Building Trust – Part 1: Security Policies (JSPG)

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

EGEE'08 Conference,
Istanbul, 22nd September 2008

www.eu-egee.org

e-infrastructure

Introduction to Session

Building Security and Trust between the Grids, their services, the Sites, the VOs and their Users

What is Trust? (one web dictionary definition)

1. **To have or place *confidence* in; depend on.**
2. **To *expect with assurance*; assume: I trust that you will be on time.**
3. **To *believe*: I trust what you say.**
4. **To *place in the care of another*; entrust.**
5. **To *grant discretion to confidently*: Can I trust them with the boat?**
6. **To extend credit to.**

Introduction (2)

- **Joint Security Policy Group (JSPG) & Grid Security Vulnerability Group (GSVG)**
  - Both are activities in EGEE SA1
  - Both involved in building “trust” on the Grid
    - Participants & middleware should do what you expect them to do
- **Aimed at all Grids and all participants**
  - Users, VOs, Sites, Operations, Developers, …
- **Agenda for today’s session**
  - JSPG (30 minutes) + 10 minutes discussion
  - GSVG – Linda Cornwall (30 minutes) + 10 minutes discussion
  - 10 minutes general discussion

Introduction to JSPG

Joint Security Policy Group

- **Main aims**
  - To develop and maintain security policies
    - These should be general, simple and interoperable
    - For use in EGEE, WLCG and other Grids
  - To liaise with other operational, middleware and policy security groups
    - OSCT, MWSG, IGTF and its PMAs
    - For feedback in both directions

JSPG mandate

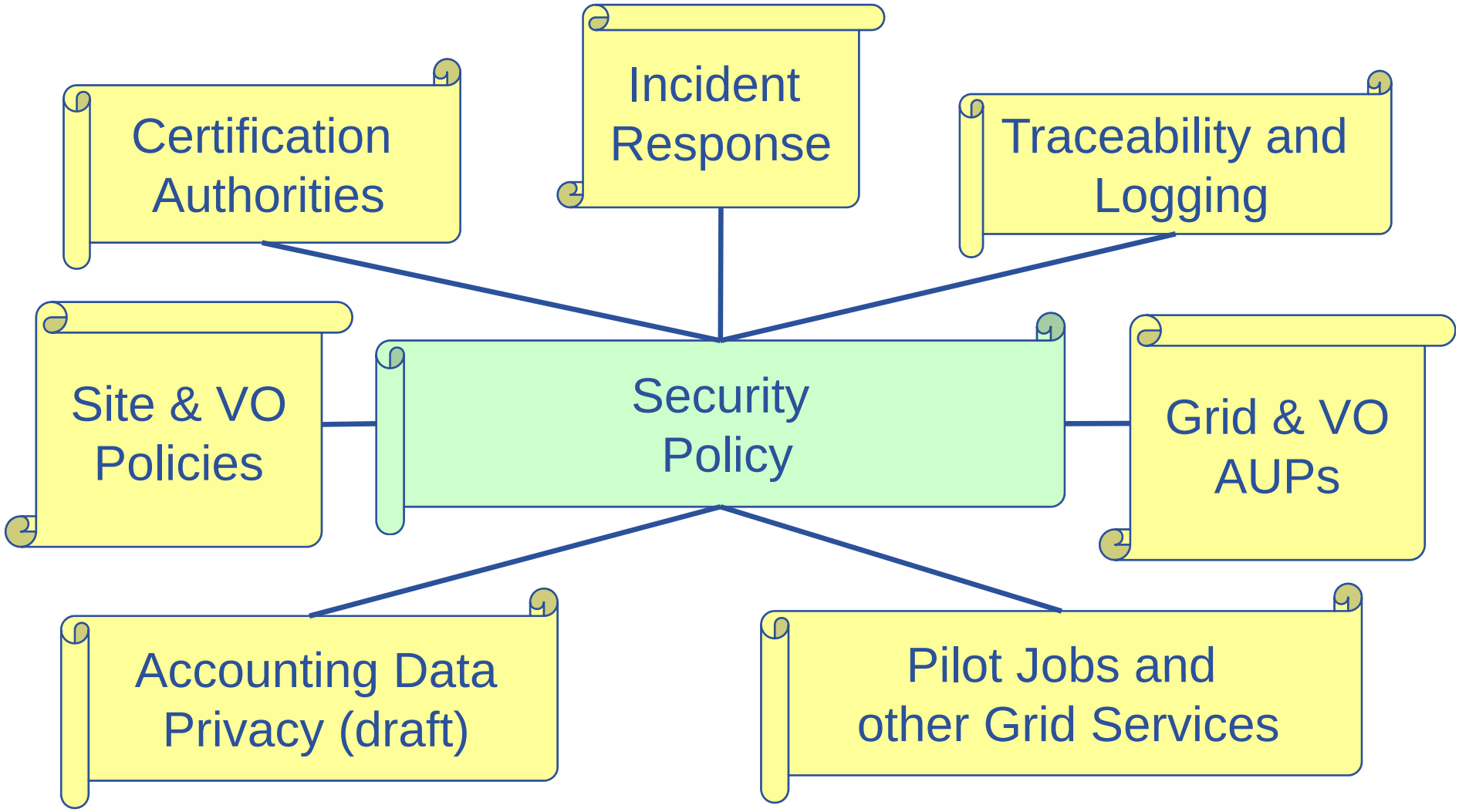
- **For EGEE-III a new mandate has been agreed**
  - See http://www.jspg.org/
  - *Jointly owned by/recommends to EGEE & WLCG*
    - *Policy for WLCG applies to all of its Grid infrastructures in so far as this relates to WLCG activities*
    - *i.e. OSG, NDGF and other national Grids and/or individual Grid sites which participate in WLCG*
  - *May also provide advice on any security matter*
  - *Aim for simple/general policies that are useable by NGIs*
    - *Common policies facilitate interoperability*
  - *JSPG does not formally approve policies*
    - *but recommends to management bodies*
      - *TMB approves policy for EGEE*
- **Plans for next two years (as move forwards to EGI)**
  - Need to revitalise membership (More ROCs, NGIs and VOs)
    - Volunteers?
  - Review all policy documents to make even more simple/general
    - And useful to many national Grids

