Certifikáty, šifry a klíče aneb jak nasadit HTTPS

Petr Krčmář

21. dubna 2018

Uvedené dílo (s výjimkou obrázků) podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

Prezentace už teď na webu

https://www.petrkrcmar.cz

Co je to HTTPS?

- přenos protokolu HTTP v šifrovaném TLS tunelu
- provoz běží po TCP portu 443
- data jsou přenášena šifrovaně a autentizovaně
- pro sestavení kanálu se používá asymetrická kryptografie
- k potvrzení identity se využívají **certifikáty**
- pro šifrování se používá symetrická kryptografie

Před čím chrání HTTPS?

- před síťovými útoky (věříte zdejší Wi-Fi?)
- před odposlechem komunikace (RFC 7258 – odposlech je útok)
- před man-in-the-middle – víme, s kým komunikujeme
- před blokováním části obsahu (Wikipedie)
- před pozměňováním dat během přenosu
- před vkládáním supercookies, malware, trackovacích kódů
- před únikem osobních údajů – nechcete e-shop bez HTTPS
- před únosemu session cookie – při přihlašování

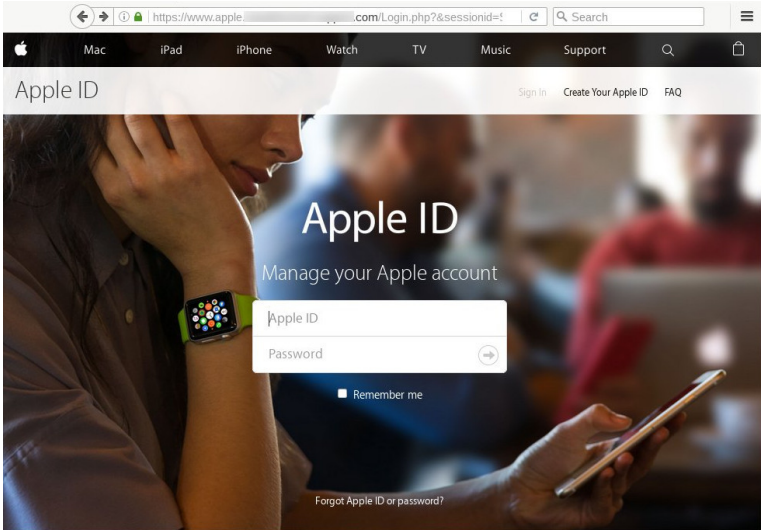
Před čím chrání HTTPS?

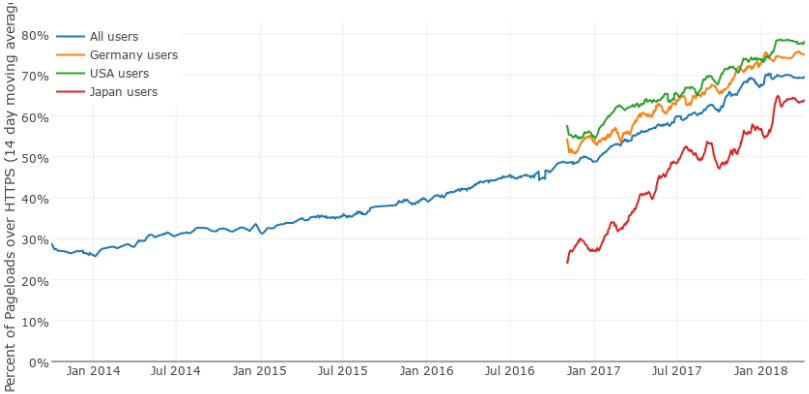
- před síťovými útoky (věříte zdejší Wi-Fi?)
- před odposlechem komunikace (RFC 7258 – odposlech je útok)
- před man-in-the-middle – víme, s kým komunikujeme
- před blokováním části obsahu (Wikipedie)
- před pozměňováním dat během přenosu
- před vkládáním supercookies, malware, trackovacích kódů
- před únikem osobních údajů – nechcete e-shop bez HTTPS
- před únosemu session cookie – při přihlašování
- příjemný bonus: možnost nasazení HTTP/2 – výkon (http2demo.io)
- používá 25 % webů (podle W3Techs)

Zařízení značky Sandvine (dnes Procera)
(Root.cz: Vlády přesměrovávají uživatele na software doplněný o malware)

Před čím HTTPS nechrání?

