

6. ?????????????? ??  
????????????????????  
?????????????????????  
????????????????  
????????????????

- [6.1. Встановлення шлюзу безпечного обміну за допомогою скрипта автоматизації](#)
- [6.2. Початкова конфігурація шлюзу безпечного обміну](#)
- [6.3. Підключення захищених носіїв особистих ключів \(апаратних або програмних токенів\)](#)
- [6.4. Реєстрація шлюзу безпечного обміну](#)
- [6.5. Створення підсистем](#)



1. Перейти до відповідної віртуальної машини, де буде здійснюватися встановлення ШБО.

2. Виконати наступну команду:

```
sudo -s
```

3. Ввести пароль користувача root для підтвердження адміністративних повноважень у системі.

4. Перейти в теку */trembita\_installation* домашньої директорії

```
cd trembita_installation
```

5. Запустити скрипт наступною командою:

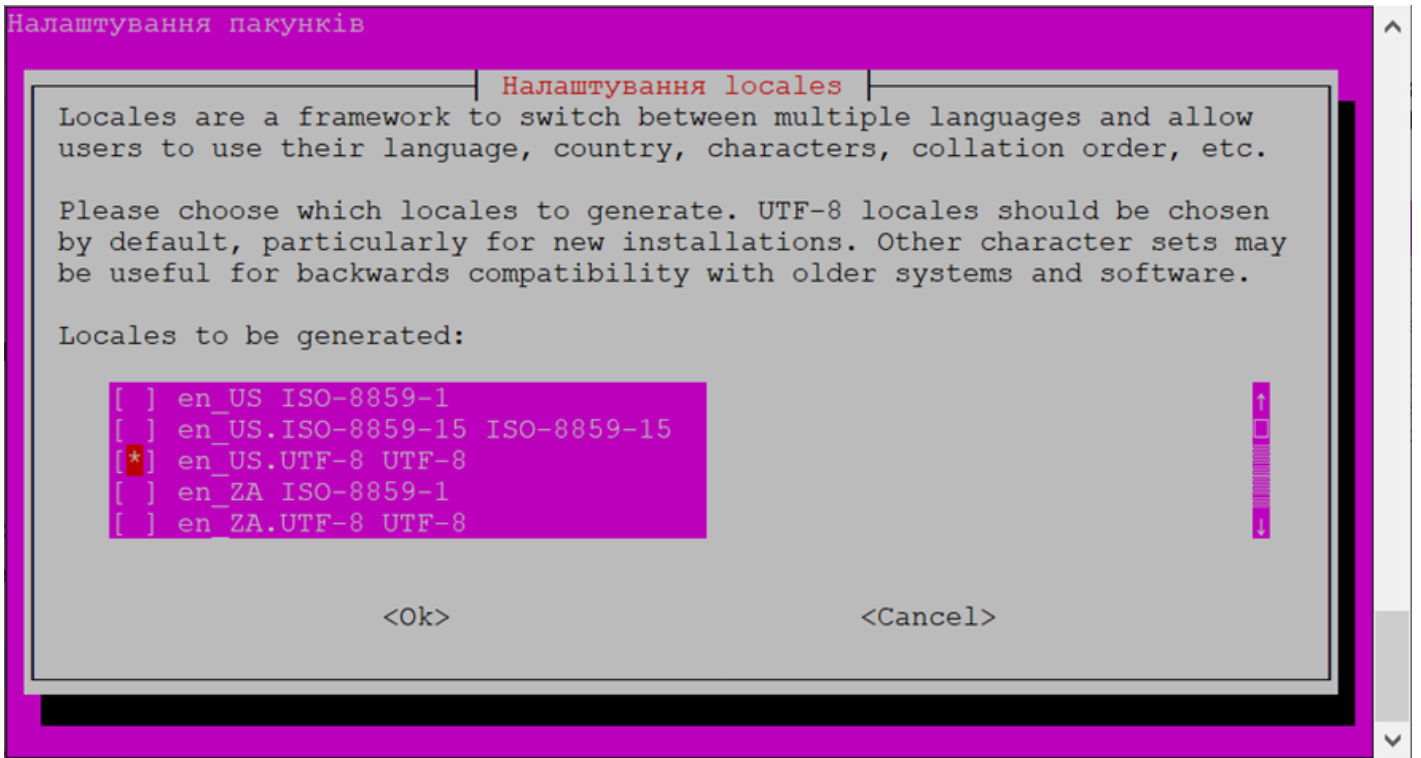
```
./install_standalone_ss.sh
```

**Важливо!** Результат роботи скрипта відмінити неможливо, тому перед його виконанням необхідно зробити резервну копію (снэпшот) віртуальної машини, на якій буде запущено скрипт.

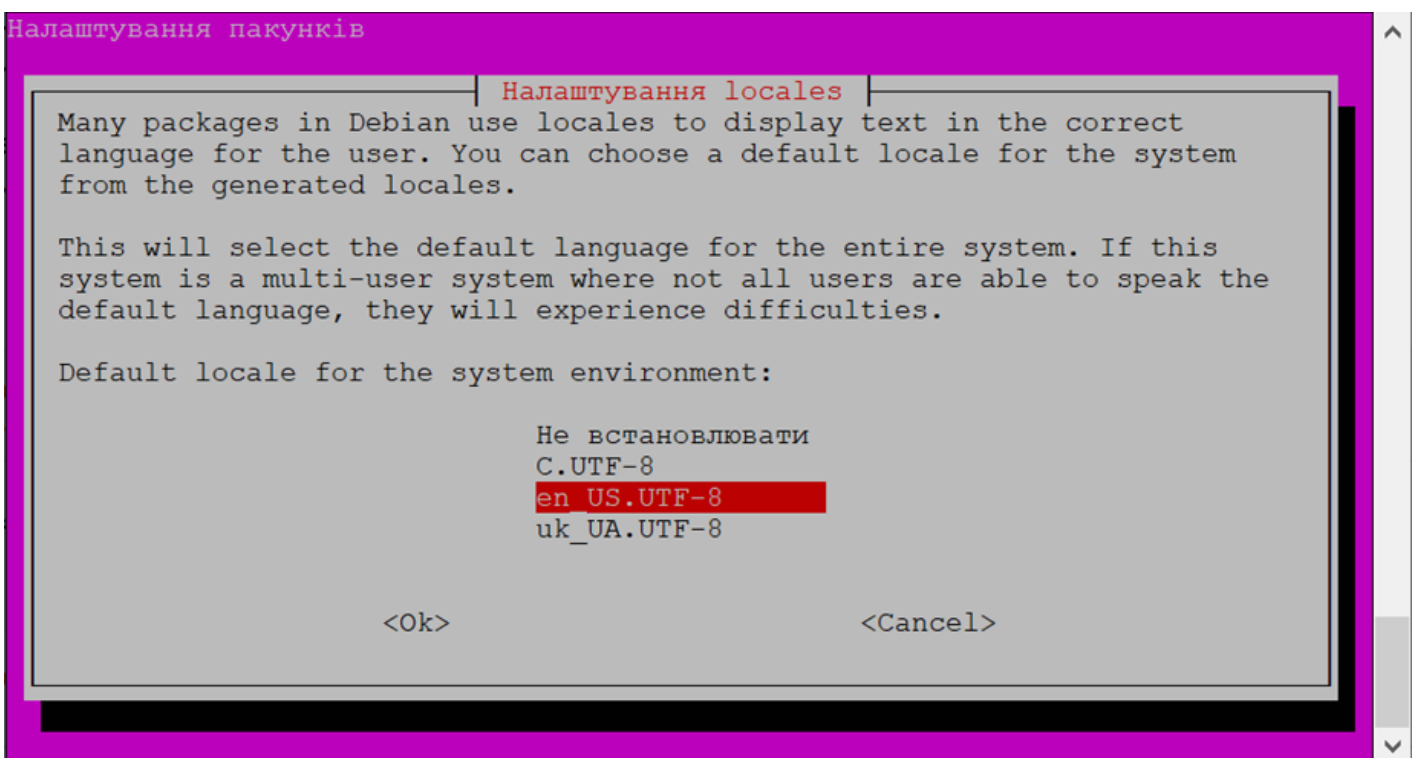
Після запуску скрипта на виконання користувачеві буде відображено наступне повідомлення: «Цей сценарій встановить шлюз безпечного обміну версії 1.12.6, будь ласка, переконайтеся, що ця машина має доступ до мережі Інтернет. Щоб почати натисніть клавішу ENTER.».

