Certification and registration for Grids in Europe

Christos Kanellopoulos, 2006.03.14

Outline

- What is the euGridPMA?
- A brief history of how we came here
- Tasks of the PMA

- EUGridPMA, TACAR, e-IRG, GGF
- International Grid Trust Federation
- Agenda outlook…

The EUGridPMA "constitution"

http://www.eugridpma.org/charter/

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

- *establishes requirements and best practices for grid identity providers*
- *enables 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 it's charter - the certificates issued by the Accredited Authorities meet or exceed the relevant guidelines.

Early beginnings: the EU DataGrid

- European DataGrid (EDG) aimed to develop middleware and provide a testbed for
  - High Energy Physic
  - Earth Observation and Ozone Modelling
  - Bio-informatics & bio-medicine
- Middleware includes
  - Job Submission and Scheduling
  - Data Management and Replication
  - Monitoring
  - Cluster Management
- Security was not considered as a separate task
  - Security Coordination Group
- EDG began in January 2001 and finished in March 2004

History

source: David O'Callaghan, EGC 2005

Early beginnings: EDG Test Bed 0

```
From: Kelsey, DP (David)
Sent: Monday, November 20, 2000 8:10 PM
To: Francois Etienne (E-mail); 'Kors Bos'
Subject: CA/Security contacts (DataGrid)

Dear Francois, Kors,

I have had no nominations for security contacts for the
meeting on "Certificates for Testbed0" for CNRS or NIKHEF yet.
Please let me know who I should invite.

Regards, Dave
-----------------------------------------------
Dr David Kelsey Computing & Resource Management
Particle Physics Department
Rutherford Appleton Laboratory
Chilton, DIDCOT, OX11 0QX, UK

e-mail: XXXXXXXXXX@XXX
Tel: [+44](0)1235 XXXXXX (direct)
Fax: [+44](0)1235 XXXXXX
-----------------------------------------------
```

History

source: David Groep

EDG Authentication Requirements

- Definite separation between AuthN and AuthZ
- SCG collected security requirements for authentication
  - Single Sign-on
  - Interoperable authentication with other Grids
  - Ability to revoke authentication credentials
- Requirements – Globus Grid Security Infrastructure (GSI)
  - X.509 Public Key Infrastructure
  - Users, Hosts and Services have certificates
  - Identity is checked by Registration Authorities (RAs) and certified by Certification Authorities (CAs)
  - Users and Hosts perform mutual authentication
  - Delegation with short-lifetime proxy credentials

History

based on: David O'Callaghan, EGC 2005

CA Coordination Group

- CACG had the task of creating this PKI
  - for Grid Authentication only
  - no support for long-term encryption or digital signatures
- Single CA not 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 Globus software
- Coordinated group of peer CAs was most suitable choice

