TCS (eScience) Personal CA

Milan Sova
Context

- TCS:
  - TERENA SSL CA
  - TERENA eScience SSL CA
  - TERENA Personal CA
  - TERENA eScience Personal CA
  - TERENA Code Signing CA
Concept

- CA as SAML SP
- RAs as SAML IdPs
- “self-service” for users
Contracts

• TERENA – Comodo
• TERENA – NRENs
  (NREN != Identity Federation)
• NRENs – member organizations
...all refer to CPS
  – identity vetting requirements
  – ...

Connecting IdPs

• SP-centric federation
  – IdPs registered with the SP
  – metadata usually distributed via federations
Control

- eduPersonEntitlement
  - IdP-based authorization
  - released by IdP for properly vetted and eligible users
Content of a certificate

- unique ID
  - traceability, naming conflicts
    - specific attribute, eduPersonPrincipalName, ...
  - in CN (eScience Personal CA)
  - in CN or unstructuredName (Personal CA)
Content of a certificate II

- commonName
  - “reasonable representation” of person's name
  - CN, displayName,...
- email
  - up to 10 addresses verified by IdP
- organization name
  - pre-registered with SP
- country
  - pre-registered with SP
Content of a certificate - example

Subject: CN=Milan Sova 6356, O=CESNET, C=CZ

Attribute: CN  TCS-ID  OrgName  CountryCode
Conclusions

● It works!

● ...not really using the existing federation fabric
  - no legal inter-federation infrastructure
  - no unified attribute set provided by IdPs