В ході інсталяції буде запропоновано виконати деякі налаштування вручну, зокрема, наступні:

1. Налаштування локалей. У діалоговому вікні необхідно знайти запис «en\_US.UTF-8 UTF-8», поставити позначку за допомогою клавіші «SPACE» (зазвичай позначку встановлено за замовчуванням) та натиснути на клавішу «ENTER»:



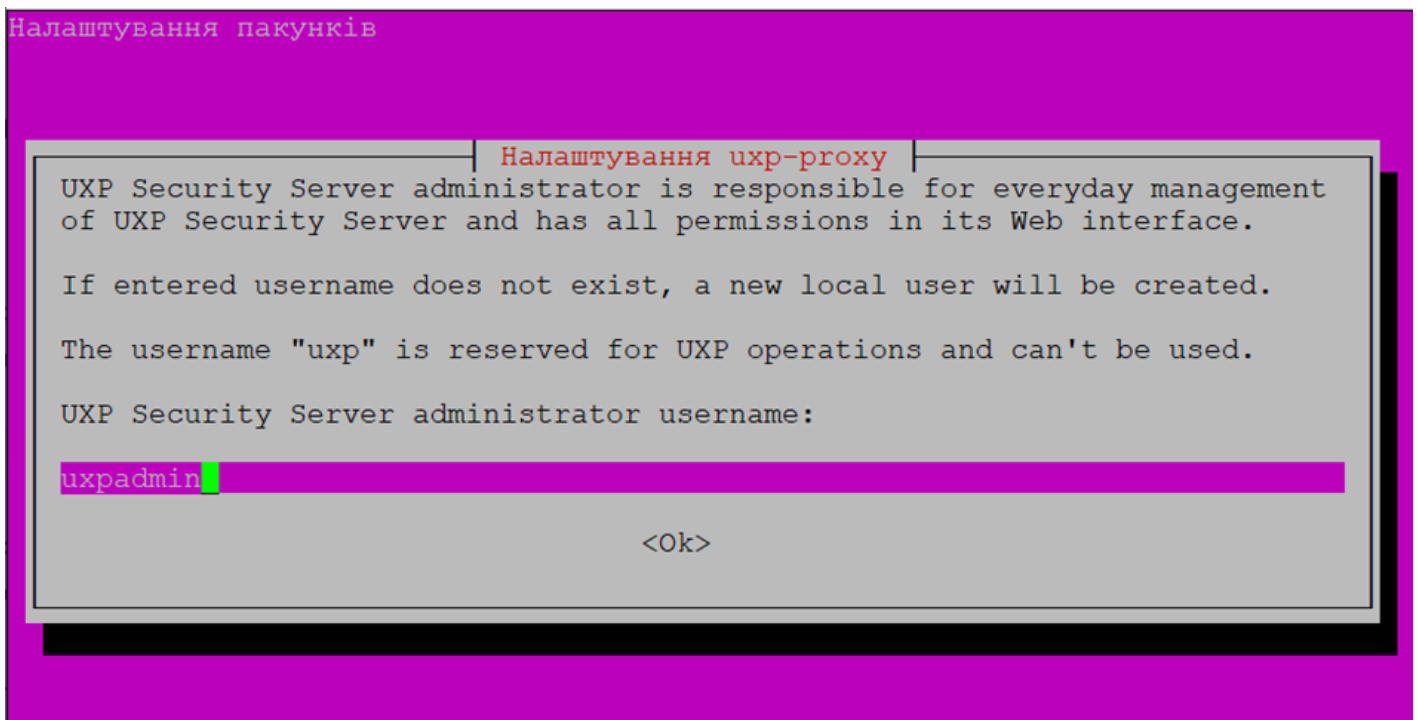
2. У діалоговому вікні «Default locale for a system environment» потрібно обрати «en\_US.UTF-8» та натиснути на клавішу «ENTER»:



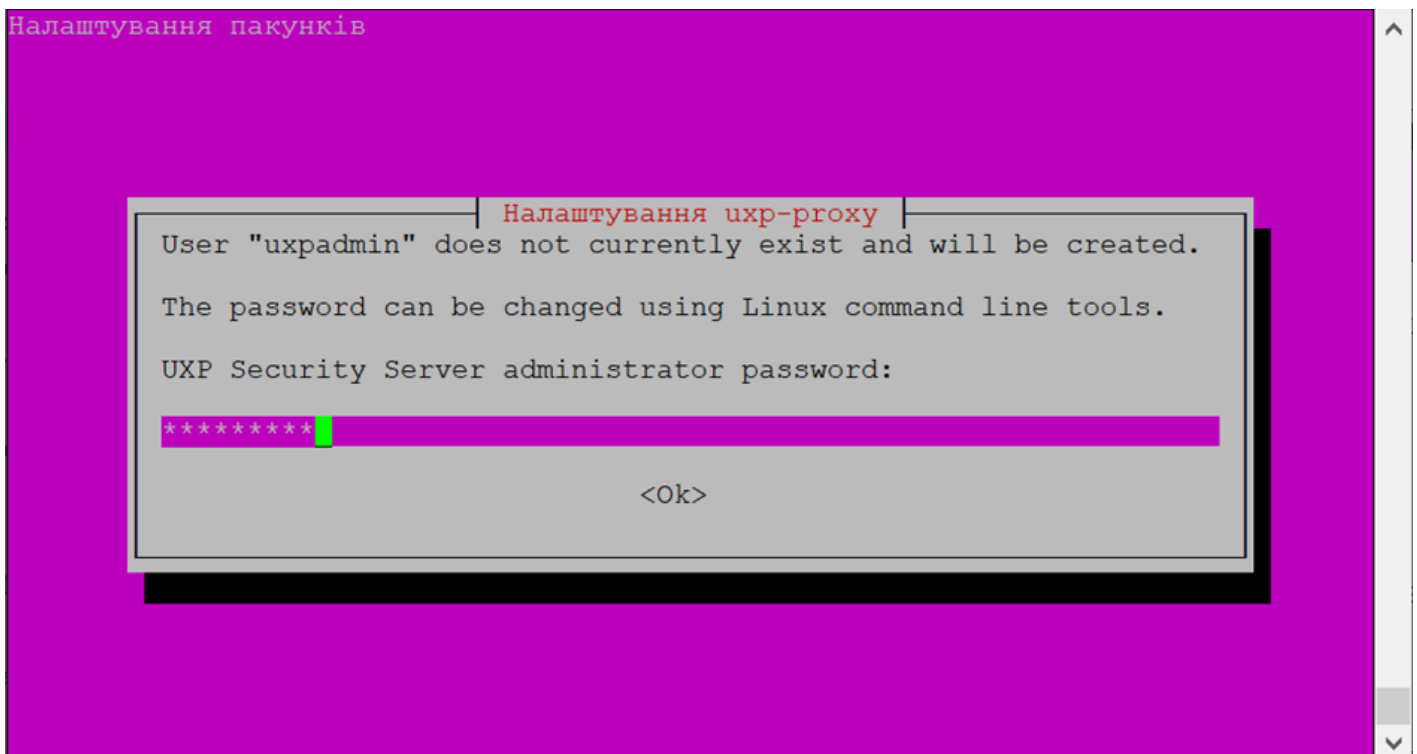
3. Ввести логін для облікового запису Адміністратора вебсервісів. Цей користувач зможе авторизуватися в вебінтерфейсі ШБО.

**Примітка.** За замовчуванням встановлено логін «ixradmin», але за бажання його можна змінити.

Для підтвердження дії необхідно натиснути на клавішу «ENTER»:



4. Встановити пароль для облікового запису Адміністратора вебсервісів. Для підтвердження дії необхідно натиснути на клавішу «ENTER»:



Для перевірки стану виконання встановлених компонентів ПЗ UXP Security Server після завершення роботи скрипта необхідно виконати наступну команду:

```
sudo systemctl list-units | grep "uxp"
```

Список сервісів UXP, які мають бути активними (active/running):

```
uxp-confclient.service
uxp-jetty.service
uxp-monitor.service
uxp-proxy.service
uxp-signer.service
```

### 6.1.3. ?????????? ?????????? ??? ??? ?????????????? ??????????

Під час роботи скрипта можуть статися помилки. Нижче наведено приклади таких помилок та шляхи їх виправлення:

Текст помилки	Шляхи виправлення
Здається, Ви використовуєте неправильну версію операційної системи. Версія операційної системи зараз XX.XX, а повинна бути 18.04.	Версія операційної системи відрізняється від Ubuntu 18.04, встановлення не може бути продовжене. Необхідно встановити операційну систему Ubuntu Server 18.04.4 LTS 64bit
Будь ласка, виконайте цей скрипт з правами суперкористувача, тобто root. Для цього перед запуском скрипту виконайте команду sudo -s.	Команда повинна запускатися з привілеями sudo чи від імені користувача root

### 6.1.4. ?????????????? ?????????????????? ?????????????????? ?????????? ?????????????????????? ??????????????????

**Важливо!** В разі, якщо виникає необхідність роботи з вебінтерфейсом ШБО у декількох співробітників Учасника системи «Трембіта», кожен з них обов'язково повинен мати власний обліковий запис!

Шлюз безпечного обміну використовує локальних користувачів і групи операційної системи для контролю доступу до вебінтерфейсу адміністрування шлюзу безпечного обміну.

Обліковий запис, що використовується для входу в вебінтерфейс адміністрування шлюзу безпечного обміну – це обліковий запис Адміністратора вебсервісів (за замовчуванням з логіном ixpadmin).

Для створення додаткового Адміністратора вебсервісів, Адміністратору локальних компонентів (системному адміністраторові) необхідно:

1. Послідовно виконати наступні команди:

```
sudo useradd -M -N <username>
sudo chsh -s /bin/false <username>
sudo passwd <username>
```

де **<username>** - логін створюваного користувача латиницею.

2. Ввести пароль нового користувача двічі.

## 6.1.5 ?????????? ?????????????? ?????????????? ??????? ?????????????????????? ?? ?????????????? ??????????

В випадку, коли локальні компоненти системи «Трембіта» адмініструє Оператор, уповноваженому співробітнику Суб'єкта електронної взаємодії, що відповідає за встановлення інформаційної взаємодії та управління особистими ключами електронної печатки (Відповідальному за управління ключами), потрібно надати доступ до функціоналу ШБО.

Для цього потрібно створити обліковий запис Відповідального за управління ключами, який буде використовуватись для входу в вебінтерфейс адміністрування шлюзу безпечного обміну, шляхом послідовного виконання наступних команд:

```
sudo useradd -M -N <security-officer>
sudo adduser <security-officer> uxp-security-officer
sudo chsh -s /bin/false <security-officer>
sudo passwd <security-officer>
```

де **<security-officer>** - логін створюваного користувача латиницею.

Після виконання цих команд необхідно ввести пароль нового користувача двічі.

# 6.2. ?????????????? ?????????????????? ?????? ?????????????????? ????????

Початкова конфігурація шлюзу безпечного обміну виконується Адміністратором вебсервісів.

## 6.2.1. ?????????????? ?????????? ??? ?????? ?????????????? ???????

Для роботи ШБО в тестовому середовищі потрібна діюча ліцензія, без неї він не працюватиме. Файл ліцензії можна знайти в Особистому кабінеті Каталогу системи «Трембіта» в розділі «Адміністрування» на вкладці «Матеріали».

Для того, щоб завантажити ліцензію на ШБО необхідно перейти до його вебінтерфейсу за посиланням: <https://<Your-security-server-IP>:4000>,

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

використовуючи атрибути доступу користувача з роллю Адміністратор вебсервісів:

АДМІНІСТРУВАННЯ СЕРВЕРА БЕЗПЕКИ

Логін

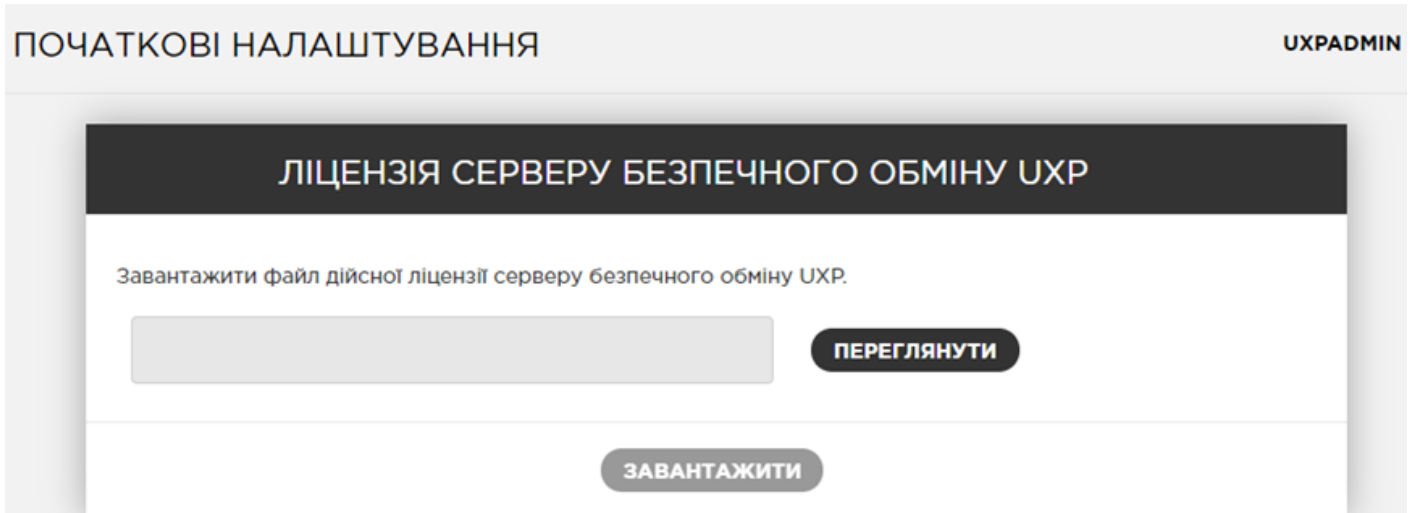
Пароль

**ВХІД**

**Примітка.** При першому доступі до вебінтерфейсу ШБО може з'явитись попередження про те, що використовується сертифікат, виданий недовіреною центром сертифікації. При встановленні ШБО використовується самопідписаний сертифікат, тому слід додати виняток для цього сертифікату у браузері.

**Примітка.** У першу хвилину після перезапуску ШБО його вебінтерфейс може відображати повідомлення «502 Bad Gateway» (зазвичай менше однієї хвилини). Необхідно оновлювати сторінку входу, поки не відобразиться форма входу.

Після першої авторизації в вебінтерфейсі ШБО користувачеві буде відображено діалогове вікно вибору файлу ліцензії, в якому необхідно завантажити файл ліцензії тестового середовища member.test.license.lic.



В даному діалоговому вікні необхідно натиснути на кнопку «Переглянути» та завантажити файл ліцензії.

Після завантаження необхідно його підтвердити, натиснувши на кнопку «Зберегти ліцензію».

## 6.2.2. ?????????????? ????? ?????????????? ???????

При ініціалізації ШБО необхідно завантажити файл якоря конфігурації тестового середовища (файл configuration anchor).

Файл якоря конфігурації тестового середовища можна знайти в Особистому кабінеті Каталогу системи «Трембіта» в розділі «Адміністрування» на вкладці «Матеріали».

Якір конфігурації необхідно завантажити в наступному діалоговому вікні та підтвердити імпорт, натиснувши на кнопку «Підтвердити» («Confirm»):

## ІМПОРТУВАТИ ЯКІР КОНФІГУРАЦІЇ

ПЕРЕГЛЯНУТИ

ІМПОРТУВАТИ

## Необхідне підтвердження



Подробиці якоря конфігурації:

**Хеш (SHA-224)** 7B:7F:64:24:5A:99:55:93:F0:13:7B:15:E9:20:DB:A9:C3:CE:91:DA:0F:CB:31:6E:8B:81:FD:93**Згенерований** UTC 2020-06-23 19:57:30

Продовжити імпорт?

ПІДТВЕРДИТИ

СКАСУВАТИ

Після чого відкриється вікно ініціалізації ШБО:

## ВЛАСНИК СЕРВЕРА БЕЗПЕКИ

Клас учасника

GOV

Код учасника \*

12345678

Ім'я учасника

ORG12345678

## СЕРВЕР БЕЗПЕКИ

Код сервера безпеки \*

12345678\_SS\_T\_1

## ТОКЕН ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

PIN \*

●●●●●●

Повторити PIN \*

●●●●●●

**ВІДПРАВИТИ**

Для ініціалізації ШБО необхідно заповнити наступні дані:

Власник сервера безпеки (Security Server Owner)	
Клас Учасника (Member Class)	GOV
Код Учасника (Member Code)	У якості коду Учасника використовується код ЄДРПОУ організації, яка є Учасником системи «Трембіта». <b>Важливо!</b> Якщо ввести неправильний Member Code, то шлюз безпечного обміну не буде функціонувати коректно і його потрібно буде переінсталювати!
Ім'я Учасника (Member Name)	Ім'я Учасника автоматично отримується з сервера Каталогу Учасників (після введення коду Учасника) відповідно до заявки на реєстрацію Учасника у системі «Трембіта».
Шлюз безпечного обміну (Security Server)	

