Základní informace

```
  Oficiální web: [[https://letsencrypt.org/|letsencrypt.org]]
  Licence: Bezplatná, open-source.
  Cíl: Vytvořit „HTTPS pro všechny“ – snížit bariéry pro nasazení TLS/SSL certifikátů.
  Podpora: Certifikáty jsou důvěryhodné všemi hlavními webovými prohlížeči a operačními systémy.
```

Technické vlastnosti

```
  Typ certifikátu: Pouze Domain Validation (DV) – ověřuje vlastnictví domény, nikoli identity organizace.
  Platnost certifikátu: Od 1. září 2020 je maximální doba platnosti 90 dní (dříve 90 dní i předtím, ale nyní je to striktně vynucováno).
  Obnovení: Certifikáty je třeba pravidelně obnovovat – doporučuje se automatizace.
  Podporované domény:
      Jednoduché domény (např. example.com)
      Subdomény (např. www.example.com, mail.example.com)
      Wildcard domény (od roku 2018, např. *.example.com) – vyžadují ověření přes DNS-01 challenge.
```

ACME protokol

Let’s Encrypt používá protokol ACME (Automated Certificate Management Environment), který umožňuje automatizované:

```
  žádosti o certifikát,
  ověření vlastnictví domény,
  instalaci a obnovu certifikátu.
```

Certbot – oficiální klient

```
  Certbot je nejznámější open-source klient pro ACME protokol.
  Automatizuje získání i obnovu certifikátů.
  Podporuje mnoho webových serverů (Apache, Nginx atd.) a operačních systémů (Linux, BSD...).
  Web: [[https://certbot.eff.org/|certbot.eff.org]]
```

Alternativní klienti

Kromě Certbotu existuje řada jiných ACME klientů:

```
  acme.sh – lehký shell skript
  Traefik – reverse proxy s vestavěnou podporou Let's Encrypt
  Caddy – webový server, který automaticky získává a obnovuje certifikáty
  Pebble – testovací CA pro vývojáře (od ISRG)
```

Ověřovací metody (challenges)

Let’s Encrypt ověřuje, že žadatel ovládá doménu, pomocí tzv. challenges:

```
  HTTP-01: Server musí běžet na portu 80 a umět vystavit specifický soubor
na adrese http://<doména>/.well-known/acme-challenge/...
  DNS-01: Vyžaduje nastavení specifického TXT záznamu v DNS. Nutné pro
wildcard certifikáty.
  TLS-ALPN-01: Alternativa k HTTP-01, používá port 443 (méně běžná).
```

Omezení a limity

Let’s Encrypt aplikuje různé limity, aby zamezil zneužití:

```
  50 certifikátů za týden na stejnou doménu (tzv. „Duplicate Certificate
limit“)
  300 nových domén za certifikát
  Rychlostní limity na počet selhání ověření
  Podrobnosti: [[https://letsencrypt.org/docs/rate-limits/|Rate
   Limits – Let’s Encrypt]]
```

Bezpečnost a důvěryhodnost

```
  Certifikáty Let’s Encrypt jsou důvěryhodné všemi moderními prohlížeči a
OS.
  Používá kryptografii na bázi RSA (2048/4096b) nebo ECDSA (P-256, P-384).
  Nepodporuje rozšířené (EV) certifikáty.
```

Integrace

```
  Mnoho hostingových služeb (např. Cloudflare, Netlify, Vercel) nyní
automaticky spravuje Let’s Encrypt certifikáty.
  Vlastní servery: doporučuje se nastavit cron job nebo systemd timer pro
```

```
automatickou obnovu.
```

Odkazy

```
  [[https://letsencrypt.org/|Oficiální
   web Let’s Encrypt]]
  [[https://certbot.eff.org/|Certbot
   – oficiální klient]]
  [[https://github.com/letsencrypt/|GitHub
   Let’s Encrypt]]
  [[https://letsencrypt.org/docs/|Dokumentace
   Let’s Encrypt]]
```

Shrnutí

Let’s Encrypt revolučně zjednodušil nasazení HTTPS na webu. Díky automatizaci, bezplatnosti a open-source přístupu se stal de facto standardem pro bezpečné webové servery všech velikostí – od jednoúčelových blogů po rozsáhlé cloudové aplikace.