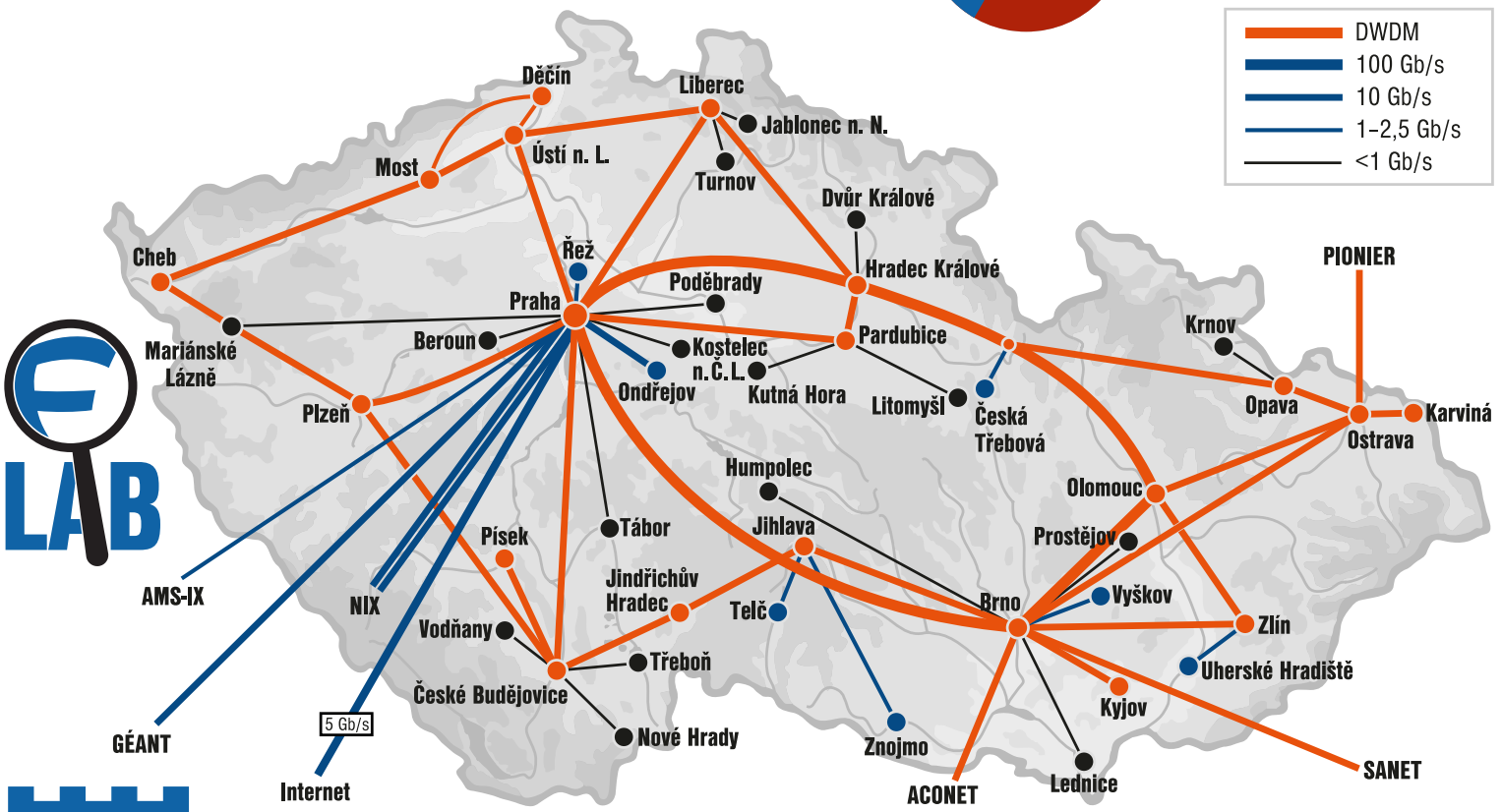
StartSSL: certifikáty zdarma

Ondřej Caletka

4. října 2014

O sdružení CESNET



Obsah

Transport Layer Security

- Nejrozšířenější standard šifrování a elektronického podpisu
- Asymetrické šifrování
- Infrastruktura veřejného klíče
- Zabezpečení internetových služeb (SSL)
- Zabezpečení e-mailové komunikace S/MIME

