

Bezpečnosť DNS a TLS v prehliadači

Praktický prehľad pre každého používateľa internetu

KC KB – FEI STU Bratislava

13. februára 2026



PLÁN [OBNOVY]



- 1 DNS
- 2 Čo sa deje, keď zadáte adresu
- 3 DNS útoky
- 4 DNS Riešenie
- 5 Čo je TLS (HTTPS) a prečo to máte v prehliadači
- 6 Prečo na DNS a TLS záleží v praxi
- 7 Čo môžete urobiť v prehliadači
- 8 Zhrnutie

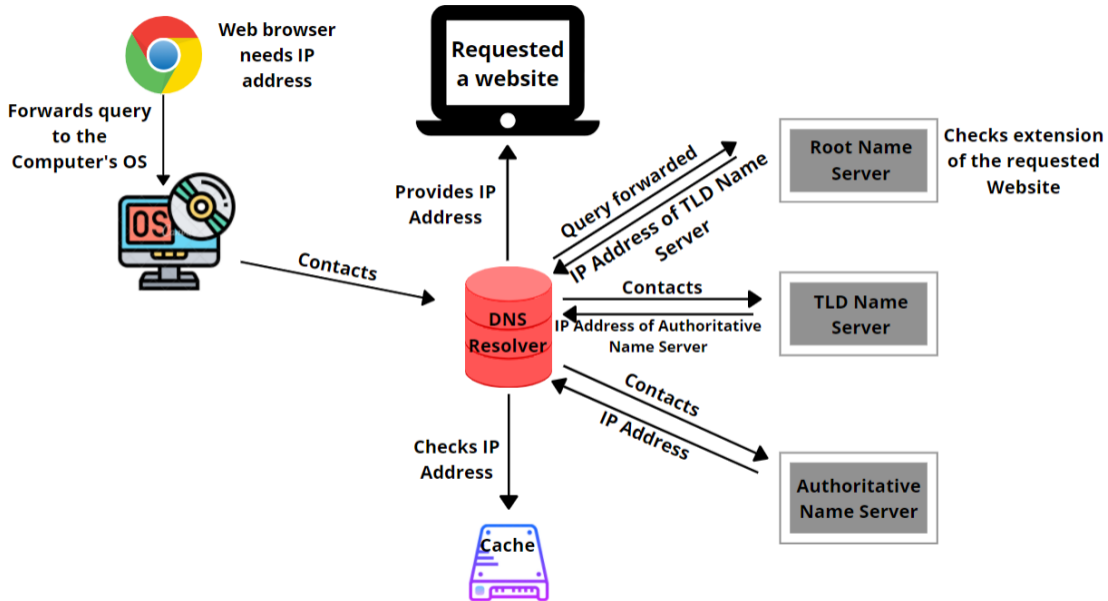
Čo je DNS? DNS je systém prekladania názvov na IP adresy.
(„facebook.com“ → „31.13.84.36“)

214 374	Bouck David 2 Třebízského 1452/10	222 733 939	- Stanislav
741 413	Boucká Růžena		- Václav Cy
740 470	4 Na Blansku 1423/18, Modřany	241 766 911	- Václav P
861 249	- Stanislava 5 Musilkova 256/54	257 216 121	- Václav 9
930 710	Boucký Jiří 4 U Spořitelny 80/15, Modřany	244 400 270	- Zdeněk 1
n-group.cz	- Libor Vraně n. Vlt. Oblouková 582	▷257 741 462	- Zdeněk 1
930 773	Boucová Kateřina 6 Na Ostrohu 2428/3	233 311 458	- Zdeněk 1
203 611	Bouček David 8 Klapkova 54/21	286 840 502	Boudarová
312 229	- František JUDr. 5 Nad Parkem 880, Zbraslav	257 920 858	Boudík Fra
214 208	- František 5 V Edenu 487/5, Radotín	▷257 912 952	- Zdeněk k
922 705	- Jakub 2 nám. Jiřího z Poděbrad 1382/2	739 612 175	Boudis Lu
860 335	- Jakub buka		- Petr 9 B
763 164	10 Čermokostecká 206/3, Strašnice	▷608 259 497	e-mail ...
357 484	URL	boucek.info/	- Petr Mgr.
216 719	- Jan doc.MUDr.CSc. 2 Mikovcova 582/8	224 239 414	Boudisov
161 856	- Jan 3 Hradecká 2355/5	272 735 294	Boudná V
126 459	- Jan 3 Táboritká 16/24	222 728 233	Boudník J
183 181	- Jan Ing.CSc. 8 Budínova 23/1, Libeň	283 843 059	- Jiří 4 Vav
140 452	- Jan 8 Legionářů 722/40	283 910 560	- Milan 10
180 505	- Jaroslav 4 Dolnojiřčanská 266/5	241 710 562	- Milošlav
116 790	- Jaroslav 4 Papírníkova 617/7	241 711 737	- Petr 4 N
111 238	- Jaroslav 6 Na Pískách 1157/62	233 322 404	

