openSSL

Generowanie klucza prywatnego

cd /etc/ssl/*nazwaSerwera/*

Generujemy klucz prywatny RSA bez hasła (gdy chcemy, aby np. serwer *Apache* startował bez pytania o hasło):

openssl genrsa 2048 -out *mojaDomena***.key** *(lub *.pem)*

Generujemy klucz prywatny RSA z hasłem:

openssl genrsa -des3 2048 -out *mojaDomena***.key** *(lub *.pem)*

Usuwanie hasła z klucza prywatnego:

openssl rsa -in *mojaDomena***.key -out** *mojaDomena***.key**

Weryfikacja klucza prywatnego:

openssl rsa -in mojaDomena.key -check

Generowanie żądania certyfikatu

Generujemy żądanie certyfikatu (prośbę o podpisanie certyfikatu) na podstawie naszego klucza prywatnego:

openssl req -new -key *mojaDomena***.key -out** *mojaDomena***.csr**

Info: Nie używamy znaków narodowych.

Common Name: (tutaj pełna nazwa domenowa FQDN szyfrowanej strony)

A challenge password []: (pozostawiamy puste)

Weryfikacja żądania certyfikatu:

openssl req -noout -verify in *mojaDomena***.csr**

Generowanie certyfikatu

Info: Certyfikat na serwerze nie służy do szyfrowania, jego zadanie to udowodnienie przed klientem, że jest tym, za kogo się podaje (uwierzytelnienie). Zawiera klucz publiczny, informacje o właścicielu, informacje o wystawcy certyfikatu i jego podpis, data ważności.

openssl req -x509 -new -days 365 -in *mojaDomena***.csr -signkey** *mojaDomena***.key -out** *mojaDomena***.crt**

Weryfikacja certyfikatu:

openssl -x509 -noout -text in *mojaDomena***.crt** *(lub *.pem)*

Certyfikat w formacie PFX. Najpierw tworzymy zwykłą parę klucz / certyfikat (na koncie root):

openssl req -new -x509 -keyout /etc/ssl/private/*kluczPrywatny***.key -out /etc/ssl/certs/** *certyfikat***.crt -days 3650 -nodes**

Zamiana na format windowsowy PFX (wymaga ustanowienia hasła dla klucza prywatnego):

openssl pkcs12 -export -out *certyfikat-oraz-klucz-prywatny***.pfx -inkey /etc/ssl/private/** *kluczPrywatny***.key -in /etc/ssl/certs/***certyfikat***.crt**

Legenda:

- **pkcs12** - moduł tworzący pliki w formacie PFX;
- **-inkey** - może także zawierać klucze prywatne w formacie *.pem;
- **-days 3650** - maksymalny okres ważności;
- **-x509** - certyfikat ma być podpisany;

Ostatnia aktualizacja: 2 maja 2019.