Let’s Encrypt – pojďme šifrovat na webu zadarmo

Petr Krčmář

5. listopadu 2016

Prezentace už teď na webu

https://www.petrkrcmar.cz

Proč nasazovat HTTPS?

- HTTPS není jen pro banky a mail
- autenticita přenášených dat
- odposlech je považován za útok (RFC 7258)
- pozměňování přenosů, supercookies, malware
- ochrana osobních údajů
- zabránění únosu session cookie
- možnost nasazení HTTP/2 – výkon

Proč nasazovat HTTPS?

- HTTPS není jen pro banky a mail
- autenticita přenášených dat
- odposlech je považován za útok (RFC 7258)
- pozměňování přenosů, supercookies, malware
- ochrana osobních údajů
- zabránění únosu session cookie
- možnost nasazení HTTP/2 – výkon
- SSH je normální, proč používat telnet?


https://www.root.cz


https://www.root.cz


I'm Green!
I'm Green!
I'm Green!

Problém: důvěryhodné předání klíče

- šifrovat bezpečně asymetrickou šifrou umíme
- autentizace stejně důležitá jako silná šifra
- protistrana je pro nás ale neznámá
- problém důvěryhodného předání veřejného klíče
- nastupují autority: důvěryhodní prostředníci
- ověří žadatele, vystaví certifikát
- veřejný dokument, který obsahuje hlavně:
  - jméno autority
  - doménová jména
  - veřejný klíč žadatele
  - podpis autority
  - a další

Řetězec důvěry

- software zná kořenové certifikáty
- od serveru dostane řetězec
- certifikáty se musí vzájemně potvrzovat
- konečný certifikát potvrzuje identitu
- zároveň obsahuje veřejný klíč
- identita je potvrzena, klíč předán
- komunikace může začít
- existuje asi 1000 důvěryhodných CA
- ve skutečnosti to jsou desítky firem

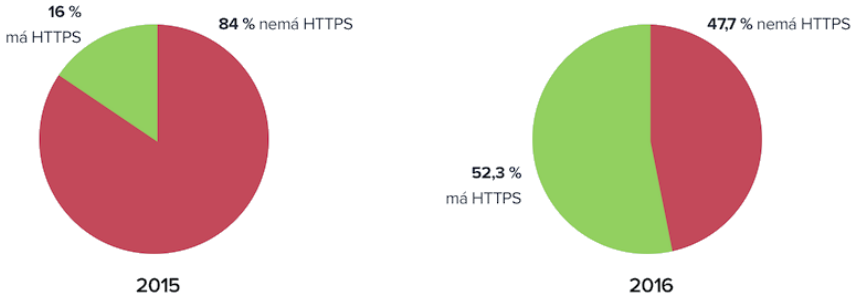
Největší překážky v nasazení

- generování klíčů a žádostí
- hledání autority
- cena certifikátu a vůbec nutnost zaplatit
- složité kolečko s ověřováním
- nutnost hlídat si platnost
- po roce až třech nutno opakovat

Největší překážky v nasazení

- generování klíčů a žádostí
- hledání autority
- cena certifikátu a vůbec nutnost zaplatit
- složité kolečko s ověřováním
- nutnost hlídat si platnost
- po roce až třech nutno opakovat

= moc práce, kašlu na to



(Studie ČeskýKošíkRoku.cz)

Let’s Encrypt

- projekt EFF, Mozilla Foundation, Akamai a Cisco Systems
- plus další partneři
- certifikační autorita
- představena v listopadu 2014
- veřejná beta běží od prosince 2015

Nicholas Bruning
@thetron

Follow

Just donated to to @letsencrypt in light of Comodo's disingenuous attempts to steal their trade marks. So, thanks Comodo? I guess? ¯_(ツ)_/¯

Vlastnosti LE

Let’s Encrypt to dělá jinak:

- **Zdarma** – stačí vlastnit doménu/ovládat server
- **Automaticky** – vše vyřídí stroje mezi sebou
- **Průhledně** – vystavení i revokace jsou zveřejněny
- **Otevřeně** – protokol i software jsou otevřené