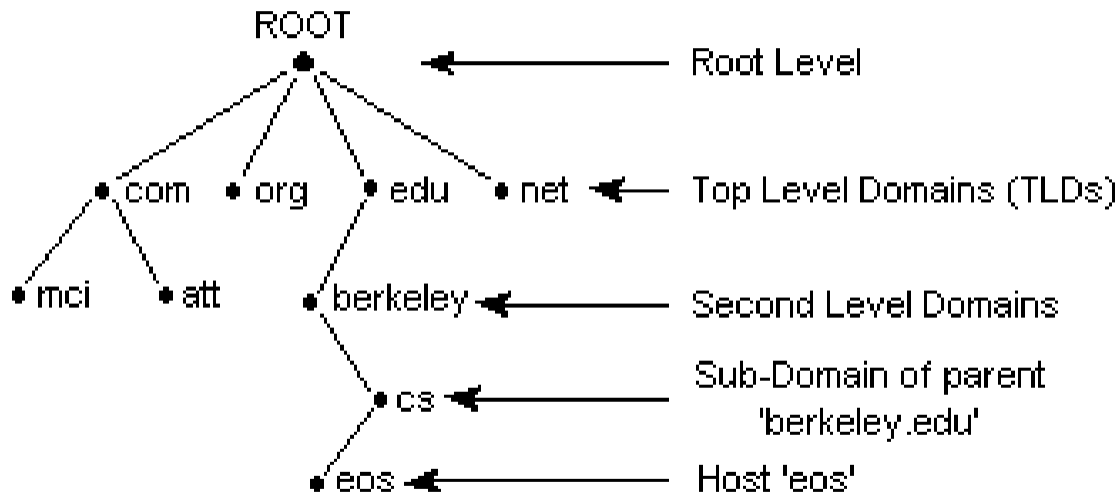
Čo vlastne robíte: Do prehliadača napíšete napr. `https://banka.sk` a stlačíte Enter.

V skratke čo sa stane:

- 1 Prehliadač potrebuje vedieť *kde* je server `banky.sk` → opýta sa **DNS** („telefonný zoznam internetu“).
- 2 DNS odpovie **IP adresou** (číslo servera).
- 3 Prehliadač sa k serveru **pripojí** a vyžiada si stránku.
- 4 Ak je v adrese **https**, prebehne ešte **TLS** – dohodnutie šifrovania, overenie certifikátu.
- 5 Zobrazí sa stránka; v adresnom riadku vidíte **zámok** (bezpečné pripojenie).



DNS Hierarchy



- **DNS Cache Poisoning / Spoofing** – falošné odpovede v cache
- **DNS Hijacking (Únos DNS)** – zmena, ktorý DNS server používate
- **DNS Tunneling** – skrytá komunikácia cez DNS
- **DNS Amplifikácia (DDoS)** – zneužitie DNS na zahltenie cieľa

Na nasledujúcich slajdoch: čo to znamená v praxi.

Čo to je: Útočník „otrávi“ vyrovnávaciu pamäť (cache) DNS servera falošnou odpoveďou. Keď sa niekto pýta „kde je banka.sk“, namiesto skutočnej IP dostane IP útočníka.

Ako to funguje (zjednodušené): DNS servery si odpovede na chvíľu ukladajú, aby nevyhľadávali stále znova. Ak útočník dostane do cache nesprávny záznam (využitím zraniteľnosti alebo man-in-the-middle), všetci, ktorí používajú ten DNS server, budú smerovaní na zlú adresu.

