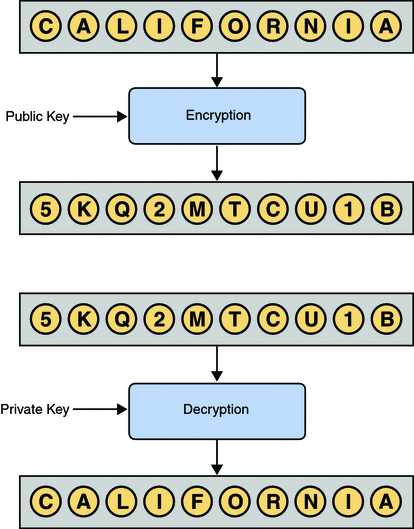
**Nyilvános kulcsok, privát kulcsok és tanúsítványok**

A hitelesítés során az SSL a *nyilvános kulcsú titkosításnak* nevezett technikát használja .

A nyilvános kulcsú kriptográfia a kulcspár fogalmán alapul, amely egy *nyilvános kulcsból* és egy *privát kulcsból* áll . A nyilvános kulccsal titkosított adatok csak a megfelelő privát kulccsal dekódolhatók. Ezzel szemben a privát kulccsal titkosított adatok csak a megfelelő nyilvános kulccsal dekódolhatók.



A kulcspár tulajdonosa bárki számára elérhetővé teszi a nyilvános kulcsot, de a titkos kulcsot titokban tartja.

A *tanúsítvány* igazolja, hogy egy entitás egy adott nyilvános kulcs tulajdonosa.

Az X.509 szabványt követő tanúsítványok tartalmaznak egy adatrészt és egy aláírás részt. Az adatrész olyan információkat tartalmaz, mint:

* A nyilvános kulcsot birtokló entitás megkülönböztetett neve
* A tanúsítványt kiállító entitás megkülönböztetett neve
* Az az időtartam, ameddig a tanúsítvány érvényes
* Maga a nyilvános kulcs

Tanúsítványt beszerezhet egy tanúsító hatóságtól (CA), például a VeriSign-től. Alternatív megoldásként létrehozhat egy *önaláírt tanúsítványt* , amelyben a tulajdonos és a kibocsátó ugyanaz.

A tanúsítványokat kibocsátó szervezet felállíthatja a CA-k hierarchiáját. A gyökér CA rendelkezik egy önaláírt tanúsítvánnyal. Minden alárendelt hitelesítésszolgáltató rendelkezik egy tanúsítvánnyal, amelyet a hierarchiában következő legmagasabb hitelesítésszolgáltató ír alá.A *tanúsítványlánc* egy adott CA tanúsítványa, valamint minden magasabb szintű CA tanúsítványa a gyökér CA-n keresztül.

### https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/

### Hogyan találhatom meg az SSL-tanúsítványom privát kulcsát?

Ha most kapott egy kiállított SSL-tanúsítványt, és nehezen találja meg a megfelelő privát kulcsot, ez a cikk segíthet megtalálni a tanúsítványhoz tartozó egyetlen kulcsot.

* [Mi az a privát kulcs?](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#1)
  + [Nyilvános kulcs vs privát kulcs](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#1.1)
  + [Hogyan hozhat létre privát kulcsot?](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#1.2)
  + [Létrehozhatok új privát kulcsot az SSL-tanúsítványomhoz?](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#1.3)
  + [Hogyan néz ki egy privát kulcs?](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#1.4)
* [Hogyan lehet visszaszerezni egy rosszul elhelyezett privát kulcsot](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#Retr)
  + [Privát kulcs lekérése különböző szerverplatformokon](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#RetrPlatforms)
* [Van több privát kulcsom](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#Several)
* [Nincs privát kulcs](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#Notlocated)

## Mi az a privát kulcs?

Először is, merüljünk el egy kicsit az alapokban. A globális nyilvános kulcsú infrastruktúra kialakítása, amelyre támaszkodik az [SSL/TLS](https://uk.wikipedia.org/wiki/Transport_Layer_Security) -en keresztüli modern biztonságos egyeztetés , azt jelenti, hogy mindig van pár egyedi kulcs –

### Nyilvános kulcs vs privát kulcs

A nyilvános kulcs be van ágyazva az SSL-tanúsítványba, a privát kulcs pedig a szerveren tárolódik, és titokban marad. Amikor a webhely látogatója kitölt egy űrlapot személyes adataival, és elküldi a szervernek, az információt a nyilvános kulccsal titkosítják, hogy megvédjék a lehallgatástól. A szerveren ezeket az információkat a privát kulcs visszafejti, és továbbítja a további feldolgozáshoz. Annak érdekében, hogy senki más ne tudja visszafejteni a továbbított üzenetet, egyedi és hamisíthatatlan kulcspárt kell használnunk. Dióhéjban tehát egyik kulcs a másik nélkül haszontalan.

