



Red IRIS

TACAR TERENA Academic CA Repository

EUGridPMA – Florence, 1 April 2004

The Itstory: TF-AACE

- Task Force on Authentication and Authorisation Coordination for Europe
- A middleware coordination activity among European NRENs
 - Promoted by TERENA
 - Oriented towards the development and deployment of interoperable AAls
- PKIs are one of its main targets
 - Although difficulties were soon found in the seek for harmonization
- Grids have also been (moving) targets of the group

The Case for the Repository

- A common root had shown unfeasible
 - Policies have incompatible purposes and even basic principles
 - Several applications impose limitations in the certificate verification procedures
 - Extending the infrastructures usually means cumbersome resigning processes
- A common bridge was perceived as too complicated
 - High costs (even in the "simpler" case of the US Federal BCA)
 - Few bridge-aware software elements

The Original Goals

- Provide a means for building a PKI-based web of trust among the European academic community (and beyond!)
 - Without the technical and administrative overhead of a root or bridge CA
- Based on two basic principles
 - Keep it simple
 - Let it happen
- Conceived as a collection of certificates
 - More formalization was rapidly requested and incorporated

The Two Basic Principles

- Keep it simple
 - Do not require extra developments
 - Make the whole system sustainable
- Let it happen
 - Follow a very pragmatic approach
 - Gain critical mass
 - Act according to user organization demands
- The better illustration is the original evolution
 - TACAR was conceived as a simple PKCS#7 distributed via TLS
 - Policy issues came into play and the TACAR policy was created

The TACAR Policy - I

- Which PKIs can be included
 - Directly managed by TERENA members
 - NRENs
 - National academic infrastructures
 - Educause, Internet2,...
 - Non-for-profit research projects directly involving the academic community
 - Grids
- Including a PKI
 - Self-signed certificate(s)
 - Policy documents (CP/CPS) and fingerprints
 - Face-to-face meeting
 - Build the initial trust links

The TACAR Policy - II

- Updating the information pertaining a PKI
 - Mandatory in case of any change
 - Certificates or policies
 - Only allowed for accredited people
 - Face-to-face
 - By e-mail, using PGP
- Measures for repository maintenance
 - Available through a secured web page
 - Periodic checking of data accuracy
- Procedures for changing the policy itself
 - Agreement among the participating organizations

Status

■ Policy approved

- Including sample documents
 - Letter of registration
 - To be collected by the TERENA officers when incorporating a new CA
 - Proof of the inclusion of the CA into the repository
 - Letter of accreditation
 - Optional
 - Aimed to simplify interactions (electronic updates)

■ Certificates being collected

- CESNET, GRNET, RedIRIS, SURFnet
- DoEGrids

What the TACAR 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
 - Although problems have been detected with certain combinations of formats and browsers

What the TACAR can provide to the EUGridPMA

- A single authoritative source for certificates and policies
 - Complementary of the EUGridPMA services
 - Simplification of maintenance procedures
- A means for extending trust links
 - Beyond the borders of the Grid community
 - Beyond the borders of the EU
- An anchor for deploying new AA mechanisms
 - TACAR could act as a trust clearinghouse for (con)federated approaches
- A model to experiment with
 - Lighter than a common root, simpler than a bridge

What the TACAR expects from the EUGridPMA

- Requirements to become acceptable on
 - The TACAR site
 - The TACAR policy
- Keep it simple
 - Do not forget it is a service for PKI admins
 - Budget issues are relevant
 - What about EGEE?
- Let it happen
 - Separate essential requirements from features
 - Make the system evolve as it is used
- Let it happen

<http://www.terena.nl/tech/task-forces/tf-aace/tacar/>