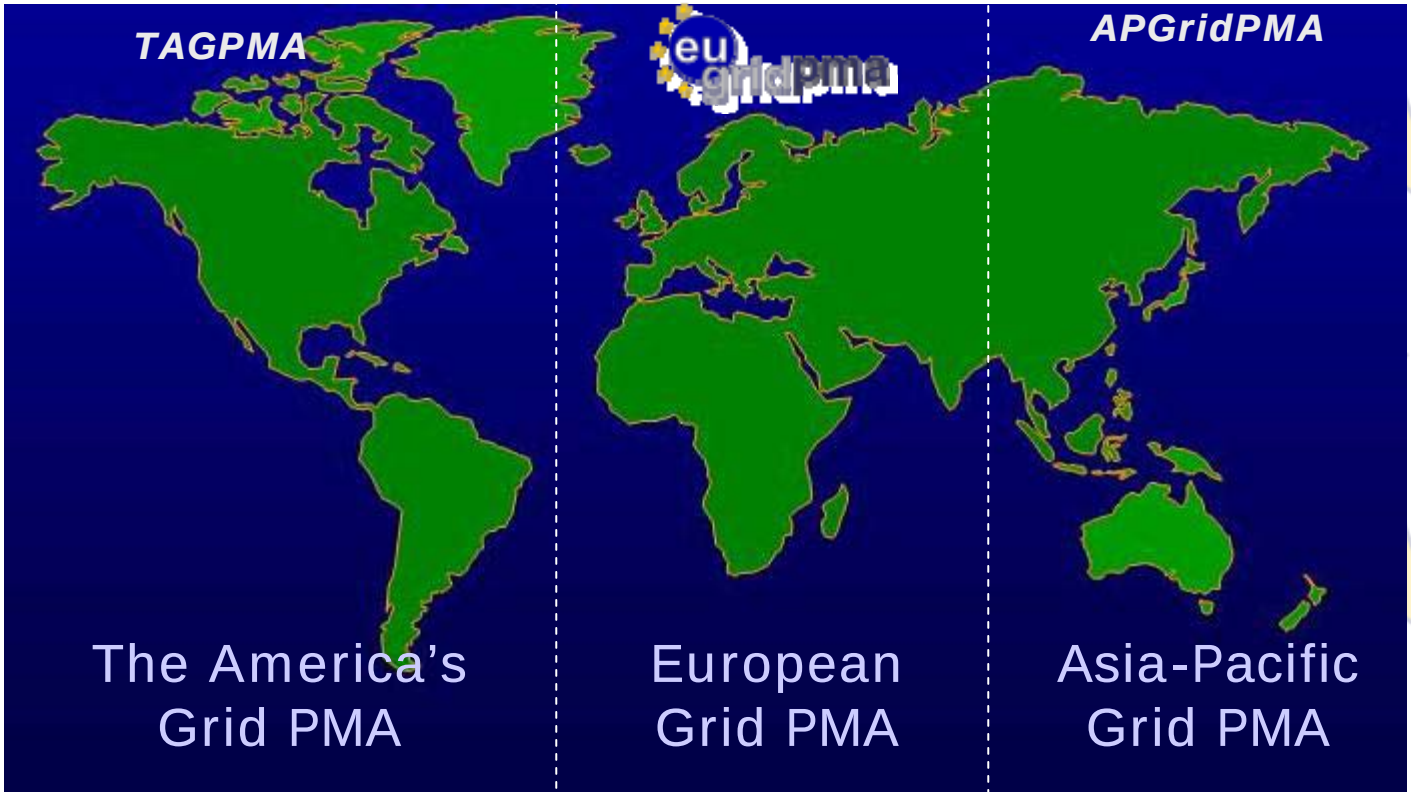
Growth of the CACG & EUGridPMA



History

Solution to Extending Trust: IGTF – the International Grid Trust Federation

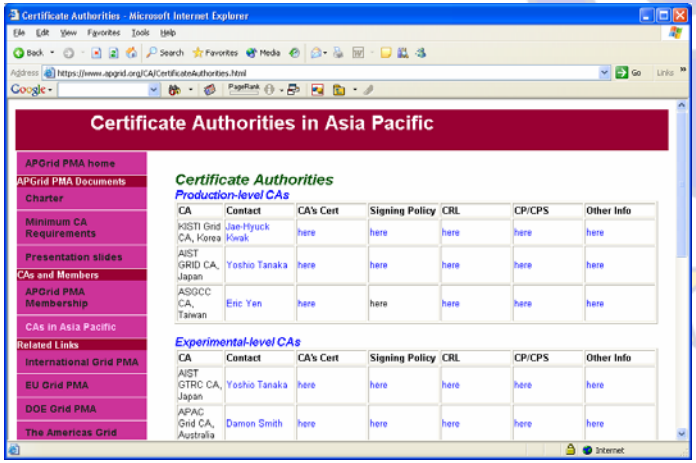
- common, global best practices for trust establishment
- better manageability and coordination of the PMAs



APGridPMA

- 13 members from the Asia-Pacific Region, chaired by Yoshio Tanaka (AIST)
  - 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
