LCG/GDB Security Group

CERN, 9 Apr 2003

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

Introduction and Aims

- LCG GDB
  - WG3 – Security (see report)
  - This group will take things forward
  - Who are we?
  - Note Taker?
- Aims of today
  - First meeting
  - Start the planning of tasks for 2003
  - Start the discussions
  - Discuss who needs to be members and plan future meetings
  - Prepare my presentation to GDB (tomorrow!)

Mandate?

- To advise and make recommendations to the Grid Deployment Manager and the GDB on all matters related to LCG-1 Security
- To continue work on the mandate of WG3 (link?)
  - Policies and procedures on Registration, Authentication, Authorization and Security
- To define tasks and commission groups to do the work
  - With the correct set of people
  - Security Contacts group already working (Dane)
- In many ways this group will act as a Steering Group
- Main aim is planning for Jan 2004

Membership?

- Experiment representatives
  - VO managers
  - Important to create the balance
- Site Security Officers
- Site/Resource Managers
- Security middleware experts
- LCG management and CERN team
- Non-LHC experiments/Grids

- Missing today: Resource managers, middleware, geographical spread (Asia/Pacific)
- Do we need reps from all 4 experiments?
- Group should remain small(ish)

WG3 report
The Security Model

- Keep it simple (and easy to use)
- Start with what we have and what works today
- But, never lose site of the Grid “vision”
- Will take time to
  - build trust
  - develop procedures
  - agree problem resolution mechanisms

The Security Model (2)

- Users
  - Certificate from national CA (need catch-all)
    - Or KCA
  - Register just once with LCG-1 Guidelines VO
    - And once per experiment VO
  - Sign one form (electronic) and one AUP
  - Accounts created at all necessary sites (automatic)
  - Single sign-on to Grid (per session)
    - From wherever they happen to be
    - Able to request the VO(s) and groups/roles at login
    - Avoid need to authenticate against a Tier 0/1
      - Must be able to use local Tier 2 when Tier 0/1 is unreachable

The Security Model (3)

- VO's
  - Control coarse-grained Authorisation
    - E.g. membership of VO
    - Allocate resources and control priorities
  - Define and manage groups, roles, capabilities
  - Overall (coarse-grained) control of resources provided by the sites
  - Must be "real" in some sense (for "trust")
    - CERN to take responsibility for VO management
  - One VO database (replicated or exported – not distributed)
  - We have the HEPCAL Use Cases. These will be reviewed by LCG GAG (May 03)
    - We need to feed into this process

The Security Model (4)

- Sites (Tier n, n=0,1,2,3?)
  - Scaling
    - negotiate with and allocate resources to VO's
  - BUT - Local authorisation – full control
  - Can exclude particular users (or groups?)
  - May use a local "site VO" for access control and resource priority
  - Full audit logs/trail (down to individuals)
  - Copy of all appropriate VO databases (legal?)
    - Authz must work when network partitioned
  - Access control lists all kept locally
  - May insist on site-specific authentication

Security Model (5)

- Authentication
  - Use existing CA's and new ones as they appear
  - One CA PMA per continent (for all HEP projects)
    - Input from LCG but not run by us (GGF, EU FP6,…)
  - KCA coming (July 03)
  - Online Repositories
- Authorisation
  - Need robust distributed Registration Authorities (per VO)
  - Use existing VO tools today
    - New tools being developed (FNAL, BNL, …)
  - Move to new technologies
    (eg VOMS/LCAS/GACL) as available

Security Model (6)

- Other topics to tackle
- Site Requirements (Dane's survey)
- Firewalls (urgent?)
- AUP/Usage Guidelines
  - Needs time, start from EDG?
- Policy (to be developed in parallel with AUP)

WG3 Recommendations

- Three timescales
  - Now (Feb 2003)
  - LCG-1 startup (July 2003)
  - Longer term (2004)
    - Beyond then to be planned during the coming year
- Constrained by
  - what is currently possible
  - plans of other projects
  - how much effort to implement (and available?)
- Move carefully

LCG-1
July 2003

- Firewalls (and network connectivity questions)
- User registration form (web)
  - *LCG must design, implement and operate (Jul 03)*
- AUP/Usage guidelines
  - *Step 1 – Modified EDG rules (Jul 03)*
  - *Step 2 – New LCG rules (2004)*
- LCG-1 VO (machine, database and schema)
  - *Start service in Jul 03 (minor schema changes)*
  - *Updated schema (2004)*
- Experiment VO's
  - *LCG to run (machine, database etc) (2004)*
- Other VO's (development, testing, other communities)
  - *LCG to run (Jul 03)*
- Interim "trust" – KCA and User-generated Proxy
- LCG-1 Security Policy