Online Authentication
SCG Meeting
EDG Barcelona, 12 May 2003

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

Background

- EDG WP6 CA managers group
  - DataGrid, CrossGrid, US (DOE), Canada
  - Growing to include new LCG-1 CA's
  - Taiwan, Tokyo, Belgium, Hungary, Israel, …
- http://marianne.in2p3.fr/datagrid/ca/
- CA's must meet minimum requirements
  - Operational and Policy (CP/CPS)
- "Catch-all" CA operated by CNRS (France)
  - With appropriate registration procedures
- CA RPM's distributed with EDG software
- Sites still free to decide their own trust list
  - Not generally used.
- Scaling problems – GGF looking into this area (PMA)
  - EDG Acceptance Matrix tools can help
- EU FP6 (EGEE) will have an important future role
  - Also - TERENA – NREN discussions on PKI

Issues – online authentication

- FNAL propose Kerberos CA (KCA) (CERN also interested)
  - User authenticates via Kerberos mechanisms
  - KCA issues short-lived certificate for Grid
- Key Management Concerns
  - User-held private keys – security concerns
- MyProxy online Certificate repository
  - Concerns over key management
- VSC proposal from SLAC (holds user private keys)
- EDG CA min requirements say
  - CA must be offline or have a secure disk module (HSM)
  - Why should KCA follow this?
    - short-lived certs only
    - Many different services provide short-lived certs

The way forward?

- Ideas – for discussion today
- *Consider Long-lived (12 months) certificates and short-lived (12 hours or few days) certificates separately*
- Long-lived certs ("traditional" CA's)
  - More severe consequences of compromise
  - Continue with strong minimum requirements
  - EDG group continues in its current form during 2003 (chaired by DPK)
    - As ever… membership of all related projects
    - Next meeting 12/13 June (CERN)
    - One further meeting in 2003 (November or December)
  - This process defines the list of trusted CA's
  - Need to plan for 2004
    - Situation clearer once EU FP6 (EGEE) funding known

The way forward? (2)

- Short-Lived certificates (max life – few days, 2 weeks?)
  - User generated proxy certificates
  - KCA's
  - MyProxy online credential repository
  - VSC? (will this be used in 2003?)
  - And indeed AuthZ services (VOMS)
    - VO membership, Groups/roles in attribute cert
- Less severe implications on compromise
- Don't require HSM during 2003 (at least)
- The short-lived service should be a sub-ordinate CA of a trusted traditional CA (to ease distribution & management)
  - Chaining would be nice
- Work with LCG, US projects (and others) to
  - Document and evaluate risk
  - Propose the way forward for 2004