Infrastruktura veřejného klíče

- Hierarchický způsob *dědění* důvěryhodnosti
- Odpovídá fyzickému světu, kdy důvěryhodná autorita (např. stát) vydává certifikáty (např. OP), vázající jméno a příjmení s fotografií dotyčného člověka.
- Jiným způsobem může být síť důvěry (web of trust) známá z PGP

Pojmy z oblasti PKI ①

privátní klíč tajné číslo, umožňující rozšifrovat zprávu a vytvořit elektronický podpis

veřejný klíč číslo, umožňující zašifrovat zprávu a ověřit elektronický podpis. Lze jej vypočítat z privátního klíče

požadavek (CSR) dokument standardu PKCS#10, obsahující veřejný klíč, identifikaci subjektu a omezení využití certifikátu

certifikát podepsaný dokument standardu X.509, obsahující veřejný klíč, identifikaci subjektu a omezení využití certifikátu

Pojmy z oblasti PKI ②

cerifikační autorita instituce nebo software, který podepisuje požadavky a vytváří certifikáty

self-signed certifikát, jehož podpis byl vytvořen klíčem, jehož veřejnou část obsahuje

pevný bod důvěry certifikát, jehož věrohodnost byla ověřena jiným způsobem a je považován za důvěryhodný

řetěz důvěry sekvence podepsaných certifikátů od pevného bodu důvěry ke koncovému certifikátu

Co autority ověřují

- že entita držící certifikát opravdu existuje
  - s důkladným prověřením (Extended Validation, €€€)
  - se zběžným prověřením (Organization Validation, €€)
- že majitel certifikátu mohl v době jeho vydání ovládat doménové jméno, případně e-mailovou adresu, pro kterou byl certifikát vydán (Domain Validation, €)

Většina uživatelů nerozezná rozdíl mezi DV a OV, *někteří nepoznají ani EV.*

StartSSL.com

- nízkonákladová komerční certifikační autorita
- zařazena mezi důvěryhodné autority u Mozilly i jinde
- obchodní model reflektující náklady daného úkonu
  platí se za validaci, nikoli certifikát
- DV certifikát je možné získat zdarma

Podmínky nabídky DV zdarma (TLS)

- pouze pro nekomerční účely
- pouze pro držitele domény druhého řádu
- pouze jedno doménové jméno třetího řádu plus doména druhého řádu v jednom certifikátu
- počet certifikátů není omezen
- platnost certifikátu 1 rok
- **pozor, revokace stojí 25 $**

Podmínky nabídky DV zdarma (S/MIME)

- pro držitele libovolné e-mailové adresy
- pouze jedna e-mailová adresa v jednom certifikátu
- platnost certifikátu 1 rok
- možnost získat certifikát vystavený na skutečné jméno a příjmení po ověření dvěma notáři StartSSL Web Of Trust

Praktický postup

1. získání S/MIME certifikátu pro přihlášení k ovládacímu panelu (validace e-mailové adresy)
2. validace doménového jména (zasláním e-mailu na `hostmaster|postmaster|webmaster@doména`)
3. vygenerování žádosti
4. odeslání žádosti a vystavení certifikátu

Vygenerování žádosti

- použijte svůj oblíbený postup na vygenerování privátního klíče a žádosti
- můžete použít i generátor na webu, ale nikdo vám nezaručí, že se na webu vygenerovaný privátní klíč někam neuložil
- privátní klíč budete pravděpodobně potřebovat v rozšifrované podobě
- na jiných polích žádosti nezáleží, StartSSL je ignoruje

```
$ openssl req -newkey rsa:2048 -nodes \
> -keyout private.pem -out request.pem
```

Instalace certifikátu

- na konci procesu máme k dispozici 3 soubory:
  - privátní klíč (střežíme)
  - žádost (tu už nepotřebujeme)
  - certifikát (ten je veřejný, stáhneme ho od CA)
- navíc budeme potřebovat všechny mezilehlé certifikáty v řetězu od našeho certifikátu k pevnému bodu důvěry, v tomto případě `StartCom Class 1`
- self-signed certifikát pevného bodu důvěry obvykle není třeba (ale neškodí)
- neexistuje jednotný postup instalace certifikátu, RTFM, případně UTFG pro daný software

