CA meeting
Minimum Requirements
CERN, 12 June 2003

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

Intro

- Start by presenting reasons for treating online CA's differently
- Then proceed to discuss changes to min requirements for traditional CA's

Online CA's - Issues

- 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

LCG Security Group Proposals (GDB agreed)

- Consider Long-lived (12 months) certificates and short-lived (12 hours or few days) certificates ***separately***
- Also discussed/agreed at EDG SCG in Barcelona (May03)
- Long-lived certs (traditional CA's)
  - More severe consequences of compromise
  - Often run by and for larger communities than HEP
  - Continue with strong minimum requirements
  - EDG/LCG group continues in its current form during 2003 (chaired by DPK)
    - Appropriate membership of new LCG-1 CA's
    - LCG inputs its requirements
  - This process defines the list of trusted CA's
  - Plan for 2004 – input from LCG
    - Need to work with EGEE

LCG Security Group Proposals (2)

- Short-Lived certificates (max life – few days, few weeks?)
  - User generated proxy certificates
  - KCA's
  - MyProxy online credential repository
  - VSC
  - 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 certificate of the short-lived service should be signed by a trusted traditional CA (to ease distribution)
- Work with EDG, US projects, GGF, … to
  - Document and evaluate risk, best practice, min requirements
  - Propose the way forward for 2004

LCG-1
CA approval procedure
For 2003

- The LCG-1 Security Group proposes the list of accepted CA's from two sources:
  - The list of "traditional" CA's, issuing long-lived (12 months or more) certificates, comes from the EDG CA Group
  - The list of additional CA's (online short-lived, special cases, etc.) is generated by the LCG-1 Security Group
- Proposed additions to these lists above will be circulated to the GDB and to the LCG-1 site security contacts for objection prior to implementation
- The LCG-1 operations team maintains the necessary information (certificates, signing policy, CRL's) and distribution mechanisms for CA's on both sub-lists
- All LCG-1 resources will install the full list of approved CA's

Min Requirements for traditional CA's

- V2 is for EDG TB1 (summer 2001)
- Need V3 for EDG TB2/3 and LCG-1 (summer 2003)

Changes to be discussed include:

- HSM instead of offline
  - FIPS-140 level 3 or above
- Need to add section on renewal
  - New key pair
  - Same DN?
  - Require intervention of RA?

GGF pma-discuss

- Offline requirement rules out KCA
- Must state that DN is unique
- NCSA issues 2-year certs
- Wildcard DNS name for host certs
- Users don't always generate keys
  - E.g. smart cards
- Does RA need to confirm identity
  - Could just bind unique DN (string) to public key
- Machine rules missing point
  - Bind unique key to public key
  - Process secure as we can make it to prevent theft of requestor private key
  - CA private key must be secure.
- Revoke cert of person leaving organisation?