# SSL Tanúsítványok

- .PFX formátumú tanúsítvány használata a cPaneles tárhelyeken
- SSL tanúsítványok és a Server Name Indication (SNI) támogatás
- SSL tanúsítvány konvertálása
- Biztonságos és nem biztonságos tartalom a weboldalon
- Hogyan készíthetek privát kulcsot és CSR fájlt Microsoft Windows rendszeren?
- Hogyan készíthetek privát kulcsot és CSR fájlt Linux paranssorból?
- Mikor javasolt a HTTPS használata?
- Hogyan irányíthatom át a látogatókat HTTPS protokollra?
- Hogyan irányíthatom át a WordPress alapú oldalam HTTP protokollról HTTPS protokollra?
- Hogyan irányíthatom át a weboldalam HTTP protokollról HTTPS protokollra?
- Hogyan készíthetek privát kulcsot és CSR fájlt a cPanel segítségével?
- Tanúsítvány kibocsátások nyomon követése

# .PFX formátumú tanúsítvány használata a cPaneles tárhelyeken

Alapértelmezésben a PKCS#12/PFX formátumot a Microsoft® Windows környezetben használják. Az UNIX alapú gépeken is lehet telepíteni a .pfx kiterjesztésű tanúsítványokat, de a telepítés előtt át kell konvertálni a .pfx kiterjesztésű tanúsítványt mivel az Apache a PEM formátumot vár (.pem, .crt, .cer, és a .key).

## KONVERTÁLÁS WEBOLDALON KERESZTÜL

Az alábbi weboldalon el lehet végezni a konvertálást:

https://www.sslshopper.com/ssl-converter.html

Ha nem szeretne a weboldalon keresztül konvertálni akkor lehetőség van parancssoros konverzióra is az alábbi parancs mintája alapján:

## KONVERTÁLÁS LINUX ALATT:

```
openssl pkcs12 -in certificate.pfx -out certificate.cer -nodes
```

## KONVERTÁLÁS WINDOWS ALATT:

Szükséges az OpenSSL library telepítése amelyet az alábbi oldalról szerezhető be:

http://slproweb.com/products/Win32OpenSSL.html

A telepítést követően Windows parancssorból elvégezhető a konvertálás az alábbi minta alapján:

```
cd C:\Program Files\OpenSSL-Win64\bin
openssl pkcs12 -in d:\Temp\cert.pfx -out d:\Temp\cert.pem -nodes
```

A konvertálást követően egyetlen fájlba fog bekerülni a tanúsítvány, a privát kulcs, ezért a kapott fájlt szövegszerkesztővel meg kell nyitni és a cPanel felületére innen kell beilleszteni a tanúsítványt, valamint a CACert-et.

A tanúsítvány a cPanel felületén az **SSL/TLS kezelő** menü a **Tanúsítványok (CRT)** almenüponton belül tölthető fel.

# SSL tanúsítványok és a Server Name Indication (SNI) támogatás

## MI AZ AZ SNI?

Az SNI a Server Name Indication rövidítése. A TLS protokoll egy kiterjesztése amely lehetővé teszi a kiszolgálók számára, hogy több SSL tanúsítványt használjanak egy IP címen. Gyakorlatilag ez azt jelenti hogy:

- a rendelkezésre álló IPv4 címek száma folyamatosan csökken ezért a jelenleg használt címeken az SNI segítségével hatékonyabban lehet üzemeltetni a kiszolgálókat.
- a legtöbb esetben az SSL tanúsítvánnyal biztonságossá tett weboldalak üzemeltetéséhez nincs szükség külön dedikált IP cím vásárlására.

## SZÜKSÉGES DEDIKÁLT IP CÍM VÁSÁRLÁSA A MEGVÁSÁROLT SSL TANÚSÍTVÁNY HASZNÁLATÁHOZ?

Ez két dologtól függ:

- az adott kiszolgáló támogatja e az SNI-t
- a látogató böngészője támogatja e az SNI-t

Jelenleg minden webszerverünk támogatja az SNI-t, ezért az SSL tanúsítvány használatához nincs szükség dedikált IP cím vásárlására.

## A BÖNGÉSZŐK SNI TÁMOGATOTTSÁGA

A szerverek SNI támogatása mellett szükséges az is, hogy a látogatók böngészői is támogassák az SNI-t. Jellemzően a legtöbb böngésző támogatja az SNI-t, azonban van néhány kivétel, ezek az alábbiak:

- Minden Internet Explorer verzió ami Windows XP operációs rendszeren fut
- Windows XP operációs rendszer alatt futó Safari böngésző
- BlackBerry OS 7.1 és a korábban kiadott verziók
- WindowsMobile 6.5 és a korábban kiadott verziók
- Android OS 2.x alatt használt alapértelmezett böngésző

Abban az esetben ha az érintett weboldal látogatói amelyet SSL tanúsítvánnyal szeretne biztosítani jelentős részében ilyen típusú böngészőkből érik el akkor javasoljuk, hogy az SSL tanúsítvány mellé vásároljon dedikált IP címet is.

