



Enabling Grids for E-science

EGEE and JSPG activities

David Kelsey

CCLRC/RAL

d.p.kelsey@rl.ac.uk

www.eu-egee.org



- **Joint Security Policy Group**
- **The set of Security Policy documents**
- **LCG, WLCG, EGEE – who is who?**
- **Recent & current work**
- **Operational Security Coordination Team**
- **Some recent security issues**
- **More general issues**

- **LCG Security Group** was created in early 2003

Mandate

- **To advise and make recommendations to the Grid Deployment Manager and LCG GDB on all matters related to Security**
 - *Policies are agreed and adopted by GDB for LCG*
- **To produce and maintain**
 - Policies and procedures on Registration, Authentication, Authorization and Security
- **Where necessary recommend the creation of focussed task-forces made-up of appropriate experts**
 - E.g. Task force on *LCG User Registration*

- **Following first EGEE collaboration meeting, scope of group extended**
 - To include a proposed EGEE SA1 Site Security Group
- **Joint Security Policy Group (JSPG)**
 - “Joint” initially means EGEE *and* LCG
 - Strong participation by USA Open Science Grid
 - Now “Joint” = EGEE/OSG/WLCG
- **An activity of EGEE SA1**
 - Discusses all documents with ROC Managers
 - Participation of site managers/security officers
- **Strong links to EGEE Middleware Security Group (and JRA1)**
- **New “task force” (added after EGEE-2 meeting)**
 - SA1 Operational Security Coordination Team (OSCT)
 - See later

- **Application representatives/VO managers**
 - Discussions with VO managers as/when required
- **Site Security Officers**
 - Bob Cowles (SLAC), Denise Heagerty (CERN), & in the past - Dane Skow (FNAL)
- **Site/Resource Managers/Security Contacts**
 - Dave Kelsey (RAL) – Chair
 - Miguel Cardenas Montes (Spain)
- **Security middleware experts/developers**
 - Joni Hahkala (JRA3), David Groep (JRA3), Andrew McNab (GridPP), Yuri Demchenko (JRA3)
- **CERN Deployment team**
 - Maria Dimou, Ian Neilson (Security Officer)
- **Now expanding to include other EU Grid projects**
 - SEE-Grid, DEISA, Diligent
- **Other EU Infrastructure projects use our policies**
 - BalticGrid, EELA, EUMedGrid, EUChinaGrid

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

<http://agenda.cern.ch/displayLevel.php?fid=68>

- **JSPG Web site**

<http://proj-lcg-security.web.cern.ch/>

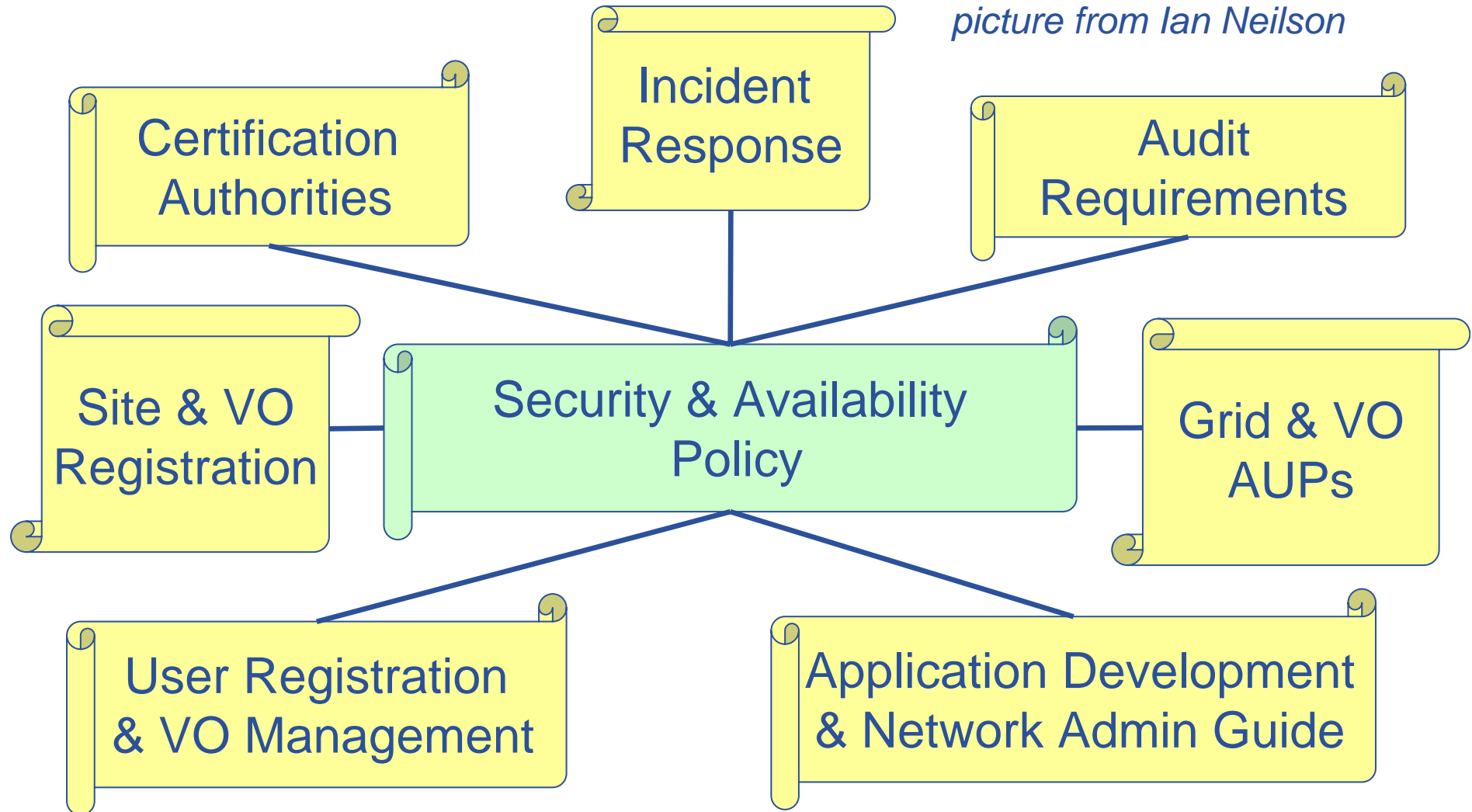
- **Membership of the JSPG mail list is closed, BUT**