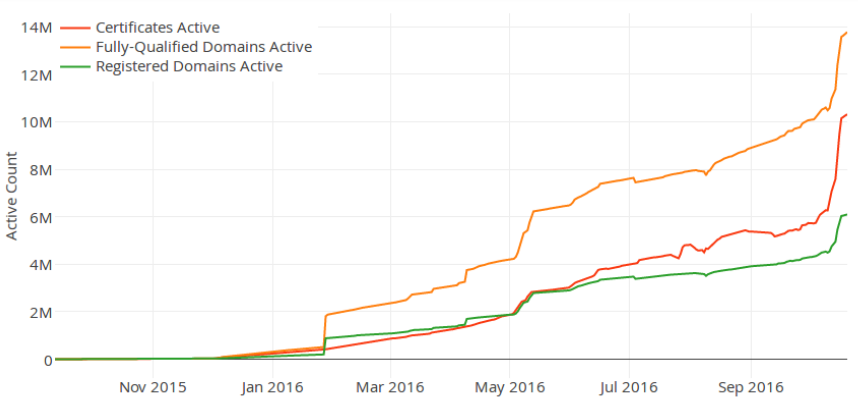
Vlastnosti LE

Let’s Encrypt to dělá jinak:

- **Zdarma** – stačí vlastnit doménu/ovládat server
- **Automaticky** – vše vyřídí stroje mezi sebou
- **Průhledně** – vystavení i revokace jsou zveřejněny
- **Otevřeně** – protokol i software jsou otevřené

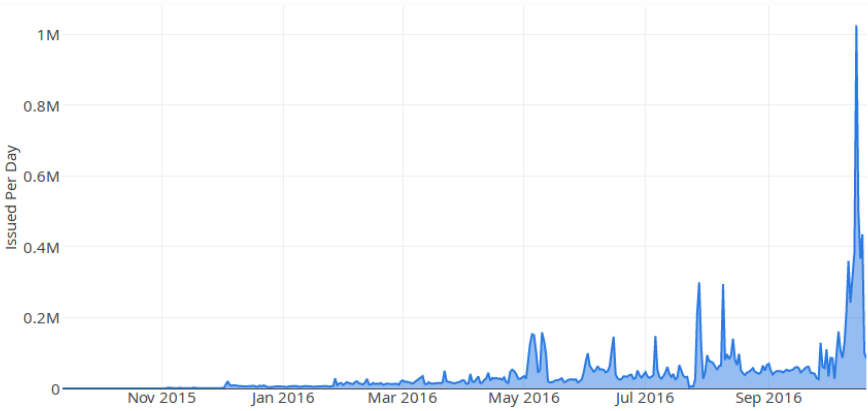
- provoz stojí 3 miliony dolarů ročně
- přispejte na provoz, pokud můžete

Počet vystavených certifikátů



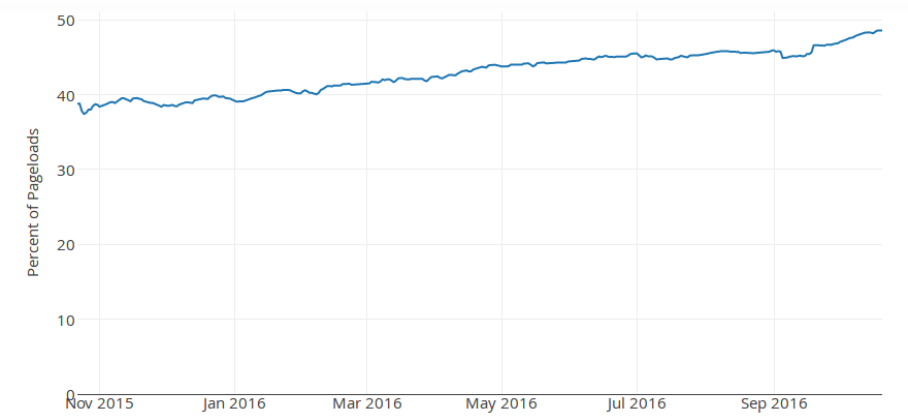
(Let’s Encrypt stats)

Denně vystavených certifikátů



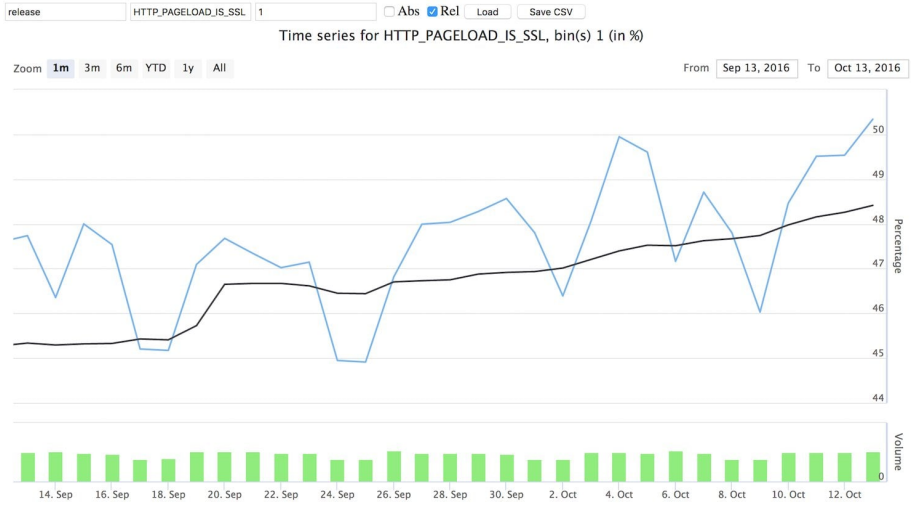
(Let’s Encrypt stats)

