LCG Security

Ian Neilson

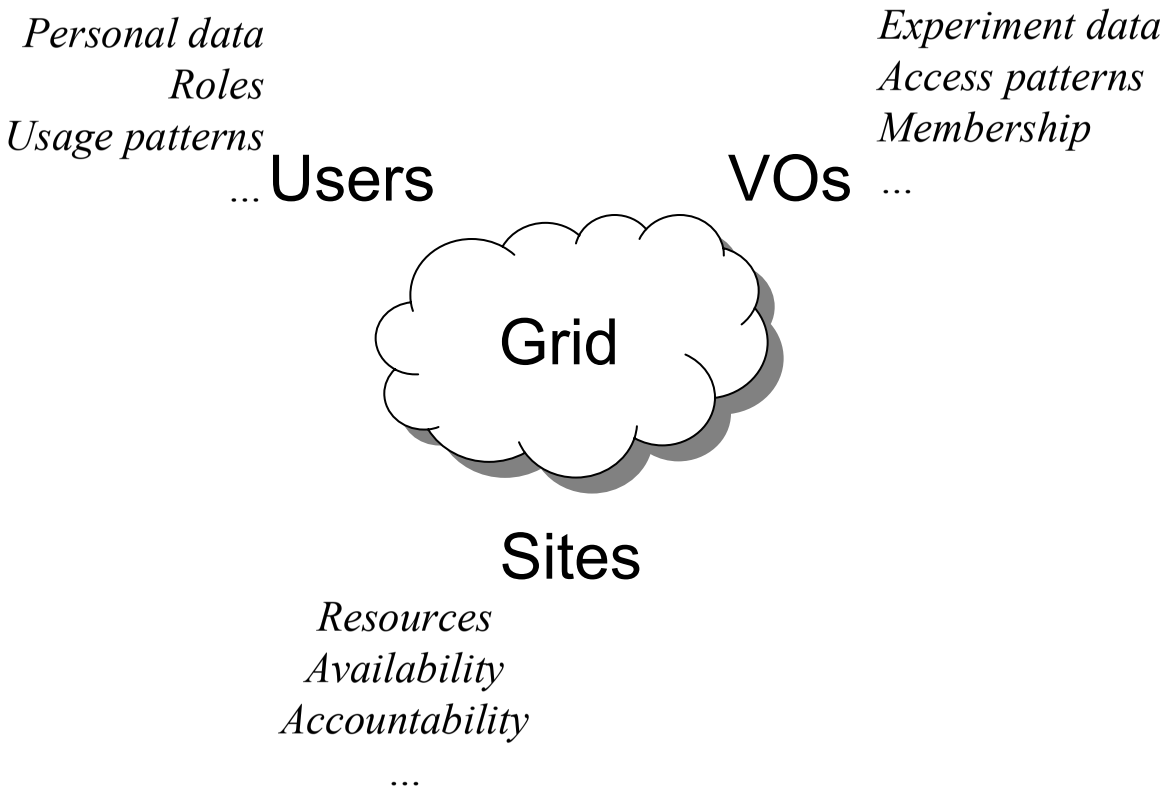
LCG Security Officer

Grid Deployment Group

CERN

LCG Security environment

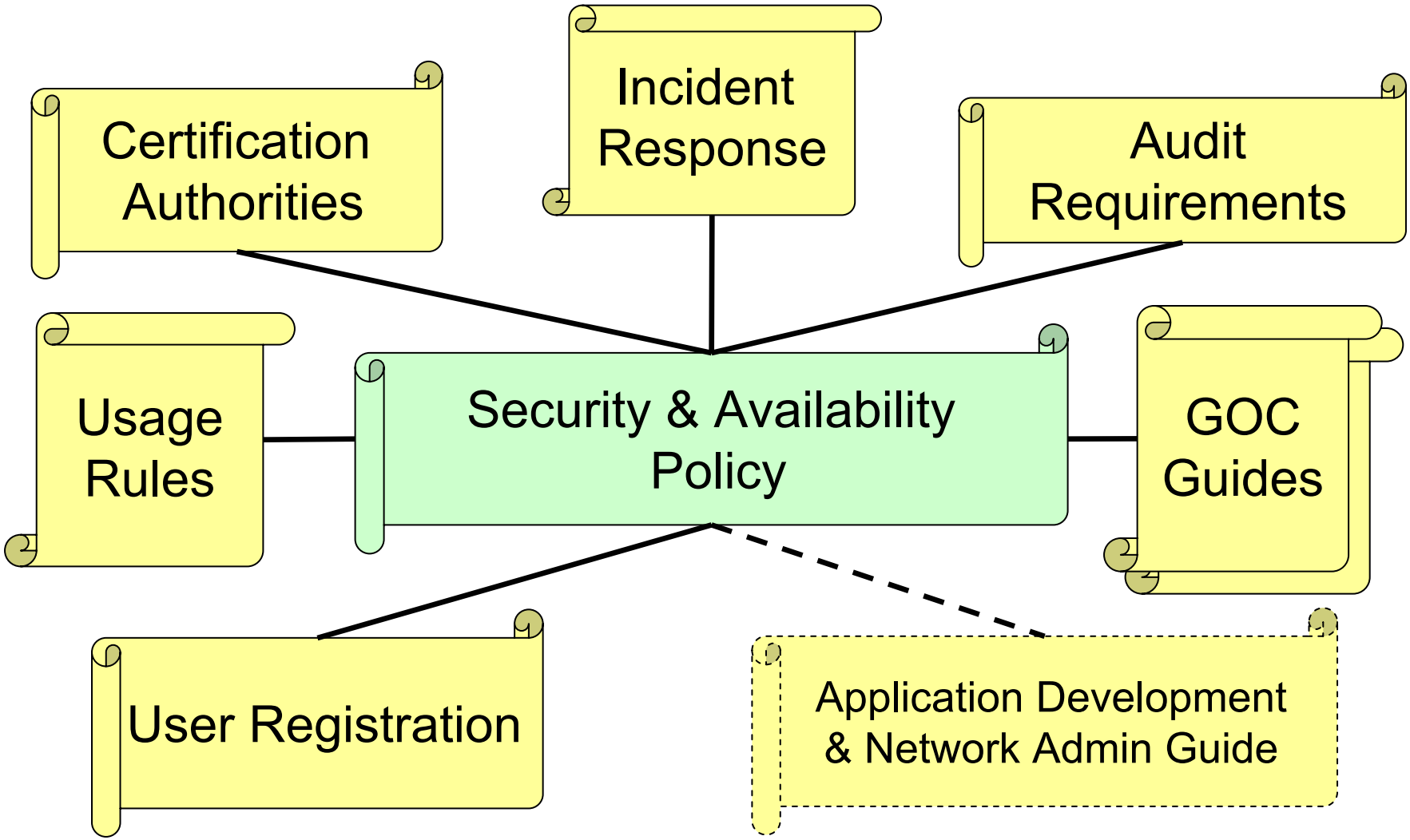
- The players



The Risks

- Top risks from Security Risk Analysis
  - http://proj-lcg-security.web.cern.ch/proj-lcg-security/RiskAnalysis/risk.html
  - Launch attacks on other sites
    - Large distributed farms of machines
  - Illegal or inappropriate distribution or sharing of data
    - Massive distributed storage capacity
  - Disruption by exploit of security holes
    - Complex, heterogeneous and dynamic environment
  - Damage caused by viruses, worms etc.
    - Highly connected and novel infrastructure