# TOVÁBBI INFORMÁCIÓK:

Az SNI-ről további információkat találhat a következő hivatkozáson:

https://en.wikipedia.org/wiki/Server_Name_Indication

# SSL tanúsítvány konvertálása

Különböző platformok és eszközök esetén szükséges lehet az SSL tanúsítványokat eltérő formátumokká alakítani. Például egy Windows kiszolgáló esetén lehetőség van .pfx fájlokat exportálni és importálni, míg egy Apache szerver egyéni PEM (.crt, .cer) fájlokat használ. A különböző SSL tanúsítványok típusairól és a tanúsítványok számítógépen az OpenSSL segítségével történő konvertálásáról további információkat találhat alább.

## PEM FORMÁTUM

A PEM formátum a leggyakoribb formátum, a tanúsítvány kibocsátó hatóságok a leggyakrabban ebben a formátumban adják ki a tanúsítványokat. A PEM tanúsítványok általában **.pem, .crt, .cer és .key** kiterjedésűek. Ezek Base64 kódolt ASCII fájlok, és „—– BEGIN CERTIFICATE —–” sorral kezdődnek illetve „—– END CERTIFICATE —–” sorral végződnek. A kiszolgálói tanúsítványok, köztes tanúsítványok és privát kulcsok mindegyike beilleszthető a PEM formátumba.

Az **Apache és más hasonló szerver szoftverek** PEM formátumú tanúsítványokat használnak. Számos PEM tanúsítvány, sőt a privát kulcs is beilleszthető egy fájlba, egyik a másik alatt, de a legtöbb szerver szoftver, mint például az Apache elvárja, hogy a tanúsítványok és a privát kulcs külön fájlokban legyenek.

## DER FORMÁTUM

A DER formátum egyszerűen a tanúsítvány bináris formája az ASCII-ben lévő PEM formátum helyett. Előfordul, hogy van **.der** fájlkiterjesztése, de gyakran rendelkezik **.cer** fájlkiterjesztéssel, így csak onnan lehet észlelni, hogy egy DER .cer fájl és egy PEM .cer fájl között a különbséget, hogy szövegszerkesztőben megnyitjuk és megkeressük a BEGIN / END utasításokat. A tanúsítványok és magánkulcsok minden típusa DER formátumban kódolható. A DER-t általában **Java platformokkal** használják. Ha a privát kulcsot DER formátumba kell konvertálni akkor kérjük, használja az OpenSSL parancsokat.

## PKCS#7 / P7B FORMÁTUM

A PKCS#7 vagy P7B formátum általában Base64 ASCII formátumban van tárolva és **.p7b vagy .p7c** a kiterjesztése. A P7B tanúsítványok tartalmazzák a fájl elején a „—– BEGIN PKCS7 —–” és a

„—– END PKCS7 —–” sorokat a fájlok végein. A P7B fájl csak tanúsítványokat és lánc tanúsítványokat tartalmaz, privát kulcsot nem. Számos platform támogatja a P7B fájlokat, köztük a **Microsoft Windows és a Java Tomcat**.

# PKCS#12 / PFX FORMÁTUM

A PKCS#12 vagy PFX formátum bináris formátum a szerver tanúsítvány tárolására, a köztes tanúsítványok és a privát kulcs tárolására egy titkosítandó fájlban. A PFX fájlok általában **.pfx és .p12** kiterjesztésűek. A PFX fájlokat általában a **Windows gépeken** használják a tanúsítványok és a magánkulcsok importálásához és exportálásához. PFX fájl PEM formátumra történő konvertálásakor az OpenSSL minden tanúsítványt és privát kulcsot egyetlen fájlba helyez. A fájlt egy szövegszerkesztőben kell megnyitni, és minden egyes tanúsítványt és privát kulcsot (beleértve a BEGIN / END részeket) külön szövegfájlba kell másolni, és egybe kell menteni őket certificate.cer, CACert.cer és privateKey.key néven.

