3.1 ????????? ???????????

В якості сертифікату можна використовувати самопідписаний TLS сертифікат, створений за допомогою утиліти OpenSSL. Такий сертифікат можна створити засобами робочої станції адміністратора.

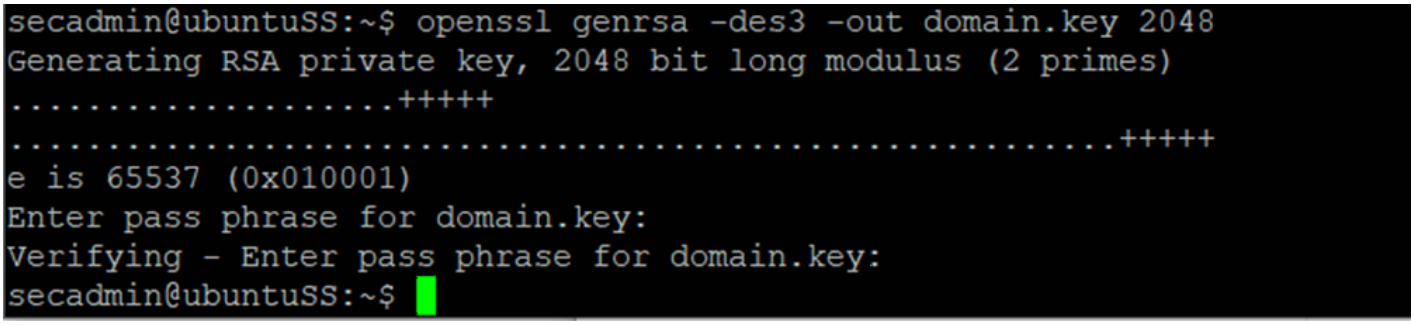
Для цього необхідно виконати наступні дії:

1. Відкрити консоль (термінал) робочої станції адміністратора за допомогою натиснення комбінації клавіш «Ctrl+Alt+T».

2. Створити особистий ключ у за допомогою виконання наступної команди:

```
openssl genrsa -des3 -out domain.key 2048
```

Під час виконання команди необхідно двічі ввести пароль для файлу особистого ключа.



Після виконання команди в директорії (за замовчуванням це /home/{username}) з'явиться файл особистого ключа domain.key.

3. Створити запит на підпис сертифіката відкритого ключа (CSR) за допомогою виконання наступної команди:

```
openssl req -key domain.key -new -out domain.csr
```

При виконанні даної команди необхідно ввести пароль заданий на попередньому кроці, після чого необхідно вказати наступні дані:

- Country Name (2 letter code) [AU] – скорочений код країни – UA,

- State or Province Name (full name) [Some-State]: – назва області, наприклад Kyiv oblast,

- Locality Name (eg, city) []: — назва міста, наприклад Kyiv,

- Organization Name (eg, company) [Internet Widgits Pty Ltd]: — скорочена назва організації, наприклад Comp,

- Organizational Unit Name (eg, section) []: — скорочена назва підрозділу організації, наприклад Unit,

- Common Name (e.g. server FQDN or YOUR name) []: — власне ім’я (можна використовувати доменне ім’я), наприклад domain,

- Email Address []: — адреса електронної пошти, наприклад email@email.com.

Поля «A challenge password» та «An optional company name» можна залишити порожніми.

```
secadmin@ubuntuSS:~$ openssl req -key domain.key -new -out domain.csr
Enter pass phrase for domain.key:
Can't load /home/secadmin/.rnd into RNG
140147556790720:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/r
and/randfile.c:88:Filename=/home/secadmin/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:UA
State or Province Name (full name) [Some-State]:Kyiv oblast
Locality Name (eg, city) []:Kyiv
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Comp
Organizational Unit Name (eg, section) []:Unit
Common Name (e.g. server FQDN or YOUR name) []:domain
Email Address []:email@email.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Після виконання команди в директорії (за замовчуванням це /home/{username}) з'явиться файл запиту на підпис domain.csr.

4. Створити самопідписаний сертифікат за допомогою виконання наступної команди:

```
openssl x509 -signkey domain.key -in domain.csr -req -days 365 -out domain.crt
```

Під час виконання даної команди необхідно ввести пароль особистого ключа, створеного при виконанні настанов пункту 2 даного розділу.

Після виконання команди в директорії (за замовчуванням це /home/{username}) з'явиться файл сертифікату відкритого ключа domain.crt.

5. Отриманий сертифікат буде створено в форматі PEM. Для подальшого використання його необхідно перетворити в сертифікат формату DER за допомогою виконання наступної

команди:

openssl x509 -in domain.crt -outform der -out domain.der

Після виконання даної команди в директорії (за замовчуванням це /home/{username}) з'явиться файл сертифікату domain.der.

Версія #2
Admin створив 2024-06-25 09:59:23 UTC
Admin оновив 2024-06-30 20:00:12 UTC