- 4 'production-quality' CAs
- Pioneered 'experimental' profile

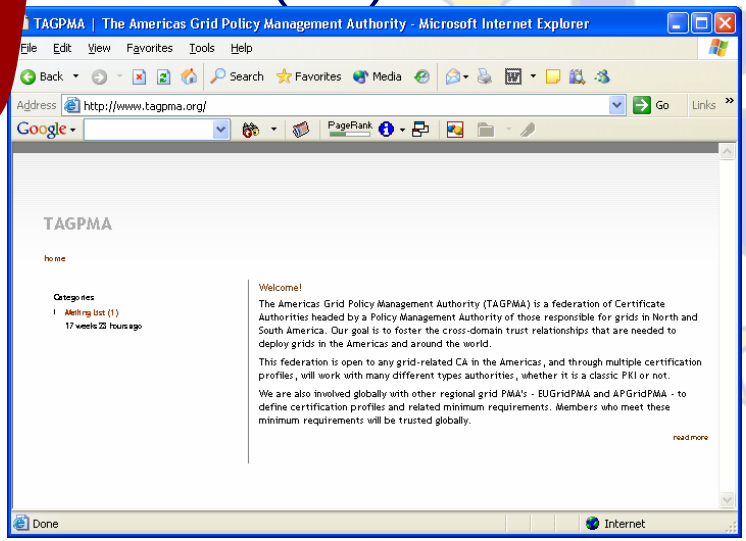
You know this already :-)



TAGPMA

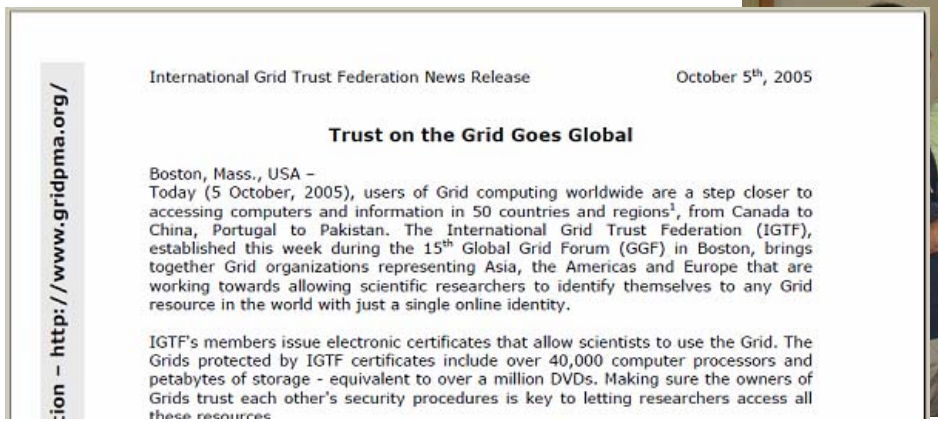
- 10 members to date, chaired by Darcy Quesnel (Canarie)
  - Canarie (.ca)
  - OSG (.us)
  - TERAGRID (.us)
  - Texas HE. Grid (.u
  - DOEG (.
  - SDSC (.
  - FNAL (.u
  - Dartmou
  - (.
  - Umich (.us)
  - Brazil (.br)
- Launched June 2
- Proposed n "SLCGS" (Lerbur s CA & al.)