# OPENSSL PARANCSOK SSL TANÚSÍTVÁNYOK KONVERTÁLÁSÁHOZ

Javasoljuk, hogy a saját gépen az OpenSSL segítségével konvertáljon .pfx fájlokról és fájlokba, így a privát kulcsot megtarthatja. Használja a következő OpenSSL parancsokat az SSL tanúsítvány különböző formátumokká konvertálásához a saját gépén:

# KONVERTÁLÁS OPENSSL-EL PEM FORMÁTUMBÓL

**PEM formátum átalakítása DER-be**

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

**PEM formátum átalakítása P7B-re**

```
openssl crl2pkcs7 -nocrl -certfile certificate.cer -out certificate.p7b -certfile CACert.cer
```

**PEM formátum átalakítása PFX-be**

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt
```

# KONVERTÁLÁS OPENSSL-EL DER FORMÁTUMBÓL

### DER formátum átalakítása PEM-be

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

# KONVERTÁLÁS OPENSSL-EL P7B FORMÁTUMBÓL

### P7B formátum átalakítása PEM-be

```
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer
```

### P7B formátum átalakítása PFX-be

```
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer
```

```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out certificate.pfx -certfile CACert.cer
```

# KONVERTÁLÁS OPENSSL-EL PFX FORMÁTUMBÓL

### PFX formátum átalakítása PEM-be

```
openssl pkcs12 -in certificate.pfx -out certificate.cer -nodes
```

Ha a Java Keystore fájlt más formátumra szeretné konvertálni, akkor általában könnyebb új privát kulcsot és tanúsítványokat létrehozni, de a Java Keystore PEM formátumra is konvertálható.

# Biztonságos és nem biztonságos tartalom a weboldalon

Abban az esetben ha a domain nevet a tanúsítvány telepítését követően átirányítjuk biztonságos HTTPS protokollra, akkor előfordulhat, hogy a böngésző címsorában egy törött lakat jelenik meg. Amely mellett figyelmeztető üzenetet is megjelenítenek a böngészők.

A törött lakat, illetve a figyelmeztető üzenetek amiatt jelennek meg, mert a weboldal kódjában egyszerre jelenítünk meg biztonságos és nem biztonságos elemeket. A weboldal csak akkor lesz teljesen biztonságos, – akkor fog megjelenni a böngésző címsorban a zöld lakat – ha minden elemet HTTPS protokollon keresztül jelenítünk meg.

Például:

```
<a href="http://www.pelda.hu/kepek/kep.jpg">Kép megtekintése</a>
```

A fenti HTML példában a hivatkozásban megadott kép URL-je nem biztonságos (http://) címre hivatkozik. Azaz a látogató a tartalom többi részét biztonságos kapcsolaton keresztül tudja megtekinteni, de magát a képet nem, tehát a böngészőben a látogató vegyes tartalmat fog látni. A problémát okozhatják a külsős forrásból meghívott képek, JavaScript, és CSS fájlok is.

# EZT A PROBLÉMÁT KÉT MÓDON LEHET JAVÍTANI:

## RELATÍV HIVATKOZÁSOK HASZNÁLATA:

Azon tartalmak esetében (például ilyenek a weboldalra feltöltött képek, CSS, és Javascript fájlok) amelyek a webtárhelyről elérhető azokra hivatkozzunk relatív módon.

Például:

```
<a href="/kepek/kep.jpg">Kép megtekintése</a>
```

# MINDEN MEGHÍVOTT FORRÁST SSL KAPCSOLATON KERESZTÜL HÍVUNK MEG:

Ebben az esetben minden olyan hivatkozást amelyet a weboldalon meg akarunk jeleníteni, – legyen szó kép, CSS, Javascript, vagy betű típus fájlról – azt biztonságos SSL (https://) kapcsolaton keresztül hívunk meg.

Például:

```
<script type="text/javascript" src="https://pelda.hu/javascript.js" />
```

Sajnos ez a módszer csak akkor használható ha a távoli tartalmat biztosító oldal elérhető HTTPS protokollon keresztül.

> Abban az esetben ha nem érhető el, akkor vagy helyileg kell tárolni a korábban távolról meghívott tartalmat, és arra relatív módon kell hivatkoznunk, vagy pedig olyan forrást kell keresni ahol a hivatkozni kívánt tartalom elérhető biztonságos kapcsolaton keresztül.

# Hogyan készíthetek privát kulcsot és CSR fájlt Microsoft Windows rendszeren?

Ahhoz hogy Microsoft Windows alatt készíthessünk az SSL tanúsítvány igényléséhez majd későbbi használatához szükséges privát kulcsot, illetve tanúsítvány aláírási kérelmet telepíteni kell az OpenSSL binárist. A telepítést követően lehetőségünk lesz a tanúsítvány aláírási kérelem és a hozzá kapcsolódó privát kulcs elkészítésére.

## 1. OPENSSL TELEPÍTÉSE

1. A következő hivatkozást nyissa meg egy böngészőben:

   https://slproweb.com/products/Win32OpenSSL.html
2. A megjelenő oldalon válassza ki az operációs rendszer architektúrájának megfelelő OpenSSL
   - 32 bites operációs rendszer esetén: Win32 OpenSSL v1.0.2p Light
   - 64 bites operációs rendszer esetén: Win64 OpenSSL v1.0.2p Light

   verziót, majd töltse le.
3. A letöltött telepíthető állományt indítsa el, majd kövesse a telepítő utasításait.

## 2. AZ OPENSSL BEÁLLÍTÁSA

Az OpenSSL telepítését követően a használathoz szükséges az OpenSSL konfigurációs fájl helyének beállítása. A beállításhoz kövesse az alábbi lépéseket:

1. Kattintson a **Start** menüre, majd a **Futtatás** parancsra
2. A megjelenő ablakba írja be: `cmd`, majd kattintson az **OK** gombra.
3. A megjelenő parancssori ablakba gépelje be a következő parancsot:
   - 32 bites verzió esetén: `cd \OpenSSL-Win32`
   - 64 bites verzió esetén: `cd \OpenSSL-Win64`

> Abban az esetben ha a telepítés során más könyvtárba került telepítésre az OpenSSL, akkor a fenti elérési úttól eltérő lehet az aktuális útvonal

4. A következő parancsot adja ki ezt követően:
   - 32 bites verzió esetén: `set OPENSSL_CONF=c:\OpenSSL-Win32\bin\openssl.cfg`
   - 64 bites verzió esetén: `set OPENSSL_CONF=c:\OpenSSL-Win64\bin\openssl.cfg`
5. A biztonság kedvéért indítsa újra a számítógépet.

# 3. PRIVÁT KULCS ÉS CSR GENERÁLÁSA MICROSOFT WINDOWS RENDSZER ALATT

A privát kulcs, és a hozzá kapcsolódó CSR fájl elkészítéséhez kövesse az alábbi lépéseket:

1. Kattintson a **Start** menüre, majd keresse meg a **Parancssor** menüt, kattintson rá jobb egér gombbal, majd válassza a **Futtatás rendszergazdaként** lehetőséget. Ezt követően kövesse a képernyőn megjelenő utasításokat.
2. A megjelenő ablakba írja be: `cmd`, majd kattintson az **OK** gombra.
   - 32 bites verzió esetén: `cd \OpenSSL-Win32\bin`
   - 64 bites verzió esetén: `cd \OpenSSL-Win64\bin`A megjelenő parancssori ablakba gépelje be a következő parancsot:

> Abban az esetben ha a telepítés során más könyvtárba került telepítésre az OpenSSL, akkor a fenti elérési úttól eltérő lehet az aktuális útvonal

4. A parancssorba gépelje be a következő parancsot:`openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.crt`

> A fenti parancs segítségével egy privát illetve egy CSR fájl fog készülni. Az elkészített privát kulcs fájl neve *server.key*, míg a CSR fájl neve *server.csr* lesz. Javasoljuk, hogy a példában szereplő elnevezések helyett olyan neveket adjanak meg amelyekről könnyen beazonosítható a CSR fájl illetve a privát kulcs.

5. A parancs elindítása az enter billentyű segítségével történik. A program először elkészíti a privát kulcsot, majd a CSR fájl elkészítéséhez szükséges adatok megadását kéri. Az adatok megadását követően az enter billyentyű lenyomásával lehet tovább lépni.
   - **Country Name**: Meg kell adnia a

    - szervezet székhelyének két nagybetűs országkódját
    - magánszemély esetén a tartózkodási ország két nagybetűs országkódját

> Ügyeljen rá, hogy a helyes két nagybetűs országkódot adja meg (például: HU vagy FR) A teljes országkód lista elérhető a következő hivatkozáson keresztül:
>
> https://www.iso.org/obp/ui/#search

- **State or Province Name**: Adja meg azt az államot, vagy megyét amelyben a:
    - szervezet székhelye található
    - magánszemély esetén annak a városnak az állama vagy megyéjét kell megadni ahova az tartozik
- **Locality Name**: Adja meg a
    - szervezet székhelyének városát
    - magánszemély esetén azt a várost ahol tartózkodik
- **Organization Name**: Adja meg a:
    - szervezet teljes vagy rövidített nevét
    - magánszemély esetén a teljes nevét
- **Organizational Unit Name**: meg lehet adni az adott szervezeten belüli részleg nevét.
- **Common Name**: Ebben a mezőben kell megadnia azt a domain nevet, vagy aldomain nevet amelyre a tanúsítványt a tanúsítvány kibocsájtó ki fogja állítani. A mezőbe a „http://” „https://” előtagokat nem kell beírni.

> A common név mezőben általában a domain nevet kell megadni, például: pelda.hu. Ha az SSL tanúsítványt egy aldomain névre igényli akkor az aldomain.pelda.hu-t kell megadni. Ha helyettesítő (wildcard) SSL tanúsítványt szeretne igényelni, akkor a * karakterrel kell megadni például: *.pelda.hu, ahol a pelda.hu a domain nevet jelöli.

- **Email Address**: Megadhat egy olyan email címet amelyen keresztül fel tudják venni a kapcsolatot Önnel.
- **Challenge password**: Itt elegendő ha üresen hagyja a mezőt, az enter billentyű lenyomásával léphet tovább.
- **Optional company name**: Itt elegendő ha üresen hagyja a mezőt, az enter billentyű lenyomásával léphet tovább.

6. Az OpenSSL az adatok megadását követően elkészíti és elmenti a privát kulcsot *server.key* néven, míg a CSR fájlt *server.csr* néven. Ezt követően az SSL tanúsítvány megrendelése során a *server.csr* fájl tartalmát kell beküldenie a tansítvány kiállításához. A privát kulcsot nem kell elküldenie.A generálást követően az alábbi parancs segítségével jelenítse meg a CSR fájl tartalmát

