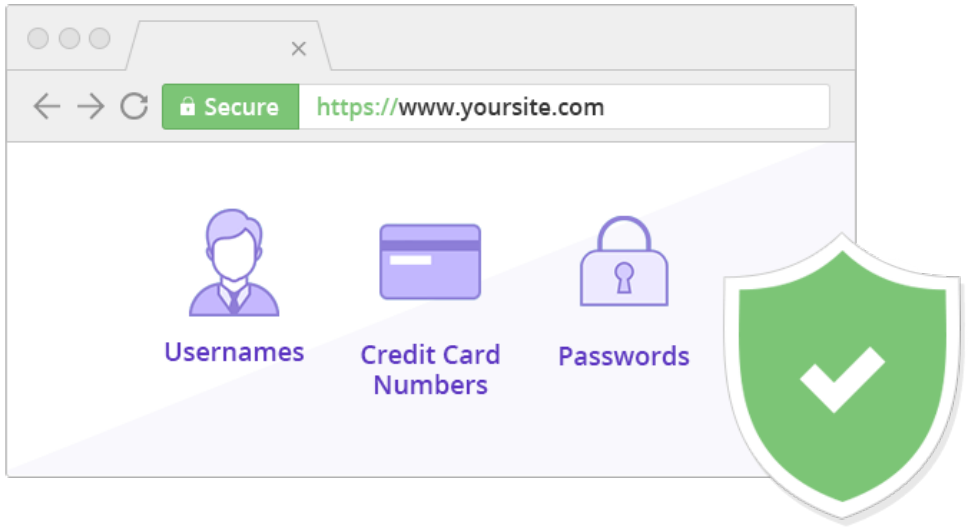

SSL certifikáty

# Co je SSL certifikát?

- SSL – Secure Socket Layer
- Digitální certifikát, který poskytuje autentizaci pro webovou stránku
- Umožňuje šifrované spojení
- Jedná se o bezpečnostní protokol, který zajišťuje, že veškerá data přenášená mezi serverem a prohlížečem zůstávají soukromá a nedotčená
- ‘http://‘ → ‘https://‘

# Důležitost SSL certifikátů

- Zvýšená bezpečnost
  - Hlavní rolí SSL certifikátu je chránit komunikaci mezi serverem a klientem
- Autentizace
  - Ověření, že informace jsou odesílány správnému serveru a ne podvodníkovi, který se snaží ukrást data
- Integrita dat
  - Zajišťují, že data nejsou při přenosu manipulována.
  - Zásadní pro citlivé informace jako ID, hesla, čísla kreditních karet atd.



# Důležitost SSL certifikátů

- SEO výhody

  - Lepší hodnocení ve vyhledávačích – Google a další vyhledávače oficiálně potvrdili, že HTTPS je faktorem hodnocení

  - Bezpečné weby se mohou načítat rychleji díky protokolu HTTP/2, který vyžaduje HTTPS

  - Nižší bounce rate (míra odchodů) – weby, které nejsou zabezpečeny SSL certifikátem, mohou být označeny jako „nebezpečné“, což může vést k vyšší míře odchodů návštěvníků z webu

- Budování důvěry

  - Vizuální indikátory bezpečí – Zámek ve vyhledávání, což uživatelům signalizuje, že jejich spojení je bezpečné

# Certifikační autority (CA)

- Důležité subjekty v infrastruktuře veřejných klíčů, které zajišťují vydávání, správu, ověřování a zneplatnění digitálních certifikátů
- Klíčové funkce
  - Vydávání certifikátů – CA vydává digitální certifikáty, které spojují veřejný klíč subjektu s jeho identitou
  - Ověřování a autentizace – CA fungují jako důvěryhodné třetí strany, jejichž úlohou je ověřit identitu subjektů, které požadují certifikát
  - Správa životního cyklu certifikátů – CA spravují životní cyklus každého vydání certifikátu, od vydání, přes obnovení, až po zneplatnění




