LCG/GDB WG3
Security
CERN, 9 Dec 2002

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

Introduction

- WG3 – Registration, Authentication, Authorization and Security
- Late getting started
- Early draft (25 Nov - V0.1) report distributed
- Today
  - Review the main issues
  - Suggest future work

Overlap with other WGs

- Much Overlap of WG3 with other WG's
- WG1 – choice of security middleware and tools
- WG2 – VO management and resources
- WG4 – security operational procedures

Definition of LCG-1

- Text distributed by Manuel to GDB (21 Nov)
  - GDB issue not just WG3
- Several comments received
  - All agree that it is useful
- We will modify and re-distribute

User Registration

- First step in User Authorisation
- Long term aim is to use LHC experiment secretariats
  - But do we need an LCG top-level registration?
- Estimates of size of community
  - and turnover
- LCG-1 - ~1000 users?
- Peak rate – 25 registrations per day in 2Q03
- Average rate – 1 registration per day

User Registration (2)

- Other issues
  - Need to register the X.509 DN and perhaps the certificate/public key
  - Registration procedure must confirm that the correct DN/Cert/Key is stored
  - May need a distributed Registration Authority
    - For those who cannot visit CERN
  - Today's VO's (EDG and elsewhere) are not sufficient
    - Need more secure machines and operations
    - Need better identity checking (RA's)

Infrastructure Registration

- For Grid – need to authenticate and authorize infrastructure
- Therefore must register Systems, Resources, Services
  - And applications?
- EDG does not do this today
- LCG-1 needs a procedure to register the infrastructure (is this WG-2 or WG-3?) (when?)
- As for users – need to register DN/cert/public key
- WILL need a distributed Registration Authority here!
- EDG Virtual Organisation Membership Service (VOMS) could be used for this

Technical issues - Registration

- Databases and tools
  - Use main User registration DB (Oracle?)?
  - BUT need to export
    - to online VO authorisation
      - E.g. EDG VOMS (MySQL) or VO/LDAP
    - to sites
    - Need tools to do this
    - Confidentiality and access rights
  - Once user registers
    - Create all the necessary accounts (automatically)

Authentication

- EDG, CrossGrid, DataTAG, US/DOE
  - Certificate Authority Managers meet in EDG WP6 CA group
- 13 trusted CA's today
- End of this week, considering 5 additional CA's
- Aiming to formalise the PMA charter
  - Regional PMA's (North America, Europe, Asia-Pacific) and cross links
- In good shape
- Nothing extra for LCG-1 to do

Authentication (2)

- Issues
- Some sites do not accept user-held long term private keys
  - Kerberos CA (FNAL)
  - Virtual Smart Card (SLAC)
  - To be discussed this week
    - Do we trust online repositories?
    - Scaling issues for many KCA's
- May need to support multiple methods of authentication
- BUT for LCG-1
  - Can we just use long-term user-held keys?

Authorisation

- Technology issues
  - Today VO/LDAP and mapfile tools
    - LCG-1 will start with this?
  - Coming in EDG: VOMS and LCAS, GACL etc
- Experiment requirements for VO and Authorisation
  - Must meet SC2 RTAG4 requirements
  - Need more discussions with experiments
    - Roles, groups, sub-groups, capabilities etc?
- Sites must be in control of local authorisation
  - Who controls what and how? (VO vs Site)
- Revocation of VO membership and authorisation

Security

- Operational security issues – WG4
- LCG-1 Access policy – paper to Computing Resources Review board (Oct 2002)
- Need to survey site security requirements
  - Also being done by PPDG-SiteAA and GGF Site-AAA
- Many issues
  - Auditing, accounting, non-repudiation, integrity, confidentiality, firewalls etc
- Firewalls (WG4?)
  - Do we use VPN's?
  - Full open access or link Tier-0 and Tier-1's?

Security Policy

- Do we need an LCG-1 Policy?
  - Or is Acceptable Use enough?
- What is the Policy?
  - A set of goals and aims
  - A set of rules
  - A mixture of both

Acceptable Use Policy

- User should only register once and sign once
  - AUP or “rules”
- EDG has an AUP that all sign (electronically) before joining a VO
- LCG-1 also needs a top-level VO which all users join first
- We need to try to agree a single document
  - Start with the EDG document?

Important Issues for LCG

- Top priority
  - VO/registration/management
- We need an LCG-1 VO
  - Machine(s), people, operations and procedures
  - Signing of AUP
  - Need to agree the data we need to collect
- LHC experiments
  - 4 separate VO's (not the same as EDG or US)
  - Or sub-groups of LCG-1?
- Export to sites
  - And create the required user accounts

Important issues (2)

- Authentication
  - Can we agree on one for LCG-1?
- Acceptable Use Policy
  - Start with EDG (?) and modify for LCG-1 sites
- Survey site requirements (together with PPDG/GGF)
  - Resolve authentication issues (KCA, VSC etc)
- Many operational issues (WG4)
- Network Firewalls (who?)