See Darcy's Talk



Timeline

- March 2005: IGTF Draft Federation Document GGF13
- July 27th : APGridPMA approved version 0.7
- September 28th: EUGridPMA approval version 0.9
- October 5th: TAGPMA approved version 1.0
- October 5th: formal foundation of the IGTF



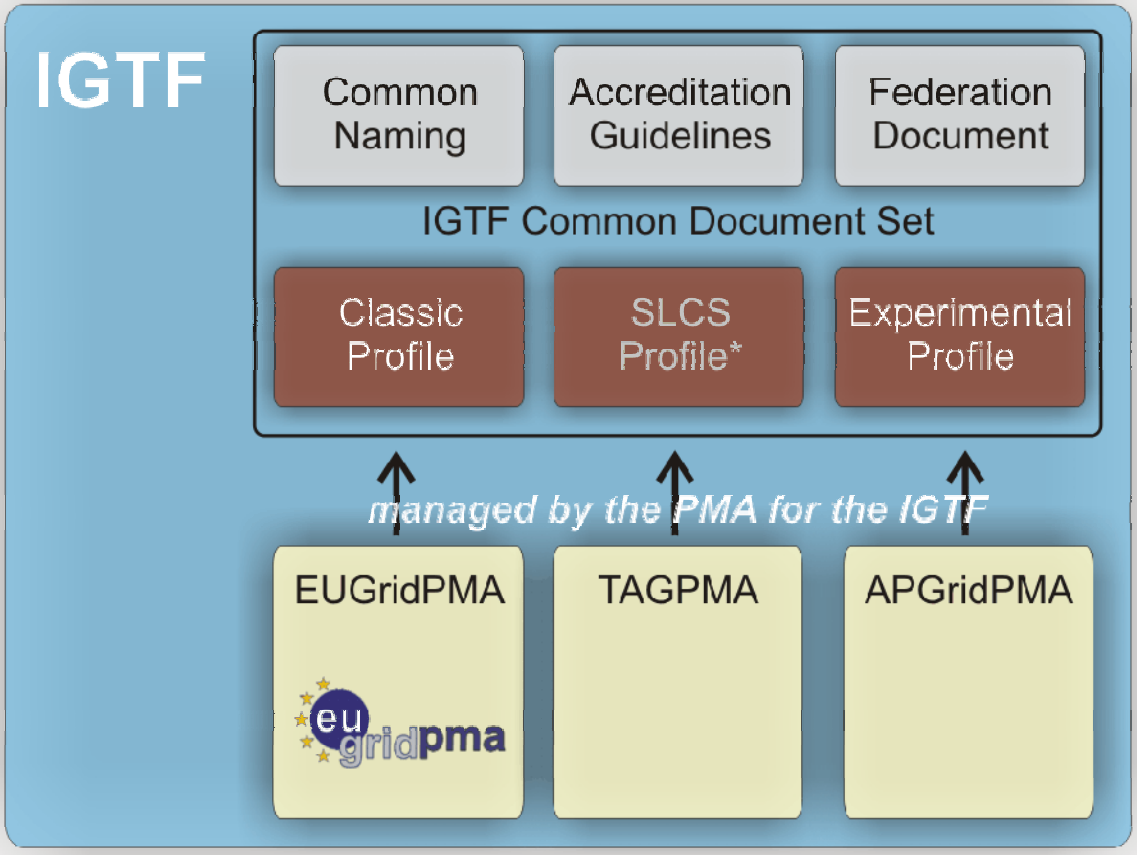
International Grid Trust Federation News Release October 5th, 2005

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

Common Guidelines across the IGTF



Relying Party issues to be addressed

Characteristics Relying Party requests

1. standard accreditation profiles sufficient to assure approximate parity in CAs

2. monitor [] signing namespaces for name overlaps and issue unique names

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)

