

Overcoming the PKI hierarchy problem. PMAs and TACAR

Diego R. Lopez
RedIRIS



RedIRIS



- **The original X509 concept implicitly assumed a common global root for certificates**
 - At least, so it was perceived in many cases
 - Similar to the old X500 idea of a single global root for *The Directory*
 - This (as with the case of LDAP) has proven unfeasible
 - This implies the need of concialiating several roots of trust
- **Traditional solutions to this problem**
 - Building a mesh of cross-certificates
 - Extending hierarchies to a common (agreed) root
 - The first one does not scale
 - The second imply policy problems
- **New solutions applied/explored in the academic arena**
 - PMAs and trust repositories
 - Bridges

- A common root is not feasible even in the "simpler" academic world
- Policies have incompatible purposes and even basic principles
 - Not even mentioning national regulations
- Several applications impose limitations in the certificate verification procedues
 - Most notably, currently used Grid software
- Extending the infrastructures usually means cumbersome resigning processes
 - Scaling problems become even worse than in the mesh case

- Keep the solution as simple as possible
- Take advantage of the already existing trust links in the community
- Explore and extend the technologies
- Seek for support in the EU and beyond
 - Endorsment of the EUGridPMA and TACAR by the eIRG as a "first step towards common EU policies for authentication for resource access and sharing for e-science"
 - International Grid Federation
 - The Cotswolds Group

- *Policy Management Authority*
- Defines a set of minimal requirements and good practices
- It accredits PKIs
 - Authentication and key management procedures
 - Signing policies
 - By means of a *peer review* process
- **Several active PMAs**
 - Basically related to Grid infrastructures
 - Europe, America, Asia-Pacific
 - The EUGridPMA is the best established
- A federation of these PMAs is in progress

- **Participants**
 - Accredited PKIs
 - User infrastructures where the accreditation is accepted
 - Trust repositories
- **The PMA does not provide identity assertions**
 - But guarantees that certificates comply to the minimal requirements
 - Verifiable through the trust repositories
 - According to the limits established by its policy
- **All accredited PKIs are to be considered equivalent**
 - As authentication providers
 - Authorization is performed by the relaying party

- Formally established in April 2004
 - <http://www.eugridpma.org/>
- Participants from Europe and beyond
 - A single PKI per country (whenever possible)
 - Relaying parties are national and trans-national Grids
 - EGEE, DEISA, LCG, SEE-GRID,...
- Identity is only applicable to e-science environments
 - Encryption and digital signature are not supported
 - The participants are not to be considered digital signature agencies according to the EU directives
 - Financial transactions are not supported
 - It is required to comply to GSI technical requirements
- TACAR is used as trust repository

- Other participant PKIs:

CERN

Catch-all for EGEE, LCG, SEE-GRID

Russia (LCG)

Israel

Armenia

DoEGrids (USA)

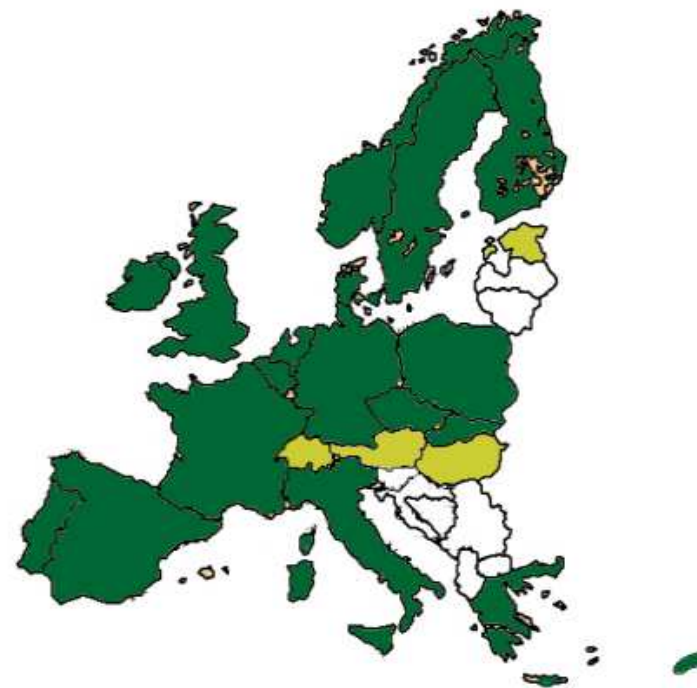
FNAL Service CA (USA)

Canada

Japan

Taiwan

Pakistan



- 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
- Initially conceived as a collection of certificates
 - More formalization was rapidly requested and incorporated

- **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

- **Which PKIs can be included**
 - Directly managed by TERENA members: NRENs
 - (Inter)national academic infrastructures: EUNIS, 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 to build the initial trust links
- **The policy document includes sample letters for**
 - Registration
 - Collected by the TERENA officers when incorporating a new CA
 - Accreditation (optional)
 - Aimed to simplify interactions (electronic updates)

- **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

- **An updated policy**
 - Some clarifications requested by new members
 - Explicit mention to the site certificate and its diffusion
 - Explicit mention to the site security measures
 - Has exercised the policy update procedures
- **Twenty certificates currently available**
- **Everything at <http://www.tacar.org/>**
- **SSL access through a self-signed certificate**
 - <https://www.tacar.org/>
 - DN: dc=org, dc=tacar, cn=www.tacar.org
 - Fingerprint:
10:AE:CE:44:A2:CC:15:C7:1D:71:61:6B:B5:70:AD:5C

- 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
- A platform to experiment with
 - Lighter than a common root, simpler than a bridge

- **A mechanism for extending trust links**
 - By means of semi-cross certificates
 - Included by each participating PKI as another certificate in its hierarchy
 - TACAR as the root verification point for issuing and renewing the semi-cross certificates
- **A certificate verification service**
 - Based on OCSP
 - TACAR as trusted source for certificates and CRLs, simplifying maintenance procedures
- **A certificate diffusion system**
 - Derived from e-mail addresses and DNS, mostly oriented to encryption and digital signatures
 - TACAR as the common trust root