**Proč by měl každý web mít SSL certifikát?**

**Bezpečnost na internetu je čím dál větší téma, a není divu. Uživatelé často provozovatelům webových stránek sdělují velmi citlivé informace - platebními údaji začínaje, datem narození konče. Aby se tato data nedostala k někomu nepovolanému, měl by každý web používat SSL certifikát, který zajistí nejen jeho bezpečnost a důvěryhodnost, ale také třeba lepší pozice ve vyhledávačích.**

Při brouzdání na internetu proudí mezi vaším prohlížečem a webovými stránkami, které navštívíte, velké množství informací. Jedná se o prakticky veškerý obsah, který se na stránce nachází, ale také data o tom, co na ní děláme. SSL (Secure Sockets Layer) protokoly se starají o to, aby tato komunikace byla bezpečná.

Protokoly SSL zajišťují identifikaci klienta a serveru - obě strany si tak mohou být jisty, že komunikace probíhá skutečně jen mezi nimi, nikoliv s někým nevyžádaným, kdo se vydává za jednu ze stran, aby například ukradl uživatelské jméno a heslo. Dalším jejich důležitým úkolem je šifrování komunikace pomocí jednorázových digitálních klíčů. Ty laicky řečeno "odemykají" data mezi klientem a serverem tak, aby se k nim nedostal nikdo jiný.

To, zda webová stránka používá některý z SSL protokolů, lze poznat jednoduše - jeho adresa nezačíná zkratkou HTTP, nýbrž HTTPS (Hypertext Transfer Protocol Secure). Pokud zabrousíte na web s prvně zmíněným (tedy nezabezpečeným) protokolem, znamená to, že cokoliv zadáte do prohlížeče, si může kdokoliv (a tím myslíme opravdu kdokoliv) přečíst. Prohlížeče jako Chrome už takové stránky [označují jako “Not Secure”, “Nezabezpečeno”](http://www.forbes.cz/sbohem-a-zamecek-proc-je-dobre-ze-symbol-zabezpeceni-z-webu-mizi/) - snaží se vás tak varovat, abyste na takový web nezadávali údaje z platební karty, neregistrovali se zde, ani nic nestahovali.

*\*zde bych dal printscreen jak vypadá adresní řádek prohlížeče s https*

**Co jsou certifikáty a k čemu slouží**

Zatím jsme mluvili o SSL protokolech, které by se ale neobešly bez certifikátů. Ty fungují jako jakési potvrzení pro klienta i server, že si mohou navzájem důvěřovat. Jde o stejný princip, jako v běžném životě - pokud se například chcete živit jako řidič, musíte se potenciálnímu zaměstnavateli prokázat řidičským průkazem. Ten vás díky tomu nebude muset testovat, protože důvěřuje autoritě, v tomto případě zkušebnímu komisaři pro autoškoly, který vaše řidičské schopnosti prověřil.

Certifikát, tedy digitálně podepsaný veřejný šifrovací klíč, vydává také autorita, v tomto případě certifikační. Jde o společnosti (např. VeriSign, Thawte, ipsCA, Comodo a další), které mají obecnou důvěru. Jejich hlavním posláním je prověřování serverů a následné (pokud je vše v pořádku) vydávání certifikátů. Každý počítač při instalaci operačního systému získá seznam certifikačních autorit, díky kterému pak kontroluje, zda ten či onen server získal svůj certifikát právě od některé z těchto autorit.

**Certifikáty lze získat i zdarma**

Pokud provozujete web, na kterém zacházíte s citlivými údaji (máte třeba e-shop, nebo jen stránku, kde se uživatelé přihlašují pomocí jména a hesla), je SSL certifikát naprostou nutností, abyste neohrozili bezpečnost svěřených informací a zároveň povzbudili důvěru návštěvníků. Nicméně i pokud vlastníte server, na kterém máte třeba jen firemní profil nebo blog, je pořízení certifikátu také na místě. Přihlíží k nim totiž významní internetoví hráči jako Google, který ve vyhledávání upřednostňuje stránky zabezpečené SSL protokolem.

Je na vás, zda se rozhodnete za certifikát zaplatit a získat tak požehnání certifikační autority, delší dobu platnosti (většinou jeden až dva roky) či např. certifikát s vlastním názvem (toho hojně využívají např. banky, platební brány, státní instituce apod., aby zvýšily svou důvěryhodnost), nebo zvolíte některý z neplacených certifikátů, jako je třeba [velmi populární Let’s Encrypt](https://techcrunch.com/2018/09/14/three-years-later-lets-encrypt-now-secures-75-of-the-web/).

V případě, že máte o SSL certifikát zájem, ale nevíte si rady s tím, jak ho získat, neváhejte se na nás obrátit - velmi rádi vám s jeho výběrem pomůžeme. Vyhnete se tak potížím, [do jakých se dovedou dostat i opravdu velké instituce](https://twitter.com/spazef0rze/status/1044167917573689344).