Guidelines: common elements

- Coordinated namespace
  - Subject names refer to a unique entity (person, host)
  - Basis for authorization decisions
- Common Naming
  - *One-stop shopping* for all trust anchors in the federation
  - Trusted, redundant, download sources
- Concerns and ‘incident’ handling
  - Guaranteed point of contact
  - Forum to raise issues and concerns
- Requirement for documentation of processes
  - Detailed policy and practice statement
  - Open to auditing by federation peers

Guidelines: secured X.509 CAs

- Long-lived identity assertions
- Identity vetting procedures
  - Based on (national) photo ID's
  - Face-to-face verification of applicants via a network of Registration Authorities
  - Periodic renewal (once every year)
- Secure operation
  - off-line signing key or special (FIPS-140.3 or better) hardware
- Response to incidents
  - Timely revocation of compromised certificates

- Version 4.0 synchronised with Federation Document
- *The Annotated Minimum Requirements* on the Wiki

Guidelines: short-lived credential service

- Issue short-lived credentials (for grid: proxies) based on another site-local authentication system
  - e.g. Kerberos CA based on existing administration
- Same common guidelines apply
  - documented policies and processes
  - a reliable identity vetting mechanism
  - accreditation of the credential issuer with a PMA
- Same X.509 format, but no user-held secrets
- *New profile by TAGPMA in the Americas*

Guidelines: ‘Active Certificate Stores’ ??

Do we need one for ACS’s, for can we re-use the SLCS?

- Secure key/cert storage for end-users
- Backed by a “traditional” CA
- Releases short-lived tokens (RFC3820 “proxy” certs)
- User key data protected by “other” (possibly UHO) mechanisms
- ACS hosted by a trusted party
  (e.g. by the CA, the NREN, or an e-Science OpCenter)
- Profile yet to be written (Jens Jensen, Tony?, …)

Common Naming: the Distribution

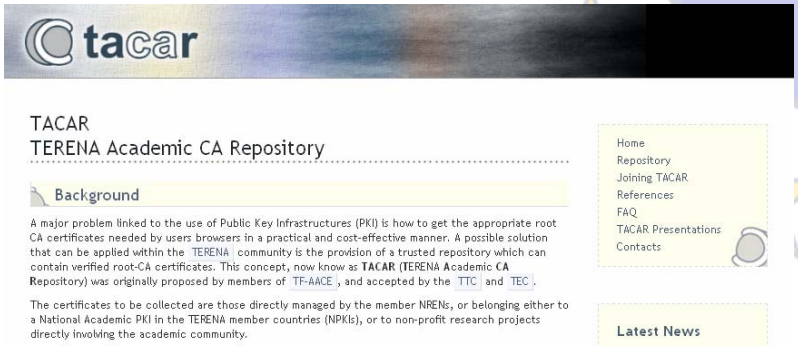
- Periodic, monthly, distribution of all trust anchors
  - Common for the entire IGTF
  - Includes all trust anchors for all profiles
    classic, SLCS, experimental*, …
  - Does not distinguished between accrediting PMAs
- Wide variety of formats
  - RedHat Package Management (RPM) system
    including a ‘meta’ package with dependencies per profile
  - ‘tar’ archives per CA, ordered per profile
  - Installation bundle suitable for ‘`./configure && make install`’
  - New formats (like JKS) on request
- Chairs can update the common back-end repository

