TERENA CA

And Comodo events…

TILBURG UNIVERSITY

TERENA CAs

- 25 NRENs www.terena.org/activities/tcs/participants.html
- Server certificates (regular and eScience)
- Personal certificates (regular and eScience)
- Code Signing certificates
- Docs www.terena.org/activities/tcs/repository/

- Small NRENs use a Comodo reseller webportal
- Large NREN Server and Codesign: DjangoRA per NREN
- Large NREN Personal: Confusa
  - Some national installations
  - 9 NRENs on common TERENA portals (8 eScience) 99.99%

TILBURG UNIVERSITY

Comodo fun and games

- 90% of validations done at Comodo (India)
- 10% customer validated, including TERENA and InstantSSL.it
- InstantSSL used an own portal with hardcoded API password…
- 2011 March 26 http://pastebin.com/74KXCaEZ
- 9 high value certs; yahoo cert online; Teheran
- Immediate revocation; fast info to domain owners and RAs
- www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html

Consequences

- TERENA CAs not involved, but share industry wide fallout
- High value domains blocked
- IP addresses accessing secure.comodo.net filtered by account
- RA authentication hardware on order
- For server certs Domain Control Validation emails to addresses that are decided by Google, MS, Moz: currently admin@domain administrator@ webmaster@ hostmaster@ postmaster@
- Until implemented Comodo DCV; delays
- http://datatracker.ietf.org/doc/draft-hallambaker-donotissue/?include_text=1 DNS CAA RR