eGee

Enabling Grids for E-sciencE

Joint Security Policy Group
- Status and plans

EGEE'07 Conference

Budapest, 3 Oct 2007

David Kelsey

STFC/RAL

d.p.kelsey@rl.ac.uk

www.eu-egee.org

Information Society
and Media

Enabling Grids for E-sciencE

- **Introduction to JSPG**
- **Interoperable policies**
- **Current policy document set**
- **Recently approved documents**
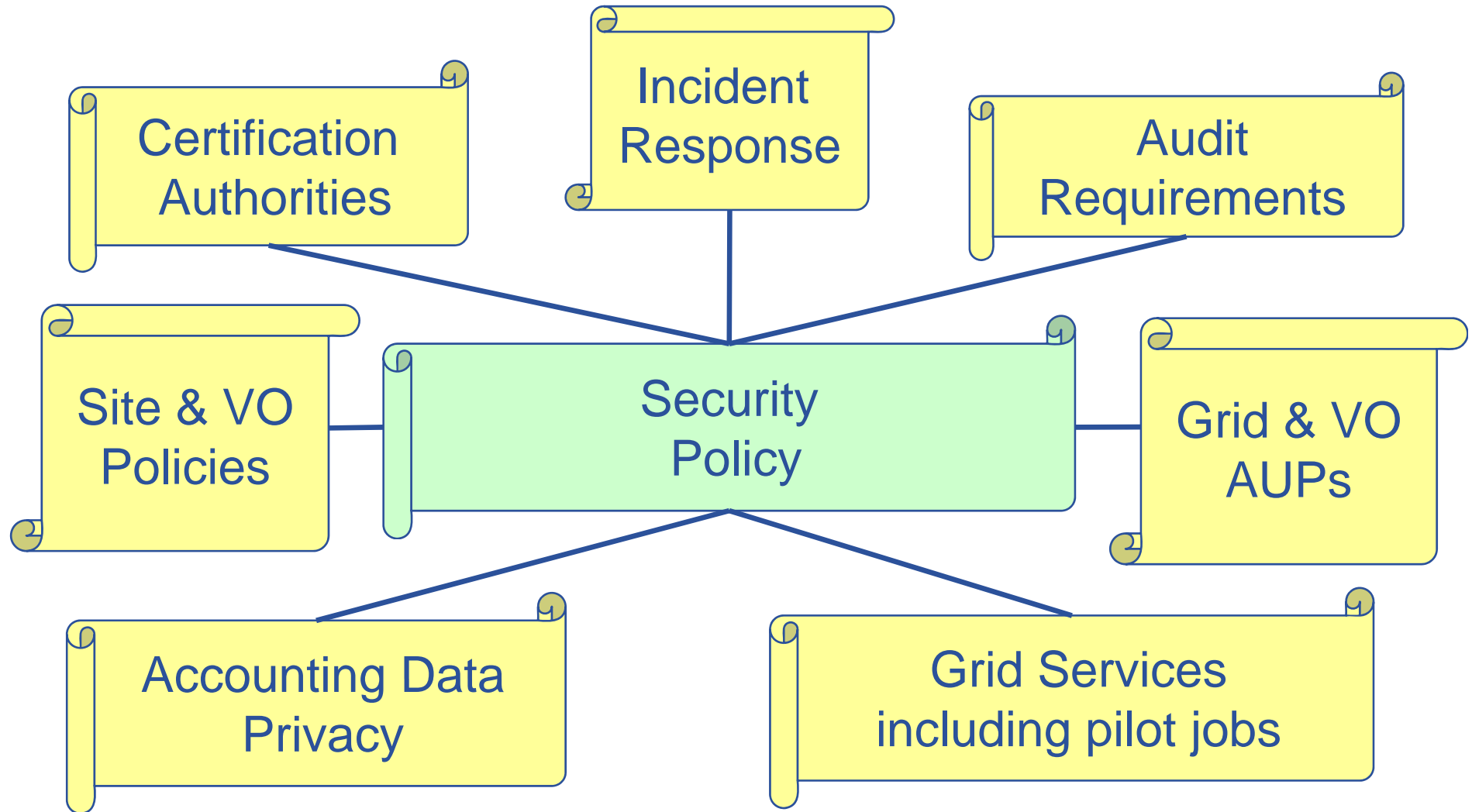- **Current work**
- **Future plans**

