7. ?????????? ???????????? ????? ??????????? ??????

7.1. ????????? ????????????? ????? ?????????? ??????

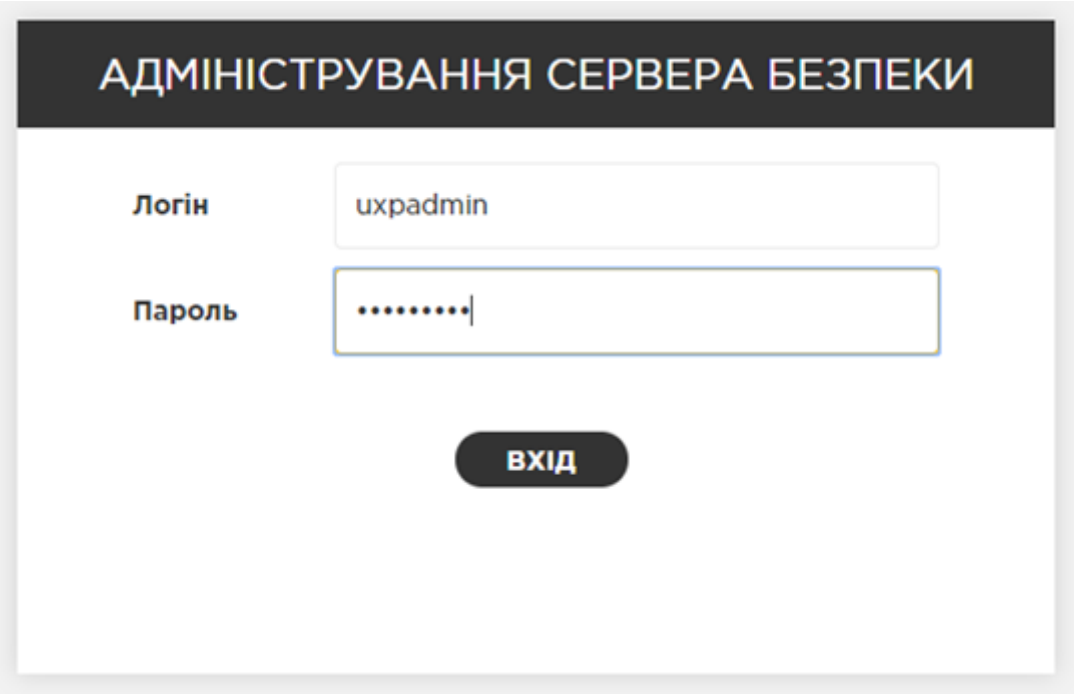
Початкова конфігурація шлюзу безпечного обміну виконується Адміністратором вебсервісів.

7.1.1. ????????????? ????? ?????????? ??????

