Security Policy Update

WLCG GDB

CERN, 10 Dec 2008

David Kelsey

STFC/RAL

david.kelsey AT stfc.ac.uk

Overview

- Update since my last GDB presentation (June 08)
- JSPG meeting (9/10 Oct 08)
- VO Policy Issues
- VO Portal Policy
- News from IGTF
- Data Privacy issues
  - And User-level accounting
- JSPG Future plans

JSPG meeting

- JSPG meeting was held at CERN
  - 9/10 Oct 2008
- Agenda included
  - Policy Coordination between Production Grids
  - Grid-specific covering documents
  - VO Policies
  - Grid/VO Portal Policy
  - Data Privacy issues
  - JSPG web site, document repository and collaborative editing

VO Policies

- VO Registration Policy
  - Replaces old VO Security Policy
  - http://www.jspg.org/wiki/VO_Registration_Policy
  - Much simplified document
    - Did think about asking VO to document its procedures
      - Idea dropped!
- VO Membership Management Policy
  - Update of old User Registration policy
  - http://www.jspg.org/wiki/VO_Membership_Management_Policy
  - Discussion within JSPG still continuing
- Aim to complete these during next JSPG meeting

VO Portal Policy

- New policy document
  - Based on Dutch BiG Grid policy (David Groep)
- https://edms.cern.ch/document/972973
- Ideas from EGEE working group on portals
- Policy applies to all Portals operated by Virtual Organisations that participate in the Grid infrastructure
- Defines 4 classes of web portals
  - Web rendering
  - Parameter
  - Data Processing
  - Job Management
- Some general policy plus class dependent statements
- Addresses private key protection and mandates use of Robot certificates
- More work on this at Jan 2009 JSPG meeting

(Some) News from IGTF

- PMA meetings held recently
  - EUGridPMA (6-8 Oct 2008)
  - TAGPMA (6-8 Nov 2008)
  - APGrids PMA (16 Sep 2008)
- Usual business of accreditation of new CAs
  - And peer-review of older ones
- Robot certificates (for web portals, monitoring etc)
  - Automated clients; key protected by h/w token
- Importantly for WLCG, the FNAL KCA policies were approved in November; awaiting operational review (Jan 2009?)
- EUGridPMA AuthZ WG making progress
  - Min requirements, best practices for running VOMS

Data Privacy issues

- There has been a draft policy on User-level Job Accounting for a long long time
- Sites rightly concerned about legal issues
- VOs need appropriate access to user-level accounting
- https://edms.cern.ch/document/855382/1
- Why has JSPG never finished this?
  - Busy on other things
  - Not sure of the legal issues re data privacy
- We do need to finish this soon!

Data Privacy (2)

- Benefited from work by EU NRENs (and TERENA) on data privacy in federated networks
  - I attended meetings in Utrecht just last week
- Useful discussions with Andrew Cormack (from Janet(UK)) – but no legal guarantees!
- The European Data Protection Directive (95/46/EC) defines “personal data” in Article 2 as follows:
- “ 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;”

Data Privacy (3)

- Research and Education federated access management systems (e.g. Internet2 Shibboleth) are avoiding use of personal data
  - Except for Identity Providers (IDP)
  - Lots of problems processing personal data
- But they use pseudonymous identifiers
  - E.g. “eduPersonTargetedID”
  - Opaque identifiers
  - Cannot be linked to human without asking IDP
  - Persistent
    - So a service can tell it’s the same user returning
  - Different per service
    - So user actions cannot be correlated between services

Data Privacy (4)

- IP address – is it personal data or not?
- The EU Article 29 Working Party gave their opinion
  - “unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side.”
- Case law, even within one country, is not clear here
- A recent development is that legal as well as technical means can be used to address the “absolute certainty” above

Data Privacy (5)

- Example of an EU medical research project
  - Hospitals provide medical data to the project under a contract
  - Pseudonymous identifiers used to hide identity but link together data from the same patient
  - The legal agreement states that the Data controller will *not* disclose the linking information to the project
- This seems to be enough to meet the data privacy requirements

User level Accounting

- The X.509 certificate contains the users name
  - Definitely personal data
- Could we use pseudonymous identifiers?
  - Sites when consulted have said “no”
  - They need to see the actual name of the user
  - Would only meet the privacy requirements if there was no possibility of linking to the human
- Targeted Identity is not possible. The IDP (in our case the CA) issues long term credentials for use at all services
- We also previously hoped that informed user consent was good enough to remove some of the requirements
  - Have recently realised that this also needs to include the ability for users to opt out

Accounting policy

- The way forward?
- We have to properly handle the data privacy legal requirements
  - Grid Sites must appropriately register with their national Data Commisioners
  - As must the GOC and Portal accounting instances
  - Have to handle issues of export of data outside of EEA
- Need to address the “contractual” requirement for accounting (billing) data (as opposed to informed consent)
  - WLCG MoU?
  - Make this a policy just for WLCG?
- The approach and current document are long the right lines
- Need to complete
  - Appropriately identify Data Controller, Data Processor etc

Future JSPG plans

- Next face to face JSPG meeting
  - 22/23 January 2009 at CERN
- Complete VO policies, accounting data and VO portals
- Review 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, …
- Discuss CA adoption at Sites, Information Service, SAM tests etc
- Discuss new EGEE AuthZ deployment – local versus central policy
- Revise whole policy set (yet) again of next 15 months
  - More simple, general and consistent
  - More applicable to EGI world
  - Broaden the membership – include more NGIs and Grids

Questions?

JSPG Meetings, Web etc

- Meetings - Agenda, presentations, minutes etc

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

- JSPG Web sites

http://www.jspg.org

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