

Budoucnost TLS certifikátů

přichází další doba zkracování

Petr Krčmář



5. dubna 2025



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

O mně

- linuxák od roku 1998
- správce serverů
- lektor a konzultant
- šéfredaktor [Root.cz](#)
- člen [vpsFree.cz](#)
- organizátor [LinuxDays](#)
- můj web je [petrkrcmar.cz](#)



Pár slov o certifikátech

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



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 authority
- celník ověří totožnost na základě dokumentu známého státu
- prohlížeč ověří identitu na základě dokumentu známé authority
- důvěryhodné authority 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

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

O revokacích

Předčasné zneplatnění

- někdy potřebujeme předčasně zneplatnit certifikát
 - unikl nám soukromý klíč
 - prodali jsme doménu
 - chceme změnit algoritmus
 - v certifikátu jsou chyby
 - ztratili jsme důvěru v autoritu
 - chyba autority – třeba chybná vystavení
- musíme tedy provést **revokaci** – oznámit dřívější neplatnost
 - ještě před vypršením obvyklé platnosti v certifikátu
 - oznamujeme všem, že tenhle certifikát neplatí
 - klient musí informaci dostat a zařídit se podle ní
- problém: jak informaci bezpečně zveřejnit?
 - klient ji musí dostat včas
 - zároveň ho to nesmí příliš zatěžovat
 - nesmějí unikat data, kdo se kam připojuje

- Certificate Revocation List – seznamy revokovaných certifikátů
- historicky první způsob revokace (květen 1999)
- autorita zveřejňuje seznam **všech** zneplatněných certifikátů
 - seznam obsahuje informace o certifikátech a je podepsaný klíčem autority
 - klient si seznamy pravidelně stahují od autorit
- **neškáluje** to – certifikátů přibývá a seznamy rostou
 - CRL se všemi certifikáty od Let's Encrypt by měl 8 GB
 - tohle nechcete pravidelně stahovat na mobilu

- Online Certificate Status Protocol – zjišťování stavu certifikátu
- modernější varianta (únor 2002)
- autorita provozuje **odpovědače** (responder), kterých se ptáme
 - odpovědí je stav certifikátu: platný, neplatný nebo neznámý
 - doplněna je platnost odpovědi mezi 8 hodinami a 10 dny
- když je ale odpovídač **nedostupný** – zamítnout či ignorovat?
 - zamítnutí dává prostor k DoS a zhoršuje chyby
 - ignorování umožňuje útočnickovi OCSP obejít
 - většina klientů ale ignoruje
- problémy se soukromím – klienti předávají informace autoritě
 - informaci může zjišťovat sám server (OCSP stapling)
 - ostatní problémy ale zůstávají

- existují další návrhy alternativních řešení
 - nejsou ale rozšířené mezi klienty
- CRLite
 - „komprese“ informací pomocí Bloomova filtru
 - provozovatel posbírání CRL a udělá menší verzi
- Let's Revoke
 - autorita vytvoří bitovou mapu certifikátů
 - uživatelé si ji stahují nebo jim je autorita posílá

Revokace jsou rozbité

- revokace jsou prostě **rozbité**
- neexistuje způsob, jak spolehlivě dostat informace k uživatelům
- Chrome má vlastní způsob, sám si distribuuje seznamy
 - nejsou tam ale všechny, jen výběr těch důležitých
- jiným řešením je krátká platnost certifikátů
 - dlouhodobý trend = postupné zkracování platnosti
- Let's Encrypt před deseti lety přišel s 90 dny
 - tenkrát naprosto předběhl dobu

- Certification Authority Browser Forum nebo CA/Browser Forum
- **dobrovolné** komunitní konsorcium organizací spojených s PKI
 - certifikační autority (57 členů)
 - tvůrci software s podporou PKI (13 členů)
 - asociace (9 členů)
 - ostatní (26 členů)
- založeno 2005, vytváří směrnice pro práci s TLS certifikáty
- skládá se z pracovních skupin
 - serverová pracovní skupina – základní pravidla
 - skupina pro podepisování kódu
 - S/MIME – podepisování elektronické pošty
- jde o nastavení jednotných pravidel napříč trhem
 - vše je ale dobrovolné a jde o důvěru
 - tvůrci prohlížečů mají typicky silnější slovo

Platnost v minulosti

Pravěk aneb deset a více let

- v pradávných dobách nebylo nastaveno **žádné omezení**
- v roce 2008 vystavovaly autority certifikáty klidně na deset let
- první omezení přišlo v roce **2012**
 - CA/B Fórum se dohodlo na platnosti 60 měsíců
 - prohlížeče nepřijímaly certifikáty s delší platností
- tato změna ale není retroaktivní (zpětně účinná)
 - to platí i pro další podobné úpravy
 - starší certifikáty tedy platí i dál
 - klidně dalších deset let či více
- autority ale nesmějí antedatovat vydávání certifikátů
 - byla u toho přistižena autorita WoSign – přišla o důvěru

