The TERENA Academic CA Repository

The Case for the Repository

- A common academic root had shown unfeasible
  - Policies with incompatible purposes and even basic principles
  - Application limitations in the certificate verification procedues
  - Extending the infrastructures usually means cumbersome resigning processes
- A PKI-based web of trust among the European academic community
  - And beyond!
- Based on two basic principles
  - Keep it simple
  - Let it happen
- Oriented to act as a trust anchor
  - Applicable in different environments

Current Status

- Policy approved
  - Including sample documents
  - What PKIs can participate
  - How data are incorporated, modified and distributed
  - Procedures for changing the policy itself
- Certificates being collected
  - Fourteen CAs (NRENs and Grid communities)
  - Direct liaison to the EUGridPMA
- Extending application domains
  - eIRG endorsment
  - EGEE
  - The *Evolvable PKI* group (Internet2)

What the TACAR Currently Provides

- A trusted source for
  - Root certificates
  - Policies
- The repository is built and updated by means of out-of-band methods
  - Face-to-face meetings
    - Required for the initial incorporation
  - PGP-enabled mail
- (Optional) bundles of available certificates
  - Problems detected with certain combinations of formats and browsers
  - Contacts with the Mozilla Foundation

What the TACAR Can Provide in the Future

- A single authoritative source for certificates and policies
  - Simplification of maintenance procedures
- A means for extending (and reinforcing) trust links
  - Grid community
  - Other geographical areas
- A model to experiment with
  - Direct installation of pre-bundled certificates
  - Peer-based models (a la GridPMA)
    - Qualified and unqualified
  - Bridge and bridge-like approaches
    - Possible integration with the Certificate Parsing Server
  - External servers for PKI operations
    - Simplify trust evaluation

What the TACAR Needs to Evolve

- Operational support
  - The TERENA project officers act as trust link initiators
  - Policy and procedures supported by the TF-AACE group
    - And, hopefully, by the coming TF-EMC
  - Direct collaboration with the EUGridPMA
- Actual applicability
  - The TACAR is hosted at the TERENA premises
    - Requirements on site access control and certificate
  - Grid projects
  - Contacts with open-source browser developers
- A touch of experiment
  - Inside the coming TFs
  - As base for GN2 services
  - In collaboration with other communities