



Certifikáty včera, dnes a zítra



Jan Chvojka (jan.chvojka@cesnet.cz)

První počátky

- Sada shellovských skriptů pracujících nad OpenSSL
- Hardware: PC DELL DX 240
- Offline CA v prostorách CESNETu
- Uživatelé přicházeli k CA s disketami



Ukázka rozhraní registračního úředníka

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01  
Transitional//EN">
```

```
<!-- $Id: form-print.html,v 1.6 2005/07/24
```

```
22:15:58 sova Exp $ →
```

RA registrační protokol ()

<u>D</u> N	
<u>K</u> řestní jméno	
<u>P</u> říjmení	
Datum <u>n</u> arození	
<u>M</u> ísto narození	
OP v	
Datum <u>o</u> věření	



Ukázka ze skriptu pro generování certifikátů

```
#!/bin/sh  
# $Id: rsv-new,v 1.10 2006/01/25 08:50:44 sova Exp $  
  
#CAfile='/home/sova/proj/RA/data/certs/cca.crt'  
bindDN='uid=ra1,ou=Special Users,dc=cesnet,dc=cz'  
CApath='/home/sova/lib/ra/certs'  
browser='/usr/local/firefox-1.0.6/firefox'  
ldapsearch='/usr/bin/ldapsearch'  
whois='/usr/bin/gwhois'
```

Entrust Luna HSM

- Online CA
- Luna CA3 HSM
- Drivery Luny pro HP-UX a Solaris (ne Linux)
- Rozhraní pro registrační úředníky jen pro OS Windows



Registrace domény cesnet-ca.cz pro Entrust

domain: cesnet-ca.cz
registrant: SB:CESNET-ZSPO
nsset: NSS:CESNET-ZSPO:1
keyset: AUTO-JYD8L03K4WOANNGQHMQOT64CY
registrar: REG-ACTIVE24
registered: 26.04.2005 14:05:00
changed: 06.09.2018 13:10:28
expire: 26.04.2022



SCS

- Terena **S**erver **C**ertificate **S**ervice
- První myšlenka v létě 2004
- Start projektu v prosinci 2004
- Září 2005 – Call for Proposals
- Leden 2006 – smlouva s GlobalSignem na 1 rok
 - Zapojeno 8 NRENů
- Start služby 16. března 2006
- Leden 2007 – smlouva s GlobalSignem prodloužena o 3 roky



Jak se z SCS stalo TCS

- Září 2008 – Call for Proposals
- Duben 2009 – Podepsán kontrakt s dodavatelem – COMODO. Služba přejmenována na TERENA Certificate Service (TCS)
 - Vydávání certifikátů serverových, osobních a code-signing
- Červenec 2009 – služba spuštěna
- Únor 2009 – CA akreditována u EUGridPMA



Další dodavatelé TCS

- 1. června 2015 podepsán kontrakt s novým dodavatelem – společností DigiCert
- V roce 2020 opět podepsán kontrakt s novým dodavatelem společností Sectigo (bývalé COMODO) – trvá dosud



Současnost TCS

Dodavatel: Sectigo

- Na portálu tcs.cesnet.cz
 - běžné serverové certifikáty
 - kořen v prohlížečích, platnost 1 rok, OV
 - běžné osobní certifikáty
 - vydávání v prohlížečích pomocí JS knihovny
 - klíč se generuje v prohlížeči
 - výsledek - pkcs12 soubor na disku
 - robotové certifikáty
 - z pohledu Sectiga speciální případ osobních
- Na individuální požadavek
 - code-signing certifikáty



RIP EV certifikáty

- Obtížně rozpoznatelné od OV, DV
- Rozšířené ověření, ale platnost jen jeden rok
- Za poslední rok několik revokačních vln DigiCertu i Sectiga
- Nevydáváme a (asi nikdy je už) nebudeme vydávat



- **TCS API**

- API pro automatizované vydávání certifikátů
- Pouze pro serverové certifikáty
- Pouze pro organizace v eduID.cz
- Autentizace klienta robotovým certifikátem od Sectiga
- Popis na <https://pki.cesnet.cz/cs/tcs-api-documentation.html>



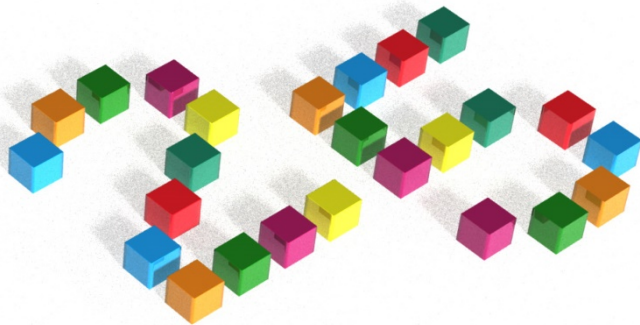
- **Let's Encrypt**
 - Výhody:
 - Bez poplatků
 - Automatizované vydávání pomocí ACME klientů
 - Nevýhody:
 - Jen DV certifikáty
 - Bez podpory
 - Krátká platnost, někde nelze automatizovat (např. HW zařízení)
 - Sledování CT logu (viz dále)
- **Pro gridy - CESNET CA 4**



- **CESNET CA - řešení pro gridy**
 - CESNET CA 4 je akreditována u EUGridPMA
 - Kořen není a nebude v prohlížečích
 - Na rozdíl od Sectiga se nemění název organizace
 - Certifikát se generuje z CSR nebo v prohlížeči



- **Co (asi) čekat v oblasti PKI**
 - Prohlížeče: zlepšení práce s CRL / OCSP
 - Chrome: CRLSets
 - Firefox: OneCRL
 - Ostatní: prostředky OS
 - CA: zkracování doby platnosti certifikátů
 - Tlak na automatické vydávání, redukce otravné manuální práce
 - Co když automaticky vydávat nejde?
 - CA: RSA? ECC? Quantum safe!
 - Prolomení klasických algoritmů přijde (ale neví se kdy)
 - CA se začínají připravovat



Děkuji za pozornost!



jan.chvojka@cesnet.cz