```
notepad server.csr
```

ez a következőhöz hasonló formában néz ki:

```
-----BEGIN CERTIFICATE REQUEST-----
CSR CODE
-----END CERTIFICATE REQUEST-----
```

A tanúsítvány aláírási kérelemben megadott adatok megtekinthetőek az alábbi parancs segítségével:

```
openssl req -noout -text -in server.csr
```

# Hogyan készíthetek privát kulcsot és CSR fájlt Linux paranssorból?

A tanúsítvány kibocsátásához szükség van egy tanúsítvány aláírási kérelemre, röviden egy CSR fájlra. A CSR fájlban megadott adatok alapján fogja kiállítani a tanúsítvány kibocsátó azt a tanúsítványt amelyet később fel lehet használni többek között weboldalak biztonságossá tételére. A tanúsítvány aláírási kérelem és a hozzá kapcsolódó privát kulcs bármikor elkészíthető parancssorból is.

A CSR fájl generálása során készül egy privát kulcs amelynek segítségével a tanúsítvány kiadását követően a tanúsítvány telepíthető lesz. A privát kulcs generálását követően javasolt a privát kulcsot olyan helyre menteni ahol a későbiekben könnyen megtalálható. A privát kulcs hiányában a tanúsítványok nem telepíthetőek, ebben az esetben a tanúsítvány kiadási folyamtot meg kell ismételni.

## PRIVÁT KULCS ÉS CSR GENERÁLÁSA LINUX KÖRNYEZETBŐL

A privát kulcs, és a hozzá kapcsolódó CSR fájl elkészítéséhez kövesse az alábbi lépéseket:

1. Jelentkezzen be a fiókjába SSH-n keresztül
2. A parancssorba gépelje be a következő parancsot:

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.crt
```

> A fenti parancs segítségével egy privát illetve egy CSR fájl fog készülni. Az elkészített privát kulcs fájl neve *server.key*, míg a CSR fájl neve *server.csr* lesz. Javasoljuk, hogy a példában szereplő elnevezések helyett olyan neveket adjanak meg amelyekről könnyen beazonosítható a CSR fájl illetve a privát kulcs.

3. A parancs elindítása az enter billentyű segítségével történik. A program először elkészíti a privát kulcsot, majd a CSR fájl elkészítéséhez szükséges adatok megadását kéri. Az

adatok megadását követően az enter billentyű lenyomásával lehet tovább lépni.

- **Country Name**: Meg kell adnia a
  - szervezet székhelyének két nagybetűs országkódját
  - magánszemély esetén a tartózkodási ország két nagybetűs országkódját

> Ügyeljen rá, hogy a helyes két nagybetűs országkódot adja meg (például: HU vagy FR) A teljes országkód lista elérhető a következő hivatkozáson keresztül:
>
> https://www.iso.org/obp/ui/#search

  - **State or Province Name**: Adja meg azt az államot, vagy megyét amelyben a:
    - szervezet székhelye található
    - magánszemély esetén annak a városnak az állama vagy megyéjét kell megadni ahova az tartozik
  - **Locality Name**: Adja meg a
    - szervezet székhelyének városát
    - magánszemély esetén azt a várost ahol tartózkodik
  - **Organization Name**: Adja meg a:
    - szervezet teljes vagy rövidített nevét
    - magánszemély esetén a teljes nevét
  - **Organizational Unit Name**: meg lehet adni az adott szervezeten belüli részleg nevét.
  - **Common Name**: Ebben a mezőben kell megadnia azt a domain nevet, vagy aldomain nevet amelyre a tanúsítványt a tanúsítvány kibocsájtó ki fogja állítani. A mezőbe a „http://” „https://” előtagokat nem kell beírni.

