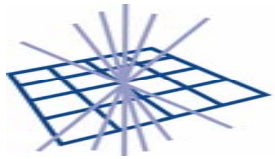
JSPG Update: Security Policies

David Kelsey

CCLRC/RAL, UK

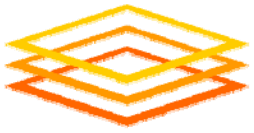
d.p.kelsey@rl.ac.uk

GDB Meeting, CERN, 5 July 2006



GridPP

UK Computing for Particle Physics



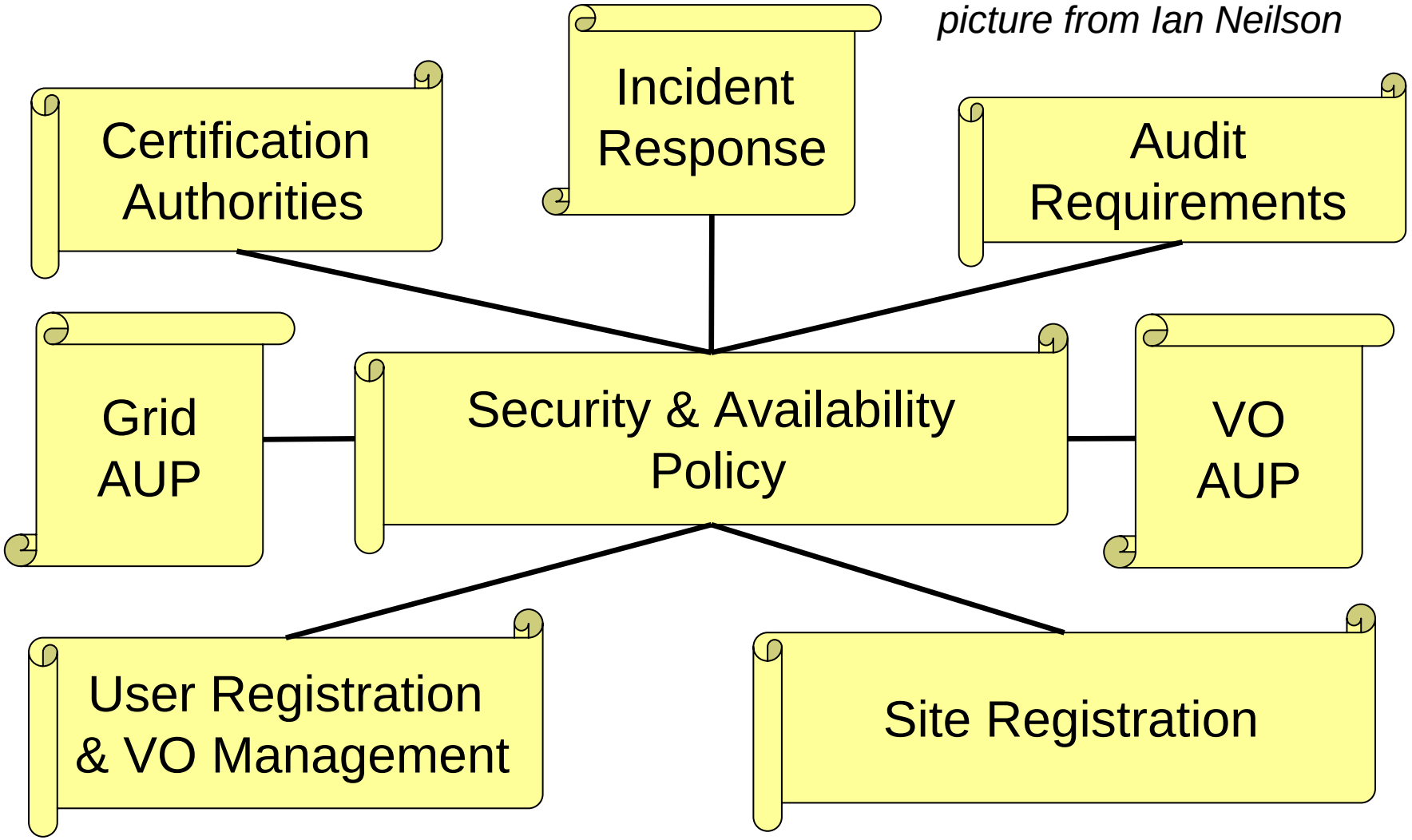
Open Science Grid

Overview

- Current Security Policy documents
- Updated/New policy documents
- Recent JSPG policy “decisions”
- Future plans
- Other JSPG news
- Request to GDB