Příklady způsobu instalace

- 3 soubory: privátní klíč, certifikát a řetěz důvěry
  - Apache HTTP server
- 2 soubory: privátní klíč a certifikát spolu s řetězem důvěry
  - Nginx
  - Postfix
  - Dovecot
  - Prosody
- 2 soubory: privátní klíč s certifikátem a řetěz důvěry
  - Lighttpd

Certifikát není všechno

- výchozí nastavení TLS **nejsou bezpečná**
- jsou podporovány zastaralé algoritmy a krátké klíče
- není vynucováno Forward Secrecy
- skoro nikdo tomu nerozumí ☺

(Perfect-) Forward Secrecy

Klíč, kterým je symetricky šifrována relace, může být získán mnoha způsoby. Algoritmy s *forward secrecy* jsou takové, které neumožní získat klíč ani při (pozdějším) vyzrazení privátního klíče serveru.

`https://bettercrypto.org` – kuchařka s návody

HTTP Strict Transport Security

Problém: Lidé nejsou zvyklí psát URL s `https://`

- očekávají přesměrování
- náchylní na SSL striping attack (viz LD 2012)

Řešení:

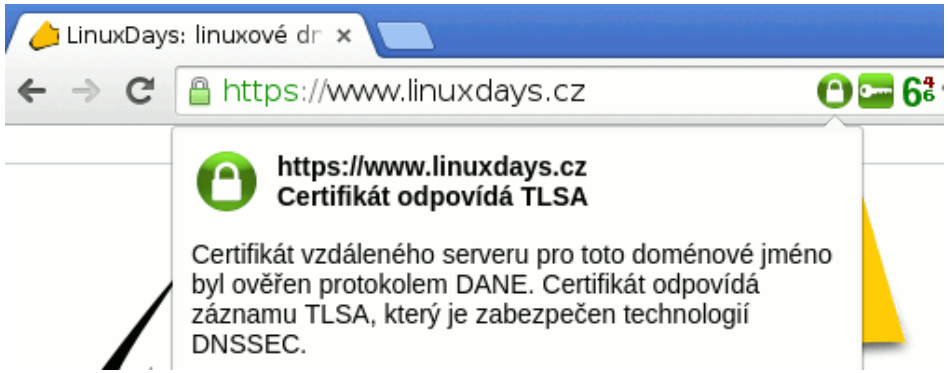
- sociální: vypnout přesměrování z `http` na `https`
- přidání hlaviček HSTS:
  - sdělí prohlížeči, že všechny další požadavky k tomuto serveru mají jít výhradně prostřednictvím `https`
  - selhání TLS validace nemůže uživatel obejít

Testujeme

- testování prohlížečem
  - pouze základní test
  - nelze zkontrolovat úplnost řetězu důvěry, prohlížeč má naučené i mezilehlé certifikáty
- testování CLI nástroji
  - `openssl s_client`
  - `gnutls-cli`
- webový tester
  - `https://www.ssllabs.com/ssltest/`

Připíchněte certifikát

- vytvořte TLSA záznamy v DNS(-SEC)
- generujte pomocí utility swede
- zvolte usage podle vašeho vztahu s CA:
  - 0 připíchnutí CA
  - 1 připíchnutí koncového certifikátu
  - 2 vložení nové CA
  - 3 vložení koncového certifikátu bez ohledu na PKI
- pro free DV certifikáty se nejvíc hodí typ 3



http://www.root.cz/clanky/pripichnete-si-ssl-certifikat-k-domene/

Závěrečné rady

- šifrování není bez obětí
  - delší trvání handshake (zvláště s FS)
  - vyšší spotřeba baterie
  - nepoužitelnost caching proxy serverů
  - nepoužitelnost webových optimalizátorů (Chrome)
- nemá smysl vynucovat TLS na nepersonalizovaných stránkách bez osobních údajů
  - špatný příklad: `http://www.linuxdays.cz`
  - správný příklad: `http://www.nebezi.cz`
  - pro absolutní odkazy používejte cestu se dvěma lomítky např. `href="//cs.wikipedia.org/"`
- vždy zkontrolujte, zda posíláte celý řetěz důvěry (nejčastější chyba)

Závěr

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz