?????????? ?
???????????
??????????
?????????? ??
????? ??????????
?????? ? ???????
ASIC-??????????

1. ?????????

Кожне з повідомлень, якими обмінюються між собою шлюзи безпечного обміну, підписується та шифрується, до підпису синхронно додається позначка часу (відразу після обробки повідомлення шлюзом безпечного обміну).

Функціонал шлюзу безпечного обміну надає можливість завантажити будь-яке повідомлення та відповідь на нього у вигляді ASiC-контейнеру (Associated Signature Containers).

У цій інструкції описано процес пошуку та завантаження підписаного та збереженого електронного повідомлення з позначкою часу.

Завантаження підписаного повідомлення здійснюється Адміністратором вебсервісів з Робочої станції адміністратора.

2. ???????? ????????? ??? ?????? ???????????? ????????????

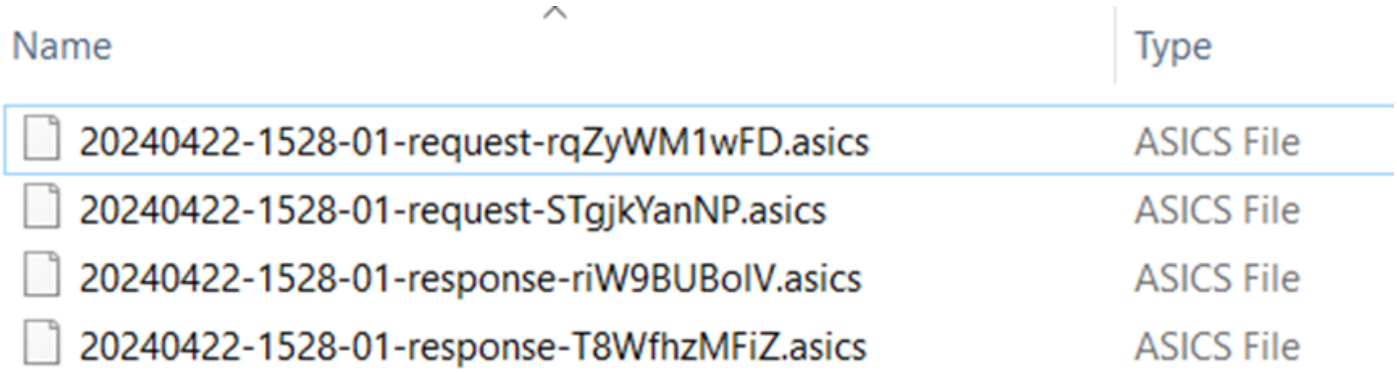
Шлюз безпечного обміну має внутрішню службу для завантаження підписаних документів.

Для завантаження ASiC-контейнеру необхідно виконати запит HTTP GET (через протокол HTTPS) до цієї служби, наприклад, за допомогою інструменту Postman.

В даному запиті треба вказати параметри, які ідентифікують на шлюзі безпечного обміну клієнта (клас, код та ім’я учасника), підсистему (код підсистеми) та транзакцію (ідентифікатор транзакції). Детальний опис цих параметрів наведено в розділі 4 даної інструкції.

Якщо всі параметри задано вірно, шлюз безпечного обміну повинен повернути у відповідь ZIP-архів, який містить контейнери ASiC-S для вказаного запиту та відповіді.

Контейнери ASiC-S, які відносяться до запиту, мають назву вигляду: «queryId-request-Z.asics», а контейнери, які відносяться до відповіді, мають назву вигляду: «queryId-response-Z.asics», де queryId — це ідентифікатор повідомлення, заданий клієнтом певного сервісу, а Z — випадковий алфавітно-цифровий рядок із 10 символів.



Усі контейнери містять підписане електронне повідомлення (message.xml).

Підписані документи доступні для завантаження, доки їх не буде заархівовано та видалено з бази даних журналу повідомлень. Цей період часу (за замовчуванням 30 днів) можна змінити в налаштуваннях шлюзу безпечного обміну, змінивши значення параметру keep-records-for у файлі конфігурації /etc/uxp/conf.d/addons/message-log.ini.