- před únikem informací o doméně (DNS, SNI)
- před sběrem metainformací (netflow, IP…)
- před phishingovými weby
- před blokováním provozu na síťové vrstvě
- před útokem na legitimního provozovatele webu (XSS, SQL…)
- před zlými úmysly autora webu


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?



- 70 % stránek načteno po HTTPS, v USA dokonce 78 %
- 81 ze 100 největších webů má HTTPS (před rokem jen 37!)

Problém: důvěryhodné předání klíče

- šifrovat bezpečně asymetrickou šifrou umíme
- protistrana je pro nás ale neznámá
- autentizace stejně důležitá jako silná šifra
- bez ní se kdokoliv může vydávat za kohokoliv
- problém důvěryhodného předání veřejného klíče
- nastupují autority: důvěryhodní prostředníci
- ověří žadatele, vystaví certifikát


EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS
EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS
EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS
EVROPSKÁ UNIE
ČESKÁ REPUBLIKA
CESTOVNÍ
PAS

Certifikát je internetový pas

- pas propojuje fotografii obličeje se jménem
- certifikát propojuje doménové jméno s veřejným klíčem
- server se prokazuje: toto je potvrzení o mém klíči
- pas vystavují jen důvěryhodné státy
- certifikáty vystavují důvěryhodné autority
- celník ověří totožnost na základě dokumentu známého státu
- prohlížeč ověří identitu na základě dokumentu známé autority
- důvěryhodné autority a jejich klíče jsou předinstalované v software
- to celé ↑ se jmenuje PKI (Public Key Infrastructure)

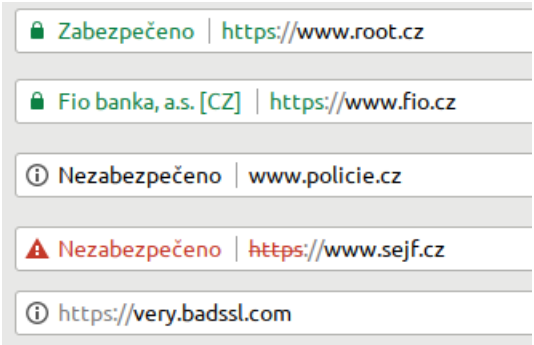
Co je to certifikát?

- **veřejný** dokument, který obsahuje hlavně:
  - jméno autority
  - doménová jména
  - veřejný klíč žadatele
  - datum platnosti
  - podpis autority
  - a další
- elektronický podpis = nezfalšovatelné
- ověříme pomocí známého veřejného klíče v software
- certifikát **není tajemstvím**, chráníme privátní klíč

Tři druhy certifikátů

- **EV** – Extended Validation
  - velmi drahý, důkladné ověření identity žadatele
  - signalizace zeleným názvem vedle adresy
  - nesmí obsahovat wildcard (hvězdičku)
  - nemůžou vydávat všechny autority
- **OV** – Organzation Validation
  - levnější varianta, zběžné prověření idenity žadatele
  - v prohlížeči nemá speciální označení
- **DV** – Domain control Validation
  - velmi levné vystavení, lze automatizovat
  - jen kontrola doménového jména
  - není nijak svázán s identitou žadatele
  - nejběžnější typ certifikátu
- max. platnost všech je 825 dnů (přibližně 27 měsíců)

ROOT.CZ vpsFree.cz

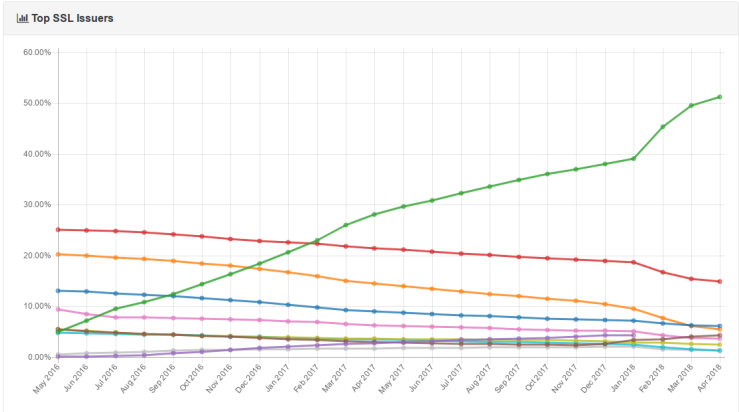

Zabezpečeno | https://www.root.cz
Fio banka, a.s. [CZ] | https://www.fio.cz
Nezabezpečeno | www.policie.cz
Nezabezpečeno | https://www.sejf.cz
https://very.badssl.com

