TCS History

- Fall 2005:
  - TERENA opens a Call for Proposals;
  - First contract with GlobalSign BV in 2006;

- SCS (Server Certificate Service)
  - NRENs participating would get SSL certificates against a yearly flat-fee;

- Started with 8 NRENs (in 2006):
  - Now 19 NRENs participate;
  - More than 15,000 SSL certificates issued in Europe;

- March 2009:
  - As result of a new Call for Proposal, Comodo appointed as new supplier;
SCS -> TCS

• New SCS service
  – Expected start in May 2009

• Model
  – yearly flat fee per NREN
  – TERENA contractual party
  – dedicated TERENA sub-CA
  – 20 NRENs
SCS -> TCS (cont.)

- Optional add-on services
  - personal (S/MIME & TLS client) certs
  - object signing certs
  - extra flat fee

=> TERENA Certificate Service

- work on progress
  - testing certificate profiles
  - writing CPS
Operational model

- Comodo
  - CA operator (hosted CA)
- TERENA
  - contractual party
- NRENs
  - RA
- Organizations
  - subscribers
  - approving agents
**BigOrg Model**

- BigOrg pre-registers with its NREN
  - BigOrg identity
    - name(s), address, proof of legal existence
    - registered domain names
- NREN verifies the registration
- BigOrg approves requests
- compliance checked by the TCS frontend
SmallOrg Model

- SmallOrg registers with its NREN
  - SmallOrg identity
    - name(s), address, proof of legal existence
- SmallOrg issues request
- NREN RA verifies & approves the request

* NRENs would prefer BigOrg model ;)*
Server Profile - Subject

- C required
- ST (optional)
- L (optional)
- O required
- OU optional
- CN required
- unstructuredName (optional)
Server profile - Extensions

- basicConstraints (critical):
  - ca:false (no pathLenConstraint)
- keyUsage (critical):
  - digitalSignature, keyEncipherment
- extendedKeyUsage (non-critical):
  - id-kp-serverAuth, id-kp-clientAuth
- subjectAltName (non-critical):
  - dNSName (min 1, max 100 names)
Server profile – Extensions (cont.)

- cRLDistributionPoints (non-critical):
  - URI: http://crl.tcs.terena.org/ssl_server.crl

- authorityInfoAccess (non-critical):
  - CA Issuer:
    - URI: http://crt.tcs.terena.org/ssl_server.crt
  - OCSP: URI: http://ocsp.tcs.terena.org
Server profile – Extensions (cont.)

- authorityKeyIdentifier (non-critical):
  - keyID:...

- subjectKeyIdentifier (non-critical): ...

- certificatePolicies (non-critical):
  - SCS policyID (no qualifiers)
eScience Server Profile - Subject

- DC "org"
- DC "terena"
- DC "scs"
- C required
- O required
- OU optional
- CN required
eScience Server Profile - Extensions

- **basicConstraints (critical):**
  - ca:false (no pathLenConstraint)

- **keyUsage (critical):**
  - digitalSignature, keyEncipherment, dataEncipherment

- **extendedKeyUsage (non-critical):**
  - id-kp-serverAuth, id-kp-clientAuth

- **subjectAltName (non-critical):**
  - dNSName (min 1, max 100 names)
eScience Server Profile – Extensions (cont.)

- cRLDistributionPoints (non-critical):
  - URI:http://crl.tcs.terena.org/eScience_server_crl

- authorityInfoAccess (non-critical):
  - CA Issuer:
    - URI:http://crt.tcs.terena.org/eScience_server.crt
  - OCSP – URI:http://ocsp.tcs.terena.org
eScience Server Profile – Extensions (cont.)

- authorityKeyIdentifier (non-critical):
  - keyID: ...

- subjectKeyIdentifier (non-critical): ...

- certificatePolicies (non-critical):
  - SCS policyID (no qualifiers)
  - 1.2.840.113612.5.2.2.1 (no qualifiers)
(eScience) Personal CA

- federated CA
- front-end - portal(s) operated by NRENs
- IdPs – RA functions
Attributes - Authorization

- eduPersonEntitlement
  - “user vetted properly”
  - “request approved by the Org”
Attributes - Naming

- Common Name
- Organization Name
  - preregistered
- “unique ID” assigned by IDP
  - ePTargetedID, ePPPrincipalName, whatever...
- email(s)
  - verified by IDP
Attributes - Naming

- Common Name
- Organization Name
  - preregistered
- “unique ID” assigned by IdP
  - ePTargetedID, ePPrincipalName, whatever...
- email(s)
  - verified by IdP
eScience Personal Profile - Subject

- DC "org"
- DC "terena"
- DC "scs"
- C required
- O required
- OU optional
- CN required
- unstructuredName optional
eScience Personal Profile - Extensions

- basicConstraints (critical):
  - ca:false (no pathLenConstraint)
- keyUsage (critical):
  - digitalSignature, keyEncipherment, dataEncipherment
- extendedKeyUsage (non-critical):
  - id-kp-emailProtection, id-kp-clientAuth
- subjectAltName (non-critical):
  - rfc822Name (min 1, max 10 email addresses)
eScience Personal Profile – Extensions (cont.)

- **cRLDistributionPoints (non-critical):**

- **URI:**
  http://crl.tcs.terena.org/TERENAAeSciencePersonalCA.crl

- **authorityInfoAccess (non-critical):**
  - **CA Issuer:**
    http://crt.tcs.terena.org/TERENAAeSciencePersonalCA.crt
  - **OCSP – URI:**
    http://ocsp.tcs.terena.org
eScience Personal Profile – Extensions (cont.)

- authorityKeyIdentifier (non-critical):
  - keyID:...

- subjectKeyIdentifier (non-critical): ...

- certificatePolicies (non-critical):
  - TCS policyID (no qualifiers)
  - 1.2.840.113612.5.2.2.5 (no qualifier)
To be continued...