TACAR

A trusted repository which contains verified root-CA certificates

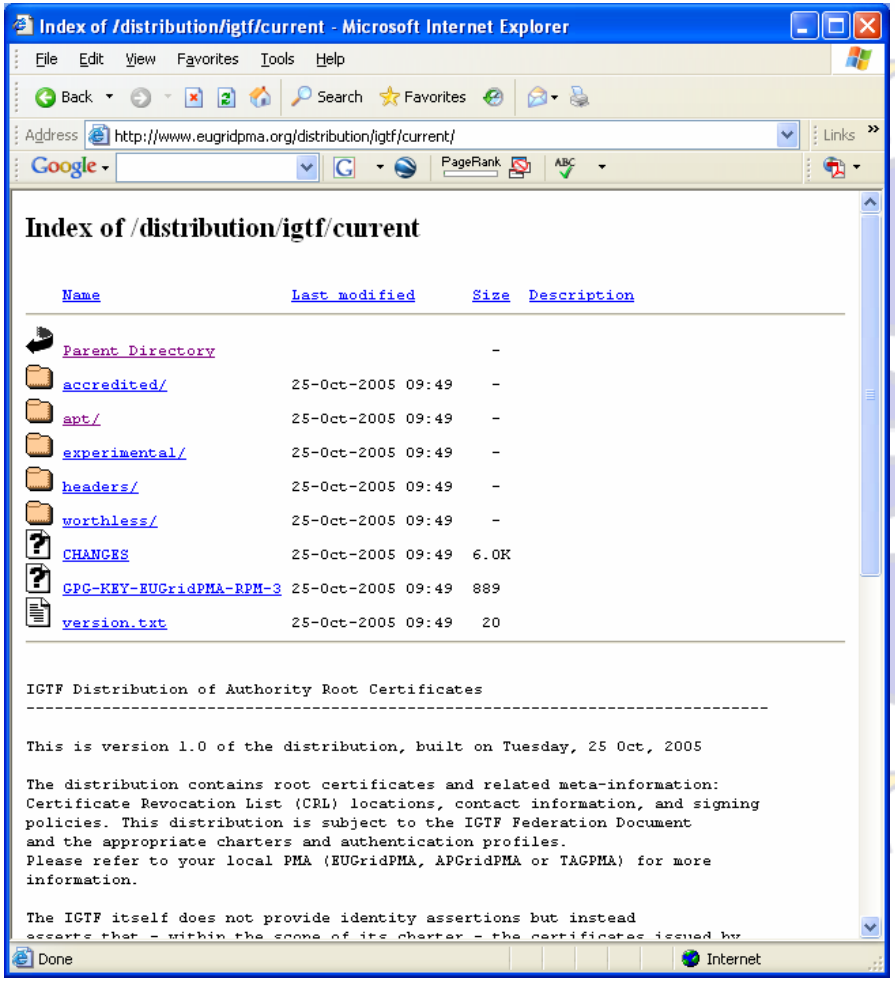
The certificates to be collected are those directly managed by the member NRENs, or belonging either to a National Academic PKI in the TERENA member countries (NPKIs), or to non-profit research projects directly involving the academic community.

- Authoritative source for validation of trust anchors
  - independent web administration makes for stronger trust
  - TACAR certificate itself published in paper/journals
- over 20 CA root certificates
  (and not exclusively for grid use)