Policy – the LCG Security Group



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

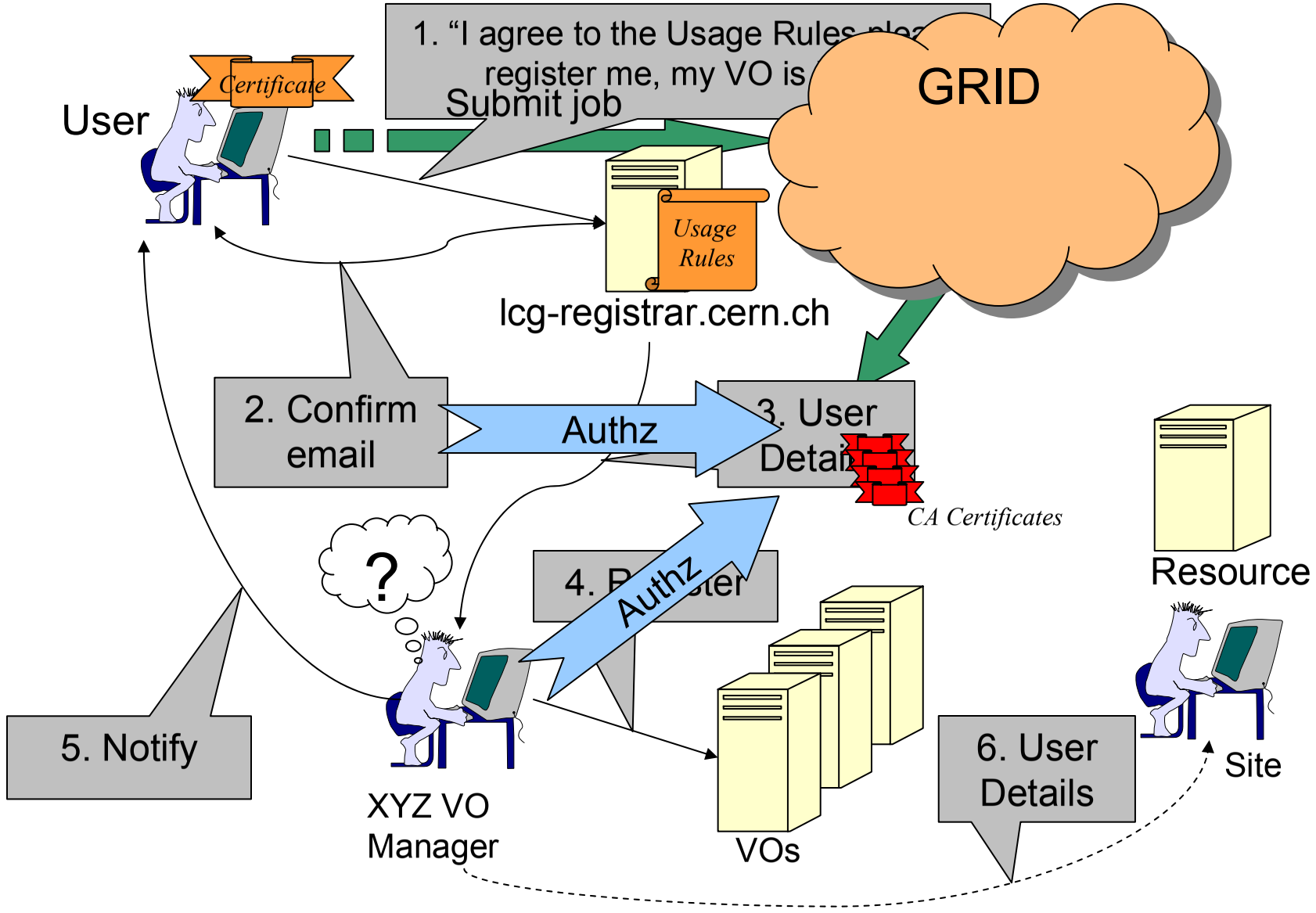
Authentication Infrastructure

- Users and Services own long-lived (1yr) credentials
  - Digital certificates (X.509 PKI)
  - European Grid Policy Management Authority
    - *"... is a body to establish requirements and best practices for grid identity providers to enable a common trust domain applicable to authentication of end-entities in inter-organisational access to distributed resources. ..."*
    - www.eugridpma.org covers EU (+ USA + Asia)
- Jobs submitted with Grid Proxy Certificates
  - Short-lived (<24hr) credential which "travels" with job
  - Delegation allows service to act on behalf of user
  - Proxy renewal service for long-running & queued jobs
- Some Issues…
  - Do trust mechanisms scale up ?
  - "On-line" certification authorities & Certificate Stores
    - Kerberized CA
    - Virtual SmartCard
  - Limited delegation

Authorization Infrastructure

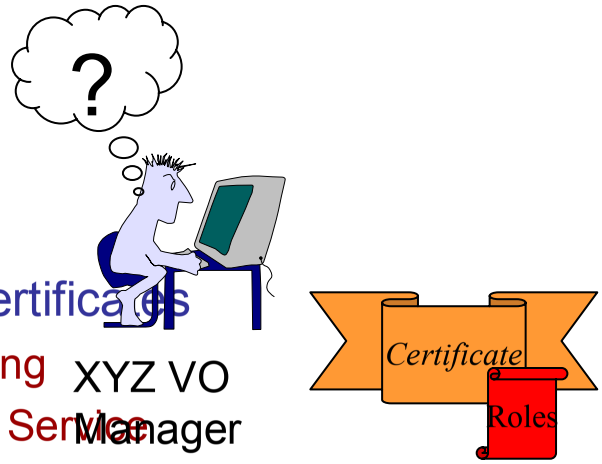
- User Registers
  - Accepts Usage Rules
  - Provides personal/contact data
  - Request to join VO
    - VO managers add to VO servers
  - Certificate Identity (DN) captured
- Submits jobs
  - Creates short-lived proxy using long-lived certificate
  - Proxy ‘travels’ with the job
- Resources authorize access
  - Checks certificate validity
    - Trusted CAs and revocation lists
  - Checks user authorization
    - Downloaded from Registration/VO servers
  - Maps certificate DN to a local account
  - Runs job

User Registration (2003-4)



User Registration (? 2004 -)

- Some Issues