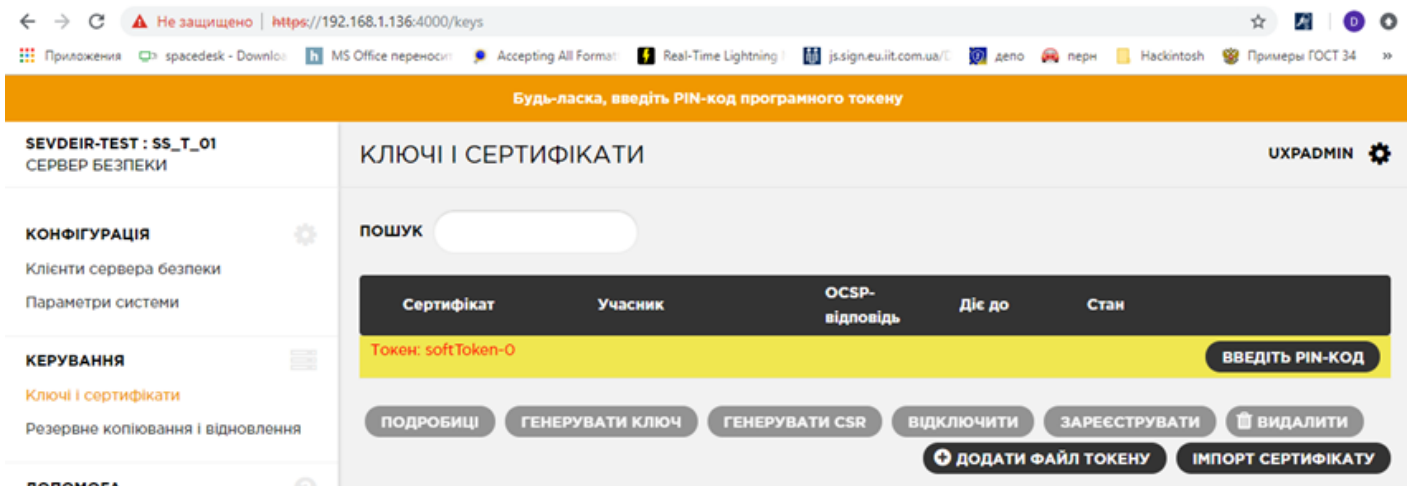
Код сервера безпеки (Security Server Code)	<p>Унікальний код ШБО («сервера безпеки» в вебінтерфейсі) в тестовому середовищі системи «Трембіта», який потрібно створити відповідно до наступного шаблону:  MemberCode_SS_T_Number_FreeSymbols, де:  <b>MemberCode</b> – код ЄДРПОУ організації;  <b>SS</b> – означення ШБО (security server);  <b>T</b> – аббревіатура тестового середовища системи, не змінюється;</p> <p><b>Важливо!</b> Варто звернути увагу, що <b>_SS_T_</b> потрібно вводити великими латинськими літерами з використанням символу нижнього підкреслення «_».</p> <p><b>Number</b> – порядковий номер ШБО організації (наприклад 01, 02, 03 і тд);</p> <p><b>Примітка.</b> Нумерація ШБО для тестового та промислового середовищ системи незалежна.</p> <p><b>FreeSymbols</b> – (за потреби) цифри та літери, які можна додавати до ідентифікатора ШБО задля власної зручності (наприклад, позначення центру обробки даних, позначення інформаційної системи, в якій використовується ШБО тощо).</p> <p><b>Важливо!</b> Додаткові символи повинні містити лише цифри та великі літери англійського алфавіту.</p>
Програмний токен (Software Token)	
PIN	<p>Необхідно придумати PIN-код, який буде використаний для захисту ключів автентифікації, що зберігаються у програмному сховищі (файловій системі ОС).</p> <p><b>Важливо!</b> Адміністратор вебсервісів має зберігати PIN-код у безпечному місці, оскільки після втрати PIN-коду необхідно відновлювати токен, повторно видавати та реєструвати новий сертифікат автентифікації.</p>
Повторити PIN	Ввести повторно значення PIN-коду.

Після введення інформації необхідно натиснути на кнопку «Відправити» («Submit»). Ініціалізація може зайняти декілька хвилин. Коли буде відображено повідомлення про те, що сервер був ініціалізований, необхідно натиснути на кнопку «ОК».

### 6.2.2.1. ????????? PIN-???? ?????????????????????????????????

Шлюз безпечного обміну прив'язує всі особисті ключі до токенів безпеки. Після ініціалізації з'явиться помаранчеве повідомлення у верхній частині сторінки з написом «Будь ласка, введіть PIN-код програмного токена». Це повідомлення вказує на те, що зазначений токен безпеки на даний час заблокований, а особисті ключі не можуть бути використані.

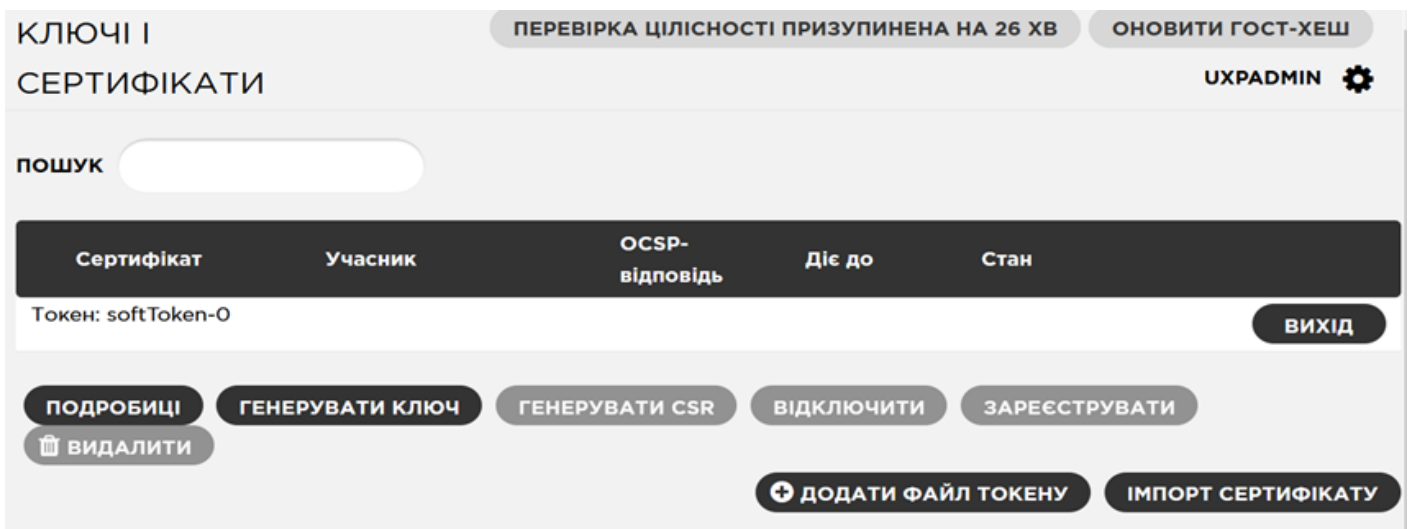
Кожен раз при перезавантаженні ПЗ UXP Security Server або всієї операційної системи ШБО, потрібно вводити PIN-код токена безпеки (у всі використовувані токени безпеки).



Адміністратор вебсервісів має увійти в програмний токен безпеки (softToken), використовуючи PIN-код, введений під час ініціалізації сервера, для чого необхідно:

1. Перейти в розділ «Ключі і сертифікати».
2. Знайти рядок із написом «Токен: softToken-0».
3. Натиснути на кнопку «Введіть PIN-код» в цьому рядку – відкриється діалогове вікно для введення PIN-коду.
4. Ввести PIN-код та натиснути на кнопку «ОК».

Якщо все зроблено коректно, повідомлення «Будь ласка, введіть PIN-код програмного токена» зникне, а кнопка «Вихід» – з’явиться замість кнопки «Введіть PIN-код»:



6.2.2.2. ?????????????? ?????????? ?????????? ??????

Шлюз безпечного обміну використовує зовнішню службу встановлення позначок часу (timestamping) для встановлення позначок часу на кожне повідомлення.

ШБО може мати декілька довірених служб позначок часу.


Адміністратор вебсервісів може обрати, які служби позначок часу будуть використовуватися даним ШБО (зазвичай, це служба, створена відповідним надавачем електронних довірчих послуг, у якого організація отримала сертифікати печатки та шифрування).

Необхідно додати цю службу в список служб встановлення позначок часу, використовуваних шлюзом безпечного обміну, наступним чином:

1. Перейти в розділ «Параметри системи». Список серверів позначок часу має бути порожнім («Немає (відповідних) записів»).
2. Натиснути на кнопку «Додати» в секції «Сервіси позначки часу».
3. Обрати зі списку доступний сервіс і натиснути на нього.
4. Натиснути на кнопку «ОК».

