SURFnet

TERENA Server Certificate Service

Towards the large-scale use of affordable popup-free server certificates for the European Research & Educational community

Jan Meijer

Amsterdam, 24 Januari 2006

.EU NRENs did something cool

Just contracted a service to deliver server certificates

- popup free
- flat rate
- unlimited number
- to the European NREN community

price is under NDA but...worth our while

high quality service

- Re-use existing RA organisation
- Certificate profile flexibility (Grids!)
- Option for fully electronic RA procedures
- Option for easy server certificate delivery
- NREN-specific branding!
- When that time comes: in the high assurance server certificate market

Service organisation

- TERENA contracts with supplier
- NRENs contract with TERENA (liability!)
- NRENs are ‘delegated RA’ for the supplier
- TERENA appoints delegated RAs
- NRENs are responsible for delivering RA services and technical support

So how, why?

- Project started in june 2004
- European NREN PKIs around for ~7 years
- Real certificate use limited:
  - webservers (popup-free and popup)
  - Grids (closed community)
- Anticipated growth in need:
  - AAI middleware services
  - Web-based ‘stuff’ (mail, e-learning, webservices etc.)
  - VPN, email

Servicing anticipated need

- Community is interested in server certificates
- Use is limited by:
  - popup problem (NREN PKI)
    or
  - cost (commercial CA)
- So solve either of these problems and the need can be serviced ☺

Solution 1: solve popup-problem

- Cost good (is it?)
- Popup problem bad
  - Fix by getting root certificate in root repositories
  - Requires webtrust audit
  - Expensive for an individual NREN PKI (~25.000 first time, annual ~25.000 for the audits, plus all the costs to do things exactly according to guidelines) --> CA hierarchy adds to cost!
- Is running our own CA that interesting?
- Own CA for smaller communities: same problem

Solution #2: Solve cost problem

- Try to contract a CA already in the browser
- To issue server certificates against NREN conditions
  - flexible certificate profiles
  - tailored RA procedures
  - no per-certificate payment

Went for option #2, together

- 8 NRENs + TERENA combined forces (proposal launched feb. 2005)
- Investigated market
- Investigated EU tender guidelines
- Ran a light-weight tender (start Sep 2005)
- Signed a contract (Jan 2006)

CSIRT benefit?

it will make it lame not to use SSL/TLS channels within the European NREN community

Thank you.

TERENA (.eu), ACOnet (.at), CARnet (.hr), CESnet (.cz), UNI-C (.dk), RedIRIS (.es), RENATER (.fr), SURFnet (Netherlands), SWITCH (.ch)