Science & Technology Facilities Council

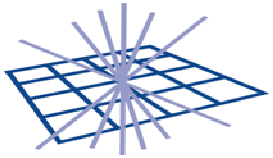
Security Policy: From EGEE to EGI

David Kelsey (STFC-RAL)

21 Sep 2009

EGEE'09, Barcelona

david.kelsey at stfc.ac.uk



GridPP
UK Computing for Particle Physics

Overview

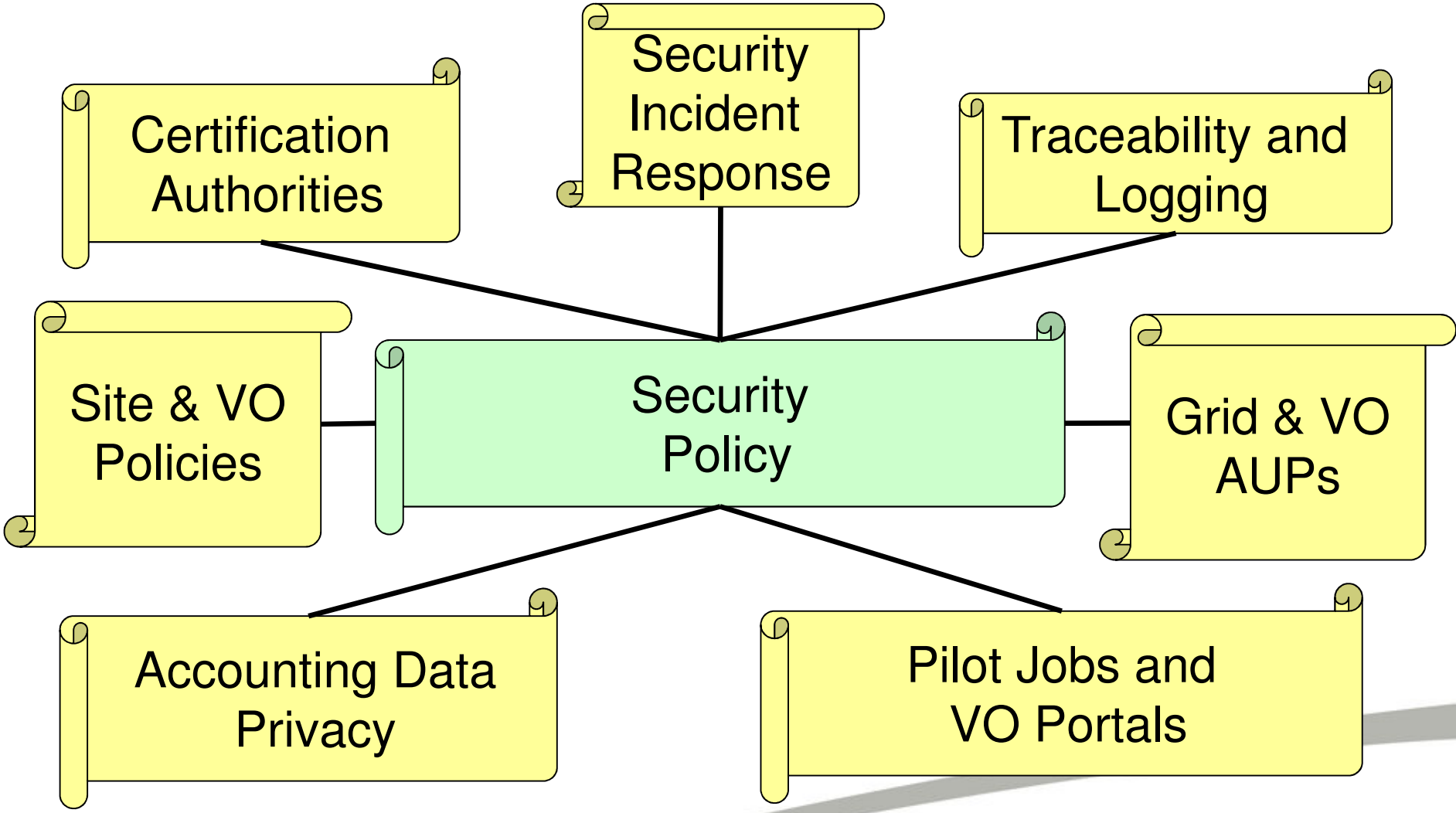
- EGEE/WLCG Joint Security Policy Group
  - Interoperable policies
- Overview of current JSPG policies
- New policy framework for EGI era
- EGI Security Policy Group
  - Proposed operation