Podíl načtení stránek po HTTPS



(Firefox telemetry)

Jeden den nad 50 %



(Firefox telemetry, 13. října 2016)

Realita není tak růžová

- podle Google Transparency Report
- 79 ze 100 nejnavšt. webů nemá HTTPS jako výchozí
- 67 má zastaralé šifrování nebo žádné
- (první stovka tvoří 25 % provozu na webu)
- 33 % webů na první stránce Google má HTTPS
- před dvěma lety to bylo jen 7 %
- podle Alexa jen 10 % z top 1M stránek používá HTTPS
- podle BuiltWith je to asi 13 % z top 1M
- za poslední rok se čísla **zdvojnásobila**

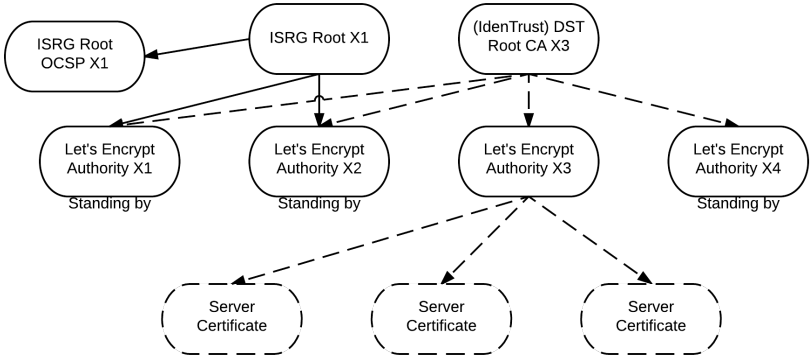
Významná data

- leden 2016 – možnost validace pomocí DNS
- únor 2016 – podpora koncových ECDSA certifikátů
- březen 2016 – nový mezilehlý X3 kvůli XP
- květen 2016 – klient přejmenován na Certbot
- červenec 2016 – plná podpora IPv6
- říjen 2016 – zapnuta podpora IDN
- březen 2017 (?) – mezilehlé ECDSA certifikáty

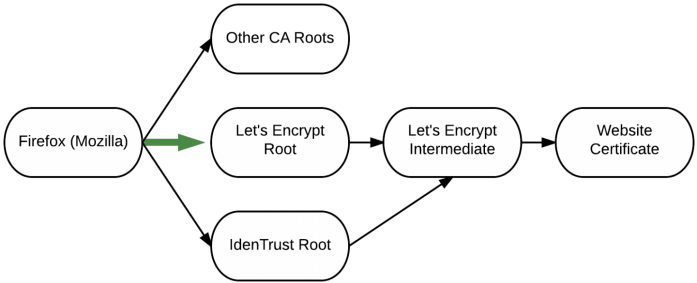
Technickou řečí

- protokol ACME
  - Automated Certificate Management Environment
  - JSON nad HTTPS
- automatické utility
- ověření pomocí výzev v /.well-known/
- nebo DNS _acme-challenge.<doménové jméno> TXT ”hex řetězec”
- vygenerujete klíč, dostanete certifikát a chain
- kořen není v prohlížečích – zatím
- cross-sign IdenTrust („DST Root CA X3“ Root CA)
- výchozí utilita konfiguruje web server
- existuje celá řada dalších implementací

