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
```

Változat #1
DotRoll Tudásbázis hozta létre 2023-09-21 08:32:03 CEST
DotRoll Tudásbázis frissítette 2023-09-21 08:32:49 CEST