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

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

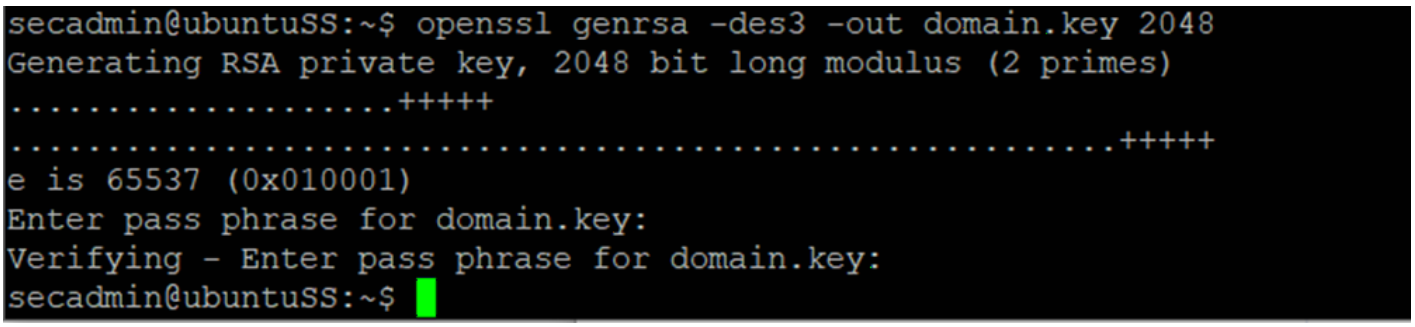
Для цього необхідно виконати наступні дії:

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,

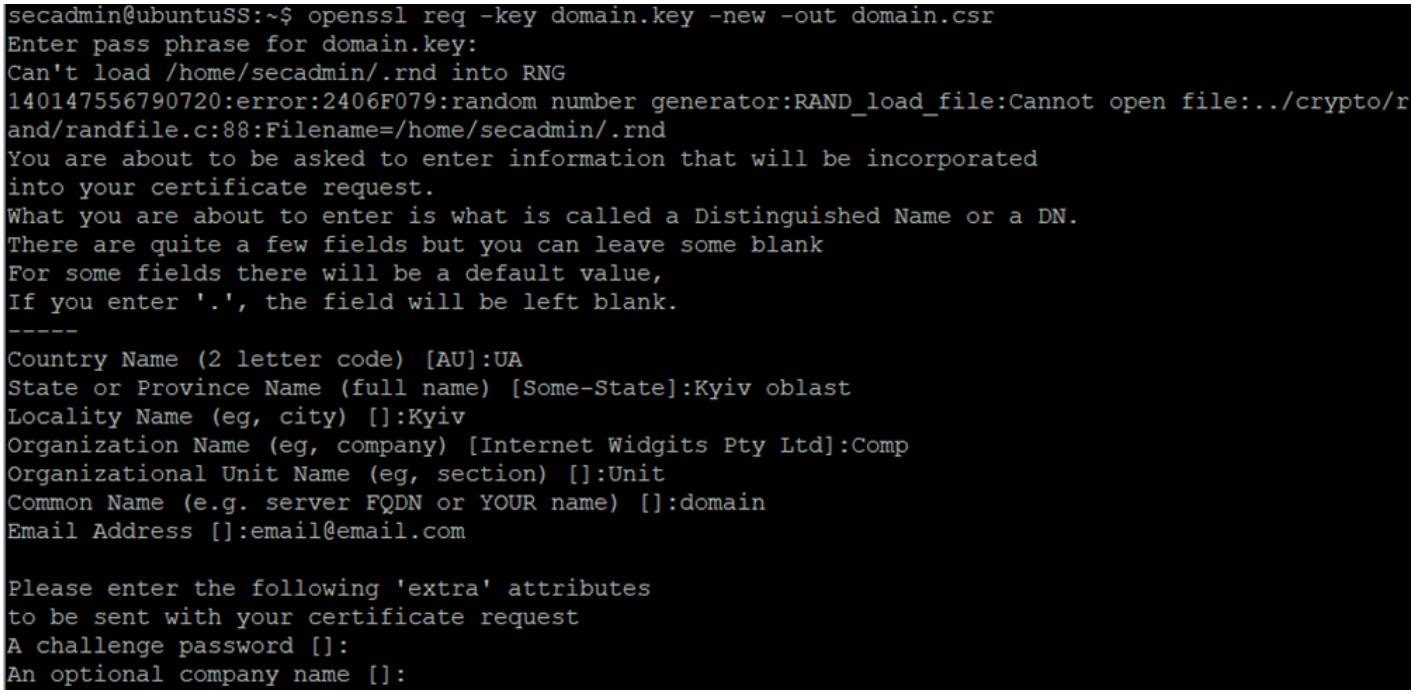
- Organization Name (eg, company) [Internet Widgits Pty Ltd]: — скорочена назва організації, наприклад Comp,

- 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.



