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».

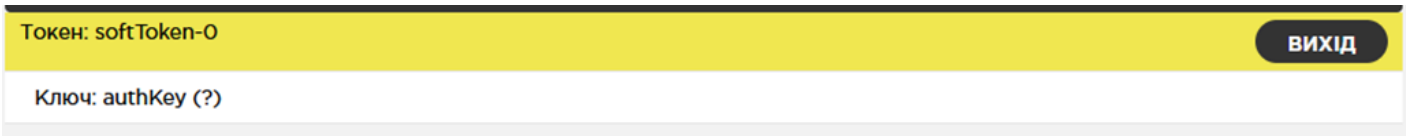
2. Обрати токен «softToken-0», натиснувши на ньому мишкою.

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 «OK».

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:

Сертифікат	Учасник	OCSP-відповідь	Діє до	Стан	
Токен: softToken-0					ВИХІД
Ключ: authKey (auth)					
Trembita CA 528690...		дійсний	2024-02-08	зареєстровано	
Токен: uacToken-файлова система (каталоги системи)-1					ВИХІД
Ключ: uaToken-encr (encr)					
АЦСК органів юстиц...		дійсний	2019-11-14	зареєстровано	
Ключ: uaToken-sign (sign)					
АЦСК органів юстиц...	GOV : 11111111	дійсний	2019-11-14	зареєстровано	

Версія #3
Admin створив 2024-09-23 06:03:21 UTC

Admin оновив 2024-09-25 09:32:49 UTC