CA's and Experiment (VO) Organisation WP8 Meeting

EDG Barcelona, 13 May 2003

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

Outline

- Certificate Authorities (CA's)
  - Authentication
  - Electronic identity
  - Prove who you are
    - like a national passport
- Virtual Organisation (VO) management
  - Authorization
  - Prove what you are allowed to do
    - Like an entry Visa
- In context of EDG, LCG (and EGEE)

CA background

- The EDG WP6 CA group
  - EDG, EU CrossGrid, US DOE, Canada, …(LCG)
- Best practice and min. standards for acceptable CA's
  - Maintains list of approved CA's
- CNRS/France acts as the "catch all" CA
  - subject to satisfactory Registration procedures
  - Users and hosts/services
- See http://marianne.in2p3.fr/datagrid/ca/

Additions in 2003

- 5 new CA's
  - Canada, Cyprus, Greece, Poland, Slovakia
- Others being developed/discussed (see later)
- New online CA's and repositories
  - Concerns about User-held private key management
  - FNAL Kerberos CA (LCG-1)
  - SLAC Virtual Smart Card (BaBar)
  - Need to define best practice for "online CA"
  - and understand/manage risks

The approved CA's

18 on the trusted list (today)

- Canada, CERN, Cyprus, Czech Republic, France, Germany, Greece, Ireland, Italy, Netherlands, Nordic, Poland, Portugal, Russia, Slovakia, Spain, UK, USA
- "Catch-all" operated by CNRS/France

Under development/consideration

- Belgium, FNAL (KCA), Hungary, Israel, Japan, Taiwan, (Austria?)
- FNAL and Taiwan the furthest down the road

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

2nd EU Review (Loomis)

CNRS CA, DataGrid Catch-All CA

Status at May 6th 2003

Country	Institute	# Certificate
Total		468
France	CNRS, CEA/DAPNIA, CS, Ecole Centrale Paris, Universities, ESRF, CNG, GridXpert	**192**
EDG Tutorials		**177**
Total Others		**99**
Taiwan	Academia of Sinica, National Central University	22
Italy	ESA/ESRIN, ITC-irst, CNR	20
Israel	Weizmann Institute	10
Austria	University of Innsbruck	9
Belgium	Louvain and Brussel Universities	7
Hungary	SZTAKI, RITPMS, KFKI-RMKI	8
Slovakia	University of Paul Joseph Safarik	8
Korean	Korean Center for High Energy Physics	3
Japan	University of Tokyo	3
China	Nanjing University	2
Switzerland	Swiss Institute of Bioinformatics	2
Croatia	University of Zagreb	2
India	Department of Atomic Energie	2
Germany	Technische Universitaet Dresden	1

CA Future Plans

- Life after DataGrid (in Europe)?
  - LHC Computing Grid (LCG)
  - EU FP6 (EGEE)
- Many of the national CA's serve a community larger than just DataGrid (and its applications)
- Sensible to manage the CA requirements and best practices in a broad forum
  - GGF now working on this
  - EGEE likely to run the EU CA PMA
  - But, LCG-1 will define its list of trusted CA's
- Online CA's and certificate repositories
  - Need more work to understand and manage risks and responsibilities
- Need to agree the LCG "catch-all" CA for 2004

VO Management

User Registration: the model

- User has ONE Grid certificate
  - From National CA (or CERN or catch-all)
  - (Hopefully) used in any HEP Grid project
- Then user registers with EDG or LCG-1
  - Two different Usage Guidelines/Rules
  - Two different Guidelines VO's (signed)
  - LCG-1 will have an expiry date
    - May also wish to collect more personal information
- Next, user requests to join an Experiment VO
  - More than one also possible
- Same VO shared between EDG and LCG-1
  - At least to start with
- Same VO services/servers (LDAP) and managers
- Authorized access if in BOTH the Guidelines and VO

VO Management

- *Today in EDG*
  - VO managers
    - Alice: Daniele Mura (INFN)
    - Atlas: Alessandro De Salvo (INFN)
    - CMS: Andrea Sciaba (INFN)
    - LHCb: Joel Closier (CERN)
    - BaBar: Tim Adye (RAL)
    - D0: Jeff Templon (NIKHEF)
  - All VO servers run by NIKHEF
    - Except BaBar (UK GridPP)
  - No robust definition of what VO manager should do to check the identity and right of a user to join
    - OK for EDG, but not LCG-1

VO Management

- We need to check carefully before registering users in VO
  - Grants access to site resources
- LCG discussing/planning how to manage User registration
- For Production Grid on large scale
  - Site managers/security officers require robust and auditable registration procedures
  - To avoid the necessity of users registering at all sites
- Initial thoughts (for LCG)
  - Distributed VO registration authorities (for AuthZ) based on National Tier1/2 contacts
- LCG now considering RA's based on the Experiment VO's
  - EDG and LCG should work together on this (now)
  - To make more robust than current procedures
  - Long term aim is to use the Experiment User Offices

Issues for discussion

- Any CA issues?
  - Catch-all should be able to cover everyone
- VO User Registration procedures
  - Need direct personal contact with end user
    - By someone who knows them
  - Can one VO manager do this?
  - Hierarchical Reg system (per country? Per site?)
- VO groups/roles
  - How would WP8 like to use these?