Pre vás: Môžete zadať banka.sk, ale prehliadač vás zavezie na útočníkov server. Adresa v prehliadači stále ukazuje banka.sk, pretože ste ju naozaj zadanú mali – prehliadač len išiel na inú IP. Obrana: šifrované DNS (DoH), DNSSEC na strane domény; u vás kontrola certifikátu a pri podozrení zadať adresu ručne.

Čo to je: Zmena toho, *ktorý* DNS server váš počítač alebo router používa – tak, že všetky vaše DNS dotazy idú na server útočníka. Ten potom môže vracat' ľubovoľné (falošné) IP adresy.

Ako k tomu môže dôjsť:

- Malvér na vašom PC zmení nastavenie DNS (napr. na falošný „ISP“ server).
- Útok na router (slabé heslo, zraniteľnosť) a zmena DNS v routeri – potom platí pre celú domácu sieť.
- Podvodná „technická podpora“, ktorá vás navádza zmeniť DNS v nastaveniach.

Pre vás: Rovnako ako pri cache poisoning – zdanlivo idete na banka.sk, v skutočnosti na server útočníka. Obrana: DoH v prehliadači (obchádza systémové DNS), silné heslo na router, neprepisovať DNS podľa neznámych inštrukcií.

Čo to je: Zneužitie DNS kanála na *skrytú* komunikáciu. Útočník (alebo malvér) posiela dáta ukryté v DNS dotazoch a odpovediach – napr. krádež dát z firemnej siete alebo príkazová linka do infikovaného zariadenia.

Prečo to útočníci robia: DNS prevádzka často prechádza cez firewall (port 53) a nie je šifrovaná ani niekedy dostatočne monitorovaná. Tým sa dá obísť blokovanie iných protokolov.

Pre vás ako používateľa: Priamo sa vás to väčšinou netýka – je to skôr problém pre firmy (exfiltrovanie dát, ovládanie botov). Dôležité je vedieť, že DNS sa dá zneužiť nielen na presmerovanie, ale aj na prepašovanie dát.

Čo to je: Typ DDoS útoku, pri ktorom útočník pošle na otvorené DNS servery veľa malých požiadaviek s *sfalšovanou* odosielateľskou adresou (adresa obete). DNS server odpovie obete – a odpoveď môže byť mnohonásobne väčšia než požiadavka (amplifikácia). Obete je tak zahltená prevádzkou.

Prečo to funguje: Protokol DNS umožňuje v jednej odpovedi vrátiť veľa záznamov; pomer veľkosti odpovede k požiadavke môže byť napr. 50:1. Útočník tak s malým objemom vlastnej prevádzky spôsobí obeti obrovský nával.

Pre vás: Priamo vaše zariadenie nie je typicky cieľom; cieľom sú servery (služby, firmy). Dôsledok môžete pocítiť ako výpadok služby (web, banka, hry). Obrana je hlavne na strane poskytovateľov (filtrovanie, obmedzenie otvorených DNS serverov).

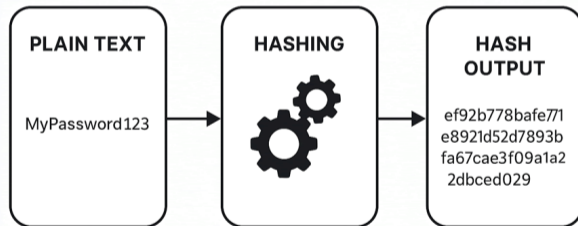
- DNSSEC
- Šifrované DNS (DoH)
- DNS over HTTPS (DoH)

Dva kryptografické nástroje:

- Hashovacia funkcia (integrita)
- Šifrovacia (podpisovacia) funkcia asymetrickým kľúčom (dôveryhodnosť/autenticita)

Hashovacia funkcia je funkcia, ktorá premení vstupné dáta na fixnú dĺžku výstupného reťazca.

SHA-256



Zabezpečuje integritu dát.

