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
```

Változat #1
DotRoll Tudásbázis hozta létre 2023-09-21 08:29:56 CEST
DotRoll Tudásbázis frissítette 2023-09-21 08:31:57 CEST