TERENA eScience SSL CA

Milan Sova

History

- TERENA SCS (*Server Certificate Service*)
  - Jan 2006 – Jan 2010
- TCS (*TERENA Certificate Service*)
  - Started Jun 2009
- TERENA SSL CA
- TERENA (eScience) SSL CA

Participants

- CA Operator
- Members
- Subscribers

TCS CA Operator

- Comodo
- Root Cert
  - UserTrust:
    C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware
  - Not Before: Jul 9 18:10:42 1999 GMT
  - Not After : Jul 9 18:19:22 2019 GMT

Members

- (”...of TERENA” i. e. NRENs)
  - manage Subscribers and their Aministrators
  - manage Subscriber Agreements
  - manage enrollment process
    - portal, database....
- **RAs**

Subscribers

- organization within NREN constituency (typically universities)
- consumers for the service
- “requesters”
  - persons applying for certificates on behalf of their organization

Relations

- CA Operator – TERENA
  - contract
- TERENA – Members
  - contracts
- Member – Subscriber
  - Subscriber agreements

Procedures

1) NREN register domains for a Subscriber
2) Requester applies for a certificate
3) Portal
   - validates the PKCS#10
   - verifies the DNS names match the Subscriber
   - accepts/reject the application
4) Subscriber's Admin verifies the application using local rules and accepts/rejects it
5) CA backend issues the certificate

Profile - Subject

- DC = “org”
- DC = “terena”
- DC = “tcs”
- C = <Country of the Subscriber>
- O = <Subscriber>
- OU = <Org. Unit within Subscriber> (optional)
- CN = <contains the hostname>

Profile - extensions

- Basic Constraints (critical):
  - ca:false (no pathlen)
- Key Usage:
  - Digital Signature, Key Encipherment, Data Encipherment
- Extended Key Usage:
  - TLS Server Auth, TLS Client Auth
- Subject Alternative Name:
  - 1 – 100 DNS or IP

Profile – extensions (2)

- Authority Key ID
- Subject Key ID
- CRL Distribution Points:
  - URI=http://crl.tcs.terena.org/ssl_server.crl
- Authority Information Access:
  - CA Issuers:
    - http://crt.tcs.terena.org/TERENAeScienceSSLCA.crt
  - OCSP:
    - http://ocsp.tcs.terena.org/

Profile – extension (3)

- Certificate Policies:
  - 1.3.6.1.4.1.6449.1.2.2.15
  - 1.2.840.113612.5.2.2.1

CRL

- Version 2
- CRL extensions:
  - Authority Key ID
  - CRL Number
- Validity: 96 hours
- Issued every 24 hours or at most 1 hour after a revocation

Current state

- Server & Object Signing CPS
  - *TCS SSL, TCS eScience SSL, TCS Object Signing*
  - the “object signing” added after September 2009
  - reactions to reviewers comments
  - sent to reviewers
  - ...