WP6 CA report
Budapest
2 Sep 2002

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

WP6 CA meeting
Prague, 27/28 June 2002

- 5 Datagrid, 6 CrossGrid, 2 USA attendees (+2 EDG Video)
- Updates to Minimum Requirements
  - continue by e-mail for TB2
  - Discussed certificate lifetime (CA and users) – no change
  - Allow online CA if special security hardware storage
  - More on RA procedures
- Plan to collect statistics of certificates issued, revoked etc.
- Acceptance Matrix
  - Good progress on automatic extraction of CP/CPS features
    - Discussion started on a profile for certificate extensions/flags
- New CrossGrid CA's
  - Karlsruhe/Germany approved, first report from Greece CA
  - Poland and Slovakia to be considered by e-mail
- More CA's to come (CERN and FNAL KCA's, Australia, Canada?)

WP6 CA (2)

- Cross Domain Trust
  - New GGF working group proposed – "CA operations"
    - We will participate – lots to feed in!
- Presentation by US DOE GRIDS CA – service and RA's
  - Issued 258 certificates to date
- Presentation on OpenCA at RAL
- Brief discussions on CRL's, Directories
- CERN will write CP/CPS for a Kerberos-based CA for discussion by e-mail
  - PPDG-SiteAA (FNAL) also active here.
- Next meeting – CERN, November 2002 (tba)

CA Acceptance procedure

- Is a new CA required?
  - For small number of users/machines use CNRS “catch all” CA
- Write CP/CPS (at least a good draft)
  - Distribute to CA group via e-mail
- If urgent, interim approval granted following e-mail discussion
- Formal approval requires presentation at a CA meeting (4 per year) and discussion of procedures
- Inclusion of CA in EDG release done by WP6 and Iteam
- Will update WP6 web to include
  - This acceptance procedure
  - A list of current candidates

Authorisation RA

- Much concern about the procedures used to Check/Register users in VO's
  - E.g. need audit logs
  - And maintained contact details and other attributes
  - Physical and network security of VO server(s)
- Authorisation **more** important than Authentication
  - Gives access to resources!
- CA's do **not** check the right to use resources
- Sites need to be convinced of VO procedures to establish "trust"
- VO RA needs to reliably confirm
  - Right to join VO
  - That the user rightfully owns the certificate (?)
- PPDG Site-AA project has important input here

Scaling AA to LCG

- Authentication
  - Ever growing number of CA's
  - Lots of work to establish trust
  - CNRS catch-all works fine for EDG but not LCG
  - CERN (FNAL and BNL) keen to use Kerberos and online CA (short lived certs) – need CP/CPS
    - Issue of user management of private key for long-lived certs.
- Authorisation (see previous slide)
  - VO's will need to work towards a more robust procedure – needs resources!

Summary (and issues)

- Currently CA's are under control
  - Acceptance procedure working
- Authentication issues
  - How to scale?
  - Does the CA group decide for everyone or do VO's need to establish their own "trust"?
  - PPDG-SiteAA project pushing for short-lived user certs.
    - But what about services/hosts?
- Authorisation is the bigger problem
  - Discuss this week how best to proceed