Для ініціалізації 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,

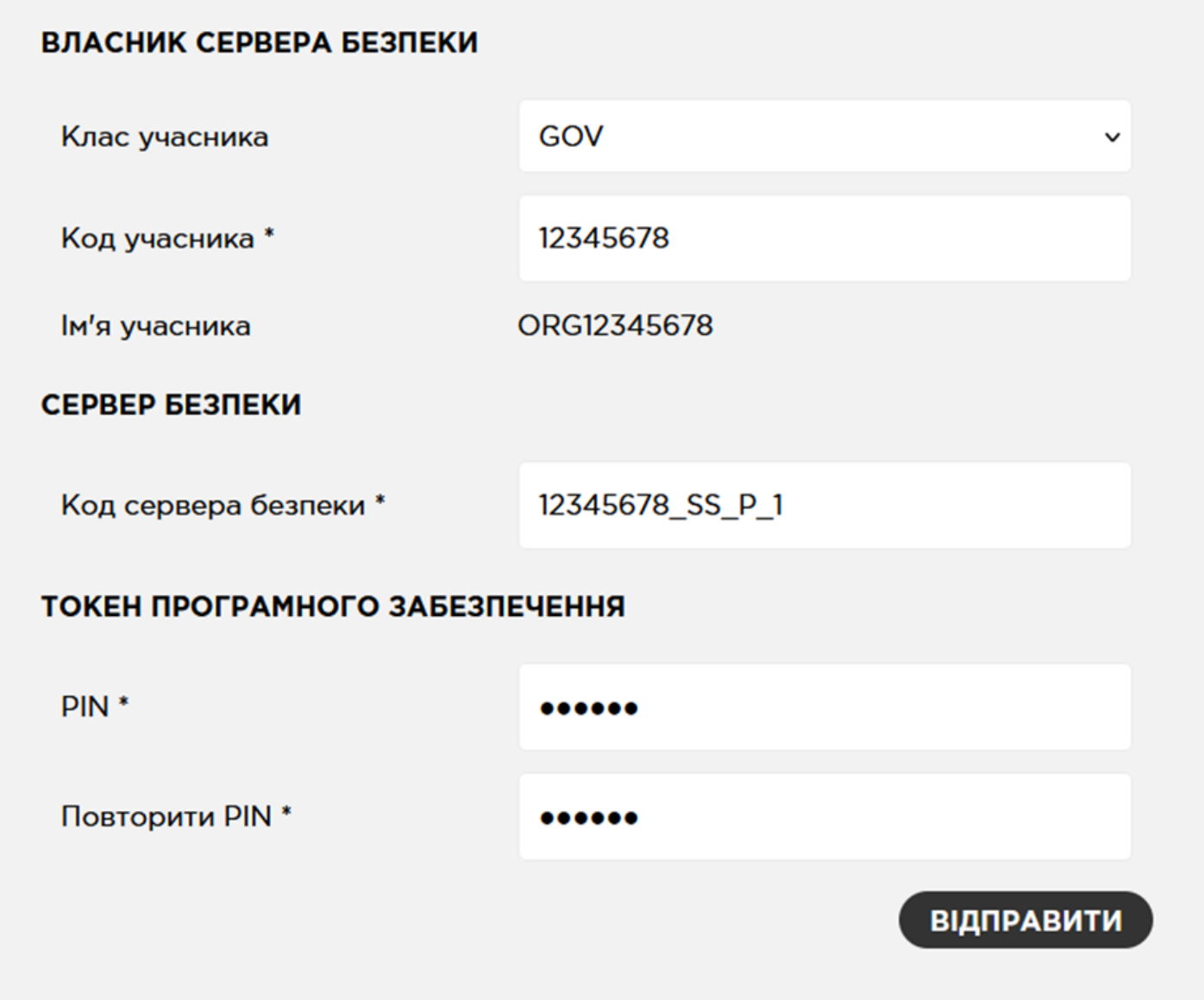
використовуючи атрибути доступу користувача з роллю Адміністратор вебсервісів:



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

> **Примітка.** У перші хвилини після перезапуску шлюзу безпечного обміну вебінтерфейс ШБО може відображати повідомлення «502 Bad Gateway» (зазвичай менше однієї хвилини). Необхідно періодично оновлювати сторінку авторизації, поки не відобразиться форма входу.

Після чого відкриється вікно ініціалізації ШБО:



Для ініціалізації ШБО необхідно заповнити наступні дані:

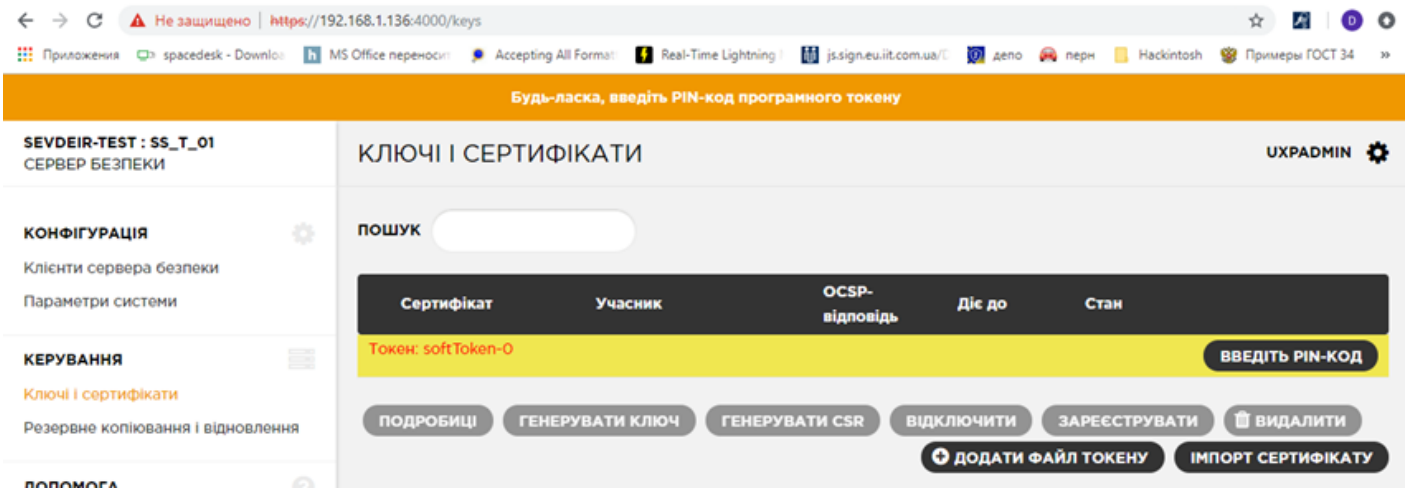
Власник сервера безпеки (Security Server Owner)	
Клас Учасника (Member Class)	GOV