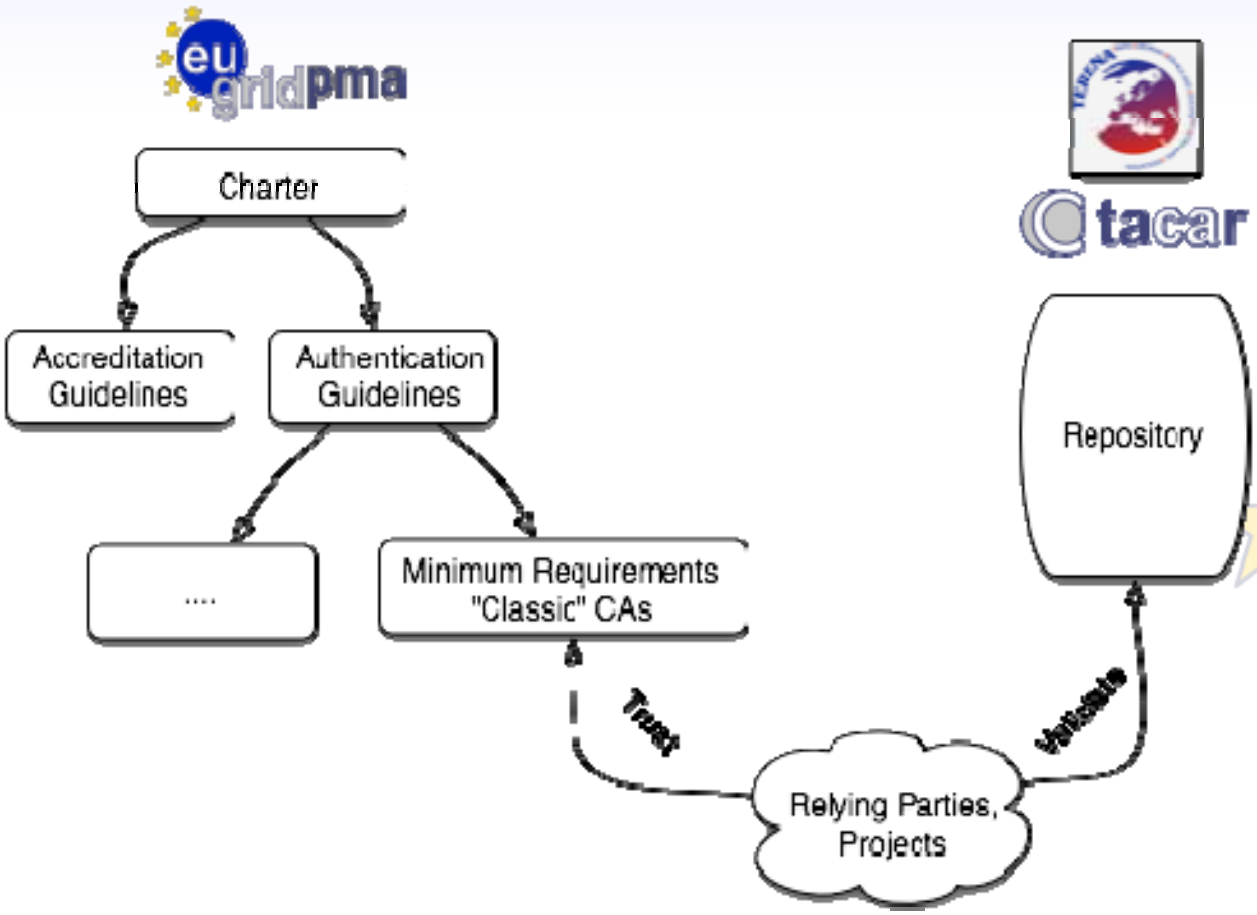


Access to the Distribution Repository

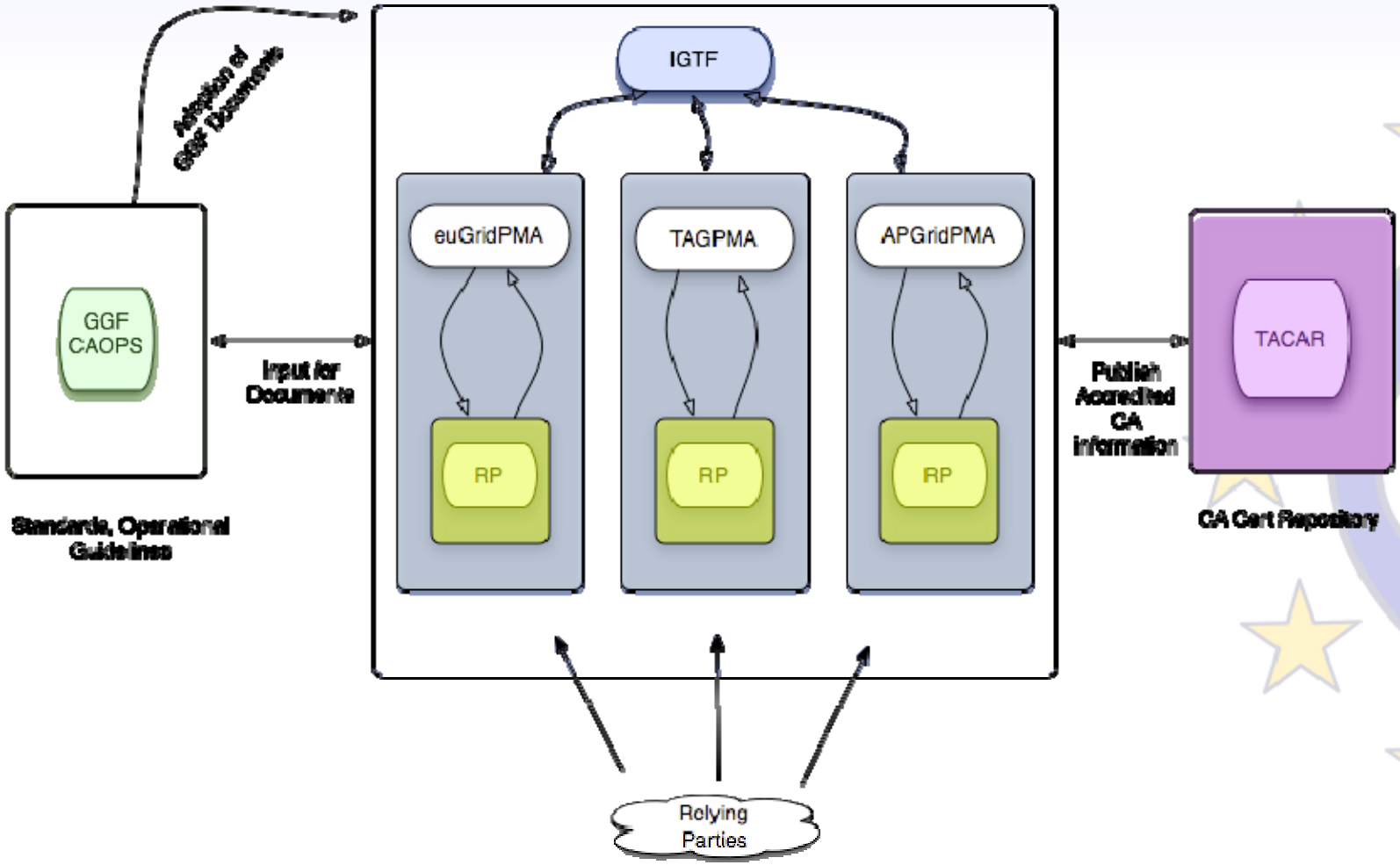
- Web site http://www.eugridpma.org/distribution/igtf
- Should be mirrored by all PMAs
- Each PMA can/should sign the RPMs with their own PGP key
- Validation of content via TACAR (where possible)