# Získávání SSL certifikátů

- Certifikační autority
- Weboví hostitelé
- Příklady známých poskytovatelů
  - Let‘s Encrypt – Populární bezplatná CA známá pro svou automatizaci vydávání a obnovování certifikátů, což usnadňuje zabezpečení webového provozu
  - DigiCert – Jedna z předních komerčních CA, která nabízí širokou škálu bezpečnostních řešení, včetně SSl/TLS certifikátů, EV certifikátů a dalších
  - Comodo (Sectigo) – Další velká komerční CA, která poskytuje různé typy digitálních certifikátů a bezpečnostních služeb pro jednotlivce a organizace
  - SSLs.cz – Český distributor SSl certifikátů nabízející širokou škálu produktů od známých mezinárodních CA jako jsou Symantec, GeoTrust a Thawte

# Různé typy SSL certifikátů

- Doménově ověřené (DV)
  - Jednoduché a rychlé řešení pro základní šifrování
- Organizačně ověřené (OV)
  - Vyšší úroveň bezpečnosti s ověřením identity organizace
- Rozšířené ověření (EV)
  - Nejvyšší standard ověření pro maximální důvěru a bezpečnost


# Doménově ověřené certifikáty (DV)

- Ověření vlastnictví domény prostřednictvím e-mailu nebo DNS
- Rychlý proces vydání, často automatizovaný
- Nízké náklady, někdy i zdarma
- Ideální pro osobní weby a malé projekty
- Příklad
  - Let‘s Encrypt nabízí DV certifikáty zdarma

# Organizačně ověřené certifikáty (OV)

- Vyžaduje ověření identity organizace
- Poskytuje vyšší úroveň důvěry uživatelům
- Trvá déle a je dražší než DV
- Doporučeno pro podnikové weby a e-commerce
- Příklad
  - DigiCert poskytuje OV certifikáty pro firmy

# Rozšířené ověření certifikátů (EV)

- Nejvyšší úroveň ověření a důvěry
- Vyžaduje důkladné ověření organizace a jejího právního stavu
- Nejdražší, ale nejlepší pro velké korporace a banky
- Příklad
  - Comodo (nyní Sectigo) má v nabídce EV certifikáty, které zahrnují rozsáhlé ověřovací procesy

# Cena SSL certifikátů

- DV
  - Cena se obvykle pohybuje od 0 Kč (pro bezplatné certifikáty) až po několik set Kč
- OV
  - Střední cenová kategorie
  - Cena může být od několika set korun do několika tisíc Kč, v závislosti na poskytovateli a úrovni služeb
- EV
  - Nejdražší, odrazuje potenciální útočníky díky důkladnému ověření
  - Ceny se pohybují od několika tisíc do desítek tisíc Kč


# Implementace SSL certifikátu

- Výběr a získání SSL certifikátu
  - Volba odpovídajícího typu SSL certifikátu od certifikační autority
- Instalace a konfigurace na serveru
  - Nastavení SSL certifikátu na hostitelském serveru pro zajištění šifrovaného spojení
- Testování a ověření
  - Kontrola, že SSL certifikát je aktivní a webová stránka je dostupná přes HTTPS

# Shrnutí

- Zabezpečení komunikace
  - SSL certifikáty jsou klíčové pro šifrování dat mezi webovými servery a prohlížeči
- Důvěryhodnost webu
  - Použití SSL zvyšuje důvěru uživatelů a je často indikátorem důvěryhodnosti pro vyhledávače
- Typy certifikátů
  - Existují různé typy certifikátů (DV, OV, EV), které se liší úrovní ověření a poskytovanou důvěryhodností
- Implementace
  - SSL certifikát lze získat a nainstalovat prostřednictvím několika kroků, od výběru až po konfiguraci serveru a pravidelnou obnovu

# Děkuji za pozornost ☺