Authentication
11 Dec 2001

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

Meetings

- WP6 Certificate Authorities Group
  - Defining procedures for Authentication/Trust
- Dec 2000, March, June, August and Dec 2001
- Agenda 6/7 Dec 2001 – CERN
  - New CA's (USA and Germany)
  - Acceptance Matrix
  - GGF CP/CPS
  - Naming issues
  - Scaling problems
- Next meeting Paris EDG Conference – March 2002

EDG CA's

- Already in TB1
  - CERN, Czech Rep, France, Ireland, Italy, Netherlands, Nordic, Portugal, Russia, Spain, UK
- In process of joining
  - USA (LBL/ESnet DOE Science Grid)
  - Karlsruhe (Germany, CrossGrid)

Acceptance Matrix

- Defined Minimum requirements for EDG CA
- Don't accept Globus certs
- N * N matrix to show status of "acceptance"
  - Matrix rather sparse right now!
- Every CA checks that it is "happy" with all others
- Aim to complete this by 15 Feb 2002

Some issues

- Host certificates
  - Need to find a CA prepared to issue them
- Privacy of Private key
- Scaling
  - Resources
- Global trust
  - GGF CP
- Authorisation vs Authentication
- Naming

Privacy of private key

- Private key must be secret or else …
  - CP violation
  - Violation of Use Guidelines
- Compromised keys **should** be revoked by CA
- Service/Host certificates must relate to a single network entity
- This will be enforced

Scaling issues

- Number of CA's growing quickly
- Number of certs per CA growing too fast
  - CERN users should apply to their national CA
- Didn't discuss the problem much
- Resources required are large
  - To run a CA
  - To check trust with all others
- Possible solutions
  - GGF CP work
  - Make Authentication lightweight
    - Bind name string to public key, but no meaning of name

GGF CP/CPS

- Discussed draft CP document
- GGF hopes to agree this in Toronto (Feb 02)
- 4 levels of assurance or just 2 levels?
- Do we need proof of possession of private key?
- Need to remove references to US Federal agencies
- Central GGF repository
  - Plus audit
- More scaling problems!

Authentication vs Authorisation

- Where do we put most effort checking identity?
- Answer
  - As close to the resources as possible
- Authorisation scheme will need to do most checking
- Don't duplicate the effort!
- Authentication cert could bind random string to public key

Naming

- Flat namespace vs hierarchy?
- What does the name mean anyway?
- examples
  - /dc=doesciencegrid /dc=org /cn=John Smith 2654
  - /c=uk /o=ESgrid /ou= GridPP/L=Manchester/ cn= John Smith
- Main reason to keep flat
  - Remove all Authorisation information
- Decided not to standardise
  - CA can do what they like