Security Policy Update

David Kelsey

GridPP DB, UCL
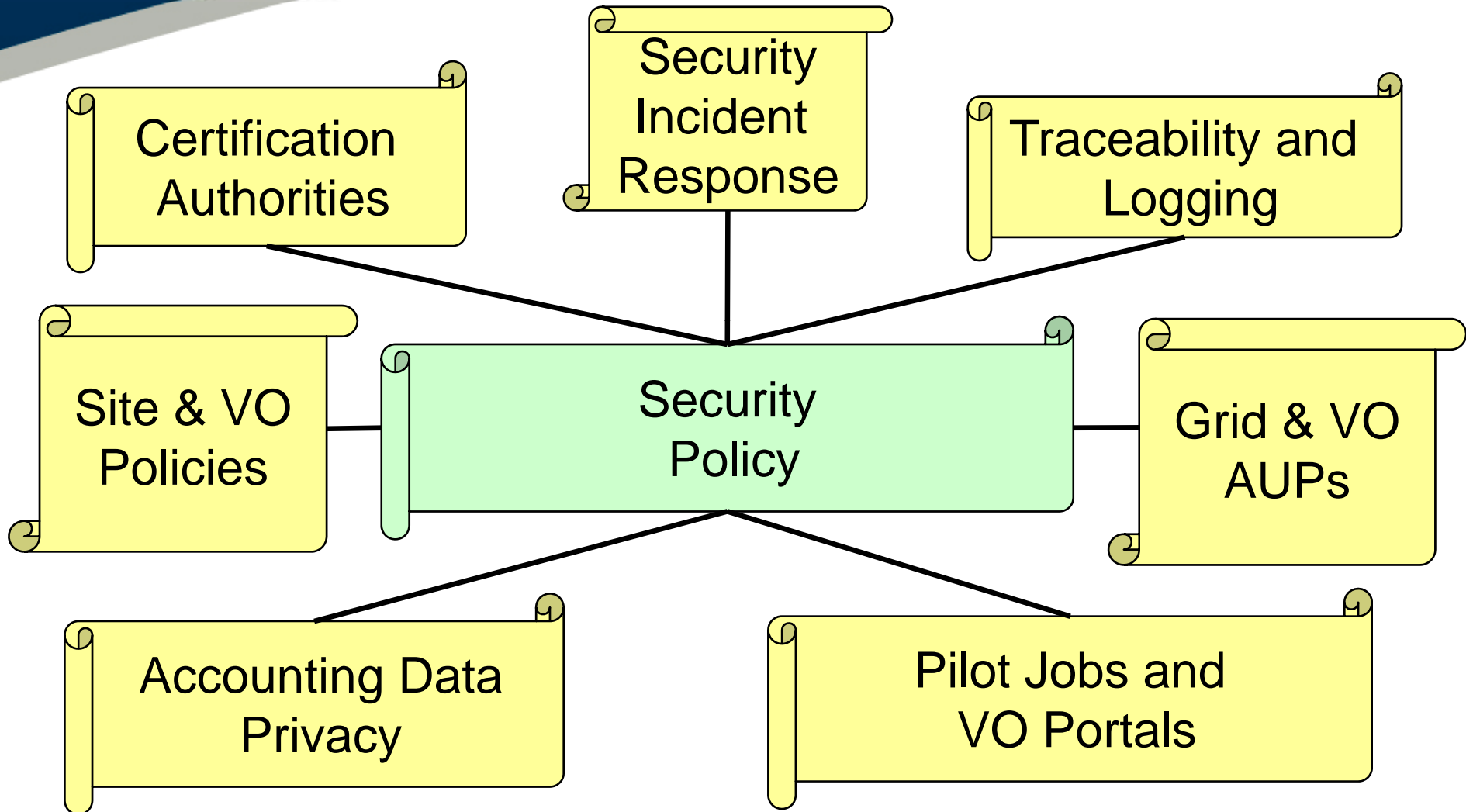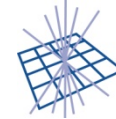
3 Apr 2009

JSPG

- Joint Security Policy Group (new mandate in 2008)
- Prepares and maintains security policy
  - For EGEE
  - For WLCG
- Policies approved and adopted by Grid management bodies
  - E.g. GridPP DB
- Aim for general common policies useable by many Grids (OSG, NDGF, DEISA, Other EU Grids,…)
  - OSG has played key role here, e.g. Grid AUP
- Tackle scaling problems of large numbers of sites, and large number of VOs
  - Single policy applies to VO (at ALL sites)
  - Aids interoperability

Security Incident Response

Certification Authorities

Traceability and Logging

Site & VO Policies

Security Policy

Grid & VO AUPs

Accounting Data Privacy
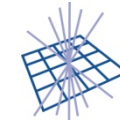
Pilot Jobs and VO Portals

2008 approved policies

- 4 approved policies
  - EGEE and WLCG in Aug/Sep 2008
    - Approval of Certification Authorities
    - Traceability and Logging
   - VO Operations
   - Multi User Pilot Jobs

Current work
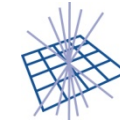
Kelsey, Security Policies

Two draft 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

- 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

- 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.
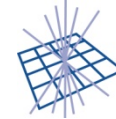
Feedback on VO registration

- Useful comments (many from UK)
  - Especially small(er) VOs
  - 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?
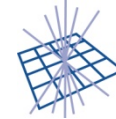
Feedback on VO membership

- 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

- Grid Policy on the Handling of User-Level Job Accounting Data (Draft Policy)

- V0.7, 23 Jan 2009

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

- This document presents the minimum requirements and policy framework for the handling of user-level accounting data created, stored, transmitted, processed and analysed as a result of the execution of jobs on the Grid.

- WLCG wants to activate this asap. Do any sites still have problems? France has given some feedback.
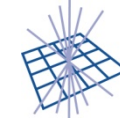
VO Portal Policy

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

Other issues

- **EUGridPMA AuthZ working group**
  - Defining min requirements and best practices for running an Attribute Authority (e.g. VOMS)

- **Identity Management via Federations**
  - E.g. national Shibboleth infrastructure
  - Raises issues of Levels of Assurance
    - Can we continue to require face to face identity vetting?
    - Do we still require an "appropriate presentation of the actual name" in the DN

Future JSPG plans

- Next face to face JSPG meeting is 14/15 May 2009 at CERN

- Complete Accounting and VO portals policies

- 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 security incident response policy

- 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

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