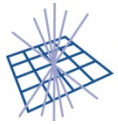

Policy Management for Grid Authorization

David Kelsey

MWSG, Bologna
28 Mar 2008

EU Grid PMA

- The Policy Management Authority which coordinates Authentication for Grids
  - Europe, Middle East, Africa …
  - X.509 PKI
  - ~40 CAs
- Member of International Grid Trust Federation
  - Along with APGridsPMA and TAGPMA

Introduction

- AuthZ is as important as AuthN
  - Gives access to resources
- In world of federations
  - AuthZ and Identity attributes are rather similar
- Many Grid VOs are global
  - or at least span two or more Grids
  - Difficult for one Grid to set the standards
- EGEE/WLCG Joint Security Policy Group (JSPG) agreed some time ago
  - We need “minimum requirements” for running VOMS
- For now, consider just AAs, not credential stores

Aspects of Attribute Authority

- User registration and renewal
  - Vetting of rights and identity
  - Assignment of groups, roles and attributes
- Operational Requirements
  - Dedicated machine with no other services
  - Physical security
  - Details of signing key and its storage
  - Other technical details

Aspects of AA (2)

- Site security
- Repository of AA certificates
- Distribution mechanisms - roots of trust
- Note
  - Unlike CA's the person/site running the AA service is not (in general) the same as the VO management responsible for attribute assignment

Who should tackle this?

- JSPG could do it, but …
- The minimum requirements are similar to an AuthN profile
- There is no other large group of experts out there waiting to take this on
- Global problem
- Don't want to create a separate IGTF for AuthZ
- Already clear that
  - Potential number of AA's would need different model for accreditation
    - E.g. IGTF sets standards and others do the actual accreditation

EU Grid PMA AuthZ wg

- In Sep 2007 – at Thessaloniki meeting – PMA agreed
- Small group in EU Grid PMA (with others interested) - D Kelsey coordinating
  - to produce rough draft of a first AA profile
  - First thoughts on accreditation procedures
  - First look at repository and distribution problems
  - For discussion in next PMA meeting - Amsterdam Jan 2008
- No face to face meeting
  - Business by e-mail and phone
- Then move forward more formally to IGTF with a proposal
  - E.g. proposal for IGTF to take on this coordination
  - Wider discussion at that point
- Mail list created but work has not yet started

Some thoughts

- AA profile for VOMS
  - One or two documents?
    - Running the service
      - Supports multiple VOs
    - Performing User Registration and VO management
      - Initial vetting, including identification
      - Renewal
      - Audit logs etc

Some thoughts (2)

- Attribute signing
  - Host certificate?
  - Service certificate?
  - Special AA certificate?
  - What is the root of trust?
- Need to interact with other academic federations

Some thoughts (3)

- How will accreditation be done?
  - By existing PMA's (but many VO's)?
  - By Grid infrastructures (EGEE, OSG, …)?
  - By National Grids?
- Relationship VOs and Grids
  - Another scaling problem
  - Define a "home" Grid for each VO

Some thoughts (4)

- Repository of AA certificates
  - Currently a list of DN's
  - Rely on IGTF to ensure uniqueness
  - Or store and distribute the full certificate?
- Where should the repository be?
  - IGTF? PMA? TACAR?
- How to distribute?

Final thoughts

- Currently an EU Grid PMA topic
  - IGTF not yet agreed to take this on
  - Will need change to charter
- We will not duplicate work going on elsewhere
  - Middleware and interoperability details
  - VOMS technical details