В результаті відобразиться інформація про обраний сервіс позначок часу і його URL в секції «Сервіси позначки часу».

## СЕРВІСИ ПОЗНАЧКИ ЧАСУ

 ДОДАТИ

 ВИДАЛИТИ

Сервіс позначки часу	URL сервісу
TSP-сервер АЦСК органів юстиції України	<a href="http://ca.informjust.ua/services/tsp/">http://ca.informjust.ua/services/tsp/</a>

**Важливо!** Повинен бути зазначений саме TSP-сервер КНЕДП, де організація отримувала електронну печатку!

## 6.3. ?????????????? ?????????????? ????????? ?????????????? ?????????? ( ????????????????? ??? ?????????????????? ?????????????)

Шлюз безпечного обміну накладає електронну печатку на кожне повідомлення (здійснює його підписання), що відправляється до іншого шлюзу безпечного обміну через систему «Трембіта». Підписання здійснюється з використанням кваліфікованого сертифікату електронної печатки, який було отримано на підготовчих кроках від кваліфікованого надавача електронних довірчих послуг.

В тестовому середовищі системи «Трембіта» використання апаратних токенів або HSM-пристроїв не є обов'язковим, замість них можна використовувати програмні токени.

Якщо особисті ключі електронної печатки та шифрування знаходяться на захищеному носії особистих ключів (апаратному токені), його необхідно правильно підключити до віртуальної машини ШБО. За дану дію відповідає Адміністратор локальних компонентів (системний адміністратор).

За налаштування використання криптографічних ключів та сертифікатів **печатки** в цілому відповідає працівник **Учасника**, що є власником ШБО.

За налаштування використання криптографічних ключів та сертифікатів **печатки Суб'єкта електронної взаємодії** відповідає користувач з роллю Відповідальний за управління ключами Суб'єкта електронної взаємодії через вебінтерфейс ШБО.

**Важливо!** Паролі до ключів та сертифікатів печатки Суб'єкта електронної взаємодії вводяться через вебінтерфейс шлюзу безпечного обміну Відповідальним за управління ключами та не повинні передаватися співробітникам Оператора та іншим третім особам.

### 6.3.1. ?????????????? CMP-????????? ?????????????????????? ?????????? ????????????????? ??????????

Для того, щоб шлюз безпечного обміну мав можливість працювати з КНЕДП, що видав сертифікати, необхідно додати інформацію про нього у спеціальний файл, для чого

необхідно:

1. Відкрити даний файл за допомогою виконання наступної команди:

```
sudo nano /etc/uxp/uac/osplm.ini
```

2. Знайти розділ (у квадратних дужках визначаються розділи) з налаштуваннями CMP-сервісу та встановити наступні параметри доступу:

```
[\\SOFTWARE\\Institute of Informational Technologies\\Certificate Authority-1.3\\End User\\CMP]  
Use=1  
CommonName=  
Address=ca-test.czo.gov.ua  
Port=80
```

У поле Address необхідно вказати адресу до сервісу CMP КНЕДП, що видав сертифікати (наприклад, ca.informjust.ua або ca.iit.com.ua тощо, залежно від КНЕДП). Зазначену адресу може надати, зокрема, надавач електронних довірчих послуг або її можна дізнатись з вебінтерфейсу ШБО на вкладці «Параметри системи» в секції «Сервіси позначки часу» (який було вказано в розділі 6.2.2.2 даної інструкції).

**Важливо!** У випадку використання апаратних токенів необхідно встановити параметр Use=1, а у випадку використання програмних токенів встановити параметр Use=0.

Приклад результату модифікації файлу:

```
OnlyOwnCRLs=0  
AutoRefresh=0  
CheckCRLs=0  
Path=/etc/uxp/uac/certificates/  
[\\SOFTWARE\\Institute of Informational Technologies\\Certificate Authority-1.3\\End User\\CMP]  
Use=1  
CommonName=  
Address=ca.iit.com.ua  
Port=80  
[\\SOFTWARE\\Institute of Informational Technologies\\Key Medias]  
[\\SOFTWARE\\Institute of Informational Technologies\\Key Medias\\File System]  
[\\SOFTWARE\\Institute of Informational Technologies\\Key Medias\\File System\\Folders]
```

### 6.3.2. ?????????????? ?????????????? ?????????????? ?????????????? ????????? (????????????? ??????????)

Встановлення підтримки захищених носіїв особистих ключів (апаратних токенів) виконується Адміністратором локальних компонентів (системним адміністратором).

Шлюз безпечного обміну версії 1.12.6 підтримує наступні захищені носії особистих ключів:

## 1. Апаратні токени:

- Алмаз-1К;
- Автор Secure Token 337;
- Автор Secure Token 338;
- EfitKey;
- Кристал-1;

## 2. Мережеві криптомодулі:

- ІІТ Гряда-301;
- Сайфер «Шифр-НСМ».

Апаратний токен (захищений носій особистих ключів) необхідно підключити до фізичного обладнання – сервера, який забезпечує функціонування ПЗ шлюзу безпечного обміну. Якщо використовується система віртуалізації на сервері – потрібно налаштувати адресацію фізичного порту, до якого підключений апаратний токен, до віртуальної машини шлюзу безпечного обміну.

Правильність адресації можна перевірити через наявність інформації про ключі у операційній системі, для чого потрібно виконати наступну команду на шлюзі безпечного обміну:

```
sudo dmesg | grep usb
```

```
2.048752] hid-generic 0003:0D9F:0004.0002: hiddev0,hidraw1: USB HID v1.00 Device [POWERCOM
2.118604] usb 3-1.3: new full-speed USB device number 4 using ehci-pci
2.215582] usb 3-1.3: New USB device found, idVendor=03eb, idProduct=9324
2.216195] usb 3-1.3: New USB device strings: Mfr=1, Product=2, SerialNumber=0
2.216802] usb 3-1.3: Product: E.Key Almaz-1C
2.217397] usb 3-1.3: Manufacturer: IIT
2.222609] usb 2-1.1.1: new low-speed USB device number 4 using ehci-pci
2.290623] usb 3-1.5: new full-speed USB device number 5 using ehci-pci
2.366959] usb 2-1.1.1: New USB device found, idVendor=05ac, idProduct=0204
2.367568] usb 2-1.1.1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
2.368173] usb 2-1.1.1: Product: Apple Extended USB Keyboard
2.368776] usb 2-1.1.1: Manufacturer: Mitsumi Electric
2.384206] usb 3-1.5: New USB device found, idVendor=03eb, idProduct=9301
2.384824] usb 3-1.5: New USB device strings: Mfr=1, Product=2, SerialNumber=3
2.385435] usb 3-1.5: Product: IIT E.Key Crystal-1
2.386042] usb 3-1.5: Manufacturer: JSC Institute of Informational Technologies
2.386420] input: Mitsumi Electric Apple Extended USB Keyboard as /devices/pci0000:00/0000:
```

З результату виконання команди можна побачити, що в системі присутні два апаратних токени – Product: IIT E.Key Crystal-1 та Product: E.Key Almaz-1C – відповідно «Кристал-1» та «Алмаз-1К».

Для роботи усіх апаратних токенів необхідно встановити пакети підтримки електронних ключів операційною системою Linux, а саме Ubuntu 18.04 Server 64bit:

```
sudo apt-get install pcscd libccid pcsc-tools libccid libpcsclite1 opensc
```

### 6.3.2.1. ?????????????? ??????-1?

Додаткових налаштувань, крім встановлення пакетів підтримки електронних ключів операційною системою Linux, виконувати не потрібно.