- 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>

picture from Ian Neilson



- **Has been lots of confusion!**
- **LCG = “LHC Computing Grid” project**
- **WLCG = The “worldwide” collaboration doing this**
- **The four LHC VO’s are global in scale**
 - ALICE, ATLAS, CMS, LHCb experiments
 - Use resources from both EGEE and OSG
- **Sites join either EGEE or OSG**
 - The operational infrastructures
- **BUT...**
 - There is an LCG Grid Deployment Board
 - All EGEE and OSG countries represented
 - And a WLCG Management Board
 - In addition to all the EGEE management groups
- **JSPG reports to both LCG GDB and EGEE ROC Mgrs**

- **Recently approved**
 - Grid AUP
 - VO Security Policy (requires a VO AUP)
- **All other documents need updating (this year)**
- **Current work**
 - Top-level Security Policy document
 - CA approval (use IGTF accredited)
 - VO Naming (use DNS style)
 - User-level Accounting data policy (privacy issues)
- **A User Registration task force has worked on**
 - VO Registration for the LHC experiments (VOMS)
 - VOMRS from FNAL (run at CERN)
 - Links to Experiment/HR databases at CERN

By registering with the Virtual Organization (the "VO") as a GRID user you shall be deemed to accept these conditions of use:

- 1. You shall only use the GRID to perform work, or transmit or store data consistent with the stated goals and policies of the VO of which you are a member and in compliance with these conditions of use.***
- 2. You shall not use the GRID for any unlawful purpose and not (attempt to) breach or circumvent any GRID administrative or security controls. You shall respect copyright and confidentiality agreements and protect your GRID credentials (e.g. private keys, passwords), sensitive data and files.***
- 3. You shall immediately report any known or suspected security breach or misuse of the GRID or GRID credentials to the incident reporting locations specified by the VO and to the relevant credential issuing authorities.***

- 4. Use of the GRID is at your own risk. There is no guarantee that the GRID will be available at any time or that it will suit any purpose.***
- 5. 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.***
- 6. The Resource Providers, the VOs and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions.***
- 7. You are liable for the consequences of any violation by you of these conditions of use.***

This acceptable Use Policy applies to all members of <The VO> Virtual Organization, hereafter referred to as the VO, with reference to use of the LCG/EGEE Grid infrastructure, hereafter referred to as the Grid. The Geant4-Spokesman, <name> owns and gives authority to this policy. The goal of the VO is to validate the software they provide to their users (HEP experiments as ATLAS, CMS, LHCb, Babar, etc, Astrophysics applications, biomedical communities) twice per year within the Grid environment. This procedure should cover a wide range of parameters and physical models which are high CPU demanding. At the same time they are planning to use regularly the LCG/EGEE resources to make analysis and studies of their toolkit. Members and Managers of the VO agree to be bound by the Grid Acceptable Use Policy, VO Security Policy and other relevant Grid Policies, and to use the Grid only in the furtherance of the stated of the VO.

- **Operational Security Coordination Team**

slides from Ian Neilson

- Members:

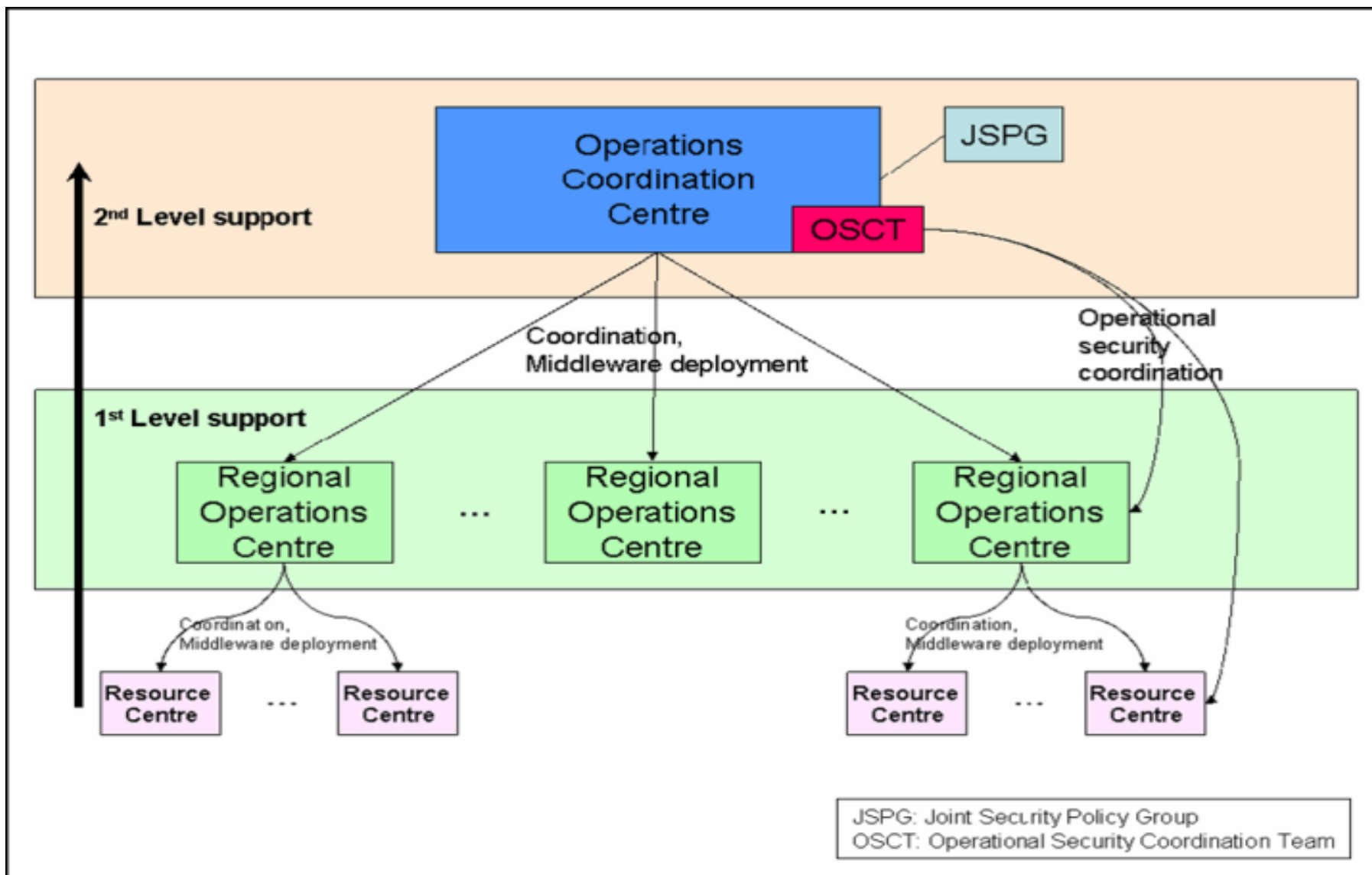
- Security Coordinators from each ROC
- Chaired by Security Officer in SCG (Ian Neilson)

- Roles:

- Members coordinate security Grid at sites within Regions
 - *Handling of Security tickets*
 - *Security contact management*
- Coordination of Grid Incident Handling Process
 - *Incident Handling and Response Guide from JSPG*
 - *Cooperation with peer Grids*
- Execution of Security Service Challenges
 - *SSC1 – job audit (completed March 2006)*
 - *SSC2 – data management audit planned*

- Meetings:

- First face to face meeting planned 21 June 2006
 - <http://agenda.cern.ch/fullAgenda.php?ida=a062198>



- **Proxy lifetime policy**
- **Requirements for Grid PMA's**
 - User full name in DN
 - But other statements required
 - (OSG has written such a document)
- **Audit requirements (discussed here yesterday)**
- **Data privacy issues (accounting, auditing etc)**
 - EU Data Privacy directives
- **VOMRS policy**
 - read access to registration, group/role membership data

- **There is work (EGEE TCG sub-group) on “Job priorities” using VOMS roles/groups**
 - Proposing how VO can centrally control Job priorities
- **Federation issues**
 - Linking in to more general AAI’s
 - Shibboleth and Grid integration
 - EGEE (Switch) working on gLite/Shib
- **GGF Security Interoperability**
 - AuthN via IGTF
 - GIN (Grid Interoperability Now) activity
 - TONIC for AuthZ – will this take off?
- **Need to review the Security Risk Analysis**
- **Have looked at Emergency Procedures for LCG ops**
 - Needs more work

- **Would like to see strong management commitment**
 - Including resource allocation!
- **Security technology is good**
 - would be happy if a normal medium sized enterprise would have this in place
- **More important issues are operational and human related factors**
 - Should implement awareness and training programs for all project members and customers
- **The EU ISSeG project is working in this area**
 - <http://isseg.web.cern.ch/ISSeG/>