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

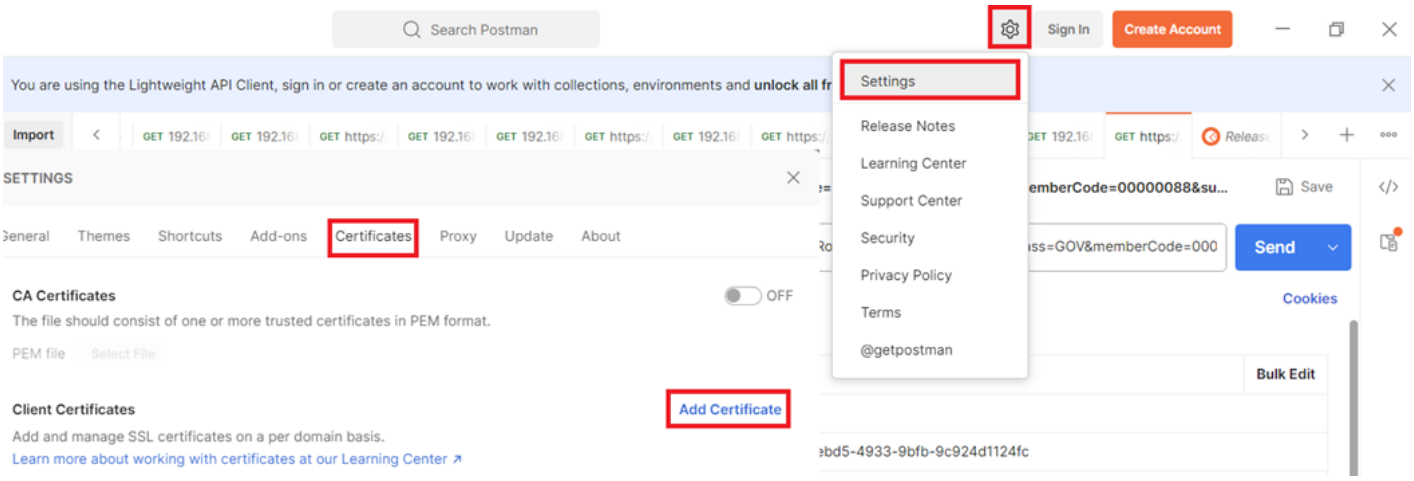
Після виконання даної команди в директорії (за замовчуванням це /home/{username}) з'явиться файл сертифікату domain.der.

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:

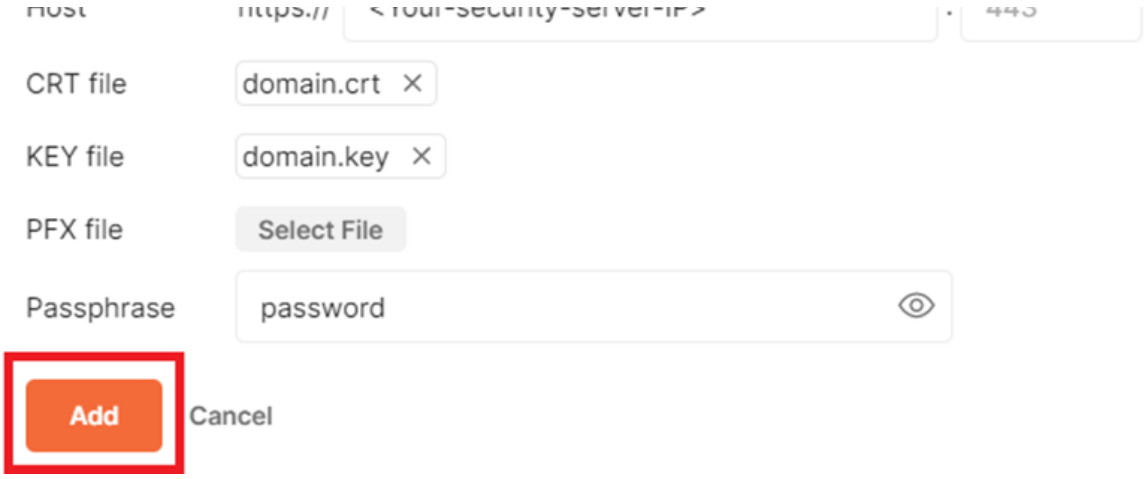
Host – вказати внутрішню (сіру) IP-адресу шлюзу безпечного обміну,