### 6.3.2.2. ?????????????? ?????? Secure Token 337/ Secure Token 338

Для зазначених токенів Автор необхідно:

1. Завантажити драйвер для 64-розрядної ОС Linux за допомогою виконання наступної команди:

```
wget https://project-repo.trembita.gov.ua:8081//files/t1/libav337p11d.so
```

2. Перемістити завантажений файл у директорію /usr/lib/:

```
sudo cp libav337p11d.so /usr/lib/
```

3. Перевірити доступність токена в системі можна за допомогою виконання наступної команди:

```
sudo pkcs11-tool -v --list-slots --module /usr/lib/libav337p11d.so
```

У випадку, якщо ключ доступний для системи, має бути виведено інформацію про нього, наприклад:

```
secadmin@ubuntuSS:~$ sudo pkcs11-tool -v --list-slots --module /usr/lib/libav337p11d.so
Available slots:
Slot 0 (0x0): Avtor SecureToken 00 00
manufacturer: Avtor
hardware ver: 1.0
firmware ver: 1.0
flags: token present, removable device, hardware slot
token label : 26320f00c6
token manufacturer : AVTOR LLC
token model : ST-338
token flags : login required, rng, token initialized, user PIN count low, PIN initialized, other flags=0x200
hardware version : 1.0
firmware version : 1.3
serial num : 26320f00c65a0902
pin min/max : 1/8
```

### 6.3.2.3. ?????????????? EfitKey

При використанні захищеного носія EfitKey необхідно виконати наступні дії:

1. Скорегувати файл Info.plist, для того, щоб додати (включити) існуючий PCSC-пристрій (токен EfitKey) до відповідного списку PCSC-пристроїв, які підтримуються системою, відкривши його за допомогою виконання наступної команди:

```
sudo nano /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist
```

2. Знайти строку «<key>ifdVendorID</key>» і після елемента «<array>» додати:

```
«<string>0xC1A6</string>»
```

3. Знайти строку «<key>ifdProductID</key>» і після елемента «<array>» додати:

```
«<string>0x0151</string>»
```

4. Знайти строку «<key>ifdFriendlyName</key>» і після елемента «<array>» додати:

```
«<string>EfitTechnologies EfitKey</string>»
```

5. Завантажити та скопіювати бібліотеку драйверів libefitkeynxt.so до директорії /usr/lib/ за допомогою послідовного виконання наступних команд:

```
wget https://project-repo.trembita.gov.ua:8081//files/t1/libefitkeynxt.so  
sudo cp libefitkeynxt.so /usr/lib/
```

**Примітка.** Для роботи libefitkeynxt.so і EfitKey необхідно мати запущений демон pcscd.

6. Під'єднати захищений носій ключової інформації EfitKey та перевірити доступність носія в системі:

```
sudo pkcs11-tool -v --list-slots --module /usr/lib/libefitkeynxt.so
```

У випадку, якщо ключ доступний для системи, має бути виведено інформацію про нього, наприклад:

Available slots:

```
Slot 0 (0x0): EfitTechnologies EfitKey (EFK4200080173) 00 00
manufacturer: EfitTechnologies EfitKey (EFK420
hardware ver: 0.0
firmware ver: 1.0
flags: token present, removable device, hardware slot
token label : AVEST KEY
token manufacturer : EfitTechnologies
token model : EfitKey
token flags : login required, rng, token initialized, PIN initialized
hardware version : 4.20
firmware version : 1.0
serial num : EFK4200080173
pin min/max : 6/80
```

#### 6.3.2.4. ?????????????? ????????-1

При використанні токена «Кристал-1» необхідно виконати наступні дії:

1. Створити файл /etc/udev/rules.d/80-uxp-iit-e-keys.rules за допомогою виконання наступної команди:

```
sudo nano /etc/udev/rules.d/80-uxp-iit-e-keys.rules
```

2. Прописати в ньому наступні правила:

```
SUBSYSTEM=="usb", ATTR{idVendor}=="03eb", ATTR{idProduct}=="9301", MODE="0660", GROUP="uxp"
SUBSYSTEM=="usb", ATTR{idVendor}=="03eb", ATTR{idProduct}=="9308", MODE="0660", GROUP="uxp"
```

3. Перевірити, чи встановлено бібліотеку libusb-0.1-4 за допомогою виконання наступної команди:

```
sudo apt list --installed | grep libusb-0.1-4
```

У випадку, якщо бібліотеку не встановлено, встановити її за допомогою виконання наступної команди:

```
sudo apt-get install libusb-0.1-4
```

#### 6.3.2.5. ?????????????? ??? ??????-301

При використанні токена безпеки ІІТ «Грядя-301» необхідно виконати наступні дії:

1. Відкрити файл /etc/uxp/uac/osplm.ini за допомогою виконання наступної команди:

```
sudo nano /etc/uxp/uac/osplm.ini
```

2. Додати в нього наступний блок параметрів:

```
[\SOFTWARE\Institute of Informational Technologies\Key Medias\NCM Gryada-301]
[\SOFTWARE\Institute of Informational Technologies\Key Medias\NCM Gryada-301\Modules]
[\SOFTWARE\Institute of Informational Technologies\Key Medias\NCM Gryada-301\Modules\
```

де **<Serial Number>** – це останні три цифри серійного номеру пристрою ІТ Гряда-301 (серійний номер пристрою має вигляд 301XXX, останні три цифри XXX необхідно додати у файл),

**<Your-Gryada-301-IP>** – це мережева адреса пристрою,

**AddressMask** – маска підмережі, у якій знаходиться пристрій.

3. Перезавантажити сервіс uxp-signer за допомогою виконання наступної команди:

```
sudo systemctl restart uxp-signer
```

### 6.3.2.6. ?????????????? ??????? «?????-HSM»

Для забезпечення роботи токена безпеки «Шифр-HSM» необхідна бібліотека libcihsm.so. Її потрібно розмістити в директорії /var/tmp/uxp/EUSign-x64-1.3.263/ файлової системи шлюзу безпечного обміну.

**Примітка.** Дана бібліотека поставляється компанією-виробником разом з токеном безпеки.

Після цього необхідно виконати наступні кроки:

1. Змінити права доступу до бібліотеки за допомогою виконання наступної команди:

```
chmod 644 /var/tmp/uxp/EUSign-x64-1.3.263/libcihsm.so
```

2. Впевнитись, що шлюз безпечного обміну має підключення до модулю «Шифр-HSM» за допомогою виконання наступної команди:

```
PKCS11_PROXY_SOCKET=tcp://<Your-CipherHSM-IP>:23454 pkcs11-tool \  
--module /var/tmp/uxp/EUSign-x64-1.3.263/libcihsm.so -
```

де **<Your-CipherHSM-IP>** – IP-адреса модулю.

Після виконання команди будуть показані усі доступні слоти на модулі, наприклад:

```
Available slots:  
Slot 0 (0x54c9ad8): Cipher Cipher-HSM slot ID 0x54c9ad8  
  token label      : empty  
  token manufacturer : CIPHER PRO, LLC  
  token model      : Cipher-HSM  
  token flags      : login required, rng, token initialized, PIN initialized, user  
  PIN to be changed, other flags=0x20  
  hardware version  : 2.5  
  firmware version  : 2.5  
  serial num       : caa78080054c9ad8  
  pin min/max      : 4/255  
Slot 1 (0xbdd1406): Cipher Cipher-HSM slot ID 0xbdd1406  
...
```

3. Відкрити файл /etc/uxp/services/local.conf за допомогою виконання наступної команди:

```
sudo nano /etc/uxp/services/local.conf
```

та додати в нього наступну строку:

```
export PKCS11_PROXY_SOCKET=tcp://<Your-CipherHSM-IP>:23454
```

4. Переглянути всі ключі та сертифікати на токени, скориставшись інструментом pkcs11-tool, за допомогою виконання наступної команди:

```
PKCS11_PROXY_SOCKET=tcp://<Your-CipherHSM-IP>:23454 pkcs11-tool \  
--module /var/tmp/uxp/EUSign-x64-1.3.263/libcihsm.so \  
--slot <SlotNumber> -0 -v -l --pin <PIN Code>
```

де **<Your-CipherHSM-IP>** – IP адреса модулю;

**<PIN Code>** – PIN-код модулю.

**Примітка.** Якщо після виконання команди було отримано помилку CKR\_USER\_ALREADY\_LOGGED\_IN, необхідно видалити розділ входу -l --pin <PIN Code> з попередньої команди.

5. Скопіювати сертифікат з попереднього кроку та сертифікат КНЕДП в директорію /etc/uxp/uac/certificates/.

6. Перезавантажити сервіс uxp-signer за допомогою виконання наступної команди:

```
sudo systemctl restart uxp-signer
```

Після проведених дій з обраним ключем обов'язково необхідно перезавантажити операційну систему:

```
sudo shutdown -r now
```

Після чого використований ключ повинен з'явитись в вебінтерфейсі ШБО в розділі «Ключі і сертифікати».

### 6.3.3. ?????????? ??????????? ?????????? ?????? ??????????? ?????? ( ????????????? ??????????)

Якщо використовується програмний (файловий) контейнер для зберігання особистих ключів електронної печатки та шифрування, його необхідно підготувати для імпорту на ШБО.



Для цього потрібно помістити файл особистого ключа (зазвичай, це Key-6.dat) та обидва сертифікати (печатки та шифрування) у ZIP-архів, без вкладення файлів у директорію. Зазначені файли повинні мати лише латинські літери та цифри у найменуванні.

**Примітка.** Для програмних (файлових) ключів та сертифікатів від КНЕДП ТОВ «ЦСК «Україна» необхідно, перед створенням зазначеного вище ZIP-архіву, файл з особистим ключем (що має розширення файлу .ZS2) перейменувати на Key-6.dat, а файлам сертифікатів (що мають розширення файлу .CRT) змінити розширення на .CER.

Далі необхідно виконати наступні кроки:

1. Перейти в розділ «Ключі і сертифікати».
2. Натиснути на кнопку «Додати файл токена».
3. У вікні «Додати файл токена» обрати значення параметру «Тип файлу токена» – DSTU4145 Token (ZIP containing Key-6.dat and DER-encoded certificates).
4. У поле «ID файлу токена» ввести зрозумілий ідентифікатор, наприклад, uaToken.
5. Натиснути на кнопку «Переглянути» та обрати з файлової системи робочої станції користувача ZIP-архів з ключем та сертифікатами.

Ввести коректний PIN-код особистого ключа, що знаходиться у файлі ZIP-архіву, у поле PIN та натиснути на кнопку «ОК».

**Додати файл токена**  

**Тип файлу токена \*** DSTU4145 Token (ZIP containing Key-6.dat and DER-encs ▾

**ID файлу токена \*** uaToken

**PIN \*** .....

C:\fakepath\Юридична особа 1 (ТЕСТ).zip **ПЕРЕГЛЯНУТИ**

---

**ОК** **СКАСУВАТИ**

## 6.4. ?????????????? ?????? ???????????????? ????????

### 6.4.1. ??????? ?????? ?????????? ?? ??????????????

Для імпорту ключа підпису та шифрування потрібно мати згенеровані ключі печатки та шифрування, а також відповідні сертифікати, видані одним з КНЕДП, що підтримуються системою «Трембіта».

Отримання сертифікатів виконується на підготовчому етапі підключення до системи.

Ключі електронної печатки та шифрування для тестового середовища системи «Трембіта» можуть зберігатися або на апаратних захищених носіях особистих ключів, які повинні бути підключені та налаштовані згідно розділу 6.3.2 даної інструкції, або на програмних захищених носіях особистих ключів, які повинні бути підключені та налаштовані згідно розділу 6.3.3 даної інструкції.

Для імпорту ключів електронної печатки та шифрування на ШБО потрібно виконати наступні дії в його вебінтерфейсі:

1. Перейти в розділ «Ключі і сертифікати».
2. Ввести PIN-код до підключеного токена або HSM.
3. Навпроти кожного сертифікату натиснути на кнопку «Імпортувати», щоб виконати цю дію для відповідних сертифікатів.

**Примітка.** У випадку використання апаратного модулю Сайфер «Шифр-HSM», PIN-код токена вводиться в форматі `##slot_id##password`. Наприклад, `##231036361##1234567890`.

### 6.4.2. ??????????? ?????? ?????????????????????? ??? ?????? ??????????????? ?????????

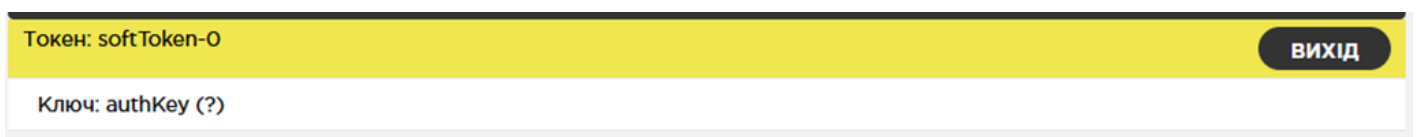
Шлюз безпечного обміну повинен автентифікуватися при відправці повідомлень до інших шлюзів безпечного обміну. Сертифікат автентифікації використовується для перевірки автентичності шлюзу безпечного обміну.

За створення ключа автентифікації та подальші дії з ним відповідає Адміністратор вебсервісів.

Для того, щоб створити новий ключ автентифікації у вебінтерфейсі шлюзу безпечного обміну, необхідно:

1. Перейти в розділ «Ключі і сертифікати».
2. Обрати токен «softToken-0», натиснувши на ньому мишкою.
3. Натиснути на кнопку «Генерувати ключ».
4. Ввести позначку для ключа автентифікації. Рекомендовано ввести позначку – authKey.
5. Натиснути на кнопку «ОК».

Генерація ключа може зайняти кілька секунд. Якщо все зроблено вірно, щойно створений ключ з'явиться під токеном безпеки з написом «authKey (?)».



### 6.4.3. Генерація ключа автентифікації (Certificate Signing Request) за допомогою центру сертифікації

Сертифікати автентифікації, які використовуються шлюзами безпечного обміну, повинні бути підписані технологічним центром сертифікації ключів тестового середовища системи «Трембіта».

Для цього спочатку необхідно створити запит на підпис сертифікату (Certificate Signing Request (CSR)) для попередньо створеного ключа через вебінтерфейс ШБО. Центр сертифікації приймає заявки на підпис у вигляді файлів в текстовому форматі PEM.

Для створення запиту необхідно виконати наступні дії в вебінтерфейсі ШБО:

1. Перейти в розділ «Ключі і сертифікати».
2. Вибрати ключ автентифікації, згенерований на попередньому кроці (authKey).
3. Натиснути на кнопку «Генерувати CSR» – відкриється діалог «Створити запит на підпис сертифіката».
4. У діалоговому вікні необхідно встановити наступні значення:

Поле	Значення
Використання (Usage)	Auth

Поле	Значення
Сервіс сертифікації (Certification Service)	Необхідно обрати технологічний центр сертифікації ключів тестового середовища системи: «Trembita CA Diia TEST».
CSR Format	PEM

5. Натиснути на кнопку «ОК».

6. Відобразиться діалог підтвердження з інформацією про шлюз безпечного обміну. Якщо найменування організації у полі «Organization (O)» не відображається – це означає, що організація ще не зареєстрована в Каталозі Учасників системи «Трембіта». В такому разі потрібно звернутися до Адміністратора системи «Трембіта» для уточнення. Якщо всі поля заповнені – необхідно натиснути на кнопку «ОК».

7. Зберегти файл з розширенням \*.pem на комп'ютері.

#### 6.4.4. ?????????? ?????????????? ??? ?????? ???????????????????

Згенерований \*.pem файл запиту (CSR) використовується для створення та отримання сертифікату автентифікації для шлюзу безпечного обміну. Сертифікат автентифікації видає Адміністратор системи «Трембіта».

Для цього необхідно згенерований \*.pem файл надіслати Адміністратору системи «Трембіта» шляхом подачі відповідної заявки засобами Особистого кабінету Каталогу системи «Трембіта» (**Видача нового сертифікату автентифікації (Тестове середовище)**).

Порядок подання зазначеної заявки вказаний у п. 7.3.3 Регламенту роботи системи «Трембіта».

Адміністратор системи «Трембіта» має обробити дану заявку та у відповідь засобами Особистого кабінету Каталогу системи «Трембіта» надати сертифікат автентифікації. Цей сертифікат потрібен для виконання наступного кроку реєстрації ШБО.

**Важливо!** Без цього сертифікату подальші кроки неможливі!

#### 6.4.5. ??????? ?????????????????? ??? ?????? ?????????????????????? ?? ?????? ?????????????????? ????????

Для імпорту виданого на попередньому кроці сертифікату автентифікації до шлюзу безпечного обміну Адміністратору вебсервісів потрібно виконати наступні дії в вебінтерфейсі ШБО:

1. Перейти в розділ «Ключі і сертифікати».

2. Натиснути на кнопку «Імпорт сертифікату».

3. Натиснути на кнопку «Переглянути» і обрати сертифікат автентифікації, отриманий на попередньому кроці.

4. Натиснути на кнопку «ОК».

Якщо все зроблено правильно, у вебінтерфейсі ШБО буде відображена інформація про доданий сертифікат під ключем автентифікації authKey.

---

## 6.4.6. ?????????? ?????????????? ?????????????????? ?? ??????????

На цьому етапі сертифікати автентифікації та електронної печатки вже імпортовані до шлюзу безпечного обміну, однак, вони за замовчуванням відключені (в колонці «OCSP-відповідь» для сертифікату вказано «відключений»).

Важливо! Відключені сертифікати не використовуються шлюзом безпечного обміну.

Для їх активації Адміністратору вебсервісів необхідно виконати наступні дії в вебінтерфейсі шлюзу безпечного обміну:

1. Перейти в розділ «Ключі і сертифікати».

2. Обрати сертифікат автентифікації, який імпортовано на попередньому кроці (наступний рядок під authKey, з числовим серійним номером).

3. Натиснути на кнопку «Активувати».

4. Вибрати сертифікат печатки (під рядком «Ключ: uaToken-sign (sign)»).

