Security Policy Update

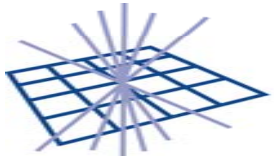
WLCG GDB

CERN, 11 Mar 2009

David Kelsey

STFC/RAL

david.kelsey AT stfc.ac.uk



GridPP

UK Computing for Particle Physics

Overview

- Update since my last GDB presentation (Dec 08)
- JSPG meeting (22/23 Jan 09)
- New/Revised draft policies
  - VO Registration
  - VO Management
  - User-level accounting
  - VO Portals
- JSPG Future plans

JSPG meeting

- JSPG meeting was held at CERN
  - 22/23 Jan 2009
- Agenda included
  - News: EGI and EGEE Security Risk Analysis
  - Discussion – policy issues
    - Review of CA Approval policy
    - VOMRS and VOMS Admin status
    - New EGEE AuthZ framework – global vs local policies
  - First look at revision of User AUP
  - New and revised policies
    - VO Policies
    - VO Portal Policy
    - Accounting Data Privacy issues

Two VO Policies

- Virtual Organisation Registration Security Policy

https://edms.cern.ch/document/573348/8

http://www.jspg.org/wiki/VO_Registration_Policy

  - Version 2.3, 22 Jan 2009
  - Distributed widely for comments on 12 Feb

- Virtual Organisation Membership Management Policy

https://edms.cern.ch/document/428034/3

http://www.jspg.org/wiki/VO_Membership_Management_Policy

  - Version 3.4, 22 Jan 2009
  - Distributed widely for comments on 12 Feb

- Clear responsibilities on VO managers
  - Sites delegate user registration to the VOs
    - procedures must be of appropriate quality
  - E.g. VO managers must assist in incident response.

VO Registration

- Replaces old VO Security Policy
  - A simplified document
- Comments received
  - Should also handle removal or de-registration of a VO (what needs to be done and kept?)
  - Existing VO names are not DNS style
    - Too difficult to change
  - Who is the VO management body who gives authority to the VO AUP?
  - CA approved by whom?

VO Management

- Update of old LCG User Registration policy
- Comments received
  - Several small VOs have concerns
    - VOMS Admin does not have the necessary functionality
      - Reg date, End date, AUP version, Prompt renewal etc etc
    - Concerns that some things are not defined properly
      - VO manager vs VOMS manager?
      - What is the VO database?
      - How does a VO manager keep “proof” of users right to belong to a group or role?
  - Can we ignore Data Privacy?
      - But then user should perhaps be able to see data

User Level Job Accounting

- Updated draft distributed on 12 Feb
- Grid Policy on the Handling of User-Level Job Accounting Data
- V0.7, 23 Jan 2009

http://www.jspg.org/wiki/Grid_Policy_on_the_Handling_of_User-Level_Job_Accounting_Data

- *Motivation and structure of the document has been presented MANY times*
  - *Don't intend to do so again!*

Accounting policy

- Crossing borders – what is definition of the “EU”?
- Local accounting records should satisfy local laws
- Accounting for Funding Bodies
  - Some countries in EGEE are requesting access to accounting views for their own users
    - What resources have our users consumed?
  - It is of course difficult to identify “our users”
    - Certificates from a particular CA (very rough!)
    - No attribute in VO database
    - Could create lists of DNs!
  - No Data Privacy concerns (no people), but …
    - Does anyone have other concerns?
    - E.g. country data should (I think) not be public

VO Portal Policy

- New policy document
  - Based on Dutch BiG Grid policy (David Groep)
  - Ideas from the EGEE working group on portals
- *http://www.jspg.org/wiki/VO_Portal_Policy*
- *V3.0, 23 Jan 2009*

Portals

- Policy applies to all Portals operated by Virtual Organisations that participate in the Grid infrastructure
- Defines 4 classes of web portals and 4 classes of User
- *Some general policy plus class dependent statements*
- Addresses private key protection and requires use of Robot certificates in some cases
- **Robot:** a software agent performing automatic functions on behalf of real person
- **Robot certificate**: Issued to a Robot with private key generated and stored on a secure hardware token (at least FIPS 140-1/2 level 2)

Portal users

Four classes of portal users:

- **Anonymous**
  - No unique credentials provided
- **Pseudonymous**
  - Human providing authenticated but non-identifying information to the Portal
- **Identified**
  - Authenticated personal information
    - but not compatible or equivalent to Grid AuthN
- **Strongly Identified**
  - Portal can authenticate to Grid resources with valid Grid credentials belonging to the user

Portal Classes

Portal Class	Executable	Parameters	Input
Simple one click	Provided by portal	Provided by portal	Provided by portal
Parameter	Provided by portal	Choose from limited set	Choose from repository vetted by portal
Data processing	Provided by portal	Choose from limited set	Provided by user
Job management	Provided by user	Provided by user	Provided by user

Portal – General policy

- All portals must comply with VO Operations Policy
- VO, Portal and Portal manager all held responsible and accountable
  - Except where user is Strongly Indentified
- Must
  - Keep audit logs
  - Manager/operators must assist in incident response
  - Be capable of rate limiting job submissions
- Private keys (proxy or otherwise)
  - Must not be transferred across network (even if encrypted)
  - Must not store private keys on behalf of users if these can be used for Grid AuthN after > 1M seconds
- Data can only be stored in locations agreed between Portal and Resources and only as long as user is associated with portal
- If user Grid credential used then data may be stored anywhere user has permission

One-click portals

- May offer services to any user
- Must use a Robot cert to interact with Grid
- Max submission rate agreed by Grid
- Portal must keep logs of association with IP address and port number of the user

Parameter Portals

- Offer services to all users except anonymous users
- Use robot certificate or Grid credential for strongly identified users
- Submission rates may be different for different user classes – agreed with Grid
- Portal must keep audit log to associate interactions with the Grid to particular user. For Identified or Strongly Identified users must keep relevant authentication information

Data Processing Portals

- Only for Identified or Strongly Identified users
- Use robot certificate or Grid credential for strongly identified users
- Must keep enough audit info to associate interactions with the Grid to particular user.
- AuthN system for Identified Users must be adequately secured
  - Users must be notified of all registrations, modifications or removal of their AuthN data
  - AuthN database must contain info to contact the User
  - Entering or modifying data in the AuthN DB must be appropriately authenticated

Job Management Portals

- Only for Strongly Identified Users
- Portal must use Grid credentials specific to the user for all interactions with the Grid
- Must comply with the Site Operations Policy

Future JSPG plans

- Next face to face JSPG meeting
  - 14/15 May 2009 at CERN
- Complete Accounting and VO portals policies (if not yet finished)
- Revise the Grid User AUP
  - Some Grids use but have modified our text
  - Explore why and standardise where possible
    - DEISA, TeraGrid, Australia, EU infrastructures, national Grids, …
- Revise whole policy set (yet) again in next 12 months
  - More simple, general and consistent
  - More applicable to EGI world
  - Broaden the membership – include more NGIs and other Grids

Requests to GDB

- Final versions of the two VO policies will be prepared soon (addressing all comments received)
  - Then seek GDB approval via e-mail
- Please comment on the Accounting and VO Portal policies
- If final drafts can be arranged in time before the April GDB, then we could seek approval at that time

JSPG Meetings, Web etc

- Meetings - Agenda, presentations, minutes etc

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

- JSPG Web sites

http://www.jspg.org and

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

- Membership of the JSPG mail list is closed, BUT
  - Volunteers to work with us are always welcome!
- Policy documents at ***http://www.jspg.org*** and

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