Security Policy

picture from Ian Neilson



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 LCG-1 Certificate Authorities***
  - V1.0, 2 June 2003
- ***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)

Obsolete Documents

No longer in use

- ***Rules for use of LCG-1 Computing Resources***
  - V2, 23 June 2003
- ***User Registration and VO management for LCG-1 in 2003***
  - V1.2, 3 July 2003
- ***LCG Resource Administrators' Guide***
  - V0.2, 16 Feb 2004
- ***Procedure for Site Self-Audit***
  - V0.2, 16 Feb 2004
- ***LCG Service Level Agreement Guide***
  - V0.3, 16 Feb 2004

Updated/New policy

- Aims
  - More general, more simple (wherever possible)
  - Common policy across multiple Grids
- Three very old documents need updating
  - ***Grid Security Policy***
  - ***Approval of Certification Authorities***
  - ***Audit Policy***
- JSPG is working on all of these
  - Today the CA document is ready for approval
- New ***Site Operational Procedure Policy*** (EGEE milestone)
  - Draft V0.3 being discussed (comments welcome)
  - https://edms.cern.ch/document/726129
- New ***Accounting Data Policy*** is needed
- The ***VO Security Policy*** needs updating
  - to include new VO naming rules (dns style names)

New CA policy

- To replace old document from 2003
- Ready for discussion/approval now
  - Draft V2.5
  - *https://edms.cern.ch/document/428038*
- Acknowledges role of IGTF
  (The International Grid Trust Federation)
- WLCG/EGEE/OSG are represented on the PMA's
- "GRID" = WLCG, EGEE, OSG
  - or any other related infrastructure
- i.e. a general common policy

CA Approval (1)

The GRID uses authentication credentials issued by

- *a CA accredited to the IGTF Classic Authentication Profile*
- *a CA accredited to the IGTF Short Lived Credential Service (SLCS) Profile*
- *other CAs which MAY be temporarily approved by the appropriate Grid management bodies*

Credentials issued by other authorities to those listed above are not approved.

CA Approval (2)

- The GRID deployment teams SHALL maintain a repository containing all accepted CA root certificates and associated data necessary for deployment
- All GRID resources SHOULD promptly install the full list of approved CAs from the repository as packaged, updated and announced from time to time by the deployment teams
- Decisions not to install or to subsequently remove an approved CA MUST be communicated immediately to the appropriate operational body
  - EGEE Regional Operations Centre or OSG Support Centre

Accounting Data Policy

- Several presentations to GDB on this topic!
  - Most recently by John Gordon in June 2006
- We need feedback (from VOs) on the proposal for treatment of user-level accounting
- ***Once we know what we are implementing we can finalise the policy document***
- One new requirement has arisen in last few days
  - GridPP Oversight Committee
    - Requests to see details of how many different users are using the GridPP resources (UK and not-UK)
- Is there a general requirement for the Operational infrastructure to see user-level accounting?
  - In the past we have always assumed just VO's

Recent JSPG policy “decisions”

Meeting at CERN on 22/23 June 2006

- *See notes from meeting (attached to GDB agenda)*

- Globus_TCP_Port_Range
- Read access to VO information in VOMRS
- Use of CERN ID number/Date of Birth in LHC User Registration
- VOMS Proxy Lifetime and blocking of user access
- Single site point of control for blocking users
- Audit Policy/Requirements
- Pilot jobs and gLexec
- Incident Response Reciprocal Agreement (EGEE/OSG)

Future plans

- EGEE SA1 milestone (MSA1.7)
  - *Update Security Policy* (Month 8 = Nov06)
- OSG Risk Analysis
  - Presented at EGEE/OSG Operations workshop
  - EGEE interested in this work
- VO AUP
  - OSG working on this
    - MWSG meeting Jun 06
  - Does EGEE adopt this approach?
    - Requires VO's to accept responsibility
- Minimum requirements for VO membership services?
- WLCG security emergency plans
  - Define communication & decision processes

Other JSPG news

- Update of mandate required
  - Today *Joint* = LCG & EGEE (with OSG input)
  - Include OSG more formally?
  - Better description of approval processes
  - Include other infrastructure projects?
- Need better understanding how OSG and EGEE policy fits together (if not common)
- Will draft this in September 06

Request to GDB

- Comment on/approve CA document
  - By e-mail discussion (by 14th July?)
    - Will also consult EGEE ROC Managers, OSG, …
  - Then to WLCG MB and EGEE PEB for formal adoption
- Comment on other documents as they become available
  - Aim to have full up to date set by November 06