<https://www.browserling.com/tools/all-hashes>

Šifrovacia (podpisovacia) funkcia asymetrickým kľúčom

Asymetrický kľúč

Dve časti: **verejný** a **privátny**. Čo urobí jedna časť, môže zvrátiť len druhá časť toho istého páru.

- **Verejný kľúč** – môže byť zdieľaný (napr. na serveri, v certifikáte).
- **Privátny kľúč** – musí zostať len na jednom mieste (server, váš počítač).

Šifrovanie

- Verejný kľúč **šifruje** dáta.
- Privátny kľúč **dešifruje** dáta.

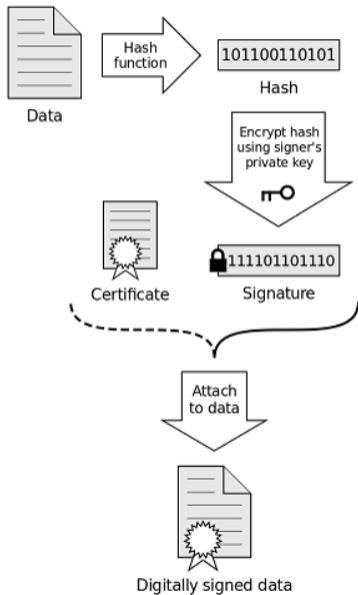
Podpisovanie

- Privátny kľúč **podpisuje** dáta.
- Verejný kľúč **overuje** podpis.

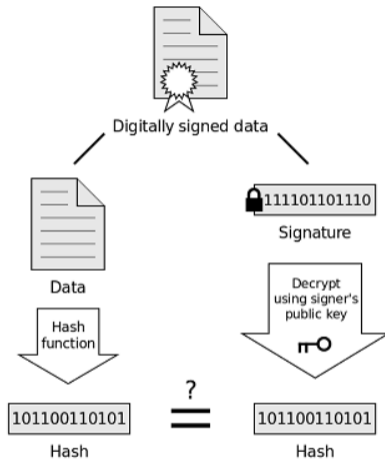
DNSSEC

DNSSEC je technológia, ktorá používa podpisovanie záznamov v DNS, aby útočník nemohol falošne zmeniť záznamy v DNS.

Signing



Verification



If the hashes are equal, the signature is valid.

Príklad: `https://www.banka.sk/login`

- `https://` – používa sa šifrované pripojenie (TLS). Bez toho by dáta leteli sieťou „čisto“.
- `www.banka.sk` – *doména*. Tu treba dávať najväčší pozor: či je to naozaj `banka.sk`, nie `banka-sk.com` alebo `banka.sk.evil.sk`.
- `/login` – cesta na stránke (méně dôležitá z pohľadu podvodu).

Prakticky

Pri bankách, e-mailoch a prihlasovaní vždy skontrolujte **presne tú doménu**, na ktorej ste. Padlock (záмок) hovorí len to, že spojenie je šifrované – nie že stránka je legitímna.

TLS = šifrovanie medzi vami a serverom

TLS (Transport Layer Security) je technológia, ktorá:

- **šifruje** obsah prenosu – nikto „na drôte“ nevidí váš heslo ani čo píšete,
- pomáha **overiť**, že hovoríte so skutočným serverom (cez **certifikát**).
Váš prehliadač používa šifrovanie pomocou „jeho“ verejného kľúča. (Ale kto je to „jeho“?)

V prehliadači to vidíte ako:

- **https://** v adrese (nie http),
- ikona **zámku** vľavo od adresy („bezpečné pripojenie“).

Dôležité

Zámok znamená: „toto spojenie je šifrované a certifikát sa zhoduje s doménou.“ **Neznamená:** „táto stránka je určite dobrá.“ Falošná stránka môže mať tiež HTTPS, ak si útočník vybaví certifikát pre svoju doménu.

General

Details

Issued To

Common Name (CN)	*.google.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	WR2
Organization (O)	Google Trust Services
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Monday, January 19, 2026 at 9:36:59 AM
Expires On	Monday, April 13, 2026 at 10:36:58 AM

SHA-256
Fingerprints

Certificate	d09628c5b0560b27849737b2785c2bfb8d40932f5886e1f08989f49 25eeaa5be
Public Key	d0c7740fef79560414a116b765a61cbf7ab9446a7e4d1d44af9898c 607cb15fb

Čo je certifikát: Elektronický „pas“ servera – prehliadač overí, či doména (napr. banka.sk) zodpovedá certifikátu vystavenému dôveryhodnou autoritou.