Řetězec důvěry

- software zná kořenové certifikáty s veřejným klíčem autority
- od serveru dostane řetězec – delegace pravomocí autority
- certifikáty se musí vzájemně potvrzovat
- konečný certifikát potvrzuje identitu žadatele (serveru)
- zároveň obsahuje veřejný klíč
- identita je potvrzena, klíč předán protistraně
- komunikace může začít
- existuje asi 1000 důvěryhodných CA
- ve skutečnosti je to asi 60 firem
- nedodání mezilehlých → velmi častá chyba

Let’s Encrypt

- projekt EFF, Mozilla Foundation, Akamai a Cisco Systems
- představena v listopadu 2014, beta od prosince 2015
- od dubna 2016 v ostrém provozu



#	SSL Issuer	Percentage
1	Let's Encrypt	51.21%
2	COMODO CA Limited	14.82%
3	GoDaddy.com	6.14%
4	GeoTrust Inc.	5.5%

(NetTrack.info)

Vlastnosti Let’s Encrypt

Let’s Encrypt to dělá jinak:

- **zdarma** – stačí vlastnit doménu/ovládat server
- **automaticky** – vše vyřídí stroje mezi sebou
- **průhledně** – od začátku všechny certifikáty zveřejňuje
- **otevřeně** – protokol i software jsou otevřené

Vlastnosti Let’s Encrypt

Let’s Encrypt to dělá jinak:

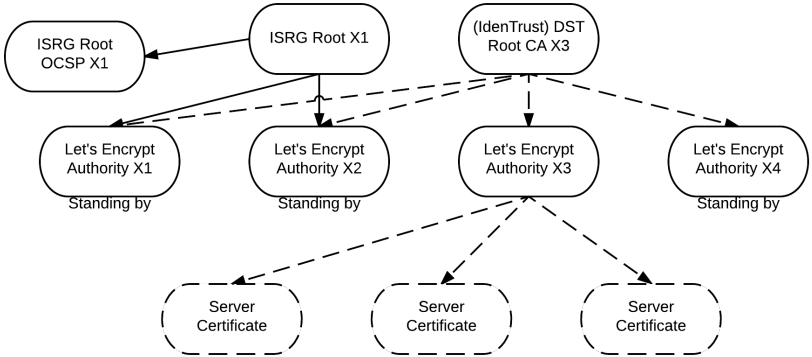
- **zdarma** – stačí vlastnit doménu/ovládat server
- **automaticky** – vše vyřídí stroje mezi sebou
- **průhledně** – od začátku všechny certifikáty zveřejňuje
- **otevřeně** – protokol i software jsou otevřené

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

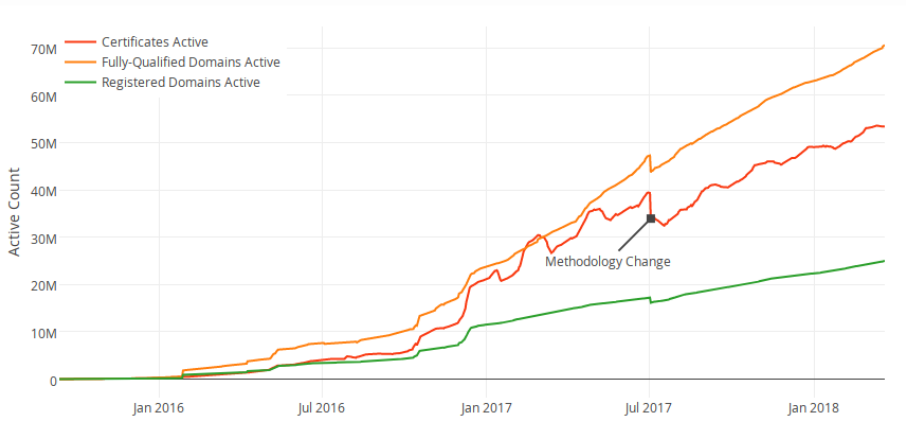
Vlastnosti certifikátů Let’s Encrypt

- pouze DV certifikáty
- ověření pomocí HTTP nebo DNS
- platnost certifikátu 90 dnů
- možno až 100 doménových jmen v SAN
- nově také wildcard (ale jen DNS ověření)
- kořenový certifikát zatím jen ve Firefoxu (50+)
- možnost certifikáty revokovat
- všechny vystavené certifikáty jsou veřejné
- využívá kořenové autority IdenTrust

