# UNLP PKIGrid

# Certificados para grid para e-science

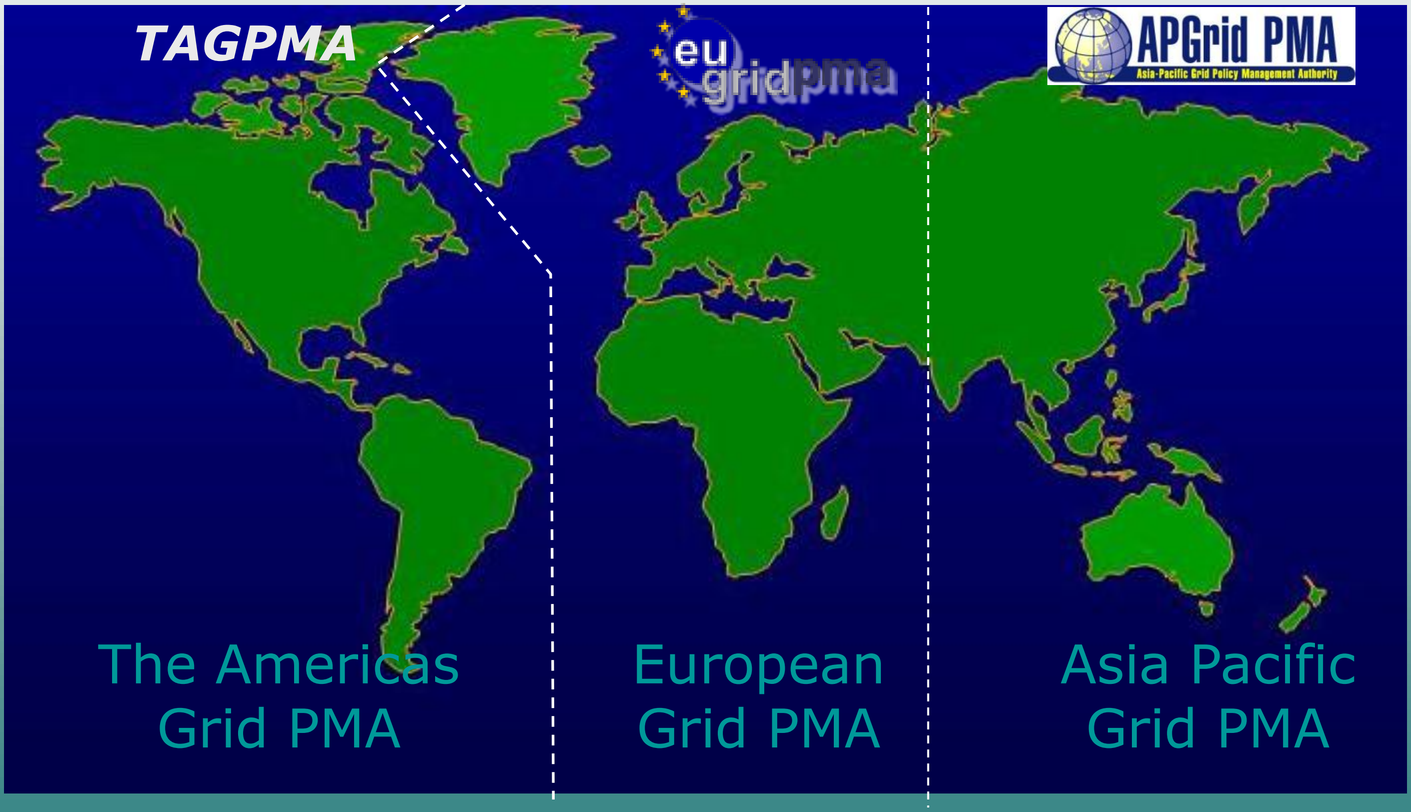
(Argentina)

