



Enabling Grids for E-science

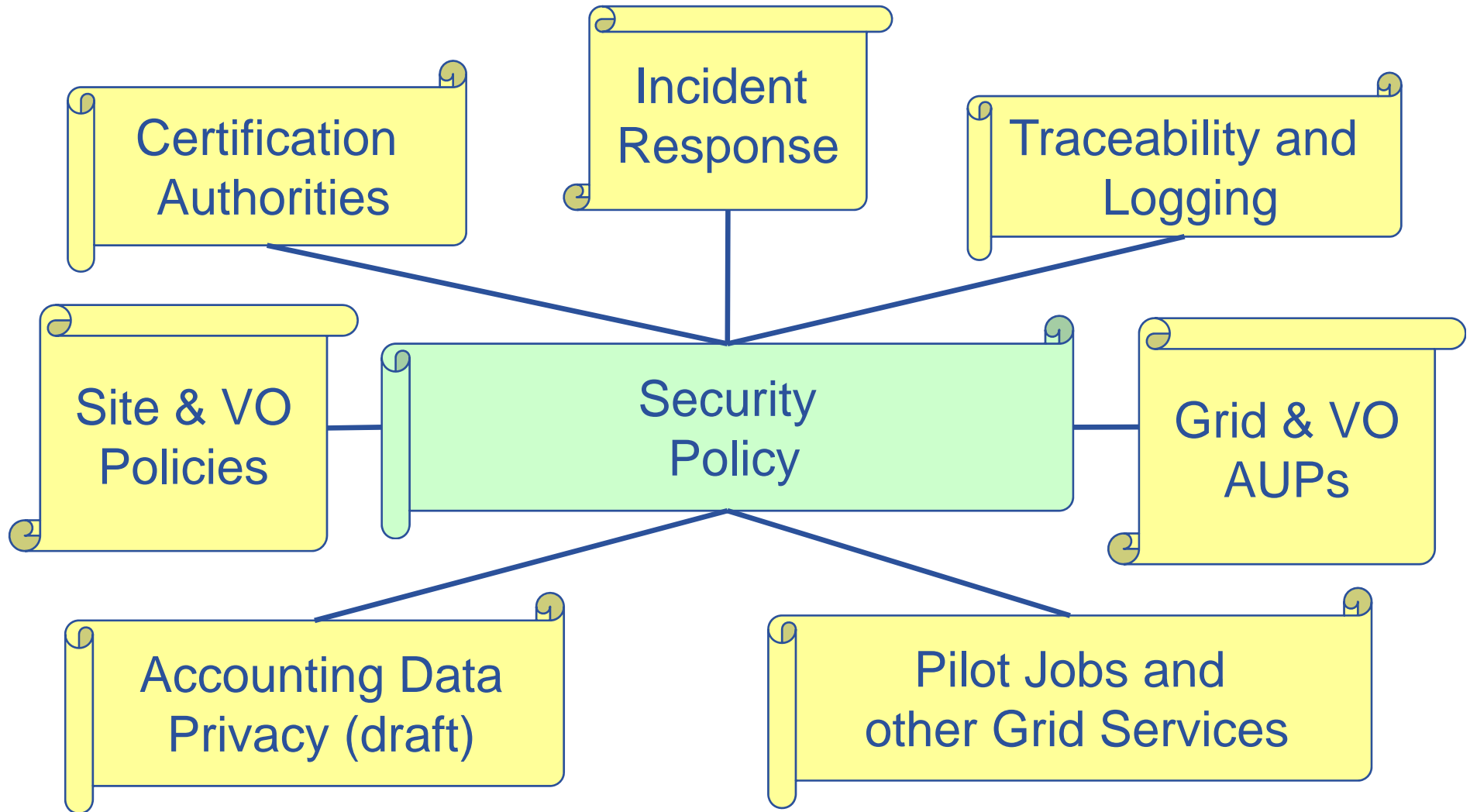
VO Security Policy

*David Kelsey RAL/STFC,
d.p.kelsey@rl.ac.uk*

*EGEE'08 Conference,
Istanbul, 25th September 2008*

www.eu-egee.org





- **Presented early draft of this in EGEE'07**
 - Now complete and approved
- <https://edms.cern.ch/document/853968/>
- **Similar aims to the Grid Site Operations Policy**
 - But for VOs
- **Documents the responsibilities of a VO**
 - They must accept and sign during registration
- **We need to define an acceptable procedure for EGEE**
 - To inform all VOs of the policy
 - To collect “signatures”

