Certificate Authorities
WP6 Meeting

EDG Heidelberg, 26 Sep 2003

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

CA group meetings

- Only one meeting since the EDG Barcelona meeting
  - 12/13 June 2003 (CERN)
- Next meeting (final EDG meeting!)
  - 11/12 December 2003 (Dublin)

New CA’s

- 3 new CA’s
  - Taiwan, FNAL (top-level and service)
- n.b. FNAL KCA treated as different class
  - approved for use in LCG (not EDG)
- 4 updated CA’s
  - Czech Rep, Germany, Ireland, Portugal
- All above were approved (some after the meeting)
- CA’s under development
  - Armenia, Belgium, Hungary, Israel, Japan, Pakistan, …

Some issues

- FNAL top-level CA – 4096 bits in key
  - Max RSA key-length supported in Java is 2048
  - Import restrictions in some countries
  - Legal situation being looked into
  - FNAL will issue new cert with 2048 bits
- Streamlining of CA RPM distribution
  - At one point the process was too slow
    - now improved
  - LCG is separating the CA distribution from middleware

Issues (2)

- Online CA’s and certificate repositories
  - Discussed in June meeting
  - Clear strong interest in these new services
  - Needs more work to understand/manage risks
    - User-held private keys
    - Versus online CA or store
  - Working on an approach based on responsibilities
  - Scaling issues
    - sites versus countries
  - A group was formed at GGF in Seattle
    - not a GGF group, though

Issues (3)

- Certificate renewal
  - Lengthy discussion
- Decisions
  - Max life stays at 12 months
  - Renew with same DN
  - Require RA intervention for renewal, although it may be a different process to initial registration
  - Require re-keying

Future Plans

- Life after DataGrid
  - LCG Security Group and GDB
    - Approves CA's for use in LCG
    - Based on the EDG CA groups approved list
    - But also additional CA's, e.g. FNAL KCA
  - EGEE
    - Plans to continue the CA Managers group (PMA)
- TERENA working on a CA repository
  - To ease distribution of CA certificates and details
  - Include GRID CA's?
- GGF discussions continue
- Agreement on a single minimum requirements spec is difficult
- Relying parties (projects, VO's, sites) need to be able to define a "trusted" list according to their requirements
  - Tools could help a lot (like the Acceptance matrix)