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
```

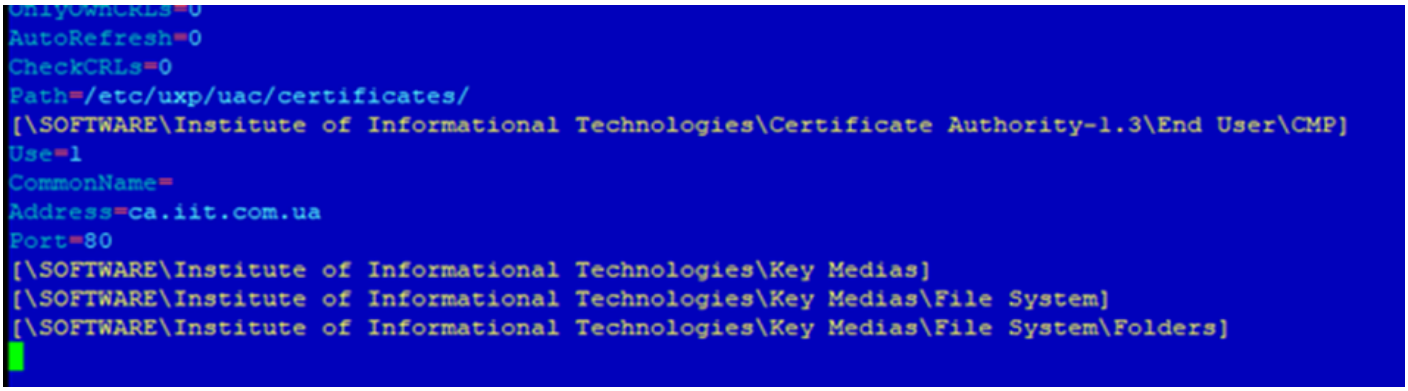
2. Знайти розділ (у квадратних дужках визначаються розділи) з налаштуваннями CMP-сервісу та встановити наступні параметри доступу:

```
[\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:



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:

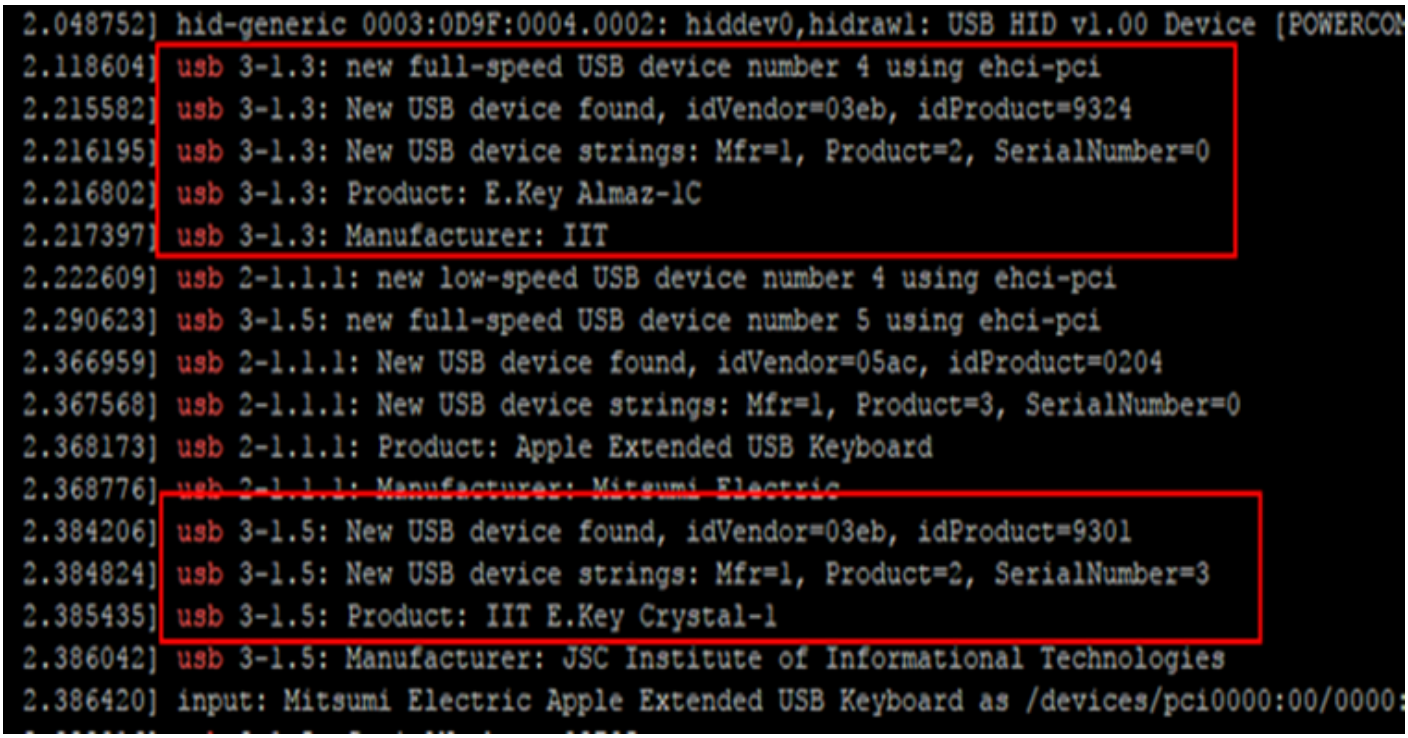
- ІІТ Гряда-301;

