cesnet

Certifikáty včera, dnes a zítra

Jan Chvojka <jan.chvojka@cesnet.cz>
oddělení síťové identity / CESNET

Bejvávalo, bejvávalo, bejvávalo dobře

Staré dobré časy

- Generování certifikátů v prohlížeči
  - Firefox, Chrome a Safari a podporou HTML tagu <keygen>
  - MS Internet Explorer: ActiveX komponenta
- Platnost certifikátů byla až 3 roky
- Relativně jednoduchá validace pro OV a EV certifikáty
- Extended Validation (EV) certifikáty žily spokojeným životem, všichni je chtěli

HTML tag <keygen> umírá

Konec podpory HTML tagu <keygen>

- **Chrome** - podpora odstraněna ve verzi 57 (2017)
- **Firefox** - podpora odstraněna ve verzi 69 (2019)
- **Firefox Extended Support Release** - zatím podporuje (ale jak dlouho?)
- **Safari** - zatím <keygen> podporuje

Generování certifikátů v MS IE / Edge

- **MS Internet Explorer** - přestal být výchozí prohlížeč, ale zatím stále podporuje ActiveX komponenty. Tag <keygen> nepodporuje.
- **MS Edge** - nepodporuje ani HTML tag <keygen>, ani ActiveX komponenty.

Jak dnes v prohlížeči generovat certifikát?

Generování certifikátů v dnešním prohlížeči

- MS Internet Explorer - ActiveX komponenta
- Safari a Firefox ESR - HTML tag <keygen>
- Spásné řešení pro všechny - JavaScriptová knihovna
  - Výsledek - pkcs#12 soubor na disku, musí se naimportovat do systému
  - Soubor musí být chráněn heslem!

A co mimo prohlížeč?

Generování certifikátů mimo prohlížeč

- OpenSSL - to je jistota, ale zvládne to běžný uživatel?
- Nativní aplikace od CA - viz Česká Pošta, Sectigo, …
- ACME
  - CA se bojí konkurence Let’s Encrypt, zjednodušují vydávání
  - OV certifikáty: validace organizace proběhne klasicky, pak lze použít ACME klienta. Platnost je stejná jako u jiných způsobů vydávání (max. 2 roky).
  - Klient doporučený od CA: Certbot

Platnost certifikátů

- Původně až tři roky
- Hlasováním CA/B fóra snížena na dva roky
- Snaha o snížení na 1 rok (zatím) neúspěšná. Pro: výrobci prohlížečů, proti: CA
- Reakce CA: zavádění podpory ACME

Velká bolest: validace

Validace organizací

- CA/B fórum vytváří tlak na lepší validaci organizací
- CA se snaží kontaktovat organizace, to je leckdy složité
  - V ARESu není kontaktní telefon
  - V telefonních adresářích jsou chyby
  - Technicky slabí operátoři
  - Praktické zkušenosti: přejmenovávání názvů organizací

EV certifikáty umírají

- EV - CA validuje nejen organizaci, ale i žadatele
- Poznat dnes stránku s EV certifikátem není úplně jednoduché
- Za rozšířenou validaci si připlatíte
- Pokud jsou dražší a lze je jen obtížně poznat, tak proč je chtít?

Trusted Certificate Service

- OV a EV certifikáty
- Zdarma pro klienty e-infrastruktury CESNET
- Zastřešuje evropská infrastruktura GÉANT
- V roce 2020 změna dodavatele: DigiCert - Sectigo (Comodo)
- Bude:
  - Podpora ACME
  - Generování v prohlížeči pomocí JavaScriptu

Vydáním certifikátu to nekončí

Certifikát už mám. Co mám dělat dál?

- Do DNS přidat Certification Authority Authorization (CAA) záznam
- Nakonfigurovat OCSP Stapling
- Kontrolovat Certificate Transparency log

DNS CAA záznam

- Záznam v DNS, od kterých CA smí být vydán certifikát. Pokud tento záznam existuje, CA ho musí respektovat. Pozor: platí i pro subdomény. Pokud CAA záznam neodpovídá aktuálnímu certifikátu, ničemu to nevadí - platí jen pro vydání.
- Samostatně pro běžné a hvězdičkové certifikáty
- DNS CAA záznam lze generovat online na https://sslmate.com/caa/

OCSP Stapling

- Při výpadku OCSP služby se klienti nepřipojí k serveru, protože nelze ověřit platnost certifikátu. Řešení: OCSP Stapling. Držitel certifikátu požádá CA o podepsaný záznam s platností a ten pak posílá klientovi. Typická doba platnosti záznamu je 7 dní.
- Certifikát může vynutit OCSP Stapling - volba *MustStaple*. Dobrý nápad u hvězdičkových certifikátů. Více viz viz Scott Helme: OCSP Must Staple
- Nginx: ssl_stapling on; ssl_stapling_verify on;
- Apache: SSLUseStapling on
- IIS: ve výchozím stavu funguje (Windows 2008+)

Certificate Transparency

- Seznam vydaných certifikátů
- Nezveřejněný certifikát berou browsery jako nedůvěryhodný
  https://invalid-expected-sct.badssl.com/
- Možnost kontroly vydaných certifikátů pro danou doménu
  - Cert Spotter
  - Sectigo - https://crt.sh/
  - Facebook CT Monitor

cesnet

Certifikáty včera, dnes a zítra

Otázky?

Jan Chvojka <jan.chvojka@cesnet.cz>
oddělení síťové identity / CESNET