  - Static user mappings will not scale up
  - Multiple VO membership
  - Complex authorization & policy handling
  - VO manager needs to validate user data
    - How ?
- Solutions
  - VO Management Service - Attribute proxy certificates
    - Groups and Roles - not just static user mapping
    - Attributes bound to proxy cert., signed by VO Service
  - Credential mapping and authorization
    - Flexible policy intersection and mapping tools
  - Integrate with Organizational databases, but …
    - What about exceptions ? (the 2-week summer student)
    - What about other VO models: lighweight, deployment, testing



Audit & Incident Response

- Audit Requirements
  - Mandates retention of logs by sites
- Incident Response
  - Security contact data gathered when site registers
  - Establish communication channels
    - maillists maintained by Deployment Team
    - List of CSIRT lists
      - Channel for reporting
    - Security contacts at site
      - Channel for discussion & resolution
  - Escalation path
- 2004 Security Service Challenges
  - Check the data is there, complete and communications are open

Security Collaboration

Enabling Grids for E-science in Europe

- Projects sharing resources & have close links
  - Need for inter-grid global security collaboration
  - ? Common accepted Usage Rules
  - ? Common authentication and authorization requirements
  - ? Common incident response channels
- LCG – EGEE – OSG - ?
  - ***LCG Security Group*** is now ***Joint Security Group***
    - JSG for LCG & EGEE
    - Provide requirements for middleware development
    - Some members from OSG already in JSG

LCG Security

Thank you.