Kde to vidíte: Klik na zámok v adresnom riadku → často „Pripojenie je zabezpečené“ a možnosť pozrieť certifikát (pre koho bol vystavený, do kedy platí).

Praktické rady:

- Ak prehliadač zobrazí **varovanie** (neplatný certifikát, neznáma autorita) – neprepisujte to a neklikajte „pokračovať“ na citlivých stránkach.
- Pri bankách a e-mailoch overte, že certifikát je vystavený pre **správnu doménu** (napr. banka.sk).

DNS môže byť zneužitý tak, že vás prehliadač „zavezie“ na inú IP adresu ako skutočná banka:

- **Cache poisoning** – niekto vloží do cache falošnú odpoveď („banka.sk = IP útočníka“).
- **Hijacking** – malvér alebo zlá konfigurácia zmení, ktorý DNS server váš počítač používa; ten potom môže vracieť falošné adresy.

Výsledok pre vás: Vyzerá to ako banka (adresa, padlock), ale v skutočnosti posielate heslo útočníkovi. Preto je dôležité nespúľahovať len na padlock – pozrieť sa na **doménu** a pri podozrení zadať adresu ručne (napr. `https://banka.sk`).

Phishing: Útočník vám pošle odkaz na stránku, ktorá *vyzerá* ako banka, ale je to `banka-sk-prihlasenie.com` alebo `banka.sk.evil.sk`.

Táto stránka môže mať:

- HTTPS a zámok (certifikát pre tú falošnú doménu),
- takmer rovnaký vzhľad ako skutočná banka.

Obrana

Vždy kontrolujte presne názov domény v adresnom riadku. Banka používa svoju oficiálnu doménu (napr. `banka.sk`, `slsp.sk`) – nie `banka-secure.com` alebo podobné. Pri pochybnostiach ísť na stránku ručne (napísať adresu alebo použiť záložku).

Problém: Klasické DNS dotazy sú nešifrované – poskytovateľ internetu (alebo niekto v sieti) môže vidieť, na aké stránky sa pýtate.

Riešenie: DNS over HTTPS (DoH) – prehliadač posiela DNS dotazy šifrovane (cez HTTPS) na vybraného poskytovateľa (napr. Cloudflare, Google). Nikto „na drôte“ nevidí, akú doménu vyhľadávate.

Kde to nastaviť (príklad):

- **Firefox:** Nastavenia → Súkromie a zabezpečenie → DNS cez HTTPS (povoliť, prípadne zvoliť poskytovateľa).
- **Chrome:** Nastavenia → Súkromie a zabezpečenie → Zabezpečenie → Použiť zabezpečený DNS (zvoliť poskytovateľa).

Praktický checklist pre bezpečné prehliadanie

- 1 Pri bankách a prihlasovaní vždy skontrolujte **doménu** v adresnom riadku (nie len zámok).
- 2 **Neklikajte** na odkazy z e-mailov/SMS na „prihlásenie do banky“ – ak potrebujete ísť do banky, napíšte adresu ručne alebo použite záložku.
- 3 **Heslo a citlivé údaje** zadávajúte len na stránkach, ktorých doménu poznáte a overíte.
- 4 Ak prehliadač **varuje pred certifikátom** – na citlivých stránkach neprepisujte a neklikajte „pokračovať“.
- 5 Zvážte zapnutie **DoH** v prehliadači (šifrované DNS) pre väčšie súkromie.

- **DNS** = preklad názvu (banka.sk) na adresu servera. Ak je DNS zlý, môžete skončiť na falošnej stránke.
- **TLS (HTTPS)** = šifrovanie a overenie certifikátu. Zámok = spojenie je šifrované a certifikát sedí na doménu; *nie* „táto stránka je určite dobrá“.
- Najdôležitejšie: **kontrolovať doménu** a neklikat' na podozrivé odkazy. Pri bankách a e-mailoch ísť ručne na známu adresu.

Ďakujem za pozornosť.
Otázky?