

Взято: <http://www.myvitebsk.by/faq/question-10135.page>

В консоли LINUX-сервера таким образом:

-----**SSL: Convert PEM to PFX**-----

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

-----**SSL: Convert PEM to P7B**-----

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

-----**SSL: Convert PEM to DER**-----

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

-----**SSL: Convert DER to PEM**-----

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

-----**SSL: Convert P7B to PEM**-----

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

-----**SSL: Convert P7B to PFX**-----

```
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
```

-----**SSL: Convert PFX to PEM**-----

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

**Где:**

- **privateKey.key** - приватный ключ начинающейся внутри со строки "-----BEGIN RSA

PRIVATE KEY-----" и заканчивается строкой "-----END RSA PRIVATE KEY-----"

- **certificate.crt** - это сам файл сертификата начинающейся внутри со строки "-----BEGIN CERTIFICATE-----" и заканчивается строкой "-----END CERTIFICATE-----"

- **CACert.crt** - корневые сертификаты центра сертификации Thawte в одной файле начинающихся со строки "-----BEGIN CERTIFICATE-----" внутри файла (как правило root.crt).

Важно заметить, что утилита **openssl** запросит у вас создание пароля для импорта конечного файла и подтверждение данного пароля, с помощью этого пароля вы сможете в последствии импортировать выходной файл в центр ваших сертификатов.