History

based on: David O'Callaghan, EGC 2005

Minimum Requirements version 1

```
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

"Reasonable procedures…acceptable methods"

- Requirements and Best Practices for an "acceptable and trustworthy" Grid CA
- Shaped by Relying Parties (RPs) of Grid projects
- Evolved over the course of the project
- Provide a common standard
  - Reduces burden on RPs to assess each CA individually
  - Clearly sets the standard for new CAs
- accredit CAs which meet the requirements

History

based on: David O'Callaghan, EGC 2005

Trust Foundations

- Mutual trust between CAs and CAs-Relying Parties
- Based on
  - Requirement to document processes in CP/CPS
  - Peer-review of the CP/CPS in the accreditation
  - Periodic face-to-face meetings and reports
  - Audit-ability requirement

  - "Reasonable procedures … [and] acceptable methods"

History

Relying Party requested tasks

- Trust establishment
  - …
- Promotion of authentication interoperability
  - also with multiple authentication profiles

- **Coordinate namespace (unique subject names)**
  - **many authorization decisions are based on DN only**
- **Distribution of trust anchors in convenient formats for RPs (“common naming”)**
- **forum**
  - **also contact point for problem resolution?**

History

Papers on the CACG!

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

J. Astalos[13], R. Cecchini[14], B. Coghlan[6], R. Cowles[20], U. Epting[11], T. Genovese[8], J. Gomes[15], D. Groep[18], M. Gug[9], A. Hanushevsky[20], M. Helm[8], J. Jensen[3], C. Kanellopoulos[1], D. Kelsey[3,*], R. Marco[12], I. Neilson[9], S. Nicoud[5], D. O'Callaghan[6], B. 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, Greece
[2] Canarie, Canada
[3] Rutherford Appleton Laboratory, UK
[4] CESNET, Czech Republic
[5] CNRS/UREC CPPM, France
[6] Trinity College Dublin, Ireland
[7] University of Cyprus, Cyprus
[8] ESnet/LBNL, USA

History

Five years of growth

November 2000:
- Invitation to the DataGrid WP6 partners

December 2000:
- First CA meeting at CERN

March 2001:
- 5 CAs: CNRS, LIP, NIKHEF, CERN, INFN, UK-HEP
- First version of the minimum requirements

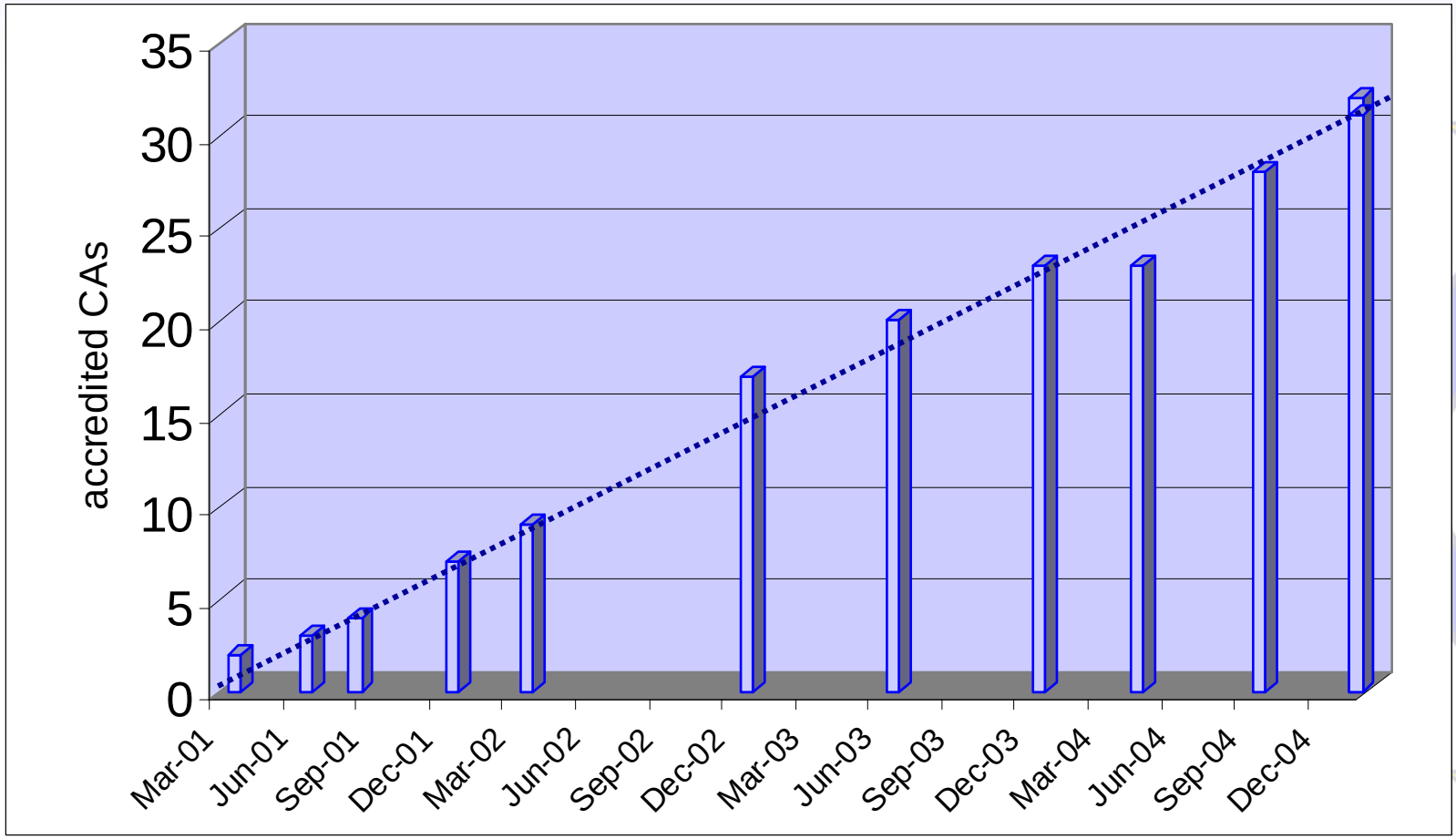
December 2002:
- Inclusion of the CrossGrid CAs

…

April 2004:
- Establishment of the EUGridPMA
