# SSL Certifikáty

# Co je to SSL certifikát

- Secure Socket Layer
- Slouží k zabezpečení komunikace proti odposlechu třetí stranou a také zajišťuje autentizaci komunikujících stran.
- Jedná se o digitální certifikát, který funguje jako „průkaz totožnosti“ pro webovou stránku
- Potvrzuje identitu webového serveru pomocí digitálního podpisu autority, která certifikát vydala
- Umožňuje šifrovanou komunikaci mezi webovým serverem a prohlížečem

# Proč je SSL certifikát důležitý?

- Zabezpečení
  - Chrání přenesená data mezi serverem a klientem (např. hesla, kreditní karty) před odposlechem a úpravami
- Ověření
  - Ujišťuje uživatele, že komunikují s ověřeným serverem a ne s falešnou kopií
- Důvěra
  - SSL certifikát zvyšuje důvěru uživatelů ve webovou stránku, což je zásadní pro e-commerce a online služby
- SEO
  - Google a jiné vyhledávače dávají přednost zabezpečeným strákám, což může vést k lepšímu umístění ve vyhledávání

# Kde se dá SSL certifikát pořídit?

- Certifikáty se dají získat od mnoha poskytovatelů
- Komerční poskytovatelé
  - GoDaddy
  - Symantec
  - Comodo
  - DigiCert
- Bezplatné certifikáty od organizací jako Let‘s Encrypt.
  - Poskytují základní úroveň zabezpečení vhodnou pro mnoho webových stránek

Let's Encrypt

Symantec

GoDaddy

COMODO SSLCERTIFICATE

digicert SECURED

10-10-21

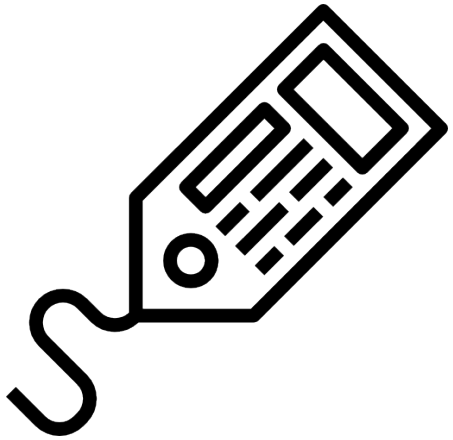
# Typy certifikátů

- Existují tři hlavní typy SSL certifikátů
- Domain Validated (DV)
  - Nejméně náročný na ověření, potvrzuje vlastnictví domény.
- Organitazion Validated (OV)
  - Vyžaduje ověření identity organizace, poskytuje vyšší úroveň důvěry.
- Extended Validation (EV)
  - Nejpřísnější forma ověření, zahrnuje důkladnou kontrolu organizace



# Cena certifikátů

- Ceny se liší v závislosti na poskytovateli a typu certifikátu
- DV certifikáty mohou být zdarma (jako u Let‘s Encrypt) nebo stát několik desítek dolarů ročně.
- OV a EV certifikáty jsou dražší, mohou stát stovky až tisíce dolarů ročně

# Aplikace na web

- Je nutno vygenerovat žádost o podepsání certifikátu na vašem serveru
- Podat žádost u certifikační autority a prokázat vlastnictví domény
- Instalovat certifikát na server, jakmile jej obdržíte od CA (Certificate Authority)
- Nastavit přesměrování z HTTP na HTTPS a zajistit, aby všechny zdroje na stránce byly zabezpečené

# Děkuji za pozornost