cesnet

CERTIFIKÁTY VČERA, DNES, ZÍTRA A POZÍTŘÍ

Jan Chvojka

jan.chvojka@cesnet.cz

Únor 2021

Seminář o bezpečnosti sítí a služeb

R.I.P. 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 už) nebudeme vydávat

Příklad revokace

- Nemocnice v Opavě
- Mimo jiné portál pro registraci k testům na COVID-19
- Certifikáty revokovány, čas na výměnu 4 dny, z toho 3 pracovní
- Definitivní potvrzení revokace den předem (v pátek odpoledne)
- Důvod: v předmětu certifikátu “Moravskoslezký kraj”

TCS - AKTUÁLNÍ STAV

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

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

Alternativa k certifikátům TCS

- **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

Certificate Transparency Log (CT log)

- **Co je to CT log**
  - Nutnost pro certifikáty s kořenem v prohlížečích (požadavek CA/B)
  - CT log obsahuje metadata vydaných certifikátů
  - Lze jen přidávat, kořen certifikátu musí být mezi definovanými
  - Existuje více fyzických logů

- **CESNETí řešení**
  - Pro správce TCS
  - Správce si vybere seznam domén, které chce sledovat
  - Systém jednou denně zpracuje vydané certifikáty z CT logu a případně pošle správci informaci o vydaných certifikátech
  - Systém nyní je v testovacím režimu

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

Dotazy?

cesnet

DĚKUJI ZA POZORNOST