Privacy and Policies
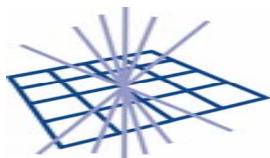## *Joint Security Policy Group*

David Kelsey
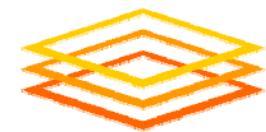
CCLRC/RAL, UK

d.p.kelsey@rl.ac.uk

WLCG CB Meeting, CERN, 25 Jan 2007

Overview

- Aims of talk
  - Policy first, then Privacy
- Joint Security Policy Group (JSPG)
- Current policy documents
- New and revised documents
- Privacy and Accounting data
- JSPG future plans

Aims of talk

To inform the Collaboration Board

- Adopted security policies
  - apply to all Grid participants
    - including all users and all Grid Sites
- Current JSPG work to revise these
- Data privacy issues
  - As related to user-level accounting
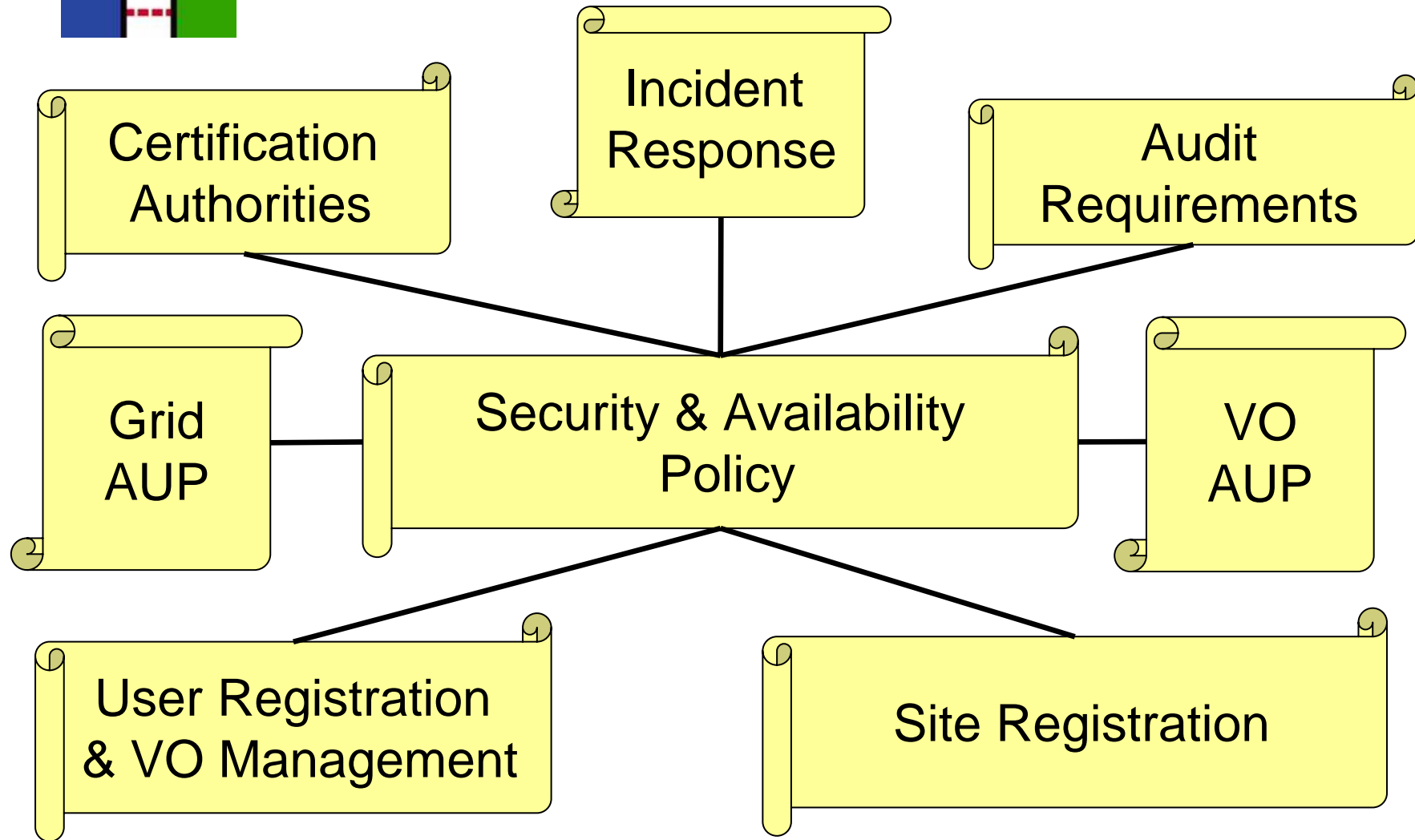- Future work of JSPG

JSPG

- "Joint" initially means EGEE *and* LCG
  - Strong participation by USA Open Science Grid
  - Now "Joint" = EGEE/OSG/WLCG and others
- Aims of policy documents
  - General and simple (wherever possible)
  - Common policy across multiple Grids
  - In general they do not override local Site Policy
- JSPG membership
  - Application representatives/VO managers
  - Site Security Officers
  - Site/Resource Managers/Security Contacts
  - Security middleware experts/developers
  - CERN Deployment team
- Policies approved and adopted by WLCB MB, EGEE PEB, …

Current Security Policy

Incident Response

Certification Authorities

Audit Requirements

Grid AUP

Security & Availability Policy

VO AUP

User Registration & VO Management

Site Registration

http://cern.ch/proj-lcg-security/documents.html

Current policy

The core set

- ***Security and Availability Policy for LCG***
  - V4c, 17 Oct 2003
- ***Grid Acceptable Use Policy***
  - V3.1, 28 Oct 2005
- ***LCG/EGEE Virtual Organisation Security Policy***
  - V1.7, 31 Oct 2005

Sub-policy documents

- ***Approval of Certification Authorities***
  - V2.5, 20 Sep 2006
- ***Audit Requirements for LCG-1***
  - V1.2, 19 June 2003

Current Policy (2)

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

- ***Guide to LCG Application, Middleware & Network Security***
  - V1.6, 19 July 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 January, 2004
- all LCG Policy documents remain valid until they are updated
- Also adopted by EGEE (and other Grids)

Revision of policy

New document

- *Agreement on Grid Site Operations*
  - V0.9, 9 Jan 2007
  - *https://edms.cern.ch/document/726129*
- Currently going through WLCG and EGEE approval
- Very important for Sites!
- All Grid Sites will have to sign when they register
  - Existing sites will also have to sign
- Puts responsibilities on Sites
- Text very close to final
  - One last round with legal experts and sites
- *If you see a show-stopper problem – please let me know!*

Revision (2)

- Old document, now under revision
- A new top-level *Grid Security Policy* document
- V5.4, 11 Dec 2006
  - *https://edms.cern.ch/document/428008/4*
- More general and simple and for use on many Grids
- Objectives
  - Gives authority for actions
  - Places responsibilities on all participants
- Scope
  - Applies to all Grid participants
  - Does not override local policies
  - Sub-documents (detailed procedures, rules and guides) are part of the policy
- Aiming for approval in April 2007
- All feedback VERY welcome

Data Privacy Issues

Grid Operations and VO managers require…

- Accounting

- Auditing

- Logging

- Monitoring

at the VO/group/role/**individual user** level

Concentrate for now on ACCOUNTING Usage records

Legal issues

- **EU Directives and national laws relating to…**
  - **processing of personal data and the protection of privacy in electronic communications**
- **Not allowed to publish data that could be used to track down the activities of a single individual**
  - **But can do individual billing (contractual)**
- *personal data* **means any information relating to an identified or identifiable natural person**
- ***Processing* of personal data**: *any operation on personal data, such as collection, storage, retrieval, dissemination* etc…
- **Informed user consent is required**
- **Issues re data protection, retention, movement (especially across national borders or outside EU)**
- **User has the right to see their own information**
- Many sites have been unwilling to give access to accounting records at user level

User consent

Grid AUP says…(accepted during registration with VO)

- *Logged information, including information provided by you for registration purposes, shall be used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed to other organizations anywhere in the world for these purposes. Although efforts are made to maintain confidentiality, no guarantees are given*

- So the User has given informed consent

- Together with a policy document on personal data management, should be enough to convince sites to allow access to the appropriate logs

Accounting Requirements

WLCG requires

- All Grid sites providing resources to WLCG
- to provide accounting information for all jobs run by members of the LHC VO's

The LHC VO managers require

- Access to accounting at individual user level
  - i.e. X.509 DN included
- Again from all sites providing resources
- Timely accounting (for monitoring) useful?
- We need a technical solution and agreed policy that allows all this to happen legally

Draft Accounting Policy

- For consideration by GDB in Feb 2007

- The accounting record not only specifies the VO but includes the User DN (encrypted)

- The data handling policy includes descriptions of …

  – What is stored and where?

  – Access rights - Who can read?

  – Access for what purposes?

  – Retention period?

  – Publication of accounting data?

  – How is the data protected from illegal or accidental disclosure?

JSPG Future plans

- Top-priority
  - *Accounting Data Policy*
- *Agreement on Virtual Organisation Operations*
  - VO's take on responsibilities
    - For user registration and management
    - For running VO-specific services
    - For assisting in incident response
- *Agreement on Grid Services Operations*
  - Anyone running Grid services has responsibilities
    - E.g. the VO box
- The last two may be just one document
- JSPG meets at CERN on 13/14 March

JSPG Meetings, Web etc

- 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

Questions?