5. Натиснути на кнопку «Активувати».

---

## 6.4.7. ?????????? ??????? ?? ?????????????? ??????????????????

Сертифікат автентифікації використовується іншими шлюзами безпечного обміну для перевірки автентичності ШБО конкретного Учасника. Для цього шлюзи безпечного обміну повинні обмінятися зареєстрованими сертифікатами автентифікації та довіряти їм.

Довірені сертифікати автентифікації поширюються через сервер Каталогу Учасників системи «Трембіта». Адміністратор системи «Трембіта» повинен перевірити отриманий запит на реєстрацію і, якщо запит дійсний, додати сертифікат автентифікації у перелік зареєстрованих у промисловому середовищі системи «Трембіта».

Варто звернути увагу, що статус сертифіката автентифікації, який імпортовано в попередньому стані, «збережений», а не «зареєстровано». Це означає, що цей сертифікат ще не був відправлений на реєстрацію до серверу Каталогу Учасників.

Для реєстрації сертифікату автентифікації та сертифікату шифрування Адміністратор вебсервісів у вебінтерфейсі шлюзу безпечного обміну повинен виконати наступні дії:

- 1.Перейти в розділ «Ключі і сертифікати».
- 2.Вибрати сертифікат шифрування (рядок під «Ключ: uaToken-encr (encr)»).
- 3.Натиснути на кнопку «Зареєструвати». Якщо всі попередні кроки виконані успішно, буде відображено повідомлення зеленого кольору з інформацією, що запит надіслано успішно, а також статус сертифіката шифрування повинен стати «в процесі реєстрації».
- 4.Обрати сертифікат автентифікації, який імпортовано на попередньому кроці.
- 5.Натиснути на кнопку «Зареєструвати». Відкриється діалог «Запит на реєстрацію».
- 6.Ввести загальнодоступну («білу/публічну») IP-адресу ШБО (яка доступна через мережу Інтернет, була виділена для цього шлюзу безпечного обміну та налаштована на підготовчих кроках) або відповідне DNS-ім'я та натиснути на кнопку «ОК».

Якщо все зроблено коректно, статус сертифіката автентифікації повинен змінитися на «в процесі реєстрації». Це означає, що запит був успішно відправлений шлюзом безпечного обміну.

Наступним кроком є подача заявки на реєстрацію шлюзу безпечного обміну засобами Особистого кабінету Каталогу системи «Трембіта» (**Реєстрація ШБО в ядрі системи (Тестове середовище)**). Порядок подачі зазначеної заявки вказаний в п. 7.3.4 Регламенту роботи системи «Трембіта».

Після чого Адміністратор системи «Трембіта» повинен обробити заявку та підтвердити запит.

Коли запит на реєстрацію буде схвалено, статус сертифікату автентифікації та сертифікату шифрування зміниться на «зареєстровано». Це може зайняти деякий час (з врахуванням часу обробки заявки), поки глобальна конфігурація не буде оновлена. Після отримання відповіді на заявку на реєстрацію шлюзу безпечного обміну можна перевірити сторінку «Ключі і сертифікати» у вебінтерфейсі ШБО. В разі необхідності можна оновлювати її, оновлення глобальної конфігурації може зайняти декілька хвилин.

Приклад вебінтерфейсу, коли всі сертифікати коректно зареєстровані:

Сертифікат	Учасник	ОСР- відповідь	Діє до	Стан
Токен: softToken-0				<a href="#">ВИХІД</a>
Ключ: authKey (auth)				
Trembita CA 528690...		дійсний	2024-02-08	zareestrovano
Токен: uacToken-файлова система (каталоги системи)-1				<a href="#">ВИХІД</a>
Ключ: uaToken-encr (encr)				
АЦСК органів юстиц...		дійсний	2019-11-14	zareestrovano
Ключ: uaToken-sign (sign)				
АЦСК органів юстиц...	GOV : 11111111	дійсний	2019-11-14	zareestrovano

## 6.5. ?????????? ????????????

Щоб опублікувати сервіси або здійснювати запити до інших сервісів через систему «Трембіта» на шлюзі безпечного обміну Адміністратор вебсервісів повинен створити та зареєструвати принаймні одну підсистему, яка представлятиме реальну інформаційну систему Суб'єкта електронної взаємодії у тестовому середовищі системи «Трембіта».

Для реєстрації підсистем у вебінтерфейсі шлюзу безпечного обміну необхідно виконати наступні дії:

1. Обрати розділ «Клієнти сервера безпеки» та натиснути на кнопку «Додати клієнта».

SEVDEIR-TEST : 00000010\_SS\_P\_01  
СЕРВЕР БЕЗПЕКИ

КОНФІГУРАЦІЯ  
Клієнти сервера безпеки  
Параметри системи

КЕРУВАННЯ  
Ключі і сертифікати  
Резервне копіювання і відновлення  
Ліцензія

ДОПОМОГА

КЛІЄНТИ СЕРВЕРА БЕЗПЕКИ

ДОДАТИ КЛІЄНТА

UXPADMIN

ПОШУК

Ім'я ^	ID
Тестова організація 10	MEMBER : SEVDEIR-TEST : GOV : 00000010
Тестова організація 10	SUBSYSTEM : SEVDEIR-TEST : GOV : 00000010 : UX...
Тестова організація 10	SUBSYSTEM : SEVDEIR-TEST : GOV : 00000010 : UX...
Тестова організація 10	SUBSYSTEM : SEVDEIR-TEST : GOV : 00000010 : UX...
Тестова організація 10	SUBSYSTEM : SEVDEIR-TEST : GOV : 00000010 : UX...

2. Обрати «Клас Учасника» – GOV.

3. Ввести в поле «Код Учасника» код ЄДРПОУ організації, яка є власником інформаційної системи (Суб'єкта електронної взаємодії).

**Примітка.** При створенні кластера підсистему можна додати шляхом вибору її з глобального списку, натиснувши на відповідну кнопку в інтерфейсі – «Виберіть клієнта з глобального списку», знайти необхідну підсистему шляхом пошуку по коду підсистеми, після чого натиснути на кнопку «ОК».

4. Ввести назву підсистеми (правила іменування зазначені у розділі 6.3 Регламенту роботи системи «Трембіта»).

5. Натиснути послідовно на кнопки «ОК» і потім «Підтвердити».

Додати клієнта
↗
✕

**ВИБЕРІТЬ КЛІЄНТА З ГЛОБАЛЬНОГО СПИСКУ**

Ім'я учасника Тестова організація 10

Клас учасника \*

Код учасника \*

Код підсистеми \*

ОК

СКАСУВАТИ

Необхідне підтвердження
↗
✕

Ви бажаєте надіслати запит на реєстрацію клієнта для доданого клієнта?

Нова підсистема '01\_Test\_IS' буде подана для реєстрації члена 'Тестова організація 10 GOV: 00000010'.

ПІДТВЕРДИТИ

СКАСУВАТИ

Якщо попередні кроки виконано успішно, буде виведено повідомлення зеленого кольору про успішність відправлення запиту. Запит ШБО буде переданий на сервер Каталогу Учасників системи «Трембіта».

Після цього необхідно подати заявку на реєстрацію підсистеми та прив'язку її до конкретного ШБО засобами Особистого кабінету Каталогу системи «Трембіта» (**Реєстрація підсистеми на ШБО (Тестове середовище)**). Порядок подання зазначеної заявки наведено в п. 7.5.2 Регламенту роботи системи «Трембіта».

Після виконання Адміністратором системи «Трембіта» заявки з'явиться зелена позначка навпроти підсистеми у вебінтерфейсі та буде забезпечено можливість використання тестового середовища системи «Трембіта». Якщо підсистеми зареєстровані вірно, інтерфейс ШБО буде виглядати наступним чином:

КЛІЄНТИ СЕРВЕРА БЕЗПЕКИ
+ ДОДАТИ КЛІЄНТА
UXPADMIN

ПОШУК

	Ім'я ^	ID	
<span style="color: green;">●</span>	Тестова організація 10	MEMBER : SEVDEIR-TEST : GOV : 00000010	i
<span style="color: green;">●</span>	Тестова організація 10	SUBSYSTEM : SEVDEIR-TEST : GOV : 00000010 : UXP_ATR_Demo	i
<span style="color: green;">●</span>	Тестова організація 10	SUBSYSTEM : SEVDEIR-TEST : GOV : 00000010 : UX...	i
<span style="color: green;">●</span>	Тестова організація 10	SUBSYSTEM : SEVDEIR-TEST : GOV : 00000010 : UX...	i
<span style="color: green;">●</span>	Тестова організація 10	SUBSYSTEM : SEVDEIR-TEST : GOV : 00000010 : UX...	i