Security Policy Update

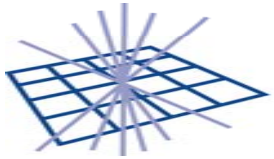
WLCG GDB

CERN, 11 June 2008

David Kelsey

STFC/RAL

d.p.kelsey@rl.ac.uk



GridPP

UK Computing for Particle Physics

Overview

- JSPG meeting (29/30 May 08)
- Revised mandate for JSPG
- Policy approval (4 documents)
- JSPG Future plans

JSPG meeting

- JSPG meeting was held at CERN
  - 29/30 May 2008
- Agenda included
  - Revised JSPG mandate
  - 4 documents now ready for approval
  - Other policy documents
    - VO Registration Policy (replaces VO Security Policy)
    - VO Membership Management Policy (replaces User Registration…)
    - Grid portals
  - Plans for the future
    - During EGEE-III as we move towards EGI
  - Plans for JSPG web site, document repository and collaborative editing

Revised JSPG mandate (V3)

- JSPG is jointly owned by and makes recommendations to both WLCG and EGEE, its primary stakeholders.
- Policy prepared for WLCG is designed to be applied to all of its Grid infrastructures in so far as this relates to WLCG activities. In addition to EGEE, this means subsets of OSG, NDGF and other national Grids and/or individual Grid sites which participate in the WLCG collaboration.
- The most important JSPG activity is that it prepares and maintains security policies for its primary stakeholders.
- It is also able to provide policy advice on any security matter.
- The topics and issues can be specified either by the stakeholders or by JSPG itself. Priority will be given to issues relevant to the primary stakeholders.
- JSPG may create special focussed sub-groups to tackle specific issues.

JSPG Mandate (2)

- JSPG should, wherever possible, aim to prepare simple and general policies which are not only applicable to the primary stakeholders but that are also of use to other Grid infrastructures (NGI's etc). The adoption of common policies by multiple Grids can ease the problems of interoperability.
- JSPG deliberations happen by face to face meetings, phone/video conferences or by the JSPG mailing list.
- The membership of JSPG and its mailing list is determined by the chair of JSPG in consultation with the management of the primary stakeholders.
- JSPG should aim to have sufficient membership to include site security officers, site system administrators, Grid operational experts, middleware experts and members from the larger VOs. Members from other Grids are particularly welcome and are encouraged to request to join.

JSPG Mandate (3)

- JSPG does not formally approve or adopt policies or advice. This is the responsibility of the stakeholder management bodies.
- The members of JSPG are treated as individual experts who do not formally represent any constituency. Individual members of JSPG agreeing to proposed policy does not imply automatic approval by their own Grid or organisation.

Policy Approval

- 4 documents ready for WLCG and EGEE approval
- General comments
  - All have been widely distributed and discussed for months
  - All comments have been addressed
  - The current proposed versions were produced at the JSPG meeting (29/30 May)
  - Word documents with change tracking on
  - Not expecting any major changes at this point
    - These can be addressed in the next policy review
  - But: a chance for final objections
- Each Grid should also provide a covering document per policy giving references, e-mail addresses and other implementation details

General changes

- General changes
  - Remove all footnotes and references
    - References should be covered in the Grid-specific covering documents
  - Updated the names of referenced policy documents
    - Particularly those related to VOs
  - Removed OSG logo (the revised JSPG mandate)
  - Removed direct references to LCG, EGEE etc.
    - Documents should be general and simple
  - Consistent style
  - use of word “*Grid*”

Virtual Organisation Operations Policy

- Version 1.6
- https://edms.cern.ch/document/853968
- No major changes
- Change to names of VO policy documents
- Minor wording improvements

Grid Security Traceability and Logging Policy

- Version 1.8a
- https://edms.cern.ch/document/428037
- Only changed sections 4 and 5
- Grid software MUST include the ability to collect logs centrally at a Site
- Make it clear who has to configure the logging
  - Service providers (including Sites)
- Logs MUST be collected centrally at service-provider level
- There may well be exceptions
  - There were SHOULDs before
  - Deal with these via the procedure for handling of exceptions
    - Report to the Security Officer etc.

Approval of Certification Authorities

- Version 2.7a
- https://edms.cern.ch/document/428038
- Main aim was to add CAs accredited to the new IGTF MICS profile
  - X.509 certs issued following authentication by another Identity Management System
    - E.g. CERN CA based on Active Directory
- Also added the ability for Sites to trust non-IGTF CA for local reasons
  - Must be allowed by local policy and they must deal with any potential non-unique names

What is MICS?

- Abstract of the profile document
- *This is an Authentication Profile of the International Grid Trust Federation describing the minimum requirements for Member Integrated X.509 Credential Services (MICS). MICS X.509 Public Key Certification Authorities (MICS PKI CAs) issue credentials to end-entities who themselves possess and control their key pair and activation data. These CAs will act as independent trusted third parties for both subscribers and relying parties within the infrastructure…*

MICS (2)

- Comment received…
- *I do understand the sentence, but not what it is about. I don't know what sort of credentials are being issued to which sort of end-entities and I am not sure what activation data is. I am not sure who is subscribing to what nor which parties are relying on what. At least it is clear from the web page that whatever they are doing, they are doing it in a secure manner as defined in the Profile. It does sound really great, but not being able to understand what it is about, I feel reluctant to say that I agree with the change*

MICS (3)

- Section 2 (a better description!)
- *A MICS is an automated system to issue X.509 formatted identity assertions (certificates) based on pre-existing identity data maintained by a federation or large organization – the end-entity certificate is thus based on a membership or authentication system maintained by the organization or federation.*
- The CERN CA is a good example – X.509 certs based on Windows Active Directory
- MICS CAs are important to WLCG and EGEE!!

Policy on Grid Multi-User Pilot Jobs

- Version 0.5a
- https://edms.cern.ch/document/855383
- Rewording of the introduction
  - Make it clearer
  - Allow for pilot jobs submitted by a service
    - VO has to name a real person responsible for this
- Reword point 1
  - “Approval” rather than “trust relationship”
- Reword point 8
  - Isolation should include inter-process comms
- Some other minor changes to words

Future JSPG plans

- Next face to face JSPG meeting
  - 9/10 October 2008 at CERN
  - Phone conference(s) before then
  - Session also at EGEE'08 in September 08 (dissemination)
- Complete work on updated VO policies, accounting data and Grid portals
- Broaden the membership – include more NGIs
- Revise whole policy set (yet) again
  - More simple, general and consistent
  - More applicable to EGI world
- Improvements planned for web site
  - Use MediaWiki
  - Better collaborative editing and inclusion of discussion
  - Clearer presentation per Grid of current policy set

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