> A common név mezőben általában a domain nevet kell megadni, például: pelda.hu. Ha az SSL tanúsítványt egy aldomain névre igényli akkor az aldomain.pelda.hu-t kell megadni. Ha helyettesítő (wildcard) SSL tanúsítványt szeretne igényelni, akkor a * karakterrel kell megadni például: *.pelda.hu, ahol a pelda.hu a domain nevet jelöli.

  - **Email Address**: Megadhat egy olyan email címet amelyen keresztül fel tudják venni a kapcsolatot Önnel.
  - **Challenge password**: Itt elegendő ha üresen hagyja a mezőt, az enter billentyű lenyomásával léphet tovább.
  - **Optional company name**: Itt elegendő ha üresen hagyja a mezőt, az enter billentyű lenyomásával léphet tovább.

4. Az OpenSSL az adatok megadását követően elkészíti és elmenti a privát kulcsot *server.key* néven, míg a CSR fájlt *server.csr* néven. Ezt követően az SSL tanúsítvány megrendelése során a *server.csr* fájl tartalmát kell beküldenie a tansítvány kiállításához. A privát kulcsot nem kell elküldenie.A generálást követően az alábbi parancs segítségével jelenítse meg a CSR fájl tartalmát

```
cat server.csr
```

ez a következőhöz hasonló formában néz ki:

```
-----BEGIN CERTIFICATE REQUEST-----
CSR CODE
-----END CERTIFICATE REQUEST-----
```

A tanúsítvány aláírási kérelemben megadott adatok megtekinthetőek az alábbi parancs segítségével:

```
openssl req -noout -text -in server.csr
```

# 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.

# Hogyan irányíthatom át a látogatókat HTTPS protokollra?

Abban az esetben ha érvényes tanúsítvány lett beállítva a domain névnél akkor javasolt a látogatókat átirányítani a nem biztonságos http:// címről a biztonságos https:// címre.

Az átirányítást legegyszerűbben az adott domain névhez tartozó dokumentum_root mappájában található .htaccess fájl módosításával oldható meg.

> A példában szereplő sorok segítségével az adott domain név minden felhasználóját át fogja irányítani a nem biztonságos (http://) URL-ről a biztonságos (https://) URL-re.

A példában szereplő pelda.hu domain nevet cserélje ki a saját domain nevére.

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://pelda.hu/$1 [R=301,L]
```

# Hogyan irányíthatom át a WordPress alapú oldalam HTTP protokollról HTTPS protokollra?

A WordPress tartalom kezelő rendszer esetében az adminisztrációs felületen keresztül lehet beállítani azt, hogy az érintett oldal *https://* címen keresztül legyen elérhető.

A beállítás menete a következő:

- Bejelentkezést követően A **Vezérlőpult** -> **Beállítások** -> **Általános** részen a **WordPress cím (URL)** és a **Honlap cím (URL)** mezőkben kell módosítani a jelenlegi *http://* előtagot *https://*-re.
  A mentést követően a WordPress ki fogja jelentkeztetni a bejelenetkezett felhasználót, annak újra be kell jelentkeznie.
- Ezt követően egy FTP kliens segítségével be kell jelentkezni a tárhelyre, és a domain névhez tartozó dokumentum root könyvtárban található ***.htaccess*** fájlt, illetve a ***wp-config.php*** fájlt kell szerkeszteni.
  A .htaccess fájl elejére az alábbi kódot kell beilleszteni:

```
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://domain-nev.hu/$1 [R,L]
```

> Az utolsó sorban található domain-nev.hu-t módosítania kell arra a domain névre amely alatt a WordPress üzemel.

- A wp-config.php fájlban meg kell keresni az „Ennyi volt kellemes bloggolást” sort , és fölé kell elhelyezni az alábbi kódrészletet:

```
define('FORCE_SSL_ADMIN', true);
// in some setups HTTP_X_FORWARDED_PROTO might contain
// a comma-separated list e.g. http,https
// so check for https existence
if (strpos($_SERVER['HTTP_X_FORWARDED_PROTO'], 'https') !== false)
	$_SERVER['HTTPS']='on';
```

- Ahhoz, hogy a közvetlen hivatkozások is helyesen jelenjenek meg a elegendő ha a Közvetlen hivatkozások menüpontban rákattintunk a mentés gombra. Ekkor a WordPress automatikusan újra fogja generálni a .htaccess fájlt.

**Amennyiben bármilyen további kérdése van, forduljon Ügyfélszolgálatunkhoz bizalommal.**

# Hogyan irányíthatom át a weboldalam HTTP protokollról HTTPS protokollra?

## AZ ÖSSZES FORGALOM ÁTIRÁNYÍTÁSA

Ahhoz, hogy az összes HTTP-re érkező kérést HTTPS protokollra tudja irányítani az alábbi kódsorozatot kell a domain névhez tartózó dokumentum_root könyvtárban található .htaccess fájlban szerepeltetnie:

