Mikor javasolt a HTTPS használata?

Ha Ön a weboldalán a látogatók adatainak megadását kéri:

- Bejelentkezési oldak esetén
- hírlevélre történő feliratkozás, vagy megrendelések leadása
- Facebook alkalmazások esetében, ugyanis a Facebook kizárólag biztonságos weboldalakról fogad tartalmakat.
- Ha tartalmaz a weboldal olyan adatlapot ahol személyes adatokat kérünk be a látogatótól
  A Google Chrome és a Mozilla Firefox böngészők figyelmeztetik a látogatókat, ha a kapcsolat nem rendelkezik SSL tanúsítvánnyal.
  A HTTPS nélküli weboldalak esetében nem biztonságos címkét fog megjeleníteni a böngésző címsorában. Ezért kevesebben fognak átkattintani a Google találati oldaláról.
- Bankkártyás fizetési felületek
  Ha ilyen szolgáltatást szeretnénk használni akkor mindenképpen Ehhez már a Szervezeti szinten ellenőrzött tanúsítvány (OV SSL) szükséges.
- Keresőoptimalizálás javítására
  A keresők esetében is egyre nagyobb hangsúllyt kap a rangsorolás során ha az adott weboldalnak van SSL tanúsítványa.

akkor javasoljuk, hogy a bekért adatokat titkosított protokollon keresztül továbbítsa a látogató böngészője és a szerver között. Az SSL tanúsítvány gondoskodik arról, hogy az adott weboldalon zajló kommunikációba illetéktelen személy ne tudjon belehallgatni. Az SSL tanúsítvány segítségével biztonságossá tett weboldalak címében a http: helyett a https: előtag szerepel, ezért az SSL-re sokan „HTTPS” néven hivatkoznak. Ha az adott weboldal elérhető https protokollon keresztül, akkor általában egy kis zöld lakat jelenik meg a böngészőkben amely jelzi a látogatók felé hogy az adatokat biztonságos titkosított csatornán keresztül továbbítja a web böngésző a szerver felé.

MI AZ A TANÚSÍTVÁNY KIBOCSÁTÓ?

A tanúsítvány kibocsátó az angol Certificate Authority (CA) megfelelője. A tanúsítvány kibocsátó az a szervezet, amely digitális (SSL és TLS) tanúsítványokat ad ki.

A digitális tanúsítvány két részből áll, egy nyilvános és egy titkos kulcsból. A tanúsítvány segítségével igazolható a nyilvános kulcs tulajdonjoga a tanúsítvány vásárlása során megadott adatok szerint.

A tanúsítványt kibocsátó szervezet hitelesíti a tanúsítvány megvásárlása során megadott adatokat.

Az SSL tanúsítványokat tanúsítvány kibocsátó szervezetek adják ki.

Például:

- Netlock Kft.
- GlobalSign
- Symantec
- Comodo

SSL TANÚSÍTVÁNYOK TÍPUSAI

Domain ellenőrzött tanúsítvány (DV SSL)

Csak az érintett domain név védelmét biztosítja, a kiállítás előtt csak a domain név létezése, tulajdonjoga kerül ellenőrzésre. A domain név hátterében álló szervezet, vagy cég nem kerül vizsgálatra. Lehetőség van több aldomain neves úgynevezett Wildcard tanúsítvány igénylésére is.

Szervezeti szinten ellenőrzött tanúsítvány (OV SSL)

Ennél a tanúsítvány típusnál a domain név tulajdonosának az adatai is ellenőrzésre kerülnek. Lehetőség van több aldomain neves úgynevezett Wildcard tanúsítvány igénylésére is.

Kiterjesztett ellenőrzésű tanúsítvány (EV SSL)

Az ilyen típusú tanúsítványoknál a tanúsítványban megjelenik a hitelesített szervezet neve is. A kiállítás előtt a domain név, a tulajdonosának az adatai és a szervezet elérhetőségeinek az ellenőrzése is megtörténik. A kiterjesztett hitelesítésű tanúsítványok esetében nincs lehetőség több aldomain neves tanúsítvány kibocsátásra.

Változat #1
DotRoll Tudásbázis hozta létre 21 szeptember 2023 08:32:53
DotRoll Tudásbázis frissítette 21 szeptember 2023 08:33:58