EDG WP7 SCG Authentication issues 19 Nov 2002

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

Topics

- EDG WP6 CA managers
- LCG/Grid Deployment
- Credential repositories, KCA etc
- GGF6 news

EDG WP6 CA managers

- DataGrid, CrossGrid, US DOE, etc
  - Establishing “trust”
  - 13 trusted CA’s today – continually growing!
- Next meeting (CERN) – 12/13 December 2002
- New CA’s under consideration
  - Canada, Cyprus, Greece, Poland, Slovakia
- Will also discuss
  - KCA, VSC, credential repositories
  - a formal PMA mandate (for EDG, EDT)
- Need to move into a larger world (LCG-1 etc)
  - Perhaps EU, US (they are discussing amongst themselves),…

LCG/Grid Deployment

- LHC Computing Grid project
- One of 4 “areas” is Grid Deployment
- Grid Deployment Board now planning for LCG phase 1
  - Summer 2003
- WG3 is Security (chaired by Manuel Delfino)
  - DPK is the technical expert
  - Will consult widely
  - Policy and procedures as much as technology

Credential Repositories, KCA etc

- Some sites do not trust users holding their own long-term private keys on disk
  - Poor encryption
  - World-readable
  - Also private key should never cross network
    - Network-mounted home file area
- Then the whole topic of Credential renewal for long jobs
  - MyProxy etc

KCA, VSC etc

- Smart cards (not yet mature enough?)
- FNAL: KCA
  - User authenticates against KDC
    - then proxy cert issued by KCA
    - Need a CP/CPS – not yet discussed by CA group
- SLAC: Virtual Smart Card (VSC)
  - Based on VOMS
  - VSC generates and stores long-term key-pair
    - Requests to CA for signing
  - User authenticates via other means (how?)
  - Needs changes to all CP/CPS
- How does all this scale (one per site)?

Authentication: Can we agree?

- A single authentication system?
  - Desirable
  - But probably impossible to achieve!
- Will need to see how to support multiple systems
  - Add some sort of authentication level to certs?
  - Resource Brokers then need to know what sites will accept which levels
- Callouts for additional authentication during single sign-on
  - How does this scale?

Protection of private keys

- Can we do better for the interim period?
  - Enforce minimum passphrase quality
  - Enforce file security (not world readable)
  - Not on network shared file system
  - Better user training

GGF6 news - Authentication

- GGF – Security Area
- GGF5
  - 2 Security work groups
    - GSI, GridCP
  - BOF on Site-AAA
- GGF6 (Chicago – 15-17 October 2002)
  - GSI WG did not meet
  - GridCP wound up
    - Turned into new CAOPs WG
  - OGSA WG, Site-AAA RG, BOF on Authorisation
    - see Andrew McNab’s talk

GGF – GridCP & CAOPs

- GridCP WG
  - GridCP – last call
  - Trust Model – last call
  - PMA charter – last call
  - Certificate Profile
- CAOPs
  - Best practice, operational procedures, guidelines
  - Automated Client Certificates (S Chan, NERSC)
    - Third type of cert, after user and host/service
    - Unencrypted private key (but needs to be distributed)