Cross-signing



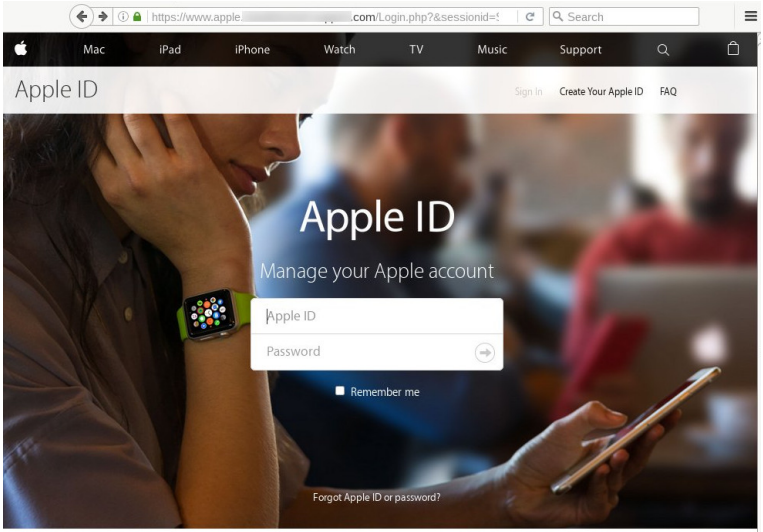
Ve Firefoxu 50



- do konce roku 2016
- Apple už do macOS přidal

Vlastnosti certifikátů

- pouze DV certifikáty
- nevystavují wildcard (hvězdička) – zatím?
- platnost 3 měsíce
- možnost SAN (Subject Alternative Name)
- limit je 100 jmen v certifikátu
- možnost kdykoliv obnovit
- možnost revokace (pokud máte klíče)
- všechny vystavené certifikáty jsou veřejné


https://www.apple
.com/Login.php?&sessionid=
Search
Mac
iPad
iPhone
Watch
TV
Music
Support
Apple ID
Sign In
Create Your Apple ID
FAQ
Apple ID
Manage your Apple account
Apple ID
Password
Remember me
Forgot Apple ID or password?

Sliby – chyby

- MIME typ `application/jose+json`
- důkaz držení předchozího klíče při změně CA
- sekvenční číslování certifikátů
- zveřejňování logů ACME komunikace
- veřejný blaclist doménových jmen

Pozor na rate limiting

- v srpnu byly výrazně uvolněny
- 100 jmen v certifikátu
- 20 žádostí v jedné doméně (SLD) za týden
- 5 duplicitních (se stejnými doménami) certifikátů za týden
- **revokace neresetuje limity**
- 500 registrací z jedné IP za 3 hodiny
- 300 nedokončených žádostí za týden – pro vývojáře
- existuje testovací (staging) prostředí bez limitů

Kompatibilita s klienty

- Požadavky: DST Root CA X3 a SHA-2
- Funguje to:
  - Firefox a Thunderbird >= 2.0 (od roku 2008)
  - Chrome všechny
  - Windows >= XP SP3
  - Android >= 2.3.6
  - iOS >= 3.1, Safari na macOS (= 4.0)
  - distribuce (Debian 6, Ubuntu 12.04)
  - Java JDK >= 8u101
  - Pidgin od verze 2.11.0
- Nefunguje to:
  - Blackberry OS (až od 10.3.3 ?)
  - Android < 2.3.6 (méně než 2 %)
  - Windows XP před SP3 (nemá SHA-2)
  - Java < JDK 8u101

Klienti

- Certbot – oficiální klient, maximální automatika
- letsencrypt-nosudo – jednodušší a malý (jeden soubor)
- letsencrypt_simpleclient – knihovna v Pythonu
- acme-tiny – jen 200 řádků kódu
- simp_le – jednoduchý, bezestavový, trochu automatický
- tyhle jsou v Pythonu ↑
- acme.sh – jeden soubor v shellu
- existují v PHP, Go, Ruby, .NET, Rust, Java, Node.js...
- dokonce i ve webovém prohlížeči
- viz gethttpsforfree.com
- některé aplikace integrují: Caddy, Own-Mailbox, Cloudfleet...
- seznam klientů je v dokumentaci Let's encrypt

Nasazení s ACME.sh v Nginx

- jednoduchý klient acme.sh
- napsaný čistě v shellu (bash, dash, sh)
- umí vše: web, DNS, obnovení, revokace...
- samostatný uživatel letsencrypt
- Nginx směruje dotazy na challenge do home

Konfigurace Nginx

```
location ^~ /.well-known/ {
                root /home/letsencrypt/webroot/;
        }
```

Spuštění příkazu

- stačí požádat jedním příkazem

Žádost

```
$ .acme.sh/acme.sh --issue -d example.com  -w /home/letsencrypt/webroot/ \
-d www.example.com -d blog.example.com -d forum.example.com \
--reloadcmd "sudo /etc/init.d/nginx reload"
```

- skript s parametrem `--install` instaluje cronjob
- testuje stáří certifikátu (> 60 dnů) a obnoví

Cronjob

```
0 0 * * * "/home/letsencrypt/.acme.sh"/acme.sh --cron \
--home "/home/letsencrypt/.acme.sh" > /dev/null
```

Konfigurace Nginx

Do kontextu server

```
ssl_certificate /home/letsencrypt/.acme.sh/example.com/fullchain.cer;
ssl_certificate_key /home/letsencrypt/.acme.sh/example.com/example.com.key;
```

Konfigurace Nginx

Do kontextu server

```
ssl_certificate /home/letsencrypt/.acme.sh/example.com/fullchain.cer;
ssl_certificate_key /home/letsencrypt/.acme.sh/example.com/example.com.key;
```

Pozor na správný řetězec! Zkontrolujte to!