Cross-signing



Počet vystavených certifikátů



(Let’s Encrypt stats)

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
- cross-sign IdenTrust („DST Root CA X3“ Root CA)
- výchozí utilita Certbot konfiguruje web server
- existuje celá řada dalších implementací (ACME.sh, Dehydrated…)
- část software integruje (Caddy, mod_md pro Apache…)

Pozor na rate limiting

- 20 žádostí v jedné doméně (SLD) za týden
- na obnovení certifikátu je výjimka
- 5 duplicitních (se stejnými doménami) certifikátů za týden
- **revokace neresetuje limity**
- 300 nedokončených žádostí za týden – pro vývojáře
- 100 doménových jmen v certifikátu
- existuje testovací (staging) prostředí s mnohem vyššími limity
- viz Let’s Encrypt rate limits

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

Funguje to celé (?)

- tohle celé funguje skvěle

Funguje to celé (?)

- tohle celé funguje skvěle
- až na případy, kdy to selhává

Funguje to celé (?)

- tohle celé funguje skvěle
- až na případy, kdy to selhává
- autority jsou „univerzálně důvěryhodné“
- kdokoliv vystavuje cokoliv
- DigiNotar, Thawte, Symantec, WoSign…
- technická chyba, omyl, útok, státní zájmy
- řetěz je silný jako nejslabší článek
  - bezpečnost neurčuje nejlepší, ale nejhorší
  - jedno shnilé jablko zničí celý košík

(Jason Bourne's Passports Prop Replicas)

Provozovatelé se bojí

- provozovatelé služeb se bojí
- PKI je jedinou ochranou
- robustní, ale stojí na bezpečnosti autorit
- pokud selže, může se kdokoliv vydávat za kohokoliv
- typicky Google, Microsoft, Apple, GitHub...
- ukradení přihlašovacích údajů, odposlech
- vkládání vlastních informací
- platný certifikát = internetová identita

Řešení = transparentnost

- donutit autority zveřejňovat **všechny** certifikáty
- možnost monitoringu i zpětného auditu
- pokud někdo vydá neoprávněně, můžu reagovat
- spustím poplach, můžu revokovat
- mám přehled o všech vydaných certifikátech
- autority se dostávají pod veřejnou kontrolu
- hlídám své domény, kdokoliv hlídá cokoliv

Certificate Transparency

- veřejné logy pro ukládání certifikátů
- lze do nich jen přidávat (Merklův hashový strom)
- kdokoliv je může mirrorovat a prohledávat v nich
- kdokoliv může přidávat certifikáty
- kvůli ochraně ale pouze od uznávaných CA
- odstranění certifikátu je detekovatelné
- není možné antedatovat certifikáty
- monitor – kontroluje logy a hledá problémy
- auditor – kontroluje konkrétní certifikát (prohlížeč)
- definováno v RFC 6962

Historie a budoucnost

- první log spustil Google v březnu 2013
- v září 2013 začala první CA vkládat (DigiCert)
- od 1. ledna 2015 vyžaduje Chrome pro EV
  - přítomnost alespoň ve dvou lozích
- od 1. června 2016 vyžaduje u všech od Symantec
- od 30. dubna 2018 bude **vyžadováno u všech**
- původně to měl být už říjen 2017
- Firefox oznámil podporu, ale bez termínů

Jak autority donutit

- bude fungovat, jen když to budou dělat všichni
- musí existovat donucovací mechanismus
- je zabudován do prohlížeče
- prohlížeč zkontroluje že je certifikát v logu
- (vedle data platnosti, domény a podobně)
- jen takový certifikát bude důvěryhodný
- technicky se vynutí zveřejňování certifikátů

Klient se neptá

- klienti se sami ptát nebudou
- to by neškálovalo a unikaly by informace
- důkazní břemeno je na serveru, který certifikát předává
- ten musí doložit, že je certifikát v logu
- ideálně ho vloží už CA, ale může i sám
- log vydává Signed Certificate Timestamp (SCT)
  - příslib budoucího zařazení certifikátu do stromu
  - server musí klientovi doručit i SCT

