



JSPG: policy issues

Portal WG

IBCP, 29 June 2007

David Kelsey

STFC/RAL

d.p.kelsey@rl.ac.uk

JSPG policy issues

- Current Grid security audit requirement
 - Able to trace all actions to an well-identified individual person
 - Assurance of Identity is high (photo-id or equivalent)
 - Sharing of identities not allowed
 - Illegal/problem actions or data traceable to a person
- AUP
 - User accepts Grid AUP on registration with VO
 - VO AUP has to exist
 - And user also accepts this on registration

New policies

- JSPG working on new policies
 - VO Operations Policy (VO will have to sign)
 - Draft finalised this week
 - Grid Service policy
 - Responsibilities and liabilities of anyone (incl VO) running services
 - Not yet started on the general policy
 - Will look like Site and VO Operations policies
 - Starting from specific examples
 - VO Box (draft already written long time ago)
 - Multi-User Pilot Jobs
 - Portals

Multi-User Pilot Jobs

- Similar in many ways to a Portal
 - Pilot Job runs under one VO identity
 - Work for multiple different users is executed
 - With or without switching ID to the user
- JSPG thinks we will need a separate Portal Policy
 - We (JSPG & Portals WG) should work on this

Multi User Pilot Jobs (2)

- Only allowed at Site that allows MUPJ for this VO
- Person responsible for pilot job must be registered
- The pilot job user-id or robot ID must be registered
 - Non-registered not allowed
- If ID is switched must use site provided utility (e.g. glxec)
- Local site AuthZ will be performed (callouts)
 - Pilot job must respect the decision
- Audit trail and accounting logs must be kept by Pilot person
- Site reserves right to block/cancel individual jobs or all jobs
 - When problems
- Pilot job owner is responsible for actions of the payload
 - If no ID switch is made
- Code of the pilot job must be made available to Site

DPK thoughts on Portals policy issues

- We need a matrix for the 5 use cases
- Per use case
 - Is Grid job well-known (canned job) or free?
 - Is Grid job executed under Portal ID or User ID?
 - Is Grid data well-known (canned data) or free?
 - Is Grid data owned by Portal ID or User ID?
- For User ID
 - Is user well identified (photo ID)?
 - Or just username/email-address and password?
 - Does user ID need to be transferred to the Grid
- Need to address accounting issues (as discussed earlier)
 - And data privacy issues
- Written policies are very important (to protect Grid and Portal)