```
RewriteCond %{REQUEST_URI} !^/[0-9]+\..+\.cpaneldcv$
RewriteCond %{REQUEST_URI} !^/\.well-known/pki-validation/[A-F0-9]{32}\.txt(?:\ Comodo\ DCV)?$
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://www.példa.hu/$1 [R=301,L]
```

Az utolsó sorban szereplő *www.példa.hu* domain nevet mindenképpen cserélje ki arra a domain névre amelynél szeretné beállítani a HTTPS protokollt.

## ADOTT DOMAIN NÉV ÁTIRÁNYÍTÁSA

Ha csak egy adott domain név esetében szeretné átirányítani HTTPS protokollra akkor az alábbi kódsorozatot kell a domain névhez tartózó dokumentum_root könyvtárban található .htaccess fájlban szerepeltetnie:

```
RewriteCond %{REQUEST_URI} !^/[0-9]+\..+\.cpaneldcv$
RewriteCond %{REQUEST_URI} !^/\.well-known/pki-validation/[A-F0-9]{32}\.txt(?:\ Comodo\ DCV)?$
RewriteEngine On
```

```
RewriteCond %{HTTP_HOST} ^példa\.hu [NC]
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://www.példa.hu/$1 [R=301,L]
```

Figyeljen arra. hogy a *példa\.hu* és a *www.példa.hu* domain nevet mindenképpen cserélje ki arra a domain névre amelynél szeretné beállítani a HTTPS protokollt.

# ÁTIRÁNYÍTÁS EGY SPECIÁLIS KÖNYVTÁRRA.

Ahhoz, hogy az összes HTTP-re érkező kérést HTTPS protokollra, és azon belül egy megadott könyvtárra tudja irányítani az alábbi kódsorozatot kell a domain névhez tartózó dokumentum_root könyvtárban található .htaccess fájlban szerepeltetnie:

```
RewriteCond %{REQUEST_URI} !^/[0-9]+\..+\.cpaneldcv$
RewriteCond %{REQUEST_URI} !^/\.well-known/pki-validation/[A-F0-9]{32}\.txt(?:\ Comodo\ DCV)?$
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteCond %{REQUEST_URI} konyvtar
RewriteRule ^(.*)$ https://www.példa.hu/konyvtar/$1 [R=301,L]
```

A *konyvtar* könyvtár nevet, valamint a *www.példa.hu/konyvtar* domain nevet mindenképpen cserélje ki arra a domain névre, és könyvtárra amelynél szeretné beállítani a HTTPS protokollt.

# Hogyan készíthetek privát kulcsot és CSR fájlt a cPanel segítségével?

A tanúsítvány kibocsátásához szükség van egy tanúsítvány aláírási kérelemre, röviden egy CSR fájlra. A CSR fájlban megadott adatok alapján fogja kiállítani a tanúsítvány kibocsátó azt a tanúsítványt amelyet később fel lehet használni többek között weboldalak biztonságossá tételére. A tanúsítvány aláírási kérelmet a cPanel felületén akár a tanúsítvány megrendelés előtt el lehet készíteni.

> A CSR fájl generálása során készül egy privát kulcs amelynek segítségével a tanúsítvány kiadását követően a tanúsítvány telepíthető lesz. A cPanel felületen kersztül generált tanúsítvány aláírási kérelmek esetén a cPanel a privát kulcsot is elkészíti, illetve tárolja, ez a cPanel felületén bármikor elérhető.

## A TANÚSÍTVÁNY ALÁÍRÁSI KÉRELEM ELKÉSZÍTÉSE:

1. Jelentkezzen be a cPanel kezelőfelületére.
2. Keresse meg az SSL/TLS kezelő menü pontot, és kattintson rá.
   SSL/TLS kezelő
   SSL/TLS kezelő
3. Kattintson a **Tanúsítvány-aláírási kérelmek (CSR)** felirat alatt található **SSL tanúsítvány aláírási kérelem generálása, megtekintése vagy törlése.** hivatkozásra.
   Új tanúsítvány-aláírási kérelem (CSR) generálása
   Új tanúsítvány-aláírási kérelem (CSR) generálása

4. A megjelenő oldalon az alábbi adatokat kell megadnia (*a csillaggal jelölt mezőket ki kell tölteni*):
   - **Kulcs**: Abban az esetben ha korábban nem készített titkos kulcsot akkor lehetőség van a titkos kulcs erősségének kiválasztására.

- **Domainek**: Ebben a mezőben kell megadnia azokat a domain neveket, vagy aldomain neveket amelyekre a tanúsítványt a tanúsítvány kibocsájtó ki fogja állítani. A mezőbe a „http://” „https://” előtagokat nem kell beírni.

> A Domainek mezőben általában a domain nevet kell megadni, például: pelda.hu. Ha az SSL tanúsítványt egy aldomain névre igényli akkor az aldomain.pelda.hu-t kell megadni. Ha helyettesítő (wildcard) SSL tanúsítványt szeretne igényelni, akkor a * karakterrel kell megadni például: *.pelda.hu, ahol a pelda.hu a domain nevet jelöli. Több domain név megadása esetén soronként egy domain nevet adjon meg.

  - **Város**: Adja meg a
    - szervezet székhelyének városát
    - magánszemély esetén azt a várost ahol tartózkodik

  - **Megye vagy állam**: Adja meg azt az államot, vagy megyét amelyben a:
    - szervezet székhelye található
    - magánszemély esetén annak a városnak az állama vagy megyéjét kell megadni ahova az tartozik
  - **Ország**: A lehulló listából válassza ki a:
    - szervezet székhelyének országát
    - magánszemély esetén a tartózkodási országát
  - **Szervezet**: Adja meg a:
    - szervezet teljes vagy rövidített nevét
    - magánszemély esetén a teljes nevét
  - **Szervezeti részleg**: meg lehet adni az adott szervezeten belüli részleg nevét.
  - **Levelezés**: Megadhat egy olyan email címet amelyen keresztül fel tudják venni a kapcsolatot Önnel.
  - **Hozzáférési kód**: Jelszót állíthat be a CSR fájlhoz. Egyes esetekben a tanúsítvány kibocsátó megköveteli hogy a CSR fájl is jelszóval legyen védve.
  - **Leírás**: A könnyebb azonosíthatóság érdekében érdemes egyedi nevet adni a CSR fájlnak.

5. Az adatok megadását követően kattintson a **Generálás** gombra.
6. A generálást követően az oldal meg fogja jeleníteni a CSR fájlt kétféle formátumban is. Önnek a **Kódolt tanúsítvány-aláírási kérelem:** résznél megjelenő szöveget kell bemásolnia a megrendeléshez amely az alábbi formában néz ki:

