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.

Változat #1
DotRoll Tudásbázis hozta létre 21 szeptember 2023 08:28:05
DotRoll Tudásbázis frissítette 21 szeptember 2023 08:28:52