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

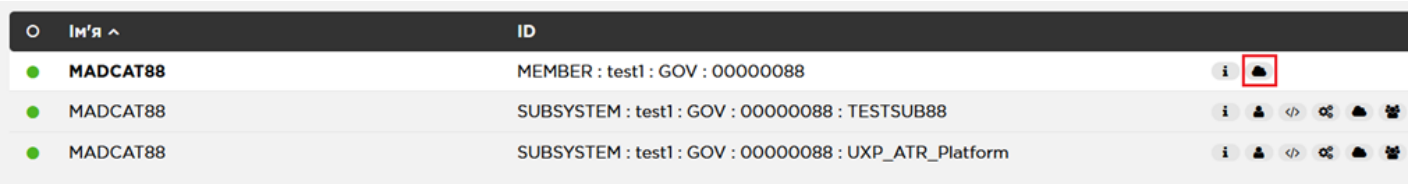


та натиснути на кнопку «Add». Сертифікат з'явиться у вікні доступних сертифікатів.

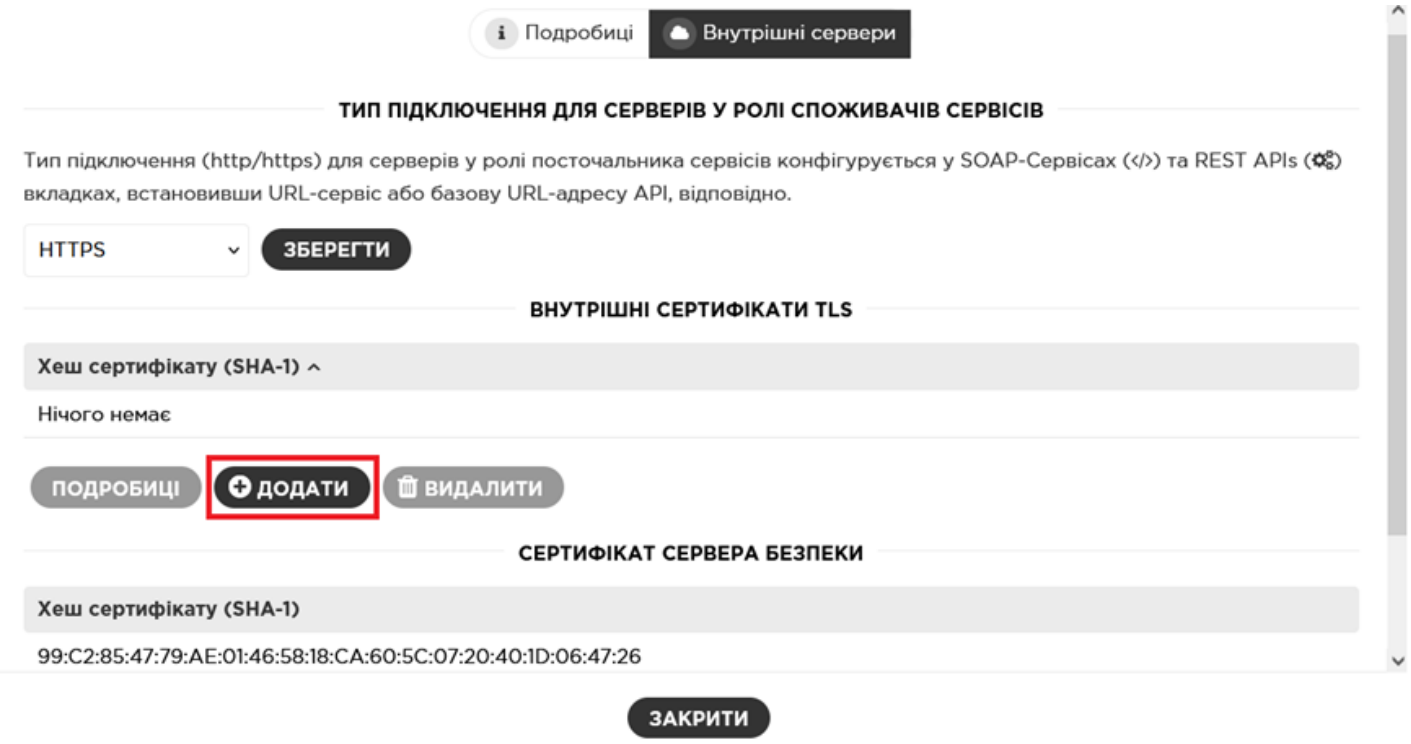
3.3. ?????????? ??????????? ?? ???? ?????????? ??????

