Security Policy Update

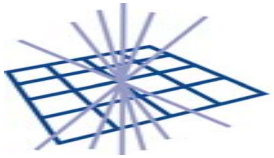
WLCG GDB

CERN, 14 May 2008

David Kelsey

STFC/RAL

d.p.kelsey@rl.ac.uk



GridPP

UK Computing for Particle Physics

Overview

- JSPG meeting (Jan 08)
- New mandate for JSPG
- Policy Management for Grid Authorization
- JSPG Future plans

JSPG meeting

- JSPG meeting was held at CERN
  - 28/29 Jan 2008
  - One day workshop cancelled
    - Bob Cowles (OSG/SLAC) leaves JSPG
    - clash with OSG/EGEE and EGI_DS meetings
  - Less progress than hoped!
- Policy documents (almost) ready for formal approval
  - VO Operations Policy
  - Pilot Jobs Policy
  - Traceability and Logging Policy
  - CA Approval (new IGTF profiles)

JSPG mandate

- For EGEE-III as move towards EGI/NGIs
- OSG requested clarity wrt their membership
- New mandate (main points)
  - *Jointly owned by/recommends to WLCG & EGEE*
  - *Policy for WLCG designed to be applied to all of its Grid infrastructures in so far as this relates to WLCG activities*
    - *i.e. OSG, NDGF and other national Grids and/or individual Grid sites which participate in WLCG*
  - *May also provide advice on any security matter*
  - *Aim for simple/general policies that are useable by NGIs*
  - *JSPG does not formally approve policies*
    - *but recommends to management bodies*
- Plans for next two years
  - Need to revitalise membership (More ROCs, NGIs and VOs)
    - New OSG member is Jim Basney
  - Review all policy documents to make even more simple/general

Policy Management for Grid Authorization

AuthZ WG - Introduction

- Authorization is as (more?) important as (than) Authentication
  - Gives access to resources!
- In world of national academic federations
  - AuthZ and Identity attributes are rather similar
- Many Grid VOs are global (e.g. LHC!)
  - or at least span two or more Grids
  - impossible for one Grid to set the standards
- JSPG agreed some time ago
  - We need “minimum requirements” for running VOMS
  - CAs very well controlled, not so for VOMS
- The minimum requirements are similar to an IGTF AuthN profile
- No other large group of experts is out there waiting to take this on!
- A global trust problem
- International Grid Trust Federation – good name for AuthZ too
  - Don’t want to create a separate IGTF for AuthZ
- EU Grid PMA has created a working group on this topic
  - DPK chairs

AuthZ WG mandate and aims

- To prepare recommendations on policy and global trust issues related to Grid Authorisation (AuthZ)
- The initial list of issues will include
  - Minimum requirements and best practice for the operation of a Grid AuthZ attribute authority
  - Minimum requirements and best practice for Virtual Organisation user and service membership management
  - Accreditation of Attribute Authorities (AA)
  - Accreditation of Virtual Organisations and their membership management procedures

Mandate (2)

  - Repositories and distribution of accredited AA and VO roots of trust
  - Technical details of attribute signing and trust validation
- To recommend how IGTF could handle the definition of AuthZ policy and related accreditation during the next 3 to 5 years, taking into account the move towards a sustainable EU Grid Infrastructure and constituent national Grids
- Aim is to tackle the scaling problem of VOs establishing trust with many Grids and hundreds of Sites

Min Requirements for Attribute Authories

- User/service registration and renewal procedures
  - Vetting of rights and identity
  - Assignment of groups and roles
- Operational Requirements for running an AA service
- Repository of AA roots of trust
  - And distribution mechanisms
- 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

Attribute signing and trust validation

- IGTF has concerns about the current VOMS practice
  - Host or Service certificate
    - Neither is appropriate
    - Where is the root of trust?
      - It currently appears to be the CA
  - Special AA certificates could be issued
  - How is trust validation performed?
    - OSG just written paper on AC validation
- WG will propose a solution

Accreditation of AAs and VOs

- How will accreditation be done?
  - By existing PMA's
    - Far too many VOs so does not scale
  - IGTF defines the standards and others do the accreditation
    - Grid infrastructures (EGEE, OSG)?
    - National Grids?
    - Each VO could have a "home Grid"
- WG will propose an approach

Future JSPG plans

- Next face to face JSPG meeting
  - 29/30 May at CERN
- Agenda will include
  - Update old VO security policy documents
    - VO Security Policy
    - User registration and VO membership requirements
  - Finalise user-level accounting
  - Look again at Grid Portal policy
  - Plan for next two years
- *VOLUNTEERS VERY WELCOME!*

JSPG Meetings, Web etc

- Meetings - Agenda, presentations, minutes etc

http://indico.cern.ch/categoryDisplay.py?categId=68

- JSPG Web site

http://proj-lcg-security.web.cern.ch/

- Membership of the JSPG mail list is closed, BUT
  - Requests to join stating reasons to D Kelsey
  - Volunteers to work with us are always welcome!
- Policy documents at

http://proj-lcg-security.web.cern.ch/proj-lcg-security/documents.html