- First formal charter and guidelines documents

History

Growth of the CACG & EUGridPMA



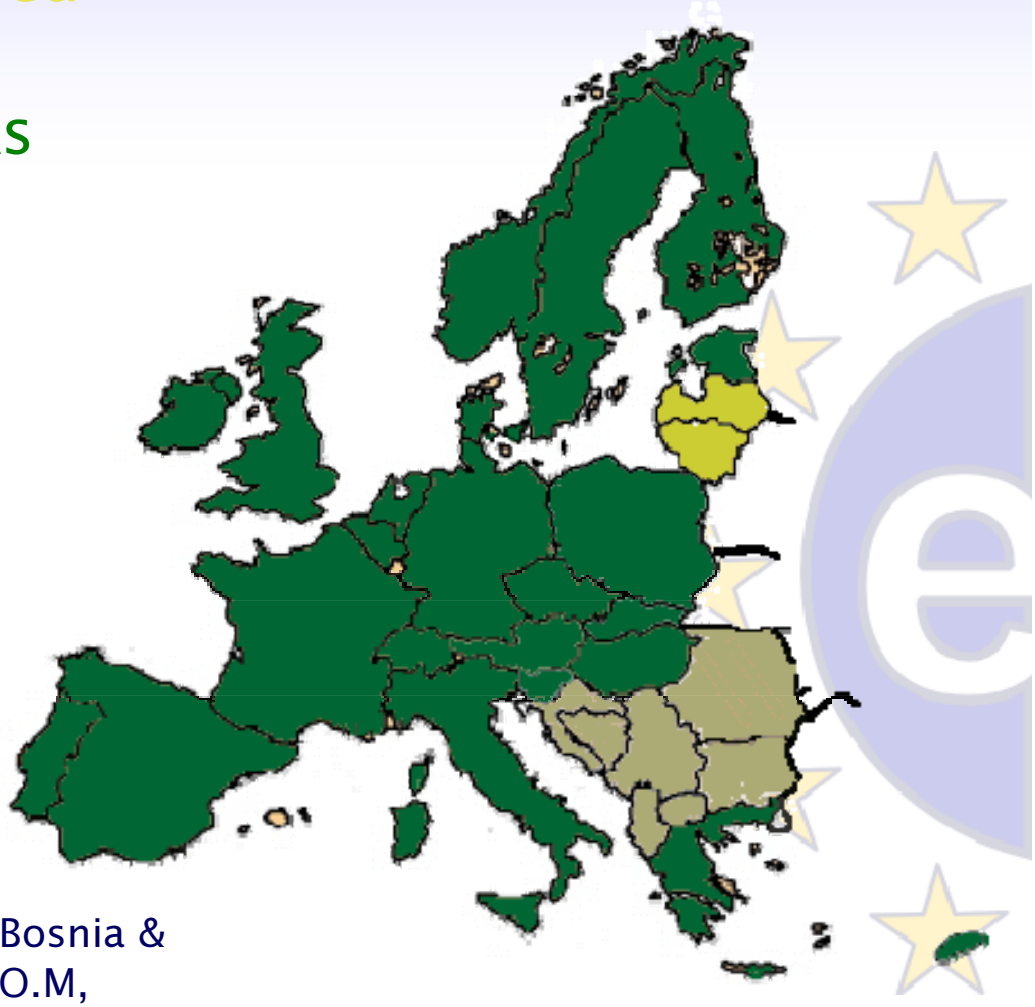
History

Coverage of the EUGridPMA

- Yellow: being discussed (DFN, BalticGrid, RDIG)
- Green: Accredited CAs

Other Accredited CAs:

- DoEGrids (USA)
- GridCanada
- ASCCG (Taiwan)
- ArmeSFO (Armenia)
- CERN
- Russia (*"DataGrid"*)
- IUCC (Israel)
- Pakistan
- IHEP (China)
- SEE-GRID Regional CA (Albania, Bosnia & Herzegovina, Bulgaria, Croatia, F.Y.R.O.M, Romania, Serbia & Montenegro, Turkey)



and can we leverage of other (national) AuthN infrastructures?

Current Situation

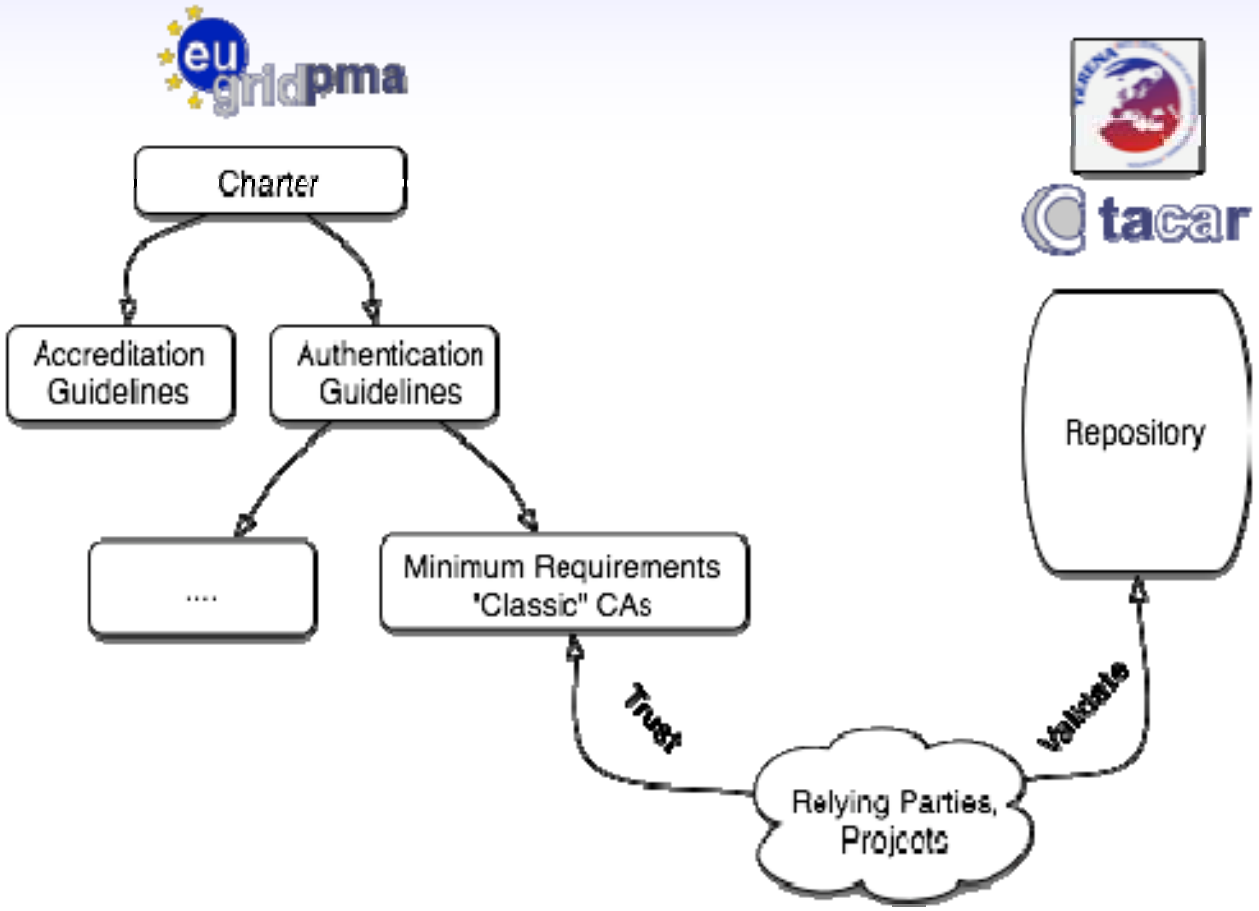
TACAR

A trusted repository which can contain 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
