TCS overview

- TERENA SSL CA
- TERENA eScience SSL CA
- TERENA Personal CA
- TERENA eScience Personal CA
- TERENA Object Signing CA
TERENA SSL CA

- TCA Server and Object Signing CPS 1.3
  - both eScience SSL and SSL
- cert validity
  - 395 days (eScience SSL)
  - 1, 2, 3 years (SSL)
- SSL operational since June 2009
  - eScience SSL expected in Apr 2010
- portal software
  - e.g. djangora by Kent Engström
(eScience) SSL CA: Procedures

• NREN
  – web portal
  – registers organizations
    • administrators
    • DNS zones
(eScience) SSL CA: Procedures

• server admin requests a certificate
  – DNS names
    • checked by the portal against the register
  – public key (PKCS#10)

• organization admin
  – checks DNS – requester relation
  – approves
TERENA Personal CA

- TERENA Personal CA CPS 1.0
  - minor changes pending
- cert validity 1, 2, 3 years
- operational February 2010
TERENA eScience Personal CA

- TERENA eScience Personal CA CPS 1.0
  - accredited Jan 2010
- cert validity 395 days
- 7bit names
- operational February 2010
“self-service” certificate issuance
federated portal
  - front-end to TCS CA
organizations – Identity Providers
  - identity checked using official ID
  - account management
  - attributes release
Attributes

- eduPersonEntitlement
  - authorization
    - ID vetted properly
  - eligibility
- uniqueID
  - traceability, naming conflicts
    - specific value, eduPersonPrincipalName, ...
    - in CN (eScience Personal CA)
    - in CN or unstructuredName (Personal CA)
Attributes

- **commonName**
  - “reasonable representation” of person's name
- **email**
  - up to 10 addresses
  - *verified* by IdP
- **organization name**
  - pre-registered with portal
TERENA Shared Portal

- TCS Personal, TCS eScience Personal
- CESNET, CSC, UNINETT, SUNET, SURFnet, UNI•C
  - open for others
- Confusa software (UNINETT)
- operated by Tilburg University