- **By participating in the Grid as a Virtual Organisation (VO), you agree to the conditions laid down in this document and other referenced documents that may be revised from time to time.**
- ***You shall provide and maintain, in a central repository provided by the Grid, accurate contact information as specified in the VO Registration Policy. These contacts satisfy the communication requirements for management decisions, security actions and operational issues relating to VO membership and Grid usage, as well as your software and services. The contacts shall respond to enquiries in a timely fashion as defined in the Grid operational procedures giving priority to security problems.***

- *You shall comply with the Grid security policies, the VO AUP and any archival, accounting and logging requirements. You shall periodically assess, at least once per year, your compliance with these policies and inform the Grid Security Officer of any violations encountered in the assessment, and correct such violations forthwith.*
- *You shall ensure that a VO membership service is provided in compliance with the VO Membership Management Policy. This shall include the appropriate interfaces and configuration details to allow the generation of authentication, authorization and other identity mapping data for the services running on the Sites. You shall take reasonable measures to ensure that the information recorded in the membership service is correct and up-to-date.*

- *You are responsible for ensuring that your software does not pose security threats, that access to your databases is secure and is sufficiently monitored, that your stored data are compliant with legal requirements, and that your VO services, including pilot job frameworks, are operated according to the applicable policy documents.*
- *You shall ensure that logged, archived and membership information is only used for administrative, operational, accounting, monitoring and security purposes. You shall ensure that due diligence is applied in maintaining the confidentiality of such information.*
- *You recognize that the Grid and the Sites may control your access to their resources for administrative, operational and security purposes.*

- *You shall ensure that any software used by you at a Site for its intended purposes, complies with applicable license conditions and you shall hold such Site free and harmless from any liability with respect thereto.*
- *Any software provided by the Grid is provided on an as-is basis only, and subject to its own license conditions. There is no guarantee that any service operated by the Grid is correct or sufficient for any particular purpose. The Grid, the Sites and other VOs are not liable for any loss or damage in connection with your participation in the Grid.*

- *You shall comply with the Grid incident response procedures and respond promptly to requests from Grid Security Operations. You shall inform users in cases where their access rights have changed.*
- *Disputes resulting from your participation in the Grid shall be resolved according to the Grid escalation procedures.*
-
- **This policy shall be signed for agreement by an Authorized Signatory of the Virtual Organisation.**

- **New VO Registration Policy**
 - Replaces old VO Security Policy
 - Similar to Site Registration Policy
 - Defines what needs to be collected during registration
 - For security-related reasons
 - Defines VO naming convention (DNS-style names)
 - Requires VO to define an AUP (gives template)
- **New VO Membership Management Policy**
 - Replaces old LCG User Registration and Membership Management
 - Defines policy requirements for various VO procedures
 - VO manager appointment, User registration, renewal, removal, suspension, audit requirements, data privacy, VO manager responsibilities, etc ...
 - Likely to require VO to complete a template form on its approach

- **Using new approach**
 - Replaces the use of MS Word (with change tracking)
 - Collaborative editing via the JSPG wiki
 - Anyone with an IGTF certificate can register and contribute
 - Discussion pages allow for comments and presentation of ideas behind the policy
 - Please contribute!
- **Two documents currently under revision**

http://www.jspg.org/wiki/VO_Registration_Policy

http://www.jspg.org/wiki/VO_Membership_Management_Policy

- **Today in EGEE we have more than 200 VOs**
 - Do all VOs understand their responsibilities?
 - Even now it is difficult for Sites to understand each VOs procedures to “trust” them
- **If a VO uses resources in several Grids**
 - Will be very difficult to build trust between the VO and Site
- **Even more problems once we have many NGIs**
- **A possible solution:**
 - One Grid establishes Trust with the VO
 - Via an accreditation procedure following agreed international standards
 - Then easier for other Grids to accept (and trust) the VO
 - If it has been accredited

- **IGTF (EUGridPMA) is investigating minimum standards and best practice for the operation of VO attribute authorities (e.g. VOMS)**
 - See draft https://grid.ie/eugridpma/wiki/AA_Profile
- **JSPG is working on standards for VO procedures**
 - See earlier reference to VO Membership Management
- **COMMENTS welcome on all these documents**
 - Use the wiki discussion (or send e-mail to me)
- **Assuming we agree accreditation that scales**
 - VOs will be able to get IGTF accreditation
 - To ease trust building (between VO and Sites)
- **BUT we do need to balance the benefits of such an accreditation against the effort needed – make it easy!**

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

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

- **JSPG web site(s)**

<http://www.jspg.org/>

<http://proj-lcg-security.web.cern.ch/> (the old web)

- **IGTF web site**

<http://www.igtf.net/>

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

- Requests to join stating reasons to D Kelsey
- Particularly keen to involve more ROCs, VOs, Grid, ...

