EGEE Security for VOs

Daniel Kouřil, CESNET
• **Joint Security Policy Group (JSPG)**
  – common policies for Grids

• **EUGridPMA**
  – CA accreditation
  – member of International Grid Trust Federation (IGTF)

• **Middleware Security Group (MWSG)**
  – Security architecture, MW-related security issues

• **Grid Security Vulnerability Group (GSVG)**
  – assessing software vulnerabilities in gLite

• **Operational Security Coordination Team (OSCT)**
  – operational security, security incident response

• **Security Coordination Group**
  – overall security coordination
• Several VOs implement their SW
  – consider if it has any security implications (proxy mgmt, …)
  – consider security from very beginning
  – implement code with security on mind
  – don’t hesitate to contact MWSG or OSCT if your SW
    ▪ any feedback/comments from real users is appreciated
    ▪ several gLite components can be re-used

• If security is underestimated/neglected, serious problems can pop up later during production
  – VO risks serious problems then
  – remember site’s concerns about pilot jobs
Security Incidents

- Usually a lot (excited) communication during investigations
  - many parties contacted

- VO should be prepared to take necessary actions
  - user traceability
  - user management, including suspension and maintaining communication channels
  - get security policies and procedures

- Fast reactions are crucial
  - not necessary to provide all information immediately
  - In doubt, always contact OSCT or closest ROC security contact

- SSC3 involves VO’s participation