Na tři a dva roky

- už v roce **2015** byla znovu hranice stanovena na 39 měsíců
 - tedy na tři a čtvrt roku
- v roce 2017 byl podán návrh na další zkrácení
 - návrh počítal s 398 dny, tedy pouhým rokem a jedním měsícem
 - neprošel, prakticky všechny authority byly proti (krom Let's Encrypt)
- později v roce 2017 prošel návrh na 825 dnů – pro byli všichni
 - zkrácení na dva a čtvrt roku
 - vstoupil v platnost v březnu **2018**

- původní návrh z roku 2017 se ale vracel
- v roce 2019 byl podán znovu – pro jen třetina
 - některé authority ale začaly zkracovat dobrovolně
- v roce **2020** do toho ale sekl Apple a rozhodl sám
 - od 1. září 2020 omezí Safari platnost na 398 dnů
 - ostatní tvůrci prohlížečů se pak samozřejmě přidali
- v září 2020 pak tuto změnu zavedlo do požadavků i CA/B Fórum
 - tomu se říká sebenaplňující se proroctví
- tak to máme doposud
 - certifikát může mít maximální platnost rok a měsíc

Další zkracování

Už se to vaří

- Google už delší dobu hlásá chuť na další zkrácení
 - chce tím řešit problémy s revokacemi
 - zároveň ulehčit obrovským databázím Certificate Transparency
- původně chtěl navrhnout postupné zkrácení na 90 dnů
- může to docela dobře **protlačit silou**
 - ostatní tvůrci prohlížečů (Apple, Mozilla, Microsoft) se přidají
 - pak se to už jen dodatečně schválí
- Google měl návrh podat v září/říjnu 2024
- nakonec to neudělal, ale zařídil to někdo jiný

Apple opět na scéně

- návrh podal Apple, 9. října 2024
 - přidala se k němu autorita Sectigo (dříve Comodo)
- návrh počítá s **postupným** zkracováním platnosti
 - po 15. září 2025 maximální platnost 200 dnů
 - po 15. září 2026 maximální platnost 100 dnů
 - po 15. dubnu 2027 maximální platnost 45 dnů
- tento návrh je pozvolnější, ale nakonec přísnější
 - proti původnímu návrhu se má dojít na poloviční platnost
 - to by ovlivnilo i Let's Encrypt, který má 90 dnů

Jak a kdy to tedy bude?

- návrh se chvíli diskutoval a padaly drobné úpravy
- aktuální stav návrhu je [vidět na GitHubu](#)
- další diskuse už ale neprobíhá
- předpokládá se, že v této podobě bude návrh předložen k hlasování
- výsledek hlasování bude záviset na hlasech autorit
 - autorita Sectigo stále tvrdí, že bude hlasovat pro
- možná ještě letos zkrátíme na **200 dnů**

Dobrovolně ještě kratší

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
- 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

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
- 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
- přispějte na provoz, pokud můžete

Platnost u Let's Encrypt

- od začátku platnost certifikátu 90 dnů
 - možno až 100 doménových jmen v SAN
 - umí wildcard (ale jen DNS ověření)
- vždy deklarovala, že bude spíše zkracovat
 - nutí tím uživatele automatizovat
 - je to levnější, bezpečnější, stabilnější

- Let's Encrypt na letošní rok plánuje **šestidenní** certifikáty
 - dobrovolně o ně můžete požádat přes ACME
 - výchozí zůstane stále 90denní certifikát
- umožní to podpora „profilů“
 - možnost nastavit různé vlastnosti certifikátů
 - zatím varianty: classic, tlserver a shortlived
- v únoru byl vystaven první testovací krátkodobý certifikát
 - v dubnu se zapojí vybraní testeři, ke konci roku pro všechny
- tyto certifikáty bude možné vystavit i na veřejné **IP adresy**
 - ale jen přes HTTP nebo ALPN, pochopitelně ne přes DNS
 - hodí se třeba pro DDR (Discovery of Designated Resolvers)

- Certifikát na tři roky už si nepořídíte, maximální platnost se zkrátila na dva
- Zkrácení platnosti certifikátů na 13 měsíců se nekoná, autority jsou proti
- Maximální délka platnosti HTTPS certifikátů bude zkrácena na 1 rok
- Google chce omezit platnost certifikátů na 90 dnů, změna zřejmě přijde brzy
- Let's Encrypt příští rok nabídne certifikáty se šestidenní platností
- Let's Encrypt bude vystavovat certifikáty na IP adresy
- Let's Encrypt představil možnost výběru profilu certifikátu v protokolu ACME

Otázky?



Petr Krčmář
petr.krcmar@iinfo.cz