Код Учасника (Member Code)	У якості коду Учасника використовується код ЄДРПОУ організації, яка є Учасником системи «Трембіта». **Важливо!** 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)	Унікальний код ШБО («сервера безпеки» в вебінтерфейсі) в промисловому середовищі системи «Трембіта», який потрібно створити відповідно до наступного шаблону: **MemberCode_SS_P_Number_FreeSymbols**, де: **MemberCode** – код ЄДРПОУ організації; **SS** – означення ШБО (security server); **P** – абревіатура промислового середовища системи, не змінюється; **Важливо!** Варто звернути увагу, що _SS_P_ потрібно вводити великими латинськими літерами з використанням символу нижнього підкреслення «_». **Number** – порядковий номер ШБО організації; **Примітка.** Нумерація ШБО для тестового та промислового середовищ системи незалежна. **FreeSymbols** – (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). **Важливо!** Додаткові символи повинні містити лише цифри та великі літери англійського алфавіту.
Програмний токен (Software Token)	
PIN	Необхідно придумати PIN-код, який буде використаний для захисту ключів автентифікації, що зберігаються у програмному сховищі (файловій системі ОС). **Важливо!** Адміністратор вебсервісів має зберігати PIN-код у безпечному місці, оскільки після втрати PIN-коду необхідно відновлювати токен, повторно видавати та реєструвати новий сертифікат автентифікації.
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 «OK».

7.1.2. ???????? PIN-???? ??????????? ??????

ШБО 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 токену». Це повідомлення вказує на те, що зазначений токен безпеки на даний час заблокований, а особисті ключі не можуть бути використані. Щоразу при перезавантаженні ПЗ UXP Security Server або всієї операційної системи ШБО, потрібно вводити PIN-код токену 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:

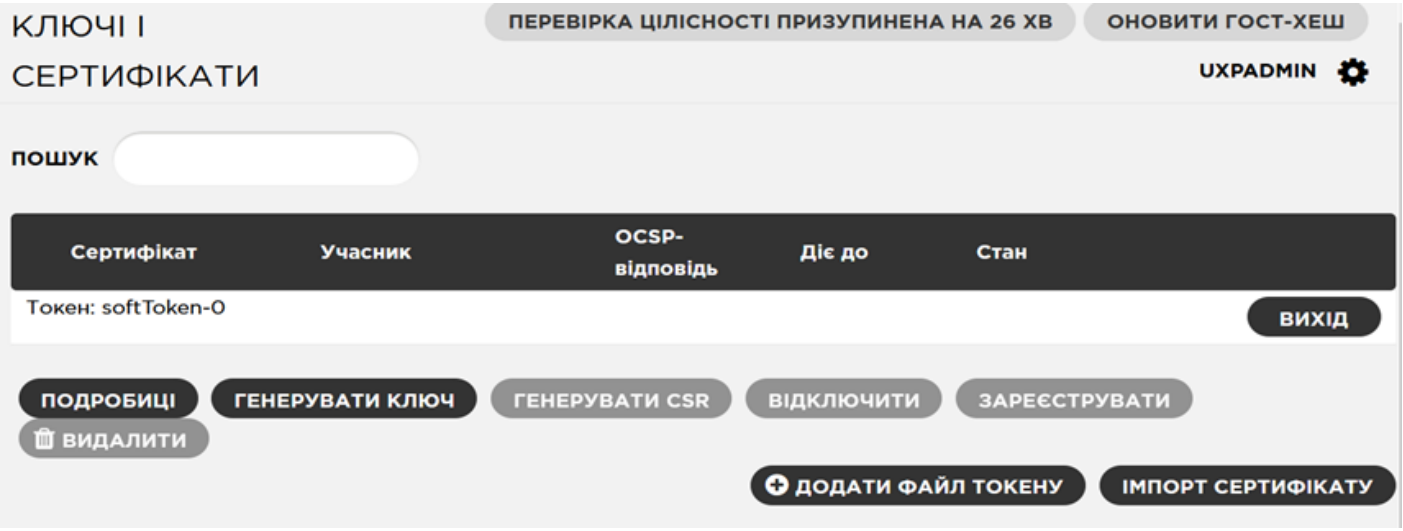
1. Перейти в розділ «Ключі і сертифікати».

