LCG/GDB
Security Issues and Planning

or Report from the Security Group

CERN, 8 May 2003

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

Draft for discussion at LCG SEC meeting 7 May

Authentication - Trust

- Two main issues
  - Who defines the list of trusted CA's?
    - LCG or other Grid projects?
  - How to introduce new types of CA (online)?
    - E.g. Kerberos CA at FNAL
- LCG-1 and EDG Application testbed
  - closely linked
  - Common approach desirable (for this year)
- For Jan 2004 onwards
  - Need to consider when fate of EGEE proposal known

Background

- EDG WP6 CA managers group
  - DataGrid, CrossGrid, US (DOE), Canada
  - Growing to include new LCG-1 CA's
    - So now really a joint EDG/LCG group
  - Taiwan, Tokyo, Belgium, 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 could help

Application Testbed Users

VO	Users
CMS	106
WP6	87
ALICE	63
ATLAS	55
Earth Obs.	29
BaBar	29
LHCb	28
ITeam	22
Genomic	22
TSTG	16
Medical Img.	6
DO	3

Certificate Authorities Group

- Evaluates & approves new CAs
- 16 currently approved.
- Collaborating w/ other grid proj.
- More on the way…
  - Cyprus
  - US FNAL (KCA)
  - Belgium
  - Taiwan

Virtual Organizations

- Also for Storage Elements
- Guidelines (EDG rules)

Course-grained Authorization.

CA	Users
INFN (IT)	113
CNRS (FR)	71
UK	58
CERN (CH)	44
NIKHEF (NL)	19
Russia	15
US DOE	10
Spain	8
FZK (D)	5
Czech Rep.	3
Portugal	3
NorduGrid	2
Poland	1
Canada	0
Greece	0
Slovakia	0
TOTAL	352

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

- 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
  - Recommend the 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 – strong input from LCG
    - Need to work with EGEE

LCG Security Group Proposals (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 certificate of the short-lived service should be signed by a trusted traditional CA (to ease revocation)
- Work with EDG, US projects to
  - Document and evaluate risk
  - Propose the way forward for 2004

Recommendations to GDB

GDB is asked to agree (at June meeting?) for LCG-1 operations during 2003 that…

1. The list of trusted traditional CA's (long-lived certificates, i.e. more than 2 weeks) is defined by the joint EDG/LCG CA group
2. The list of trusted online (short-lived certificates, i.e. less than 2 weeks) authentication and authorization services and servers is defined by the LCG-1 Security Group
3. That all LCG-1 sites install and trust the 2 lists.