

TERENA Certificate Service



Milan Sova
CESNET

Agenda

- History
- TCS Structure
- Procedures
- Conclusions

History

“pop-up free server certificates”

History: SCS

- TERENA Server Certificate Service
 - summer 2004: first idea
 - Dec 2004: SCS project started
 - Sep 2005: Call for Proposals
 - Jan 2006: Contract with GlobalSign (1 year)
 - 8 NRENs
 - March 16 2006: service operational
 - Jan 2007: Contract prolonged (3 years)

History: SCS -> TCS

- Sep 2008: new Call for Proposals
- Apr 2009: Contract with Comodo CA Ltd.
 - server, personal, object signing certificates
 - => TCS (TERENA Certificate Service)
- Jul 2009: TERENA SSL CA operational
- Feb 2009: TERENA eScience Personal CA accredited by EUGridPMA, operational
- Feb 2009: TERENA Personal CA operational

TCS

“PKI that works”

TCS Characteristics

- 22 NRENs
- flat fee – unlimited number of certificates
- 5 CAs operated by Comodo
 - including CRL, OCSP
 - access via HTTP API
 - implicitly trusted by major OSs and software
- RA roles and issuance managed by NRENs
 - except for object signing

Legal Structure

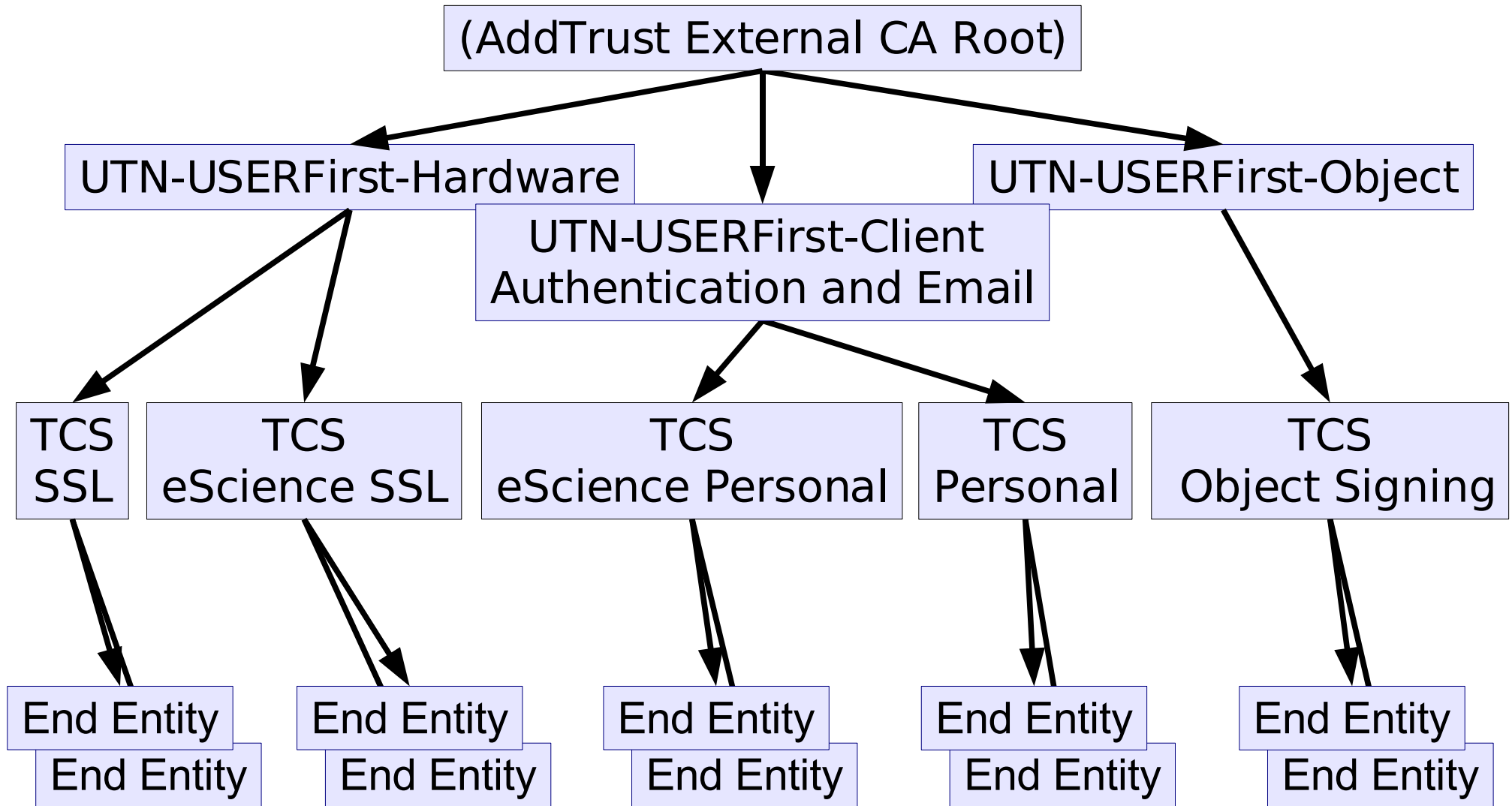
- Contract TERENA – Comodo
- Contracts TERENA – NRENs
- Contracts NREN – member organizations
 - all referring **CPS**
- 3 CPs
 - Server & Object Signing
 - including eScience Server
 - Personal
 - eScience Personal

TCS CAs

- TERENA SSL CA
- TERENA eScience SSL CA
- *TERENA Personal CA**
- *TERENA eScience Personal CA**
- *TERENA Code Signing CA**

** optional (surcharge)*

TCS Certificate Chain



Procedures

“solid and usable”

Procedures: Server

- NREN
 - web portal
 - register of organizations
 - administrators
 - DNS zones

Procedures: Server

- 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

Procedures: Personal

- “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 & eligibility
- uniqueID
 - traceability, naming conflicts
- commonName
- email

Conclusions

- cost-effective
- implicitly trusted by common software
- SSL server authentication
- S/MIME, user authentication
- grid user authentication
 - grid SSL server accreditation pending
- easy to use