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 «OK».

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



Примітка. Варто звернути увагу, що на шлюзі безпечного обміну в промисловому середовищі працює модуль контролю цілісності. Необхідно перевіряти значення таймеру у верхній частині сторінки. Якщо користувач не встигатиме завершити необхідні налаштування, він має натиснути на кнопку «Перевірка цілісності призупинена на ## хв», щоб отримати більше часу. Після завершення налаштувань обов'язково потрібно натиснути на кнопку «Оновити ГОСТ-ХЕШ».

Важливо! Якщо користувач не встиг виконати всі необхідні налаштування та зберегти зміни шляхом оновлення ГОСТ-хешу, модуль контролю цілісності може призупинити роботу сервісів шлюзу безпечного обміну, а вебінтерфейс адміністрування стане недоступним. У цьому випадку Адміністратору локальних компонентів (системному адміністраторові) необхідно виконати наступні команди в командному інтерфейсі ШБО:

```
sudo uxp-ua-integritychecker.sh recalc_all
sudo uxp-ua-integritychecker.sh check
sudo uxp-ua-integritychecker.sh start_all
```

7.1.3. ???????????? ??????? ???????? ????

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:

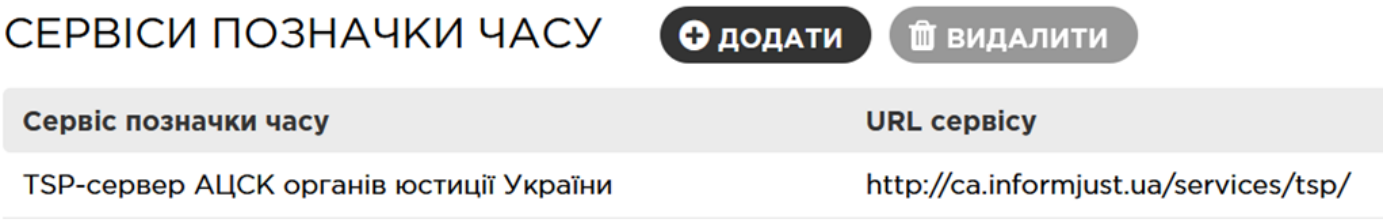
1. Перейти в розділ «Параметри системи». Список серверів позначок часу має бути порожнім («Немає (відповідних) записів»).

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».



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

7.2. ?????????? ????????? ?????? ????????? ?????? (????????? ???????)

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 промисловому середовищі системи «Трембіта» є обов’язковим використання апаратних токенів або HSM-пристроїв.

Захищений носій особистих ключів (апаратний токен), на якому знаходяться особисті ключі електронної печатки та шифрування необхідно правильно підключити до віртуальної машини шлюзу безпечного обміну. 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** 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.

7.2.1. ????????????? 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:

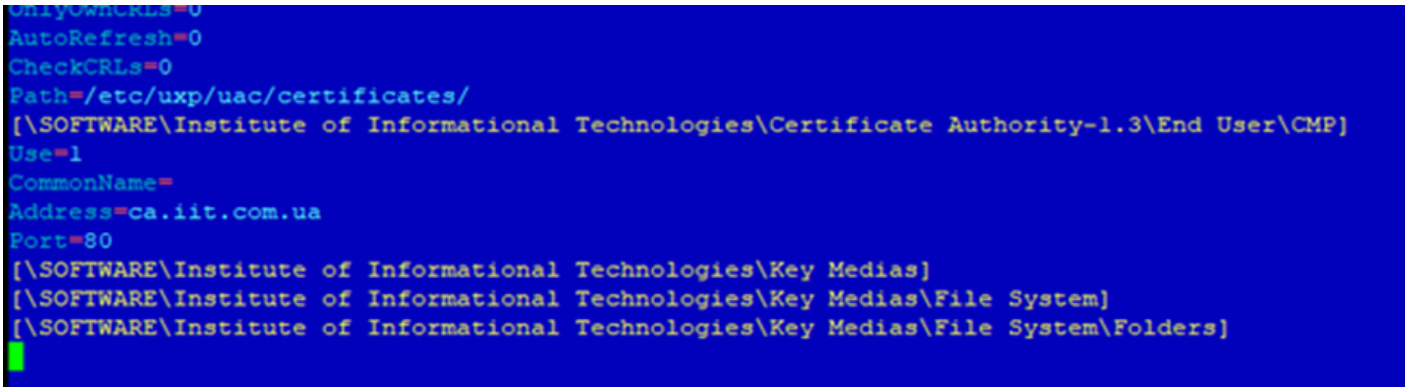
```
sudo nano /etc/uxp/uac/osplm.ini
```