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»):



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



4. ?????????? ASIC ??????????

Для завантаження ASiC-контейнеру необхідно відправити запит до внутрішньої служби завантаження документів із зазначенням параметрів запиту на завантаження. URL запиту має виглядати наступним чином:

```
https://<Your-security-server-IP>/signature?&queryId=<message_
queryId>&xRoadInstance=<Instance_Name>&memberClass=GOV&memberCode=<Member_Code>&subsystemCode=
<Subsystem_Code>
```

де **<Your-security-server-IP>** — внутрішня (локальна) IP-адреса шлюзу безпечного обміну,

<message_queryId> — ідентифікатор транзакції повідомлення, який є частиною заголовка повідомлення (queryId),

<Instance_Name> — середовище системи «Трембіта», SEVDEIR-TEST – для тестового середовища та SEVDEIR – для промислового середовища,

<Member_Code> —код ЄДРПОУ Суб’єкта електронної взаємодії, що запитує інформацію від сервісу,

<Subsystem_Code> — код підсистеми, що представляє клієнт сервісу в системі «Трембіта».

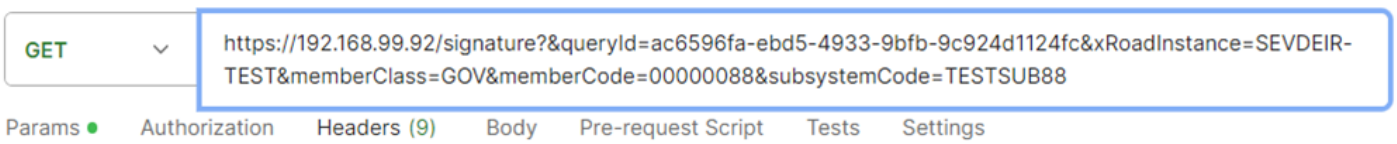
Якщо необхідно завантажити лише запит або відповідь, це можна зробити вказавши один з двох параметрів:

- requestOnly – включати лише підписані документи для повідомлень запитів;

- responseOnly – включати лише підписані документи для повідомлень-відповідей.

Приклад запиту з заданими параметрами виглядає наступним чином:

```
https://192.168.99.92/signature?&queryId=ac6596fa-ebd5-4933-9bfb-
9c924d1124fc&xRoadInstance=SEVDEIR-
TEST&memberClass=GOV&memberCode=00000088&subsystemCode=TESTSUB88
```



Якщо всі параметри задано вірно, шлюз безпечного обміну повинен повернути у відповідь ZIP-архів, який містить контейнери ASiC-S для вказаного запиту та відповіді.

5. ??????? ???????

В таблиці нижче наведені приклади найбільш поширених помилок та способи їх вирішення.

Повідомлення	Причина	Шляхи виправлення
400 Bad Request	Комбінація отриманих параметрів недійсна або відсутній якийсь необхідний параметр	Перевірити правильність заданих параметрів в запиті
401 Unauthorised	Підключення було здійснено через HTTP або при підключенні через HTTPS користувач не зміг надати правильний сертифікат	Перевірити правильність додавання сертифікатів на шлюзі безпечного обміну та у Postman, зробити запит через HTTPS
404 Not Found	Не знайдено підписаних документів, що відповідають наданим параметрам	Перевірити правильність заданих параметрів в запиті
500 Internal Server Error	Сталася неочікувана внутрішня помилка (наприклад, наданий ідентифікатор клієнта служби не відповідає жодному зареєстрованому на шлюзі безпечного обміну клієнту)	Перевірити правильність заданих параметрів в запиті