JSPG membership

- Application representatives/VO managers
- Site, ROC and Grid Security Officers
- Site/Resource Managers/Security Contacts
- Security middleware experts/developers
- Operations and Deployment experts
- Other EU Grid infrastructures and projects

- Volunteers ALWAYS welcome (please contact me!)

Security Policy



Recently approved policies

- **Since EGEE'07**
  - Formal approval of
    - Revised top-level Grid Security Policy
    - Grid Site Operations Policy
- **4 recently approved policies**
  - EGEE TMB meetings in Aug/Sep 2008
    - Approval of Certification Authorities
    - Traceability and Logging
    - VO Operations
    - Multi User Pilot Jobs
- **JSPG must also provide a covering document per policy giving references, e-mail addresses and other implementation details (for EGEE)**
  - Then will announce to all EGEE participants

General changes

- **General changes during revision**
  - Remove all footnotes and references
    - References should be covered in the Grid-specific covering documents
  - Updated the names of referenced policy documents
    - Particularly those related to VOs
  - Removed direct references to LCG, EGEE etc.
    - Documents should be general and simple
  - Consistent style
  - use of word "*Grid*"

Approval of Certification Authorities

https://edms.cern.ch/document/428038

- **Revision to an existing policy document**
- **Main change: add CAs accredited to the new IGTF MICS profile**
  - *A MICS is an automated system to issue X.509 formatted identity assertions (certificates) based on pre-existing identity data maintained by a federation or large organization – the end-entity certificate is thus based on a membership or authentication system maintained by the organization or federation*
- **Also added the ability for Sites to trust non-IGTF CA for local reasons**
  - Must be allowed by local policy and they must deal with any potential non-unique names

Traceability and Logging

- ***Grid Security Traceability and Logging Policy***
  - Replaces the old “Security Audit Requirements”
  - See *https://edms.cern.ch/document/428037*
- **General text setting out the motivation and requirements for logging**
  - Middleware must produce appropriate logs
  - Site and service managers must keep logs for at least 90 days
- **Detailed implementation is defined by the EGEE Operational Security Coordination Team (OSCT)**
  - Operational notes on the OSCT web
    - Some core logs need to be kept for 180 days
- **Other Grid implementations defined by their own security teams**

Motivation for traceability

- **Management of risk is important**
  - Appropriate controls are essential
- **Identifying cause of security incidents is essential**
  - To prevent them happening again
- **Goal is to contain impact of an incident**
  - While keeping services operational
- **Response to incidents must be commensurate with scale of the problems**
  - Blocking a whole large VO because of one compromised user account is often not possible

Motivation (2)

- **The minimum: identify the source of all actions**
  - and the individual who initiated them
- **Fine-grained monitoring and controls are needed**
  - at individual user-level
- **Essential to understand the cause and to fix any problems before re-enabling access**
  - If did decide to block a whole VO …
  - Unless we understand the details of an incident
    - how can we ever re-enable?

VO Operations Policy

- **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"

Multi User Pilot Jobs

- **Presented early draft of this in EGEE'07**
  - Now completed and approved
- **Defines the responsibilities of VOs and pilot job owners**
- **First in a set of policy documents aimed at the responsibilities of those running Grid services**
  - Next will be Grid Portals
- **https://edms.cern.ch/document/855383/**
- **Again we need to define an acceptable procedure**
  - Sites can choose if they support pilot jobs for a given VO
    - Could be an opt-in or an opt-out approach
    - Could be announced via technical means (Information service)
      - *Or via out-of-band negotiation*

Current JSPG work

- **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

New JSPG documents

- **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

VOs, EGI and scaling problems

- **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

- **International Grid Trust Federation**
  - Builds trust for Global CAs (authentication)
  - Has three regional PMAs (Europe, America, Asia-Pacific)
- **We have lots of policies and standards for operating a trustworthy Identity service for Grids**
- **BUT … nothing equivalent exists for VOMS services!**

IGTF & JSPG Developments

- **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!**

JSPG Meetings, Web etc

- **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, …

Questions?