



Security meetings Report to EDG PTB 3 Jul 2002

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



WP6 CA meeting Prague, 27/28 June 2002

- 5 Datagrid, 6 CrossGrid, 2 USA attendees (+2 EDG Video)
- Updates to Minimum Requirements
 - continue by e-mail for TB2
 - Discussed certificate lifetime (CA and users) – no change
 - Allow online CA if special security hardware storage
 - More on RA procedures
- Plan to collect statistics of certificates issued, revoked etc.
- Acceptance Matrix
 - Good progress on automatic extraction of CP/CPS features
- New CrossGrid CA's
 - Karlsruhe/Germany approved, first report from Greece CA
 - Poland and Slovakia to be considered by e-mail
 - More still to come



WP6 CA (2)

- Cross Domain Trust
 - New GGF working group proposed – “CA operations”
 - We will participate – lots to feed in!
- Presentation by US DOE GRIDS CA – service and RA’s
 - Issued 258 certificates to date
- Presentation on OpenCA at RAL
- Brief discussions on CRL’s, Directories
- CERN will write CP/CPS for a Kerberos-based CA for discussion by e-mail
- Next meeting – CERN, ~ first week of October 2002



WP7 SCG meeting CERN, 2 July 2002

- Review of To-Do list (12 items)
- WP2 Security
- Authorisation
- Scaling Authentication and Authorisation to LCG
- Delegation
- Dynamic Accounts in TB 1.3
- Plans for GGF5
- Plans for Budapest
- Reviews of Security Design and implementation(s)
- Firewall settings – machine level



Authorisation

- New version of mkgridmap tool
- Virtual Organisation Membership Service (VOMS)
 - Basic functionality working
 - Time to release not yet known
 - “Groups/Roles” added to User Proxy
 - Signed by VOMS
 - Globus CAS also going this way now
 - Will also take another look at EU PERMIS s/w
- Grid ACLs and SlashGrid from Andrew McNab et al



Authorisation RA

- Both Security groups concerned about the procedures used to Check/Register users in VO's
- Authorisation more important than Authentication
 - Gives access to resources!
- CA's do **not** check the right to use resources
- Sites need to be convinced of VO procedures to establish "trust"
- VO RA needs to reliably confirm
 - Right to join VO
 - That the user rightfully owns the certificate (?)
- PPDG Site-AA project has important input here



Scaling AA to LCG

- Authentication
 - Ever growing number of CA's
 - Lots of work to establish trust
 - CNRS catch-all works fine for EDG but not LCG
 - CERN (FNAL and BNL) keen to use Kerberos and online CA (short lived certs) – need CP/CPS
- Authorisation (see previous slide)
 - VO's will need to work towards a more robust procedure – needs resources!



Dynamic Accounts TB1.3

- TB 1.2 Dynamic accounts in use – but difficult to recycle if permanent files created
 - Need NFS to share locking directory
- TB 1.3 SlashGrid developments (optional)
 - Grid DN based home directory
 - No mapping to a particular UID – can recycle
 - No need for NFS
- SCG still concerned about other non-file uses of UID's – but OK to test and welcomed by WP5



GGF5 - Edinburgh

- We have lots of interesting work and ideas on Authorisation – but no GGF WG yet.
- Andrew McNab tried to get BOF on Authorisation but failed
 - DPK will try again, particularly with support from US PPDG-AA project
 - Would like to make a number of presentations



Budapest

SCG requests for joint parallel sessions (2 hours each) in order of priority – if WP's agree of course!

(the security implications of all of these of course)

- Biomedical Data Security: WP2/5/10 and SCG
- Accounting: WP1 and others?
- Quotas (who is doing resource quotas?): WP1? WP4?
- ACL's (not just files, but applied to other objects): WP1? WP4?



Reviews of EDG Security

- Is desirable to check/audit/review the Security Design and Implementation(s) (for next EU Review)
 - 2 separate activities
- D7.6 (M25) is an important document for the design review – internal and external
 - Oxford SCG members will contribute
- How to do the implementation review?
 - CNRS are looking into external review
 - Not sure whether design or implementation
- Training of developers in writing secure code?