

3. ?????????????

?????????????????

????????????????

????????

Запити до внутрішньої служби для завантаження підписаних документів завжди повинні надходити через протокол HTTPS (незалежно від того, яке з'єднання між клієнтом сервісу та шлюзом безпечного обміну налаштовано адміністратором).

Для завантаження повідомлень необхідно, щоб TLS сертифікат відкритого ключа HTTPS клієнта був завантажений на шлюз безпечного обміну, а програмне забезпечення, за допомогою якого виконується запит (наприклад, інструмент Postman) було налаштоване на використання відповідного особистого ключа TLS.

- [3.1 Створення сертифікату](#)
- [3.2 Додавання сертифікату у Postman](#)
- [3.3. Додавання сертифікату на шлюз безпечного обміну](#)

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.

```
secadmin@ubuntuSS:~$ openssl genrsa -des3 -out domain.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for domain.key:
Verifying - Enter pass phrase for domain.key:
secadmin@ubuntuSS:~$ █
```

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
```

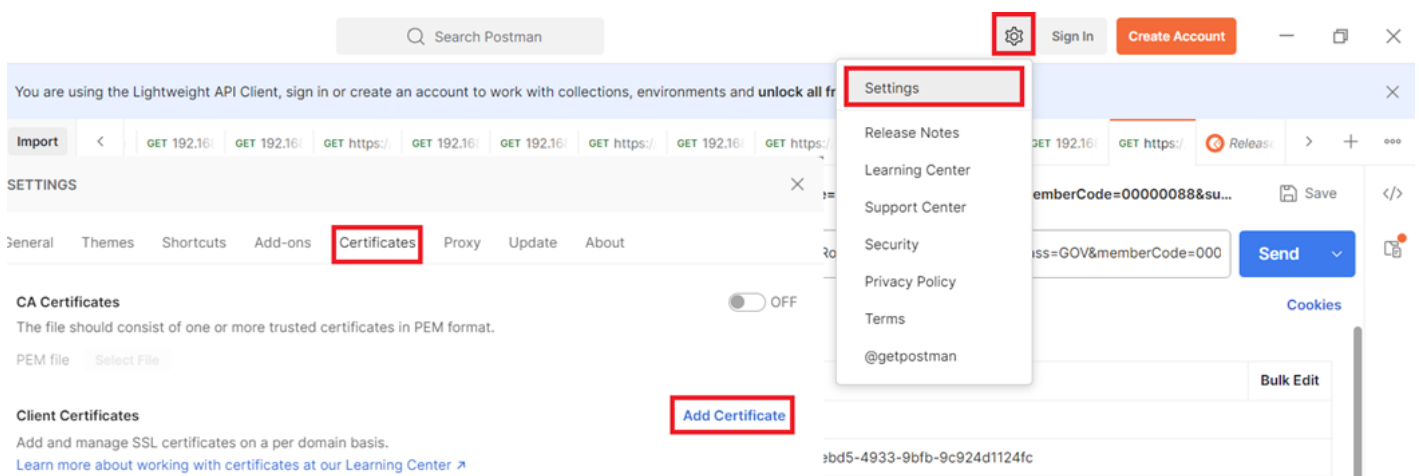
Після виконання даної команди в директорії (за замовчуванням це /home/{username}) з'явиться файл сертифікату domain.der.

3.2 ?????????? ?????????????? ?

Postman

Для того, щоб додати створений сертифікат та відповідний особистий ключ у Postman необхідно виконати наступні дії:

1. Натиснути на позначку «⚙️» та обрати пункт «Settings».
2. У вікні, що відкриється, необхідно обрати вкладку «Certificates» та натиснути на кнопку «Add Certificate»:



3. У наступному вікні необхідно для полів:

Host – вказати внутрішню (сіру) IP-адресу шлюзу безпечного обміну,

CRT – завантажити файл сертифікату відкритого ключа, який було створено в розділі 3.1 на кроці 5,

KEY — завантажити файл закритого ключа, який було створено в розділі 3.1 на кроці 2,

PFX – залишити порожнім,

Passphrase — ввести пароль, який було задано при створенні закритого ключа, в розділі 3.1 на кроці 5

host

CRT file

KEY file

PFX file















Passphrase

та натиснути на кнопку «Add». Сертифікат з'явиться у вікні доступних сертифікатів.



3.3. ?????????? ?????????????? ?? ????? ?????????????? ????????

Для додавання сертифікату на шлюзі безпечного обміну необхідно виконати наступні дії:

1. Відкрити вебінтерфейс шлюзу безпечного обміну та натиснути на кнопку «Внутрішні підсистеми» у рядку з ідентифікатором організації шлюзу (тип об'єкта – «MEMBER»):

Ім'я ^	ID	
MADCAT88	MEMBER : test1 : GOV : 00000088	 
MADCAT88	SUBSYSTEM : test1 : GOV : 00000088 : TESTSUB88	     
MADCAT88	SUBSYSTEM : test1 : GOV : 00000088 : UXP_ATR_Platform	     

2. У наступному вікні натиснути на кнопку «Додати» та обрати файл сертифікату, створеного в розділі 3.1 на кроці 5:

 **Подробиці**  **Внутрішні сервери**

ТИП ПІДКЛЮЧЕННЯ ДЛЯ СЕРВЕРІВ У РОЛІ СПОЖИВАЧІВ СЕРВІСІВ




Тип підключення (http/https) для серверів у ролі постачальника сервісів конфігурується у SOAP-Сервісах (</>) та REST APIs (⚙️) вкладках, встановивши URL-сервіс або базову URL-адресу API, відповідно.

HTTPS

ВНУТРІШНІ СЕРТИФІКАТИ TLS

Хеш сертифікату (SHA-1) ^

Нічого немає

 **ПОДРОБИЦІ**  **ДОДАТИ**  **ВИДАЛИТИ**

СЕРТИФІКАТ СЕРВЕРА БЕЗПЕКИ

Хеш сертифікату (SHA-1)

99:C2:85:47:79:AE:01:46:58:18:CA:60:5C:07:20:40:1D:06:47:26