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
```

3. У поле Address необхідно вказати адресу до сервісу CMP КНЕДП, що видав сертифікати (наприклад, ca.informjust.ua, ca.iit.com.ua тощо, залежно від КНЕДП). Зазначену адресу може надати, зокрема, надавач електронних довірчих послуг або її можна дізнатись з веб інтерфейсу ШБО на вкладці «Параметри системи» в секції «Сервіси позначки часу» (який було вказано в розділі 7.1.3 даної інструкції).

Приклад результату модифікації файлу:



7.2.2. ???????????? ????????? ????????? ?????? ????????? ?????? (????????? ???????)

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-1K;

- Автор Secure Token 337;

- Автор Secure Token 338;

- EfitKey;

- Кристал-1;

2. Мережеві криптомодулі:

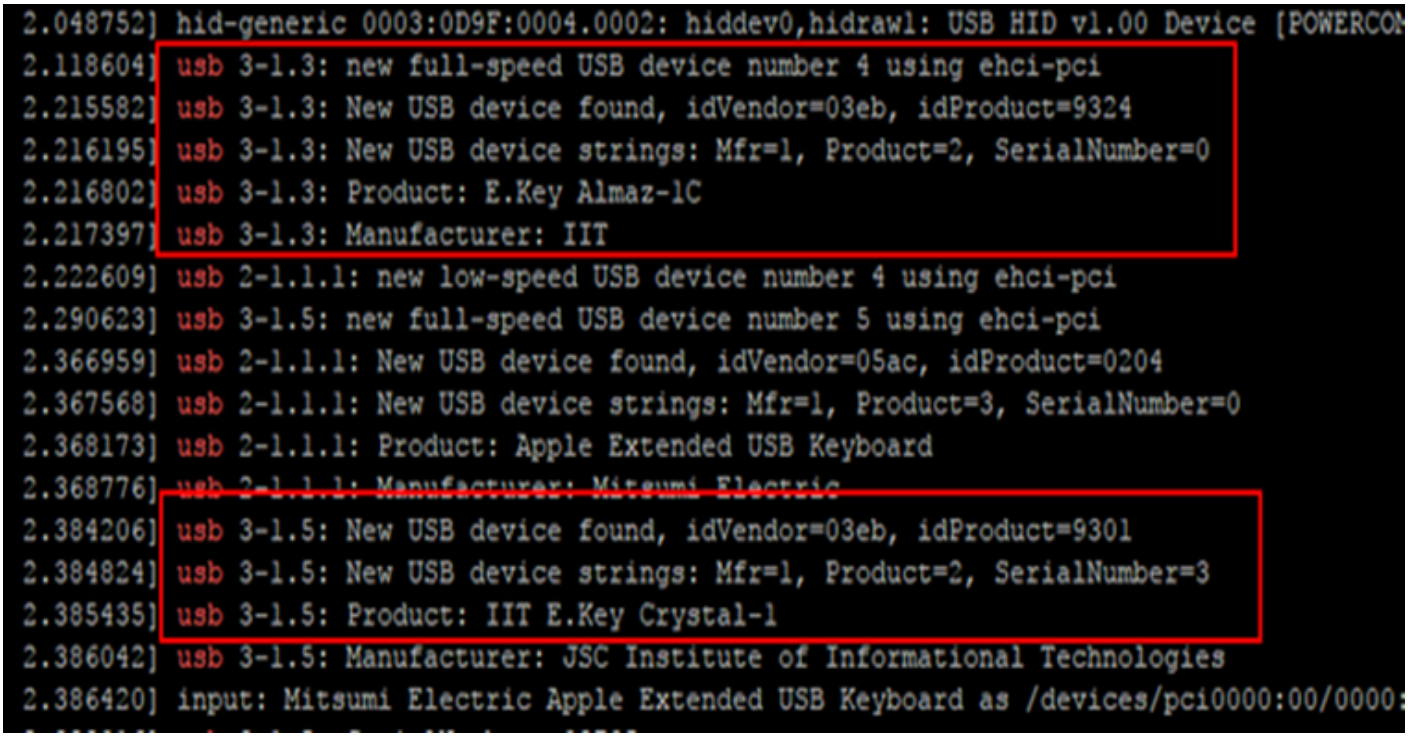
- ІІТ Гряда-301;

- Сайфер «Шифр-HSM».

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
```



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
```

7.2.2.1. ???????????? ?????-1?

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

7.2.2.2. ???????????? ????? 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 токену 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:

7.2.2.3. ???????????? 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 елементу «<array>» додати:

```
«<string>0xC1A6</string>»
```

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

```
«<string>0x0151</string>»
```

4. Знайти строку «<key>ifdFriendlyName</key>» і після елементу «<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
```

7.2.2.4. ???????????? ???????-1

При використанні токену «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
```

7.2.2.5. ???????????? ??? ?????-301

При використанні токену безпеки ІІТ «Гряда-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\<Serial Number>]
OrderNumber=0
SN=<Serial Number>
Address=<Your-Gryada-301-IP>
AddressMask=255.0.0.0
```

де **<Serial Number>** – це останні три цифри серійного номеру пристрою ІІТ 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
```

7.2.2.6. ???????????? ?????? «????-HSM»

Для забезпечення роботи токену 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 токені, 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 <SlotNunber> -O -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 використовуваний ключ повинен з’явитись в вебінтерфейсі ШБО в розділі «Ключі і сертифікати».

7.3. ?????????? ????? ?????????? ??????

7.3.1. ?????? ????? ??????? ?? ??????????

Для імпорту ключа підпису та шифрування потрібно мати згенеровані ключі печатки та шифрування та відповідні сертифікати, видані одним з КНЕДП, що підтримуються системою «Трембіта». Отримання сертифікатів виконується на підготовчому етапі підключення до системи.

Ключі електронної печатки та шифрування можуть зберігатися на програмних захищених носіях особистих ключів, які повинні бути підключені та налаштовані згідно розділу 7.3.3.

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 сховища ключів uacToken (це PIN-код до особистого ключа, що імпортований з ZIP-архіву).

3. Навпроти кожного сертифікату натиснути кнопку «Імпортувати».

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

7.3.2. ????????? ????? ????????????? ??? ????? ?????????? ??????

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».

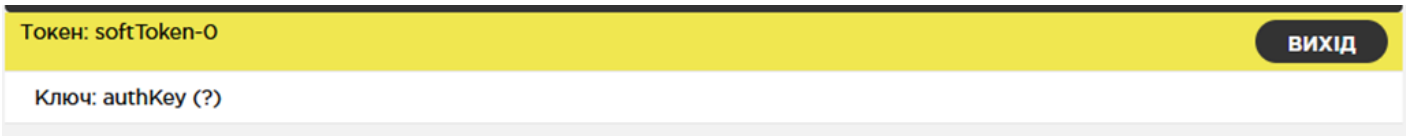
2. Обрати токен «softToken-0», натиснувши на ньому мишкою.

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 (?)».