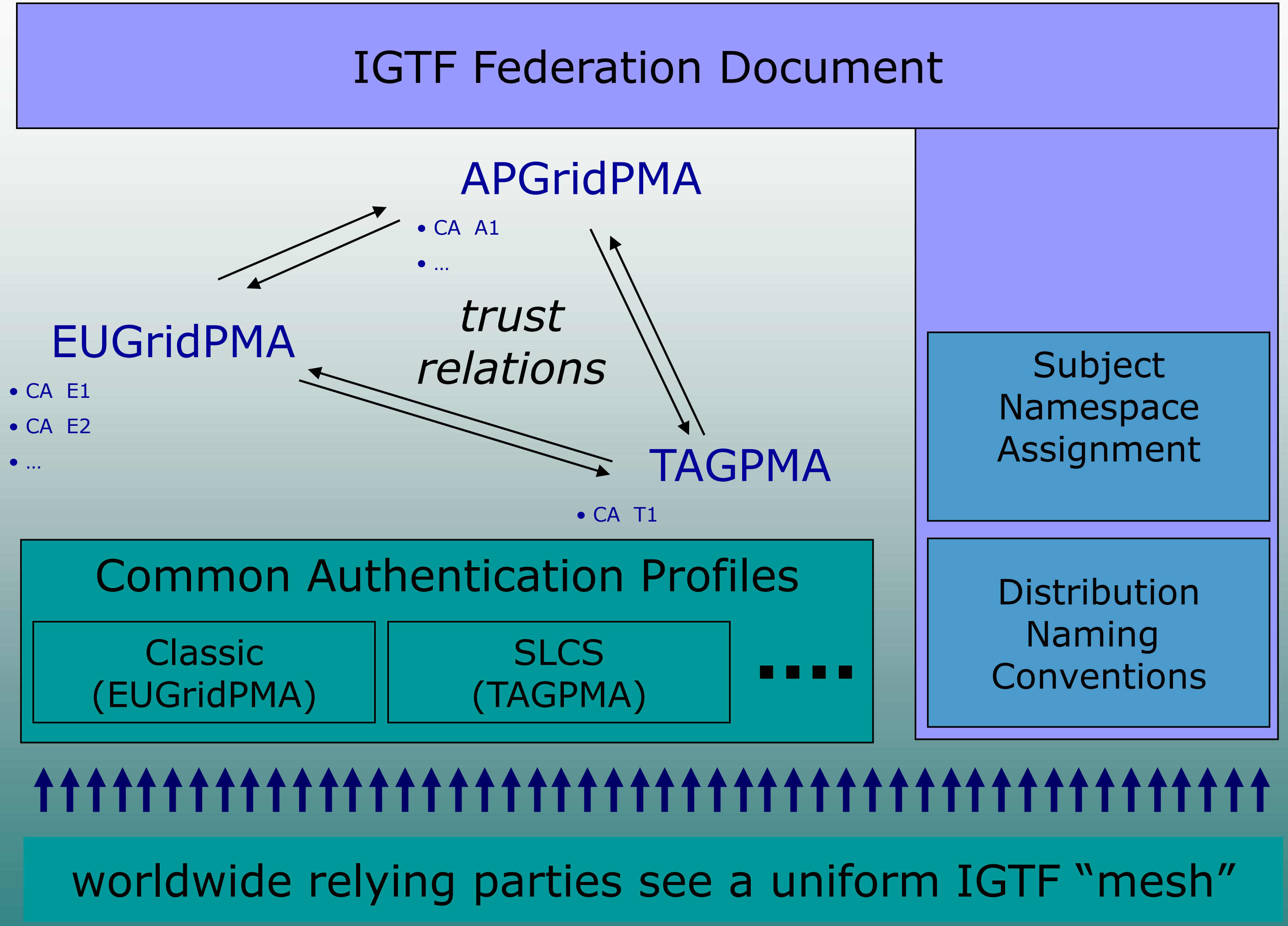
A member of TAGPMA

In distribution of IGTF since november 2007

# IGTF – the International Grid Trust Federation

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





IGTF Federation Document

APGridPMA

- CA A1
- …

EUGridPMA

- CA E1
- CA E2
- …

*trust relations*

TAGPMA

- CA T1

Subject Namespace Assignment

Distribution Naming Conventions

Common Authentication Profiles

Classic (EUGridPMA)

SLCS (TAGPMA)

....

worldwide relying parties see a uniform IGTF “mesh”

# EUGridPMA

- www.eugridpma.org
- Member organizations/countries:
  - Canonical list: http://www.eugridpma.org/members/index.php
  - Membership includes many European national and regional (eg Nordunet, Baltic Grid) Grid projects; Canarie (Canada); DOEGrids and FNAL (US); significant relying parties such as LHC, OSG;
- Features:
  - ~44 members: most from EU, some from closely affiliated countries
  - Chaired by David Groep (NIKHEF)
  - Completed 12th Face-to-face meeting
  - The senior partner
  - “Classic” X.509 Grid Authentication Profile

# APGridPMA

- www.apgridpma.org
- Member organizations/countries:
  - Canonical list: https://www.apgrid.org/CA/CertificateAuthorities.html
- Features:
  - ~16 members from the Asia-Pacific Region, chaired by Yoshio Tanaka (AIST),
  - + 10 Production CAs are in operation

# TAGPMA

- www.tagpma.org
- The newest PMA, first Face-to-Face meeting in Rio de Janeiro, March 2006.
- Member organizations/countries:
  - Canonical list: http://www.tagpma.org/members

Features:

- 20 members: CA, US and Latin America
- Chaired by Vinod Rebello (UFF)

# UNLP PKIGrid (Argentina)

PKI Deployment

- Human resources involved in the project
- Infrastructure description
- Implementation tasks
- Policies and Procedures
- Documents Management
- Web Site description
- Updates since last meeting
- Other tasks
- Related tasks
- Future tasks

# UNLP PKIGrid (Argentina)

## Human resources involved in the project

- CA Manager: Javier Díaz
- Policies, Procedures: Lía Molinari & Viviana Ambrosi (internal & external)
- Internal Auditor: Vicente Franco
- Test and Modification of OpenCA to feet our needs: Paula Venosa, Miguel Carbone
- Security Administration: Nicolás Macia
- Network Administration: Pedro Brisson
- Site implementation and Development of one bilingual interface (English & Spanish): Miguel Carbone/ Juan Pablo Giecco

# UNLP PKIGrid (Argentina)

## Human resources involved in the project (cont.)

- RA Manager: María del Carmen Lago
- RA Operator 1: Teresa Di Pietro
- RA Operator 2: Ana Clara Carrion
- CA Operator 1: Andrés Barbieri
- CA Operator 2: Matias Banchoff
- CA Operator 3: Leandro Bilbao
- CA Operator 4: Alejandro Sabolansky
- Translator: Aldana Gomez Ríos

# UNLP PKIGrid (Argentina)

## Infrastructure Description

The deployment of the PKI has required:

- One portable PC to act as the CA offline
- One sure place in order to protect the CA offline
- One dedicated server to support the public site of the CA (holding the Certificates & the CRLs). It also supports the functional aspects of the main RA.
- One PC for the RA operators
- Several *Aladdin* e-tokens to provide for the secure management of operators certificates
- A deployment environment (two separate servers are used for implementing & testing the information & services provided by the PKI)

# UNLP PKIGrid (Argentina)

## Infrastructure Description – Security Components

- One firewall was extended in order to provide a separate DMZ for the PKI service. Default policy is DROP and denials are reported.
- Distributed sensor infrastructure to report events in a central security console  to detect security incidents.
- NTP synchronization with a local time source (GPS stratum 0)
- Phisical Security: RA and public sites resides in a Server Rack in the UNLP Data Center. The access to the rack is controlled (redundant energy supply, RFID+biometric access).

# UNLP PKIGrid (Argentina)

## PKI Implementation tasks

- Operative Systems Secure Installation
- OpenCA installation
- OpenCA GUI adaptation
- Checking of the implementation for the fulfillment of the CP/CPS
  - Certificates profiles
  - Configuration of secure operators access (use of certificates stored in tokens, control of roles)

# UNLP PKIGrid (Argentina)

## PKI Implementation tasks

- Token´s drivers (32K & 64K) testing
- CA/RA Operator´s trainning
- PKI CP/CPS compliance testing
- Digital signature tools testing

# UNLP PKIGrid (Argentina)

## Policies and Procedures:

- CP/CPS
- Procedures (public & published in the website)
- Internal Procedures (some public, some internal)

# UNLP PKIGrid (Argentina)

## Policies and procedures (cont.):

- Procedures (public & published in the website)
  - BEST PRACTICES
    - ✓ Operators best practices
  - OBLIGATIONS
    - ✓ Suscriber obligations
    - ✓ CA obligations
    - ✓ RA obligations
  - HOW TO
    - ✓ How to obtain digital certificate
    - ✓ How to verify a digital signature
    - ✓ Others….
  - DOCUMENTS MANAGEMENT
    - ✓ Nomenclature of documents

# UNLP PKIGrid (Argentina)

Policies and Procedures (cont.):

- Internal Procedures and others (some public, some internal mark with *):
  - Contingency Plan *
  - Security Policy *
  - Agreement of Confidentiality and Responsibility *
  - Staff
  - RA Operator Administrative Procedures Manual *
  - Operations Procedures Manual for RA Operator
  - Operations Procedures Manual for CA Operator
  - Operations Procedures Manual for Technical Operator
  - Project Lider Obligations *
  - Relaying Party Obligations
  - Implementation Procedures.*
  - Guides (useful for future auditings). *

# UNLP PKIGrid (Argentina)

## Documents Management

Document Specification (published in the website)

| | | |
|---|---|---|
| • Assigned by IGTF: | 1.2.840.113612.5.4.2.3 | |
| • Document type | 1 | CP/CPS |
| | 2 | Procedures |
| | 3 | Descriptions |
| | 4 | General Information |
| • Subtype: (i.e., in the case of procedures) | | |
| | 1 | Subscriber's obligations |
| | 2 | CA´s obligations, structure and operation |
| | 3 | RA´s obligations, structure and operation |
| • Version | X | |
| • Sub -Version | XS (S only for the spanish version) | |

# UNLP PKIGrid (Argentina)

## Web Site

**https://www.pkigrid.unlp.edu.ar**

- Bilingual site (english & spanish)
- Site deployment with AJAX
- The site contains:
  - UNLP PKIGrid CP/CPS
  - Procedures and documentation
  - A customized view of OpenCA public interface

# UNLP PKIGrid (Argentina)

## Updates since 2° semester 2007

- We add:
  - Tacar link
  - Signing policy
  - Contact person
  - Changelog ( CP/CPS version update to 2.7)

# UNLP PKIGrid (Argentina)

## Information updated

- Hide suscribers sensitive information published in the web site
- Certificates extensions were changed according to reviewers suggestions
- CRL URL update (https --->http)
- Fixed CP/CPS according to reviewers suggestions (ver 2.7)

# UNLP PKIGrid (Argentina)

## Other tasks

- Functionality testing:
  - Certificates format according to CP/CPS
  - Testing in Gilda environment (Colaboration with the UNLP Physical Department and IFLP)

- Collaboration with ONTI (Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública de la Nación)

# UNLP PKIGrid (Argentina)

## Related Grid tasks

- Several  EELA/EELA2/GISELA Tutorials
- Besides PKI CA operation, operation of funtional node of EELA2/GISELA
- **Next Tutorial scheduled for: 3 to 7 December 2012**

# UNLP PKIGrid (Argentina)

## Uptades in course

- Several RA for UNLP CA PKIGrid (UNMisiones, UNRioCuarto….)
- OCSP (experimental)
- Programming in 2013 Change to SHA-2 (512 / 256)

# UNLP PKIGrid (Argentina)

## NIST: Secure Hash Algorithm (SHA-3)

- The winning algorithm, Keccak (pronounced “catch-ack”)
- The team’s entry beat out 63 other submissions that NIST received after its open call for candidate algorithms in 2007, when it was thought that SHA-2, the standard secure hash algorithm, might be threatened. Keccak will now become NIST’s SHA-3 hash algorithm

# UNLP PKIGrid (Argentina)

## current tasks

- CSIRT UNLP since 2007

www.cert.unlp.edu.ar

# UNLP PKIGrid (Argentina)

## Questions & answers

- ca@cespi.unlp.edu.ar
- jdiaz@unlp.edu.ar