- Сайфер «Шифр-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
```

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 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:

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 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
```

6.3.2.4. ???????????? ???????-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
```

6.3.2.5. ???????????? ??? ?????-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
```

6.3.2.6. ???????????? ?????? «????-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».

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».

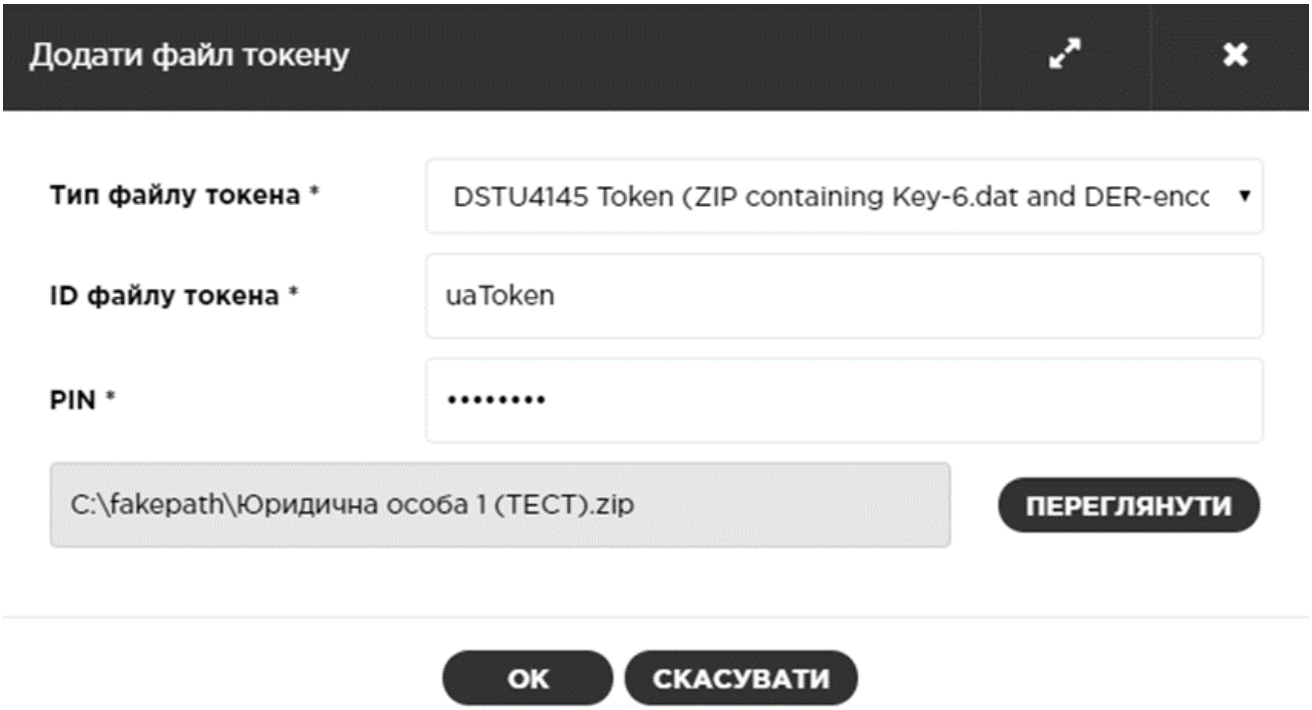
2. Натиснути на кнопку «Додати файл токену».

3. У вікні «Додати файл токену» 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 «OK».



Версія #5
Admin створив 2024-06-30 21:00:01 UTC
Administrator оновив 2025-11-27 12:35:22 UTC