SSL/TLS (Šifrovaná komunikace)

Ačkoliv se dodnes běžně používá zkratka **SSL**, původní protokol SSL (verze 1.0, 2.0 a 3.0) je již zastaralý a bezpečnostně překonaný. Jeho přímým nástupcem je **TLS**. Hlavním účelem těchto protokolů je zajistit tři věci:

```
1. **Šifrování:** Data nemůže nikdo cestou "odposlechnout" (stávají se nečitelnou změtí znaků).
2. **Autentizace:** Máte jistotu, že komunikujete se skutečným serverem (díky [[ca|certifikačním autoritám]]).
3. **Integrita dat:** Záruka, že data nebyla během přenosu nikým záměrně změněna.
```

Jak probíhá navázání spojení (TLS Handshake)

Než se začnou posílat skutečná data (např. obsah webové stránky), musí se prohlížeč se serverem „domluvit“. Tento proces se nazývá **Handshake** (podání ruky):

```
1. **Client Hello:** Prohlížeč pošle serveru informaci o tom, jaké verze TLS a šifrovací algoritmy podporuje.
2. **Server Hello:** Server vybere nejlepší společný algoritmus a pošle svůj digitální certifikát (obsahující veřejný klíč).
3. **Ověření:** Prohlížeč zkontroluje u [[ca|certifikační autority]], zda je certifikát platný a důvěryhodný.
4. **Výměna klíčů:** Obě strany si vygenerují unikátní "symetrický klíč", který budou používat pouze pro tuto konkrétní relaci.
5. **Šifrovaný kanál:** Od této chvíle je veškerá komunikace šifrovaná.
```

Rozdíl mezi SSL a TLS

Verze	Rok vydání	Stav
SSL 2.0 / 3.0	1995 / 1996	**Zastaralé** – obsahují vážné bezpečnostní chyby.
TLS 1.0 / 1.1	1999 / 2006	**Vysloužilé** – většina prohlížečů je již nepodporuje.
TLS 1.2	2008	**Běžně používané** – stále bezpečné, pokud je správně nastaveno.
TLS 1.3	2018	**Moderní standard** – rychlejší a bezpečnější (zkracuje proces Handshake).

Symetrické vs. Asymetrické šifrování

TLS chytře kombinuje oba typy šifrování:

- **Asymetrické (Veřejný/Soukromý klíč):** Používá se pouze na začátku (Handshake) k bezpečnému předání informací. Je výpočetně náročné.
- **Symetrické (Jeden sdílený klíč):** Používá se pro následný přenos dat. Je extrémně rychlé a efektivní pro velké objemy informací.

Proč je to důležité?

Bez SSL/TLS by internet, jak ho známe, nemohl existovat. Kdokoliv v kavárně na veřejné Wi-Fi by mohl:

- Vidět vaše hesla k e-mailu a do banky.
- Přečíst si vaše soukromé zprávy.
- Podvrhnout obsah stránek, které si prohlížíte.

Přítomnost aktivního TLS poznáte v prohlížeči podle ikony **visacího zámku** vedle adresy URL.

Související pojmy: HTTPS, CA (Certifikační autorita), Šifrování, Klient-server, IP adresa, Firewall.