Joint Security Policy Group

- **Main aims**
  - To develop and maintain security policies and procedures
    - These should be general, simple and interoperable
    - For use in EGEE, OSG, NDGF, WLCG and others
  - Policies are agreed and adopted by PEB for EGEE
    - Agreed and adopted by GDB/MB for WLCG
    - Agreed and adopted by management of other Grids (OSG, NDGF)
  - To liaise with other operational, middleware and policy security groups
    - OSCT, MWSG, IGTF and its PMAs
    - For feedback in both directions

Enabling Grids for E-sciencE

- **Application representatives/VO managers**
  - Discussions with VO managers as/when required
- **Site Security Officers**
  - Bob Cowles (SLAC and OSG), Denise Heagerty (CERN)
- **Site/Resource Managers/Security Contacts**
  - Dave Kelsey (RAL) – Chair
  - Romain Wartel (CERN, EGEE Security Officer)
- **Security middleware experts/developers**
  - Joni Hahkala, David Groep, Andrew McNab
- **CERN Deployment team**
  - Maria Dimou, Ian Neilson
- **Now expanded to include other EU Grid projects**
  - SEE-Grid, DEISA, …
- **Others:** various people participate from time to time
  - Apologies to anyone not mentioned by name here
- **Other EU Infrastructure projects (may) use our policies**
  - BalticGrid, EELA, EUMedGrid, EUChinaGrid, …
- **Volunteers ALWAYS welcome (please contact me!)**

Enabling Grids for E-sciencE

- **Allow VOs (applications) to easily use resources in multiple Grids**

- **The simplest approach**
  - Common Policies (and to some extent procedures)
    - Security Policy
    - User AUP
    - Site Operations
    - VO Operations
    - Operational procedures and other policies

- **If not common then at least not conflicting**
  - To augment local site and network security policy

- **JSPG is happy to work with other EU Grid projects**
  - On common policies and procedures

- **EU eInfrastructure Reflection Group (eIRG)**
  - Common approach at highest level
    - JSPG inputs policy for consideration

eGee

Enabling Grids for E-sciencE

Certification Authorities

Incident Response

Audit Requirements

Site & VO Policies

Security Policy

Grid & VO AUPs

Accounting Data Privacy

Grid Services including pilot jobs

Enabling Grids for E-sciencE

The core set

- *Grid Security Policy (approval in progress)*
  - V5.7, 28 June 2007
- *Grid Acceptable Use Policy*
  - V3.1, 28 Oct 2005
- *LCG/EGEE Virtual Organisation Security Policy (needs update)*
  - V1.7, 31 Oct 2005
- *Grid Site Operations Policy (approval in progress)*
  - V1.4, 19 Apr 2007

Sub-policy documents (several in need of updates)

- *Approval of Certification Authorities*
  - V2.5, 3 July 2006
- *Audit Requirements for LCG-1*
  - V1.2, 19 June 2003

Enabling Grids for E-sciencE

Sub-policy documents (continued)

- *Requirements for LCG User Registration and VO Membership Management*
    - V2.7, 1 June 2004

- *Site Registration Policy & Procedure*
    - V2.0, 16 Mar 2005

- *LCG/EGEE Incident Handling and Response Guide*
    - V2.1, 15 June 2005

It was agreed by the GDB on 13th Jan 2004
- **all LCG Policy documents remain valid until they are updated**
- **Also adopted by EGEE (and other Grids)**

eGee

Enabling Grids for E-sciencE

- **Recently finished documents – approval underway**
  - Grid Security Policy (V5.7)
    - https://edms.cern.ch/document/428008/4
  - Grid Site Operations Policy (V1.4)
    - https://edms.cern.ch/document/819783/1
- **Current work**
  - VO Operations Policy
  - Grid Services
    - Multi-user pilot jobs
  - Audit requirements
  - User-level job accounting data policy (privacy issues)
- **Several other documents need updating**
  - E.g. VO security policy and LCG User Registration/VO membership
- **All new documents are aimed to be simple and general, e.g. apply to "Grid" not "EGEE" (like the Grid AUP)**

Enabling Grids for E-sciencE

- **JSPG must be able to modify policy documents**
- **Process must allow for full consultation and feedback**
- **Once a new/updated policy is adopted, it applies to all**
  - Even those who don't agree to the new policy!
- **Full consultation includes**
  - ROC managers, VO managers, Site security contacts, OSCT
- **For EGEE, failure to agree in PEB is escalated to PMB**
- **Adoption of new policy**
  - Will be announced to all sites and VOs
  - **Includes a Grid-specific cover document** which explains the implementation, e.g. defines the terms
  - Anyone unable to implement must inform Grid Security Officer
    - Resolved by escalation to SA1, then PEB, then PMB
- **We will document this process**

Now look at two policy documents currently being prepared

Enabling Grids for E-sciencE

- **A new policy document**

- ***https://edms.cern.ch/document/853968/1***
  - Version 1.2

- **Similar aims to the Site Operations Policy**
  - But for VOs

- **Documents the responsibilities of a VO**
  - They must accept and sign during registration

- **This is getting close to final**
  - Currently inviting comments from VO managers and others
  - Legel experts also giving advice

Enabling Grids for E-sciencE

- **Show VO policy document**
- **Some of the discussion points**
  - What does "the Grid" mean?
  - Who is the Grid Security Officer and Security Operations?
  - Where do I find the referenced policy documents?
  - Don't like wording of
    - Standard disclaimer – No guarantee, no liaibility, own risk
    - Grid may "control" your access
  - Open ended nature (blank cheque) of future changes
  - Other reasons for sites blocking access
  - Lack of tools to keep VO membership up to date
  - Can someone else run the VO membership service?
  - Does VOMS have the appropriate logging and backup?
  - Require a VO security officer (for clear responsibilities)?
  - How do we manage the VO signing process?
  - VO should ensure they have necessary licences
  - There are too many policy documents – why not just one?

Enabling Grids for E-sciencE

- **First in a set of policy documents aimed at the responsibilities of those running Grid services**
  - Others will be VO Boxes, Grid portals, …

- **https://edms.cern.ch/document/855383/1**
  - Version 0.3

- **Show policy document**

- **Some issues**
  - Cleanup between each separate user job
    - Delayed transfer of job output
  - gLExec on worker nodes (for identity switching in pilot job)

- **Minimum requirements for VO membership services**
  - JSPG agreed this would be very useful
    - But the work did not yet start
  - EU Grid PMA recently agreed to form a working group looking at
    - Minimum requirements for AuthZ Attribute Authorities (AA)
    - Repository and distribution of AA trust anchors
  - AuthZ has had much less policy work than AuthN
    - IGTF seems a very good body to take on some of the aspects of trust
- **Grid portals**
  - Important requirement for many VOs (and hence for EGEE)
  - EGEE has a working group on this
  - Policy issues being addressed
    - similar in many ways to pilot jobs
  - JSPG will produce a policy on this
- **Complete revision of the other old documents**
- **New policy: User-level job accounting, Grid Service Operations**

Enabling Grids for E-sciencE

- **Move to EGI/NGIs**
  - JSPG will perform a revision of the full document set (EGEE-III)
  - Make policies even simpler and more general
    - Remove duplications and overlaps
  - Need to work with (some) NGIs to see how best to achieve this
- **VO scaling problems**
  - Many VOs will wish to use resources in many NGIs
  - If trust relationships (registration and policy acceptance) have to happen everywhere this will be difficult
  - I would like to see a VO register just once (not a JSPG view yet)
    - Either with EGI or one NGI
    - Accreditation of VO membership service happens once
      - *Against agreed IGTF standards*
  - We need to discuss the best way to achieve this
    - For example, a VO could have a "home" in one NGI

Enabling Grids for E-sciencE

- **Meetings - Agenda, presentations, minutes etc**

http://agenda.cern.ch/displayLevel.php?fid=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://cern.ch/proj-lcg-security/documents.html