EUGridPMA and TACAR



Relationships: IGTF, PMAs, TACAR and GGF



Developments in Europe: Along the e-IRG Roadmap

e-IRG: e-Infrastructure Reflection Group Roadmap for *i*2010:

- commitment to the federated approach
- vision of an integrated AA infrastructure for *e*Europe

Towards an integrated AAI for academia in Europe and beyond

- The e-IRG notes the timely operation of the EUGridPMA in conjunction with the TACAR CA Repository and it expresses its satisfaction for a European initiative that serves e-Science Grid projects. […] The e-IRG strongly encourages the EUGridPMA / TACAR to continue their valuable work […]
  (Dublin, 2004)

- The e-IRG encourages work towards a common federation for academia and research institutes that ensures mutual recognition of the strength and validity of their authorization assertions.
  (The Hague, 2005)

Recent developments in this direction

- From the policy side
  - Push for global interoperability
- From TERENA
  - NRENs-GRID workshop series
  - TF-EMC2 / TF-Mobility
  - TACAR extensions?
- REFEDS: Research and Education Federations
  (includes authorization as well, and even software discussions)
  - IGTF, eduroam, A-Select, PAPI, SWITCH-AAI, InCommon, HAKA, FEIDE/Moria
  - http://www.terena.nl/tech/refeds/

Current Fuzzy Issues in the EUGridPMA

In no particular order …

- Real Names in the certificate subject?
  - commonName vs. pseudonym
  - Relying parties like the “warm and fuzzy feeling of trust”
- One-statement certificate policies - implementation
- CSR delivery and linking with identity vetting trail
- Steady move to the use of HSMs for CAs
  - USB hardware token delivery has started as well
  - What’s the future interoperability/software support? And cost?
- OCSP re-/transponder network, how to run it?
  - Setup together with certiVer and with discussions in GGF
- Format and distribution
- CA monitoring and availability …

Discussion on the Wiki, e.g.

`https://grid.ie/eugridpma/wiki/Annotated_Classic_AP`

EUGridPMA **http://www.eugridpma.org/**

IGTF **http://www.gridpma.org/**

Graphic by David O'Callaghan, Poznan 2005