Tři způsoby doručení

1. OCSP stapling
   - složité a nespolehlivé (umí prohlížeč OCSP?)
   - server i autorita musí spolupracovat
   - autorita získá SCT a vloží do OSCP responderů
   - server musí podporovat stapling
   - s OCSP zprávou předává i SCT

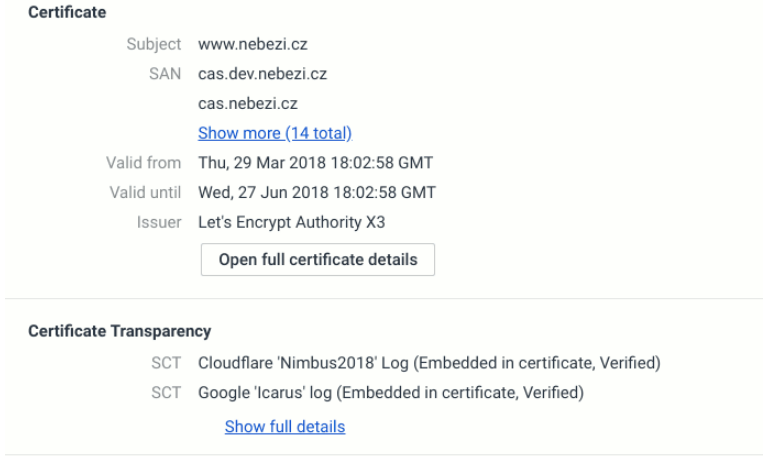
Tři způsoby doručení

1. OCSP stapling
   - složité a nespolehlivé (umí prohlížeč OCSP?)
   - server i autorita musí spolupracovat
   - autorita získá SCT a vloží do OSCP responderů
   - server musí podporovat stapling
   - s OCSP zprávou předává i SCT
2. rozšíření TLS
   - server pošle certifikát a získá SCT
   - změní konfiguraci web serveru (podpora?)
   - rozšíření TLS signed_certificate_timestamp

Tři způsoby doručení

1. OCSP stapling
   - složité a nespolehlivé (umí prohlížeč OCSP?)
   - server i autorita musí spolupracovat
   - autorita získá SCT a vloží do OSCP responderů
   - server musí podporovat stapling
   - s OCSP zprávou předává i SCT
2. rozšíření TLS
   - server pošle certifikát a získá SCT
   - změní konfiguraci web serveru (podpora?)
   - rozšíření TLS signed_certificate_timestamp
3. rozšíření certifikátu
   - nulová zátěž na provozovatele serveru
   - vše zařídí CA, pošle do logu, získá SCT
   - SCT je pak přímo součástí certifikátu

ROOT.CZ vpsFree.cz


Certificate
Subject www.nebezi.cz
SAN cas.dev.nebezi.cz
cas.nebezi.cz
Show more (14 total)
Valid from Thu, 29 Mar 2018 18:02:58 GMT
Valid until Wed, 27 Jun 2018 18:02:58 GMT
Issuer Let's Encrypt Authority X3
Open full certificate details
Certificate Transparency
SCT Cloudflare 'Nimbus2018' Log (Embedded in certificate, Verified)
SCT Google 'Icarus' log (Embedded in certificate, Verified)
Show full details

Současný stav logů

- v tuto chvíli je v Chrome uznáváno 27 logů od 10 firem
- Certly, DigiCert, Comodo, Google, Cloudflare...
- jsou různé velké (statisíce až desetimiliony certů)
- Google uvádí, že je v nich přes 1,3 miliardy záznamů
- infrastruktura se bude časem zahušťovat
- Google nabízí i webové rozhraní
- případně vyhledávače třetích stran jako crt.sh
- další info na www.certificate-transparency.org

Kde to uvidím?

- Chrome devtools → Security → Main origin
- chrome://net-internals „signed_cert…“
- na webu crt.sh
- Certspotter služba, GitHub
- pomocí řady nástrojů a knihoven
- OpenSSL má od verze 1.0.2 podporu pro SCT
- Facebook má vlastní monitoring posílající maily

Otázky?

Petr Krčmář
petr.krcmar@iinfo.cz