Policy Interoperability

- Wherever possible, JSPG aims to
  - prepare **simple** and **general** policies
  - applicable to the primary stakeholders, but
  - also of use to other Grid infrastructures (NGI's etc)
- The adoption of common policies by multiple Grids eases the problems of interoperability (and scaling)
- Users, VOs and Sites all accept the same policies during their (single) registration (with Grid or VO)
- Other participants then know that their actions are already bound by the policies
  - No need for additional negotiation, registration or agreement

Overview of current JSPG Policies

JSPG Security Policies



Recent JSPG work

Five recently approved and adopted policies

- Virtual Organisation Registration Security Policy

https://edms.cern.ch/document/573348/8

- Virtual Organisation Membership Management Policy

https://edms.cern.ch/document/428034/3

- Grid Policy on the Handling of User-Level Job Accounting Data

https://edms.cern.ch/document/855382/5

- VO Portal Policy

https://edms.cern.ch/document/972973/6

- Security Incident Response Policy

https://edms.cern.ch/document/428035/7

Ongoing revisions

- Site Registration Security Policy

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

  - Remove EGEE-specific procedures
  - Use same simple style as the VO Registration Security Policy

- Grid AUP

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

  - Some Grids use it but have modified our text
  - Some infrastructures do not have VOs
  - Revise to include these modifications

From EGEE to EGI

Problems with current Policies

- Many different documents
  - Overlaps and inconsistencies
- Includes operational issues as well as security-related issues
- Participants find it difficult to know which policy applies to them
- Many policies are rather EGEE-specific

New policy framework for EGI

- **A framework to enable interoperation of collaborating Grids**
  - aimed at managing cross-Grid operational security risks
- Identify policy components to help trust building between Grids
- Not imposing a single policy for all
  - But Grids can use JSPG policies if they wish
- Present the current set of JSPG policies
  - Taking high-level view to identify those components which are necessary
- Other components are either too EGEE-specific or are operational rather than related to security – separate them
- Each Grid will have security policies consisting of the framework components and their own Grid-specific components

Framework (2)

- Specifies **the issues** that need to be addressed in a Grid's security policy
- At this stage does **not** define minimum standards or requirements
  - Standards (may) come later
- Aimed at Grids preparing or revising security policies, not at end users, sites, application communities etc.
- As an aside ... we found it very useful to have been through the whole JSPG "experience" to identify those issues which need to be addressed!

Policy Framework: Participants

Infrastructure

Includes

- Grid Operations
- Security Officer
- Sec Operations

Users

Includes

- Grid users
- VOs
- Application Communities

Providers

Includes

- Grid Sites
- Resource Providers
- Service Providers, e.g. VO running services

Policy Components

Infrastructure

Includes

- Incident Response
- Vulnerability Handling
- Patching
- Data protection
- Registration
- etc

Users

Includes

- AUP
- Traceability
- VO Management
- Data protection
- Incident response
- Data protection
- Registration
- etc

