HTTPS a TLS

HTTPS (Hypertext Transfer Protocol Secure) je zabezpečená verze protokolu HTTP. Využívá protokol **TLS** (Transport Layer Security) k šifrování komunikace mezi webovým prohlížečem a serverem.

Dříve se pro tento účel používal protokol **SSL** (Secure Sockets Layer), který je však dnes považován za zastaralý a nebezpečný. TLS je jeho moderním nástupcem.

Jak HTTPS funguje?

HTTPS zajišťuje tři klíčové věci:

1. **Šifrování:** Data jsou nečitelná pro kohokoliv, kdo by je cestou odposlouchával.
2. **Integrita dat:** Data nemohou být během přenosu změněna bez odhalení.
3. **Autentizace:** Uživatel má jistotu, že komunikuje se skutečným serverem (např. bankou) a ne s podvrženou stránkou.

Vrstvy protokolu

HTTPS není samostatný protokol, ale kombinace dvou vrstev:

- **Aplikační vrstva:** Standardní HTTP (požadavky GET, POST atd.).
- **Transportní vrstva:** TLS (zajišťuje šifrovaný kanál).

Standardně HTTPS komunikuje na portu **TCP 443** (klasické HTTP používá port 80).

Průběh navázání spojení (TLS Handshake)

Než se odešlou první data (např. webová stránka), proběhne tzv. „podání ruky“ (handshake):

```
1. **Client Hello:** Prohlížeč pošle serveru seznam podporovaných šifer a
verzi TLS.
2. **Server Hello:** Server vybere nejlepší společnou šifru a pošle svůj
**digitální certifikát**.
3. **Ověření certifikátu:** Prohlížeč zkontroluje u certifikační autority,
zda je certifikát platný a patří dané doméně.
4. **Výměna klíčů:** Pomocí [[asymetrické šifrování|asymetrického
šifrování]] si strany dohodnou společný "symetrický klíč".
5. **Šifrovaný přenos:** Veškerá další data už proudí pomocí rychlého
[[symetrické šifrování|symetrického šifrování]].
```

Evoluce verzí

Verze	Stav	Poznámka
SSL 2.0 / 3.0	**Zastaralé**	Obsahují kritické chyby (POODLE atd.). Nesmí se používat.
TLS 1.0 / 1.1	**Zastaralé**	Již nejsou považovány za bezpečné pro moderní weby.
TLS 1.2	Používané	Stále široce rozšířené, velmi bezpečné, ale pomalejší handshake.
TLS 1.3	**Aktuální**	Nejnovější standard. Rychlejší (1-RTT) a bezpečnější (odstraněny staré šifry).

Digitální certifikáty

Aby HTTPS fungovalo, musí mít majitel webu certifikát vystavený důvěryhodnou **Certifikační autoritou (CA)** (např. Let's Encrypt, DigiCert). Certifikát obsahuje:

- Název domény.
- Veřejný klíč serveru.
- Digitální podpis autority.
- Datum platnosti.

> **Zajímavost:** TLS se nepoužívá pouze pro web (HTTPS), ale i pro zabezpečení e-mailů (IMAPS, POP3S, SMTPS), souborových přenosů (FTPS) nebo VPN.

— **Viz také:** Šifrování, IPsec, Digitální podpis