  - distribution from the EUGridPMA is not digitally signed
  - independent web administration makes for stronger trust
  - TACAR certificate itself published in paper/journals
- 20 CA root certificates collected

EUGridPMA & TACAR Structure



e-IRG Roadmap

e-IRG: eInfrastructures Reflection Group (EU body of natl. reps.)

Towards an integrated AAI for academia (& beyond ?) in Europe

- 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 […]

- 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.

GGF CA Operations WG

https://forge.gridforum.org/projects/caops-wg

"The purpose of the Certificate Authority Operations (CAOPS) Working Group is to develop operational procedures and guidelines that facilitate the use of X.509 and other technologies for cross grid Authentication. "

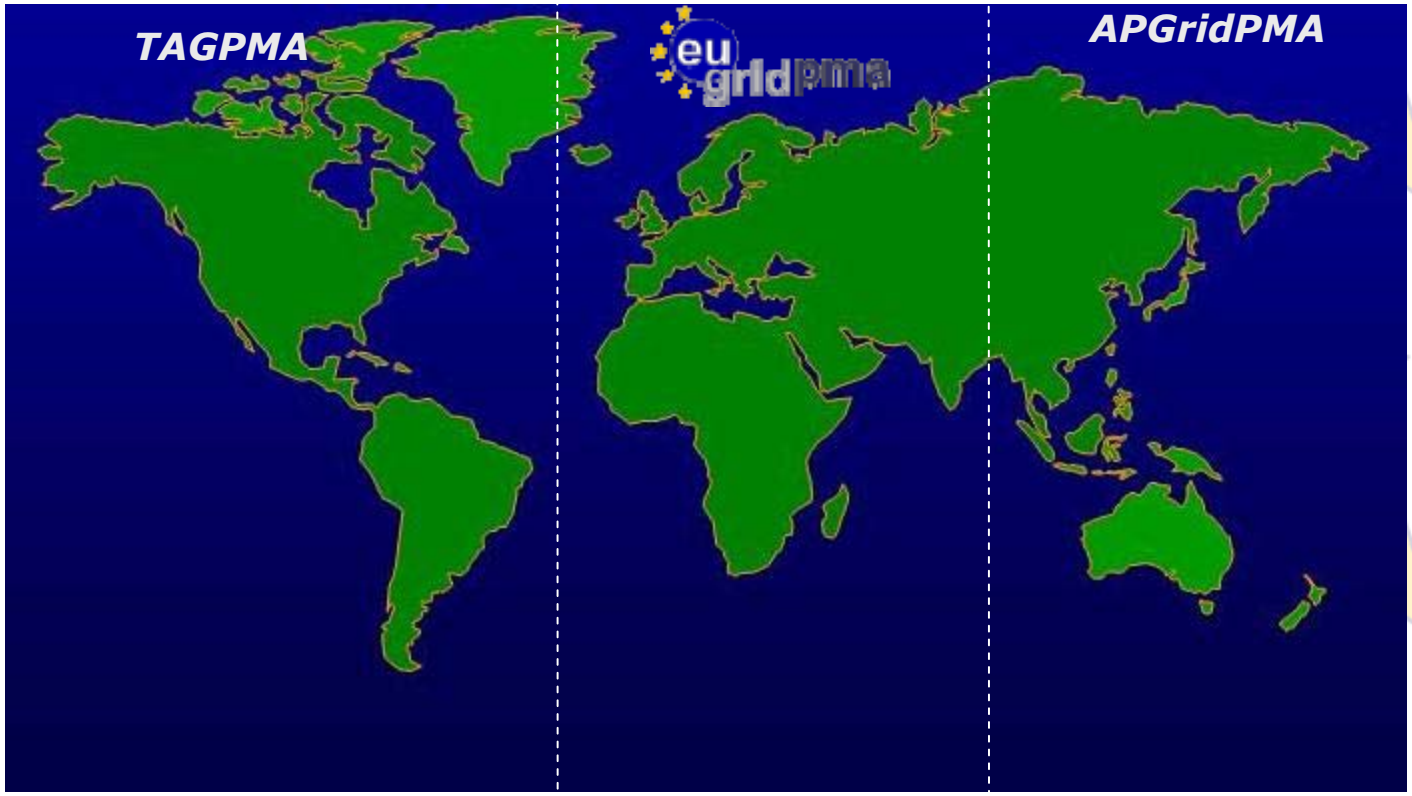
- Strong cooperation with euGridPMA

Working Group Chair(s): Christos Kanellopoulos, Darcy Quesnel

The IGTF

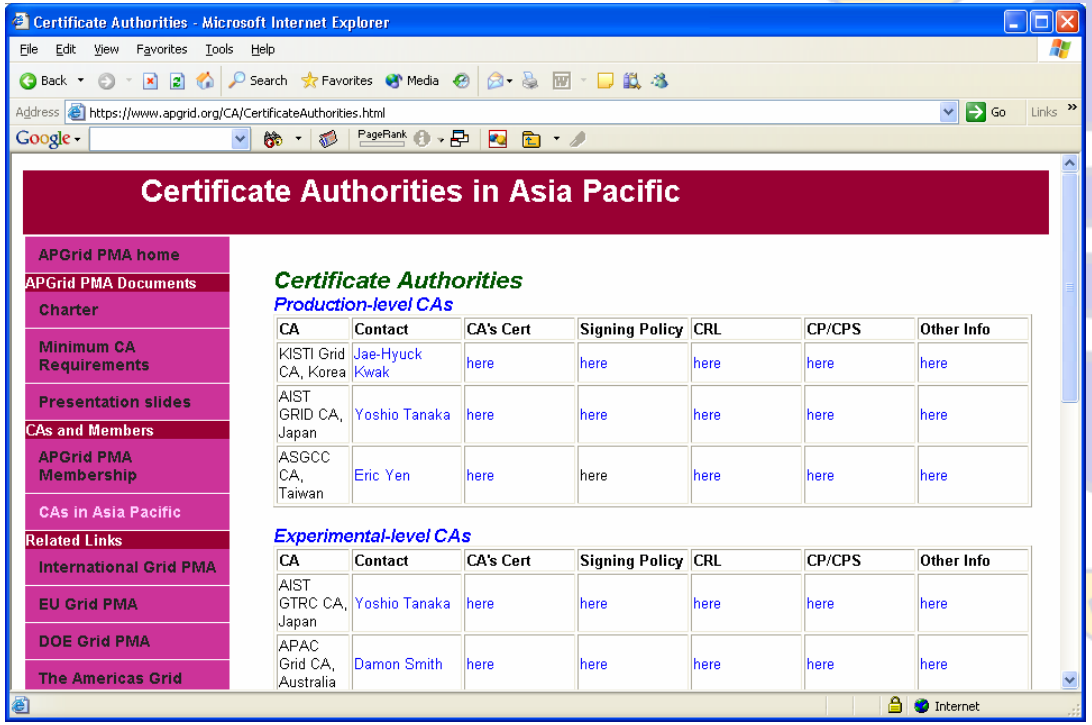
International Grid Trust Federation

- improve trust building through better face-to-face contact
- better manageability of the PMA



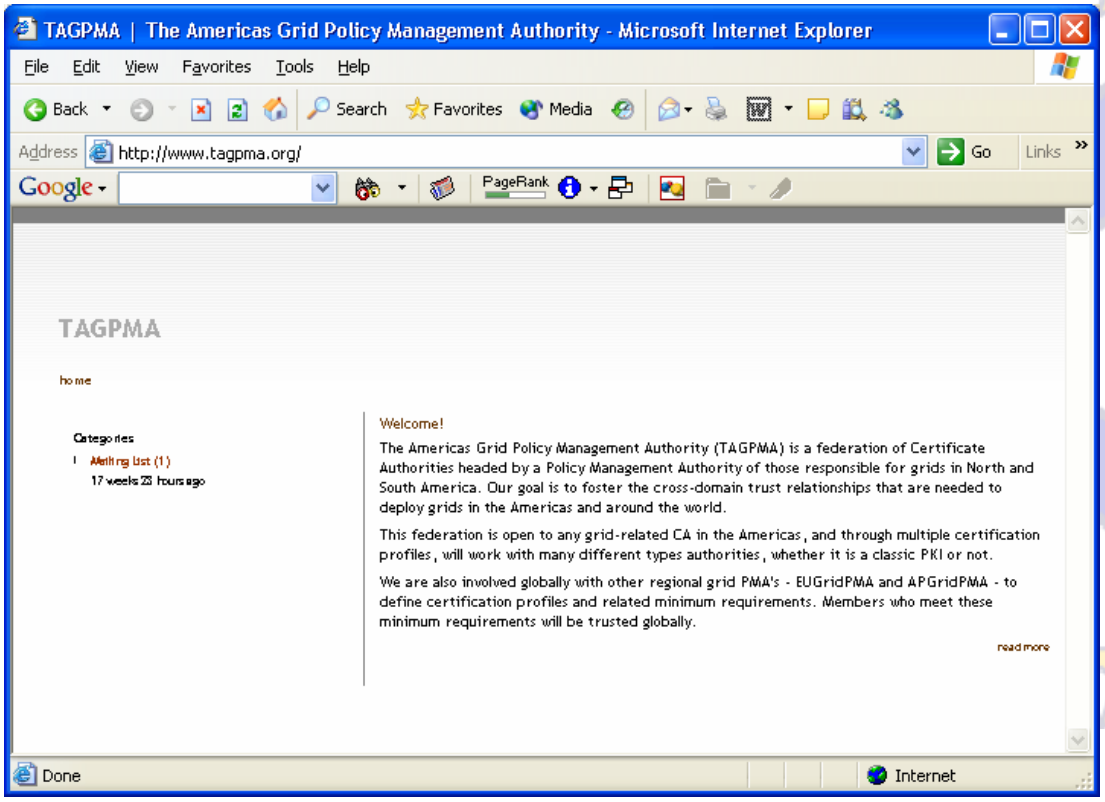
APGridPMA

- Launched June 1st, 2004
- 13 members from the Asia-Pacific Region
- chaired by Yoshio Tanaka



TAGPMA

- Launched May, 2005
- chaired by Darcy Quesnel



Issues to be addressed

Relying Party requests:

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

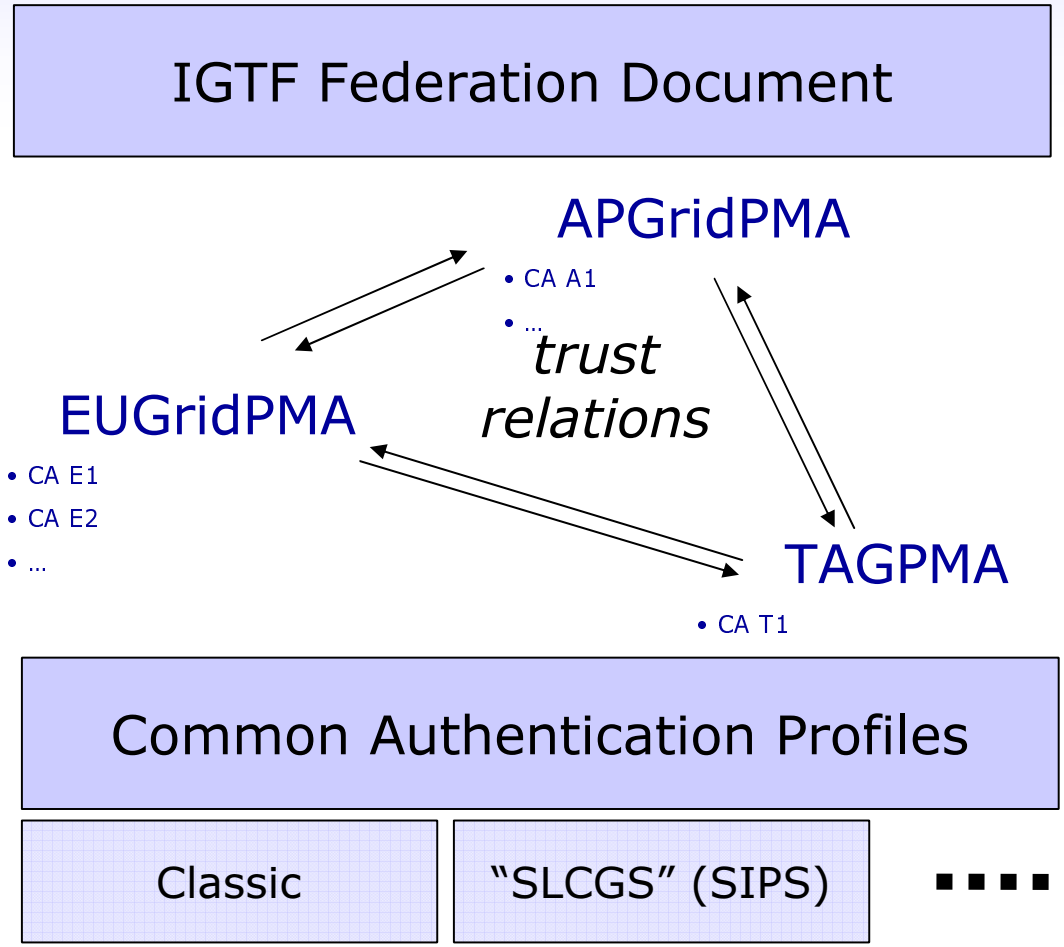
4) [operation of] a secure collection point for information about CAs which you accredit