### Hogyan hozhat létre privát kulcsot?

[A privát kulcs a tartománynevet, a nyilvános kulcsot és a további kapcsolattartási információkat tartalmazó CSR](https://www.namecheap.com/support/knowledgebase/article.aspx/467/2290/how-to-generate-csr-certificate-signing-request-code/) -rel (tanúsítvány-aláíró kérelem) egyidejűleg jön létre . [A CSR-t a tanúsítvány aktiválása](https://www.namecheap.com/support/knowledgebase/article.aspx/794/67/how-do-i-activate-an-ssl-certificate) után azonnal el kell küldeni a tanúsító hatóságnak (CA) érvényesítés és aláírás céljából a Namecheap felhasználói fiók panelen. A privát kulcsot titokban kell tartani, ideális esetben ugyanazon a szerveren, amelyre a tanúsítványt telepítik.

### Létrehozhatok új privát kulcsot az SSL-tanúsítványomhoz?

Mivel egy nyilvános kulcsot a kiegészítő információkkal (azaz a domain névvel és az adminisztratív kapcsolattartási adatokkal) alá kell írnia egy megbízható tanúsító hatóságnak ahhoz, hogy alkalmazható és legitim legyen az Ön szerverével való kommunikáció biztosításához, nem lenne sok értelme, ha csak létrehozhat egy új privát kulcsot egy már érvényesített nyilvános kulcshoz. Másrészt biztosnak kell lennünk abban, hogy senki sem hozhat létre megfelelő privát kulcsot nyilvános kulcs alapján. Így a modern kriptorendszerek szinte lehetetlenné teszik ezt a feladatot.

### Hogyan néz ki egy privát kulcs?

A privát kulcs egy kódolt adatrész, általában néhány tucat sor véletlenszerűen kinéző szimbólumból, amelyeket a következőhöz hasonló fejlécekkel zárnak: -----BEGIN RSA PRIVATE KEY----- és -----END RSA MAGÁNKULCS -----



Ennek ellenére a legtöbb esetben ez a kód nem kerül a látókörébe a CSR generálásakor. Általában a háttérben jön létre, és csendben menti a szerver fájlrendszerébe. És nyilvánvaló, hogy az [SSL tanúsítvány telepítése](https://www.namecheap.com/support/knowledgebase/article.aspx/795/69/how-to-install-ssl-certificates) során a kulcsot automatikusan le kell kérni a tanúsítványhoz. Néhány rendszer azonban nem rendelkezik ilyen viselkedéssel, vagy néha egy másik szerverre kell telepítenünk a tanúsítványt. Ezek a példák azokra az esetekre, amikor valóban tudnunk kell a privát kulcs pontos helyét.

## Hogyan lehet visszaszerezni egy rosszul elhelyezett privát kulcsot

Ez egy bizonyos szerver operációs rendszertől függ, és attól, hogy CLI-t (command line interface) vagy egy adott típusú web-hoszting vezérlőpanelt használtak a CSR generálásához. És itt jön a fő rész.

Az alábbiakban tippeket, példákat és tanácsokat találhat, amelyeket érdemes követnie annak érdekében, hogy egy hiányzó rejtvényt kapjon, és elkerülje a tanúsítványok újrakiadását (azaz az aktiválási és érvényesítési folyamat megismétlését a semmiből).

### Privát kulcs lekérése különböző szerverplatformokon

* [Linux operációs rendszerek (Apache, Nginx, Lighttpd, Heroku)](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#lnx)
* [Windows operációs rendszerek (IIS, Exchange, Small Business szerver)](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#wndws)
* [Mac OS X](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#mcsx)
* [Tomcat (keytool használatával)](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#tmctkt)
* [cPanel](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#cpnl)
* [WHM](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#whm)
* [Plesk](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#plsk)
* [Synology NAS DSM](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#snlgns)
* [Webmin](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#wbmn)
* [VestaCP](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#vstcp)
* [DirectAdmin](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#drctdmn)
* [Webuzo](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#wbz)
* [A CSR egy online eszközön keresztül készült](https://www.namecheap.com/support/knowledgebase/article.aspx/9834/69/how-can-i-find-the-private-key-for-my-ssl-certificate/#OnlineTool)

**Linux operációs rendszerek (Apache, Nginx, Lighttpd, Heroku)**  
  
Hagyományosan a magánkulcsok Linux alapú operációs rendszereken (Ubuntu, Debian, CentOS, RedHat stb.) **openssl által generált kulcsok a titkosítási eszközkészlettel** , és a .key-vel menthetők fájlba vagy .pem kiterjesztéssel. Mivel azonban Linux rendszereken az egyszerű szövegfájlokhoz nem kötelező bizonyos kiterjesztések, a privát kulcs kódja gyakorlatilag bármilyen nevű fájlba helyezhető.

Ha emlékszik a .key fájl teljes vagy részleges nevére, megpróbálhatja megtalálni a helyét a "find" parancs futtatásával az alábbiak szerint:

sudo find [search\_start\_folder] -type f -iname 'private.key'

- [search\_start\_folder]paraméter azt a könyvtárat jelöli, ahol a keresést a benne lévő összes könyvtárból indítani kell, például a „root”-ból történő kereséshez a / jelet kell megadni;  
- részleges fájlnév alapján történő kereséshez a fájl feltételezett nevét csillaggal (\*) kell megadni, például a „\*.key” érték lehetővé teszi minden „.key”-re végződő fájl megtalálását.

***TIPP****: A kulcsfájl neve nagyon gyakran hasonlít arra a domain névre, amelyre a tanúsítványt kiállították, pl. „example.com.key”, „example\_com.key”, „example-com.key” stb.*