Grid Incident Response in the CE federation

Daniel Kouřil
CESNET
Grid incident response

- Incident – “Any real or suspected event that poses a real or potential threat to the integrity of service, resources, infrastructure, or identities” (from OSG’s Grid Security Incident Handling and Response Guide)

- Incidents must be handled as fast and effectively as possible – grid incident response framework necessary

- Quotation from the project (p. 190)
  - Central coordination of incident response by the OCC, involvement in incident response is a role of all ROCs
  - EGEE-II-wide incident response team (consisting of members from the ROCs) that coordinates incident response
  - Well documented and pre-agreed response procedures are essential
  - Security challenges to test the procedures
Proposed Solution

• Policy document for CE specifying procedures for incident response
  ■ For every step of incident report handling
  ■ Responsibilities, maximum response time
  ■ Procedures to escalate problems coming from the CE federation

• The whole process must be auditable
  ■ We should also mount internal audits

• Collaborations with CSIRTs operated by NRENs

• Implementation inspired by the user support tools (RT)
  ■ Complete history
  ■ Limited access, proper access control
  ■ Mail and web interface