Providers

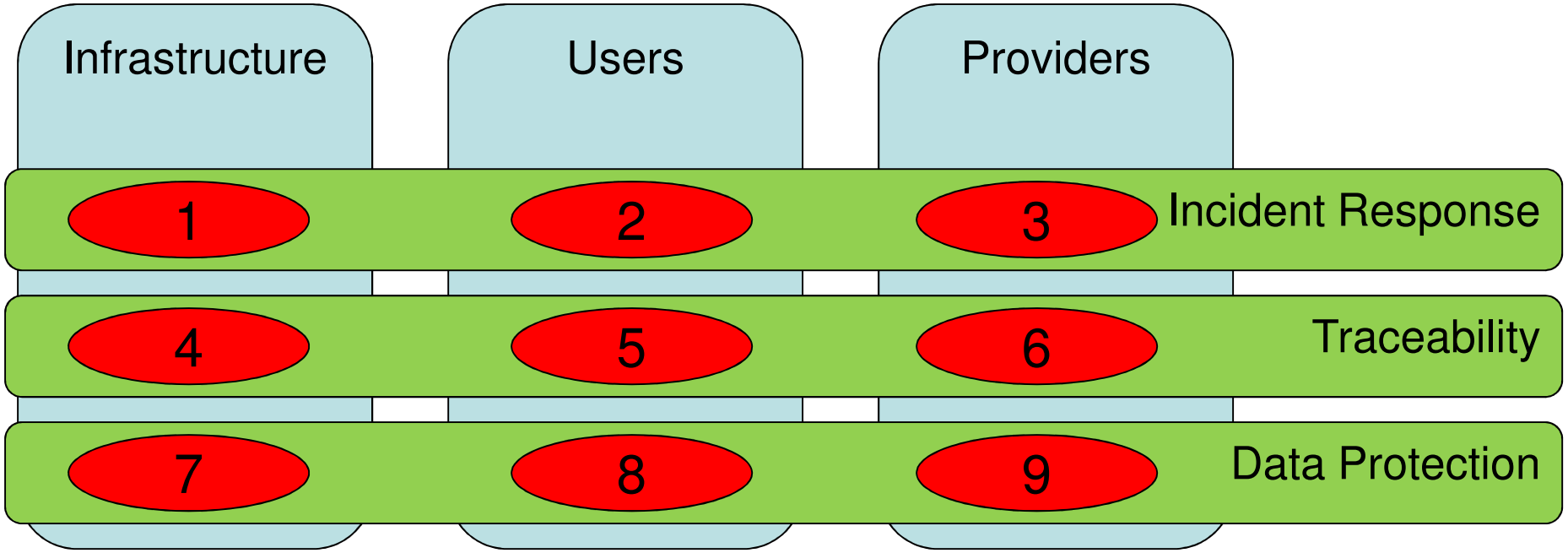
Includes

- Traceability
- Incident Response
- Access control
- Registration
- etc

Policy Framework: Functions

We have considered and deliberately excluded: IPR, liability, software licensing, copyright.

Security Policy Framework



etc etc etc

Policy Components (numbered) at matrix intersections

Science & Technology Facilities Council

An example component: Security Incident Response

- **Infrastructure (component #1)**
  - Contact details to report incidents
  - Incident response procedure for Sites
  - Ensure they are quickly investigated
  - Collaborate with others
    - Grids & NREN CSIRTs
- **Users & Providers (component #2 and #3)**
  - Must participate in Incident Response
  - Must keep audit logs

Framework – Next steps

- During next few months
  - JSPG will finalise the draft framework
  - Ensure nothing is missing
- Then before end of EGEE-III
  - Create generic description of the policy components
- In EGI first year
  - Consult many more stakeholders and tune framework
- Beyond EGI year one
  - Work on minimum policy standards and common wording

Security Policy Group

- SPG – initial plans (feedback very welcome!)
  - Development and maintenance of security policies
  - Advice on any security policy issue
  - Primary stakeholders: NGIs, Sites, Application communities
    - and include other infrastructures for interoperation
  - Build on JSPG work

EGI SPG(2)

- Membership: NGI reps, Sites, VOs, middleware, security ops
- Participate in EUGridPMA, IGTF, OGF, TERENA federations, Middleware etc policy discussions
- Small editorial team to prepare policies
  - Meet face to face
- Full consultation by e-mail (all stakeholders)
- Annual face to face meeting if possible
- Coordination with other security activities and informing everyone are both important

JSPG Meetings, Web etc

- Meetings - Agenda, presentations, minutes etc

http://indico.cern.ch/categoryDisplay.py?categId=68

- JSPG Web sites

http://www.jspg.org and

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

- Membership of the JSPG mail list is closed, BUT
  - Volunteers to work with us are always welcome!
- Policy documents at ***http://www.jspg.org*** and

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

Where are JSPG security policies?

- http://www.jspg.org/wiki/JSPG_Docs
- http://proj-lcg-security.web.cern.ch/proj-lcg-security/documents.html
- https://edms.cern.ch/nav/CERN-0000022711

Discussion