5) Common practices where possible

6) Strong interaction with GGF CAOPS WG on standardization

[based on a list from the Open Science Grid]

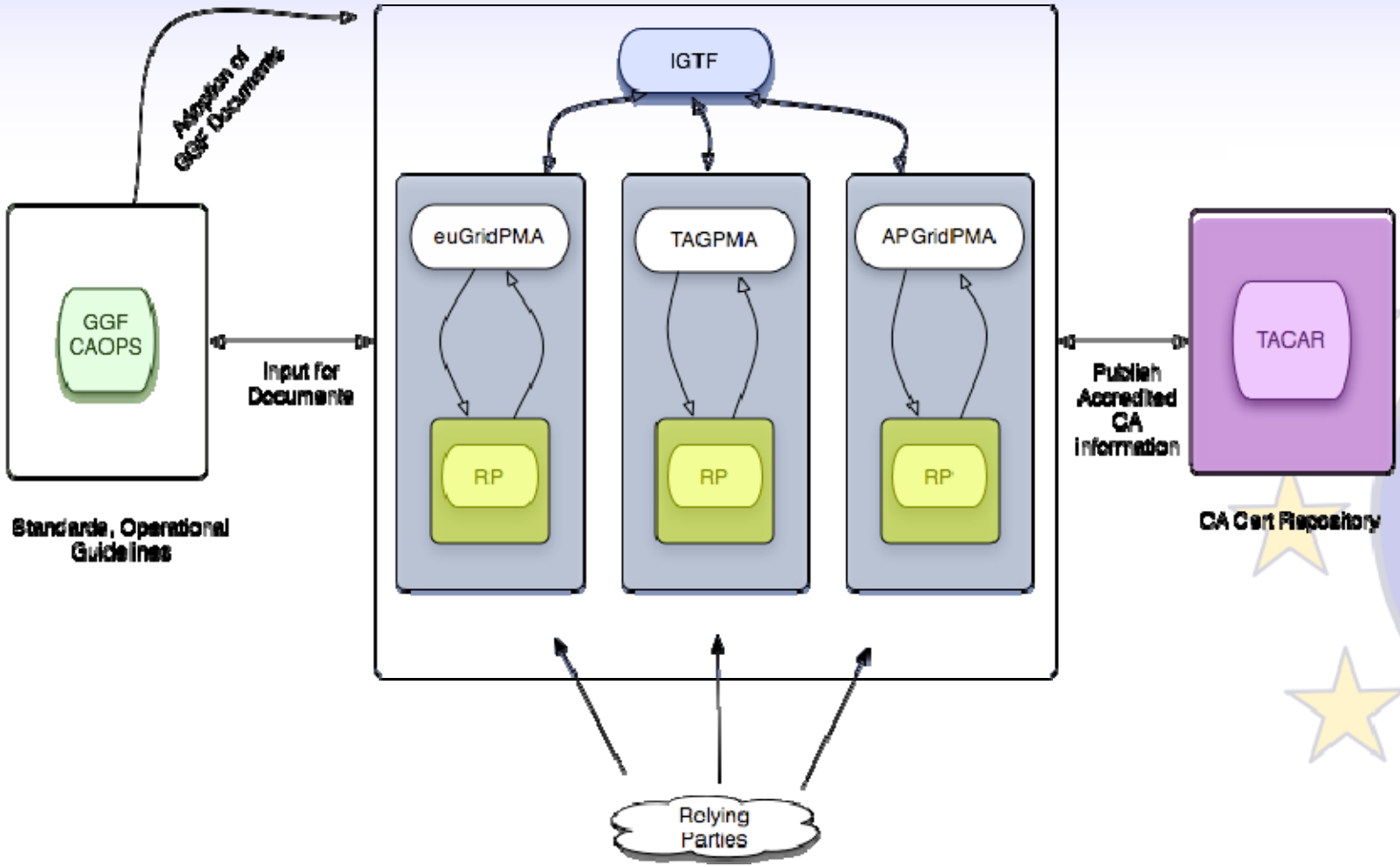
Proposed IGTF structure (@GGF13)



Subject Namespace Assignment

Distribution Naming Conventions

The Whole Picture



Summary

- A global PKI for the Research and Academic "Grid" community is in place
- IGTF will strengthen the global reach of the PKI.
- The infrastructure was built arround the actual needs of the users – relying parties.
  - The Success Factor: Actually the Rps were the ones who initiated the process and they play a key role in the PMAs and the IGTF.
- On the road to converge the "Grid" and "NREN" PKIs

http://www.eugridpma.org/