```
-----BEGIN CERTIFICATE REQUEST-----
CSR CODE
-----END CERTIFICATE REQUEST-----
```

# Tanúsítvány kibocsátások nyomon követése

Elérhető már legújabb biztonsági funkciónk, a tanúsítvány kibocsátások nyomon követése. Minden olyan ügyfelünk, akinek van domain neve cégünknél, tudja használni.

## Mi az a tanúsítvány kibocsátások nyomon követése?

A különböző domain nevek számára több millió tanúsítvány kerül naponta kibocsátásra, ezek pedig naplóban kerülnek rögzítésre. Ennek a funkciónak a segítségével átvizsgáljuk ezeket a naplókat és e-mailt küldünk az Ön számlavezető e-mail címére, amikor találunk egy tanúsítványt az Ön domain nevére. Ha Ön például a mintadomain.hu-t kezeli, akkor észleljük a *.mintadomain.hu tanúsítványokat is, hogy segítsünk észre venni a rosszindulatú vagy váratlan tanúsítványokat.

## Hogy lehet bekapcsolni a funkciót?

1. Jelentkezzen be az admin.dotroll.com oldalon fiókjába!
2. Domainek - Domain neveim menüpontban válassza ki azt a domaint, ahol be akarja kapcsolni a funkciót!
3. Kattintson rá, majd az Áttekintés rész után kapcsolja be a Tanúsítvány kibocsátások nyomon követése funkciót!

## Kiknek ajánlott a funkció bekapcsolása?

Azoknak ajánlott, akik technikailag fel tudják mérni, hogy egy adott tanúsítvány valós vagy hamis. Azoknak az ügyfeleinknek viszont mindenképpen erősen ajánlott, akik nagyértékű vagy különlegesen kezelt adatokat kezelnek, továbbítanak vagy védenek az adott domain névvel összefüggő tanúsítványokkal.

## Mi a teendő, ha rosszindulatú tanúsítványról kap értesítést?

Ha úgy gondolja, hogy  hamis tanúsítványt adtak ki az Ön domain nevéhez, akkor vegye fel a kapcsolatot e-mailben a kibocsátóként megadott tanúsító hatósággal, ők tudnak csak visszavonni rosszindulatú tanúsítványokat. Ha rosszindulatú domaint vett észre, akkor vegye fel ügyfélszolgálatunkkal a kapcsolatot.