7.3.3. ????????? ?????? ?? ?????????? (Certificate Signing Request) ????? ?????????????

Сертифікати автентифікації, які використовуються шлюзами безпечного обміну, повинні бути підписані технологічним центром сертифікації ключів промислового 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
Сервіс сертифікації (Certification Service)	Необхідно обрати технологічний центр сертифікації ключів промислового середовища системи – «Trembita Diia CA»
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 такому разі потрібно звернутися до Адміністратора системи «Трембіта» для уточнення. Якщо всі поля заповнені – необхідно натиснути на кнопку «ОК».

Зберегти файл з розширенням *.pem на комп’ютері.

7.3.4. ????????? ??????????? ??? ????? ?????????????

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» засобами Особистого кабінету Каталогу системи «Трембіта» (**Видача нового сертифікату автентифікації (Промислове 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!

7.3.5. ?????? ??????????? ??? ????? ????????????? ?? ???? ?????????? ??????

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 «Ключ: authKey».

7.3.6. ????????? ???????????? ????????????? ?? ???????

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 «Ключ: authKey», з числовим серійним номером).

3. Натиснути на кнопку «Активувати».

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

Натиснути на кнопку «Активувати».

7.3.7. ????????? ?????? ?? ?????????? ???????????

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 ШБО 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 шлюзу безпечного обміну (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».

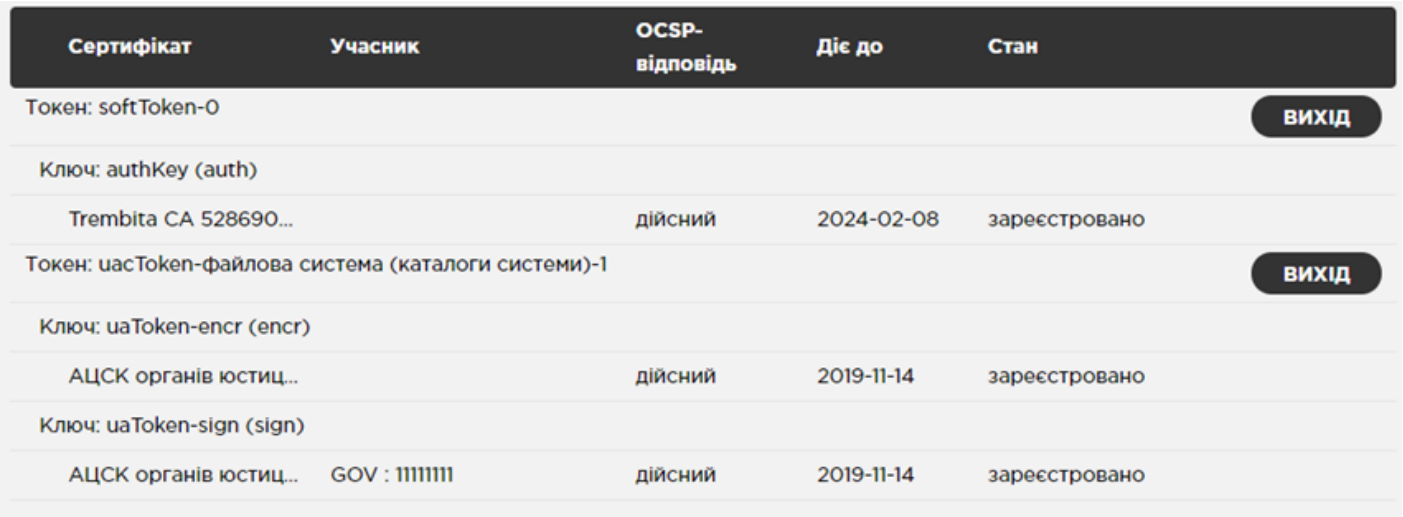
Якщо все зроблено коректно, статус сертифіката автентифікації повинен стати «в процесі реєстрації». Це означає, що запит був успішно відправлений шлюзом безпечного обміну.

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

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 шлюзу безпечного обміну. В разі необхідності можна оновлювати її. Оновлення глобальної конфігурації може зайняти декілька хвилин.

Приклад вебінтерфейсу, коли всі сертифікати коректно зареєстровані:



7.4. ?????????? ??????????

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».

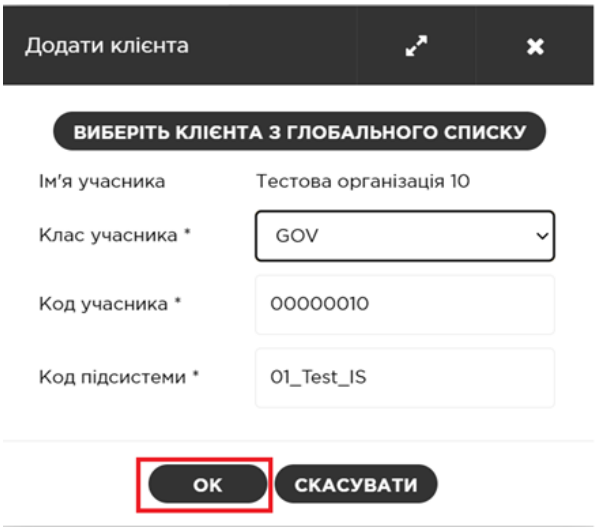
2. Обрати «Клас Учасника» – GOV.

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».



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 (Промислове 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: