HTTPS (Hypertext Transfer Protocol Secure)

HTTPS je rozšíření protokolu HTTP, které využívá šifrovací vrstvu **TLS** (Transport Layer Security, dříve SSL) k zabezpečení přenášených dat. Zatímco u běžného HTTP může kdokoli na cestě mezi vámi a serverem (např. poskytovatel internetu nebo útočník na veřejné Wi-Fi) vaše data číst nebo měnit, u HTTPS je obsah čitelný pouze pro koncové body komunikace.

V prohlížečích je přítomnost HTTPS signalizována **ikonou zamknutého visacího zámku** v adresním řádku.

Tři pilíře bezpečnosti HTTPS

HTTPS zajišťuje ochranu pomocí tří klíčových mechanismů:

```
1. **Šifrování (Encryption):** Veškerá vyměňovaná data jsou šifrována. I kdyby útočník data zachytil, uvidí pouze nesmyslnou směs znaků. To chrání hesla, čísla platebních karet i soukromí uživatele.
2. **Integrita dat (Data Integrity):** Protokol zajišťuje, že data nebyla během přenosu záměrně ani neúmyslně změněna. Pokud by někdo do dat zasáhl, systém to okamžitě detekuje a spojení ukončí.
3. **Autentizace (Authentication):** Pomocí digitálních certifikátů prokazuje, že komunikujete se skutečným serverem (např. se skutečnou bankou) a nikoliv s podvrženou stránkou útočníka.
```

Jak HTTPS funguje (Handshake)

Navázání spojení probíhá procesem zvaným **TLS Handshake**:

```
1. **Pozdrav:** Klient (prohlížeč) pošle serveru seznam podporovaných šifrovacích algoritmů.
2. **Certifikát:** Server pošle svůj **digitální certifikát** obsahující veřejný klíč.
3. **Ověření:** Prohlížeč ověří platnost certifikátu u důvěryhodné certifikační autority.
4. **Výměna klíčů:** Klient a server se dohodnou na unikátním **symetrickém klíči**, který bude použit pro šifrování samotných dat v této relaci.
5. **Šifrovaný přenos:** Od tohoto okamžiku probíhá veškerá komunikace šifrovaně.
```

Digitální certifikáty

Aby HTTPS fungovalo, musí mít majitel webu vystaven certifikát od **certifikační autority (CA)** (např. Let's Encrypt, DigiCert). Existují různé úrovně certifikátů:

Typ certifikátu	Popis
DV (Domain Validation)	Základní úroveň, ověřuje se pouze vlastnictví domény. Dnes nejčastější (např. zdarma od Let's Encrypt).
OV (Organization Validation)	Autorita ověřuje i existenci a identitu konkrétní firmy/organizace.
EV (Extended Validation)	Nejpřísnější ověření identity. Dříve zobrazovalo název firmy v zeleném řádku prohlížeče.

Výhody a význam

- **Bezpečnost uživatelů:** Ochrana citlivých údajů před odposlechem.
- **Důvěryhodnost:** Prohlížeče (Chrome, Firefox) označují weby bez HTTPS jako „Nezabezpečené“, což odrazuje návštěvníky.
- **SEO:** Google a další vyhledávače upřednostňují weby s HTTPS ve výsledcích vyhledávání.
- **Výkon:** Moderní a rychlý protokol **HTTP/2** a **HTTP/3** funguje v prohlížečích výhradně přes HTTPS.

Související pojmy: HTTP, TLS, SSL, Šifrování, Certifikát, Browser, Soukromí, MitM útok.