Čím to otestovat?

- SSL Labs Test – velmi podrobný test
- SSL Decoder – vypíše všechny detaily o certifikátech
- Symantec CryptoReport – protokoly, chyby, díry
- GeoCerts SSL Checker – ukazuje řetězec
- COMODO SSL Analyzer – a ještě jeden
- gcr-viewer v balíčku gnome-keyring

```
openssl s_client -showcerts -connect www.root.cz:443 < \
/dev/null | openssl x509 -outform DER > cert.der
```

Jak to ještě vylepšit: hlavička HSTS

- HTTP Strict Transport Security (HSTS)
- hlavička v HTTP odpovědi (RFC 6797)
- tento web musí mít vždy důvěryhodný certifikát
- prohlížeč sám přepíše http:// na https://
- TOFU = Trust On First Use

Jak to ještě vylepšit: hlavička HSTS

- HTTP Strict Transport Security (HSTS)
- hlavička v HTTP odpovědi (RFC 6797)
- tento web musí mít vždy důvěryhodný certifikát
- prohlížeč sám přepíše http:// na https://
- TOFU = Trust On First Use

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

Jak to ještě vylepšit: hlavička HSTS

- HTTP Strict Transport Security (HSTS)
- hlavička v HTTP odpovědi (RFC 6797)
- tento web musí mít vždy důvěryhodný certifikát
- prohlížeč sám přepíše http:// na https://
- TOFU = Trust On First Use

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

- možno i HSTS preload
- chrome://net-internals/#hsts
- rozšíření HTTPS Everywhere

Jak to ještě vylepšit: hlavička HPKP

- HTTP Public Key Pinning (HPKP)
- hlavička obsahující hashe klíčů (RFC 7469)
- klient se je naučí a očekává je
- možno více klíčů, ale minimálně dva
- jeden **musí** ležet v cestě, druhý **nesmí**
- alespoň jeden je vždy záložní

Jak to ještě vylepšit: hlavička HPKP

- HTTP Public Key Pinning (HPKP)
- hlavička obsahující hashe klíčů (RFC 7469)
- klient se je naučí a očekává je
- možno více klíčů, ale minimálně dva
- jeden **musí** ležet v cestě, druhý **nesmí**
- alespoň jeden je vždy záložní

```
Public-Key-Pins: max-age=5184000;
  pin-sha256="WoiWRyIOVNa9ihaBciRSC7XHjliYS9VwUGOIud4PB18=";
  pin-sha256="RRM1dGqnDFsCJXBTHky16vi1obOlCgFFn/yOhI/y+ho=";
  pin-sha256="k2v657xBsOVe1PQRwOsHsw3bsGT2VzIqz5K+59sNQws=";
  pin-sha256="K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q=";
  pin-sha256="IQBnNBEiFuhj+8x6X8XLgh01V9Ic5/V3IRQLNFFc7v4=";
  pin-sha256="iie1VXtL7HzAMF+/PVPR9xzT80kQxdZeJ+zduCB3uj0=";
  pin-sha256="LvRiGEjRqfzurezaWuj8Wie2gyHMrW5Q06LspMnox7A=";
  includeSubDomains
```

Jak to ještě vylepšit: DANE/TLSA

- DNS-based Authentication of Named Entities (DANE)
- přidává TLSA záznam do DNS (RFC 6698)
- podobné jako HPKP, ale v doméně
- záznamy jsou podepsané DNSSEC
- nezávislý kanál pro ověření klíče
- ověření proběhne ještě před TLS (odpadá TOFU)
- umí vložit nový bod důvěry nebo přímo koncový otisk

Jak to ještě vylepšit: DANE/TLSA

- DNS-based Authentication of Named Entities (DANE)
- přidává TLSA záznam do DNS (RFC 6698)
- podobné jako HPKP, ale v doméně
- záznamy jsou podepsané DNSSEC
- nezávislý kanál pro ověření klíče
- ověření proběhne ještě před TLS (odpadá TOFU)
- umí vložit nový bod důvěry nebo přímo koncový otisk

```
$ dig +short _443._tcp.www.root.cz tlsa
3 1 1 5ABAD14B64277B28E1DE7550548A4EE4A09DF18A0584963A360F0DD0 F98D9686
```

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz