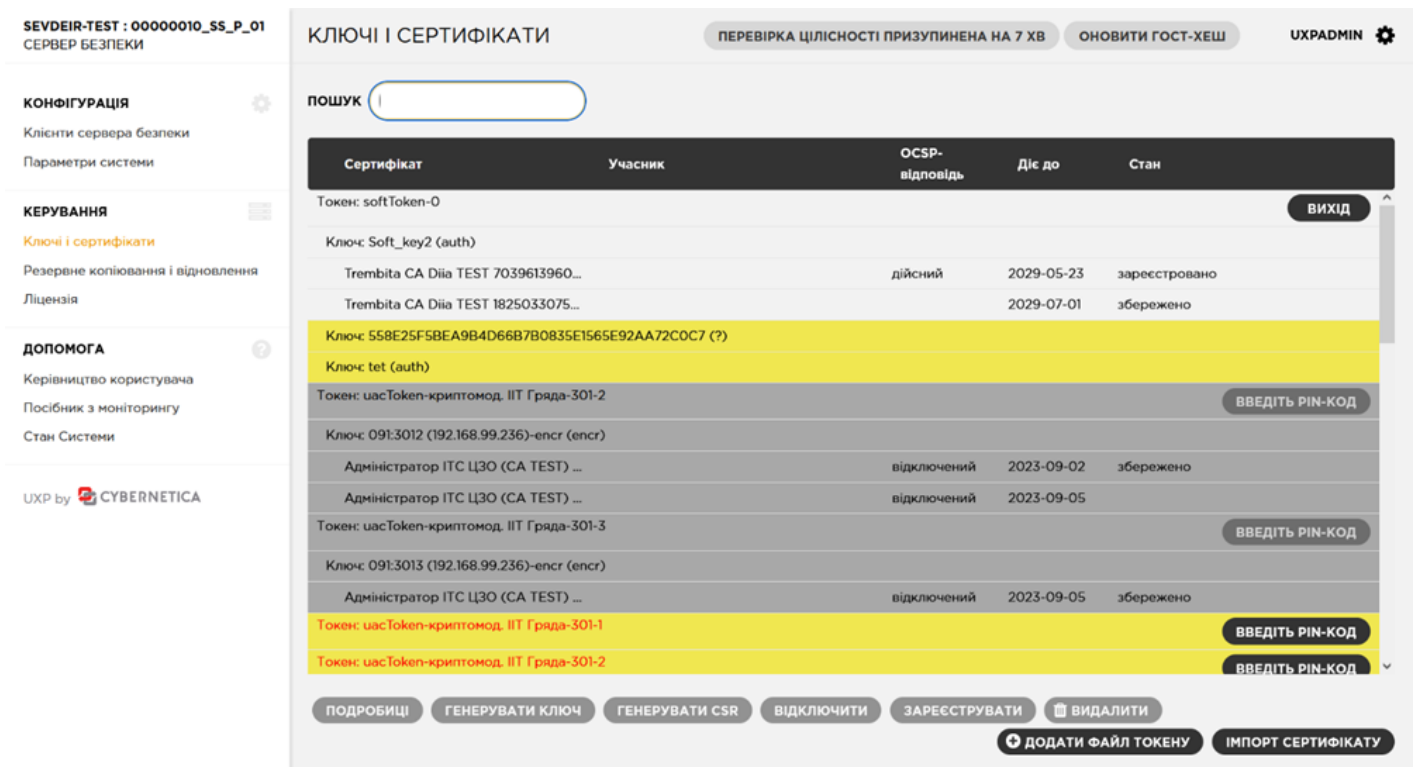


3.4. ????????? «?????? ?? ????????????????»



На вкладці «Ключі та сертифікати» користувач може:

1. Переглянути завантажені носії особистих ключів, сертифікати аутентифікації, підписання та шифрування, які використовуються на даному ШБО, їх статуси (дійсний чи відключений), термін дії та поточний стан (зареєстровано, в процесі реєстрації, збережено, помилка).

Шлюз безпечного обміну підтримує два типи носіїв особистих ключів:

- апаратний токен, що повинен бути підключений 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. За дану дію відповідає Адміністратор локальних компонентів (системний адміністратор). Після підключення апаратний токен буде автоматично відображено в вебінтерфейсі ШБО.

- файловий токен, що використовується в тестовому середовищі системи «Трембіта». Файловий токен необхідно попередньо імпортувати на ШБО, користуючись настановами п.11 розділу 2.4 даної інструкції.

Активні (дійсні) токени кольором не відмічені:

Ключ: uacTokenNew3-encr (encr)				
Адміністратор ІТС ЦЗО (CA TEST) ...	відключений	2024-02-15	глобальна пом...	
Ключ: uacTokenNew3-sign (sign)				
Адміністратор ІТС ЦЗО (CA TEST) ... GOV : 00000010	відключений	2024-02-15	зареєстровано	
Токен: uacToken-файлова система (каталоги системи)-6				ВИХІД
Ключ: token-encr (encr)				
Адміністратор ІТС ЦЗО (CA TEST) ...	дійсний	2025-02-27	зареєстровано	
Ключ: token-sign (sign)				
Адміністратор ІТС ЦЗО (CA TEST) ... GOV : 00000010	дійсний	2025-02-27	зареєстровано	

Темно-сірим кольором відмічені токени, недоступні на ШБО на даний момент (відключені або ті, в яких не введено PIN-код):

Токен: uacToken-файлова система (каталоги системи)-5				ВВЕДІТЬ PIN-КОД
Ключ: uacTokenNew3-encr (encr)				
Адміністратор ІТС ЦЗО (CA TEST) ...	відключений	2024-02-15	глобальна пом...	
Ключ: uacTokenNew3-sign (sign)				
Адміністратор ІТС ЦЗО (CA TEST) ... GOV : 00000010	відключений	2024-02-15	зареєстровано	
Токен: uacToken-файлова система (каталоги системи)-6				ВИХІД
Ключ: token-encr (encr)				
Адміністратор ІТС ЦЗО (CA TEST) ...	дійсний	2025-02-27	зареєстровано	
Ключ: token-sign (sign)				
Адміністратор ІТС ЦЗО (CA TEST) ... GOV : 00000010	дійсний	2025-02-27	зареєстровано	

Жовтим кольором відмічені токени, підключені до ШБО на даний момент, але сертифікати з яких не завантажені на ШБО:

Токен: softToken-0				ВИХІД
Ключ: Soft_key2 (auth)				
Trembita CA Diia TEST 7039613960...	дійсний	2029-05-23	зареєстровано	
Trembita CA Diia TEST 1825033075...		2029-07-01	збережено	
Ключ: 558E25F5BEA9B4D66B7B0835E1565E92AA72C0C7 (?)				
Ключ: tet (auth)				
Токен: uacToken-криптокод. ІІТ Гряда-301-1				ВВЕДІТЬ PIN-КОД
Токен: uacToken-криптокод. ІІТ Гряда-301-2				ВВЕДІТЬ PIN-КОД
Токен: uacToken-криптокод. ІІТ Гряда-301-3				ВВЕДІТЬ PIN-КОД
Токен: uacToken-криптокод. ІІТ Гряда-301-4				ВВЕДІТЬ PIN-КОД
Токен: uacToken-криптокод. ІІТ Гряда-301-5				ВВЕДІТЬ PIN-КОД
Токен: uacToken-криптокод. ІІТ Гряда-301-6				ВВЕДІТЬ PIN-КОД
Токен: uacToken-криптокод. ІІТ Гряда-301-2				ВВЕДІТЬ PIN-КОД
Ключ: 091:3012 (192.168.99.236)-encr (encr)				
Адміністратор ІТС ЦЗО (CA TEST) ...	відключений	2023-09-02	збережено	
Адміністратор ІТС ЦЗО (CA TEST) ...	відключений	2023-09-05		

2. Увійти до необхідного токену.

Примітка. Дана дія виконується щоразу після запуску, перезавантаження ШБО або підключення чи імпорту нового токена.

Для входу до певного токена необхідно натиснути на кнопку «Введіть PIN-код» напроти нього, а в наступному вікні ввести PIN-код та натиснути на кнопку «ОК».

Токен: uasToken-файлова система (каталоги системи)-1					ВВЕДІТЬ PIN-КОД
Ключ: UaToken1-encr (encr)					
Адміністратор ІТС ЦЗО (CA TEST) 3...		дійсний	2024-12-01	зареєстровано	
Ключ: UaToken1-sign (sign)					
Адміністратор ІТС ЦЗО (CA TEST) 3...		GOV : 00000088	дійсний	2024-12-01	зареєстровано

Важливо! Необхідно звернути увагу на те, що більшість апаратних токенів обмежують кількість неуспішних спроб введення PIN-коду, при перевищенні якої особистий ключ автоматично видаляється з токена.

3. Переглянути детальну інформацію про токен. Для цього необхідно виділити потрібний токен (шляхом натискання), після чого натиснути на кнопку «Подробиці» в нижній частині вікна.

Сертифікат	Учасник	ОСП-відповідь	Діє до	Стан	
Токен: softToken-0					ВИХІД
Ключ: authKey1 (auth)					
UXP Class3 CA 376750702783673873		дійсний	2028-11-29	зареєстровано	
Токен: uasToken-файлова система (каталоги системи)-1					ВИХІД
Ключ: UaToken1-encr (encr)					
Адміністратор ІТС ЦЗО (CA TEST) 3...		дійсний	2024-12-01	зареєстровано	
Ключ: UaToken1-sign (sign)					
Адміністратор ІТС ЦЗО (CA TEST) 3...		GOV : 00000088	дійсний	2024-12-01	зареєстровано
ПОДРОБИЦІ	ГЕНЕРУВАТИ КЛЮЧ	ГЕНЕРУВАТИ CSR	ВІДКЛУЧИТИ	ЗАРЕЄСТРУВАТИ	ВІДАЛИТИ
				ДОДАТИ ФАЙЛ ТОКЕНУ	ІМПОРТ СЕРТИФІКАТУ

4. Вийти з токена. Для виходу з певного токена необхідно натиснути на кнопку «Вихід» напроти нього.

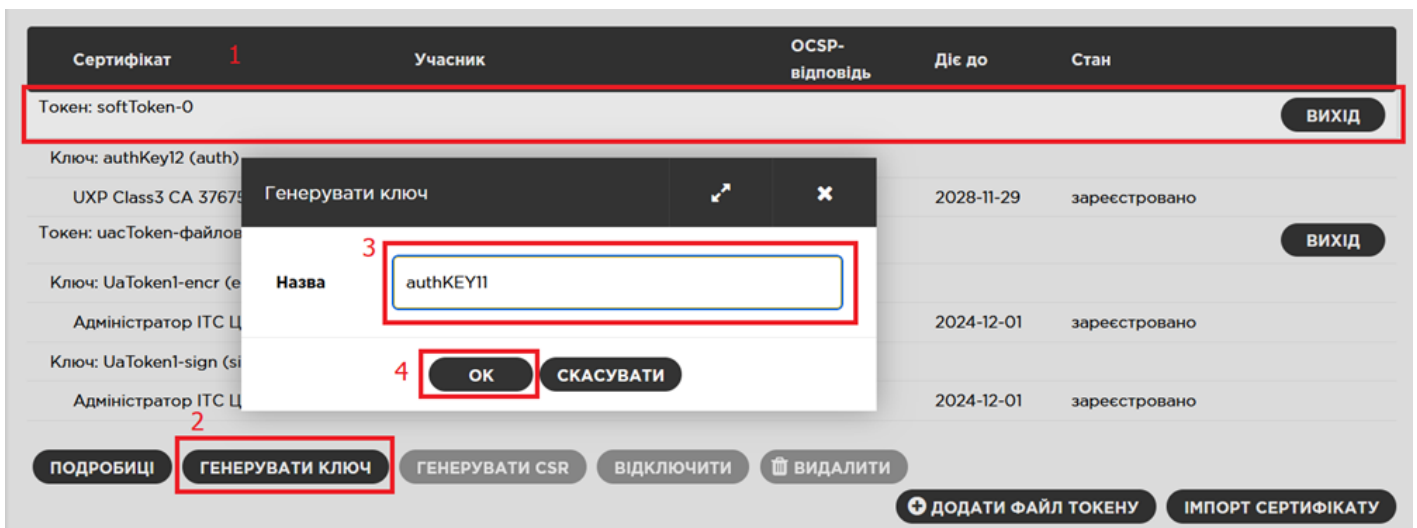
Сертифікат	Учасник	ОСП-відповідь	Діє до	Стан	
Токен: softToken-0					ВИХІД
Ключ: authKey1 (auth)					
UXP Class3 CA 376750702783673873		дійсний	2028-11-29	зареєстровано	

5. Створити новий ключ аутентифікації.

Примітка. Дана дія виконується вперше на етапі ініціалізації ШБО та в подальшому в процесі експлуатації ШБО, при необхідності створення нового ключа аутентифікації (перевипуску сертифікату аутентифікації).

Для створення ключа аутентифікації необхідно:

- Обрати токен «softToken-0», натиснувши на ньому мишкою.
- Натиснути на кнопку «Генерувати ключ».
- Ввести позначку для ключа аутентифікації. Рекомендовано ввести позначку «authKey».
- Натиснути на кнопку «ОК».



6. Створити запит на сертифікат для ключа аутентифікації.

Примітка. Дана дія виконується вперше на етапі ініціалізації ШБО та в подальшому в процесі експлуатації ШБО, при необхідності створення нового ключа аутентифікації (перевипуску сертифікату аутентифікації). Цей запит необхідно подати Адміністратору системи «Трембіта» засобами Особистого кабінету Каталогу системи «Трембіта» в заявці «**Видача нового сертифікату аутентифікації**».

Для того, щоб створити даний запит необхідно:

- Вибрати ключ аутентифікації (authKey), який було попередньо створено.
- Натиснути на кнопку «Генерувати CSR» в нижній частині вікна – відкриється діалог «Створити запит на підпис сертифіката».
- У діалоговому вікні необхідно встановити наступні значення:

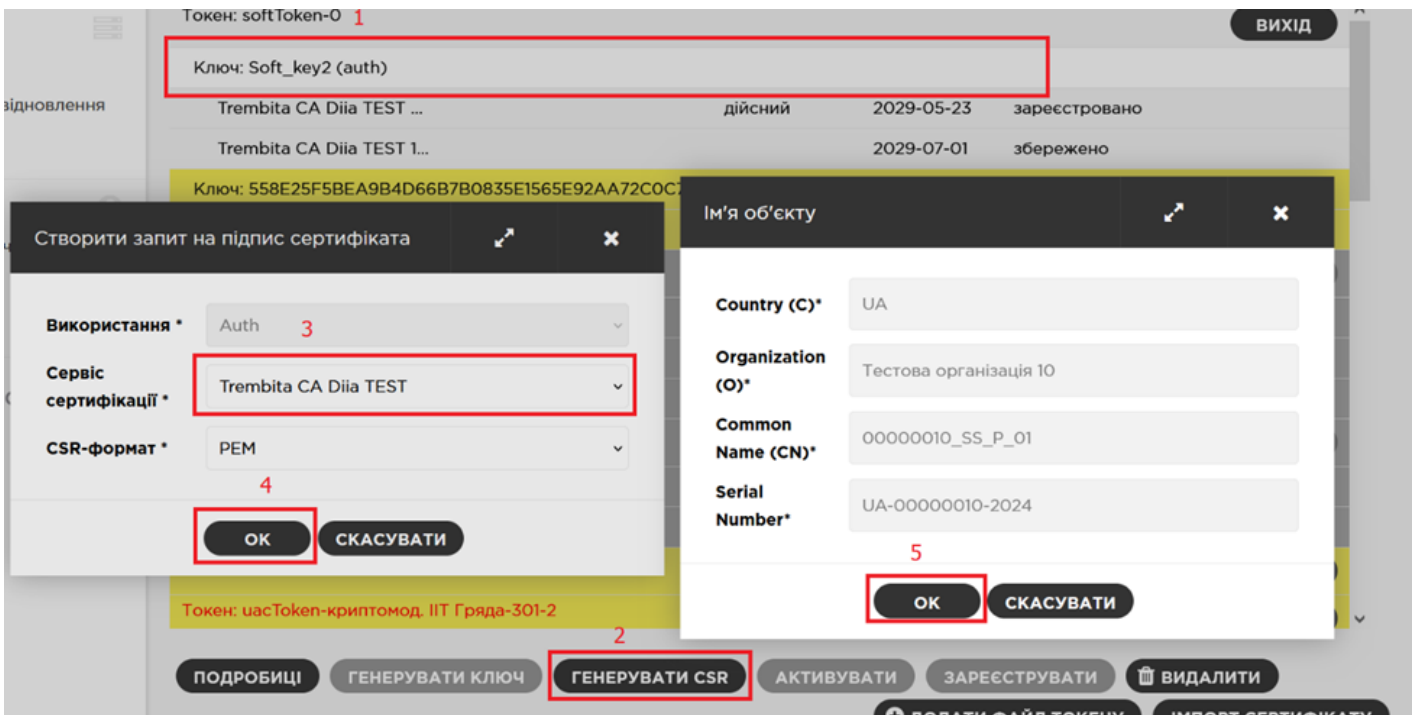
Поле	Значення
------	----------

Використання (Usage)	Auth
Сервіс сертифікації (Certification Service)	Необхідно обрати технологічний центр сертифікації ключів: - для тестового середовища системи: «Trembita CA Diia TEST». - для промислового середовища системи: «Trembita Diia CA»
CSR Format	PEM

- Натиснути на кнопку «ОК».

- 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».

- Зберегти файл з розширенням *.pem на робочій станції адміністратора.

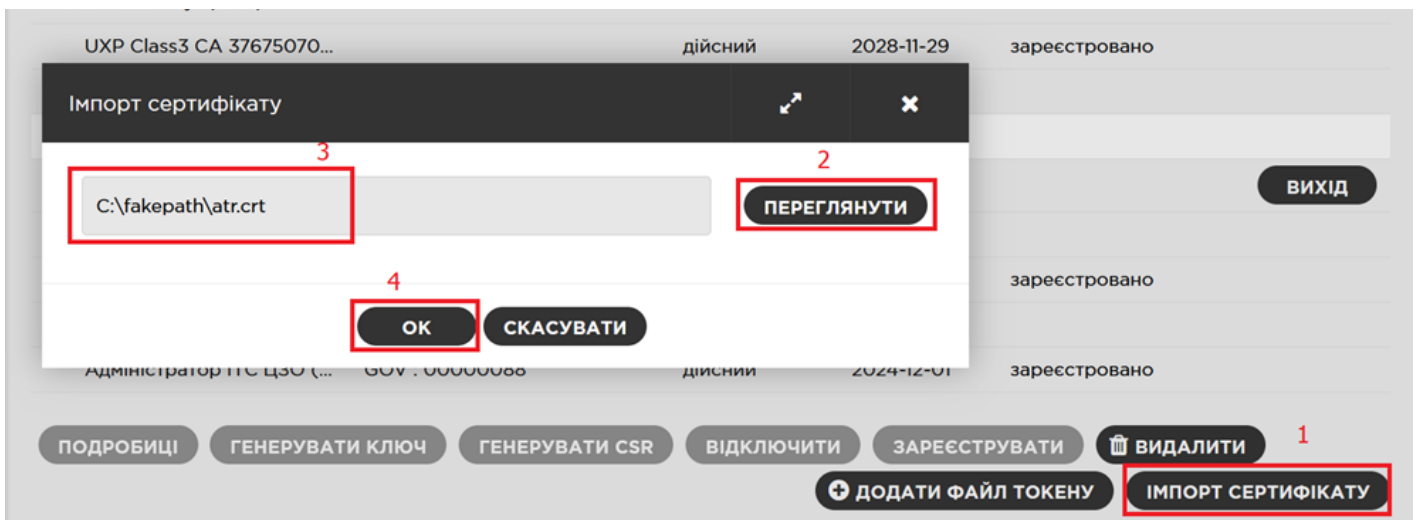


7. Імпортувати новий сертифікат аутентифікації на ШБО.

Примітка. Дана дія виконується вперше на етапі ініціалізації ШБО та в подальшому в процесі експлуатації ШБО, при необхідності створення нового ключа аутентифікації (перевипуску сертифікату аутентифікації). Даний сертифікат надається Адміністратором системи «Трембіта» у відповідь на заявку «**Видача нового сертифікату аутентифікації**» засобами Особистого кабінету Каталогу системи «Трембіта».

Для імпорту сертифікату аутентифікації необхідно:

- Завантажити з Особистого кабінету Каталогу системи «Трембіта» сертифікат аутентифікації.
- Натиснути на кнопку «Імпорт сертифікату» в нижній частині вікна.
- В діалоговому вікні «Імпорт сертифікату» натиснути на кнопку «Переглянути».
- Обрати виданий сертифікат аутентифікації та натиснути на кнопку «ОК».
- Після цього буде відображено інформацію про доданий сертифікат під ключем аутентифікації.



8. Зареєструвати сертифікат аутентифікації.

Примітка. Дана дія виконується при ініціалізації ШБО або при створенні нового (перевипуску) сертифіката аутентифікації.

Для реєстрації сертифікату аутентифікації необхідно виділити його (шляхом натискання на відповідний рядок під відповідним ключем з позначкою «auth», з числовим серійним номером) і натиснути на кнопку «Зареєструвати» в нижній частині вікна.

ПОШУК

Сертифікат	Учасник	ОСР-відповідь	Діє до	Стан
Токен: softToken-0				
Ключ: Soft_key2 (auth)				
Trembita CA Diia TEST 703...	1	дійсний	2029-05-23	зареєстровано
Trembita CA Diia TEST 18250330750182659096672 2427473540075080286234 461			2029-07-01	збережено
Адміністратор ІТС ЦЗО (С...		відключений	2023-09-05	
Токен: uacToken-криптокод. ІІТ Гряда-301-3				
Ключ: 091:3013 (192.168.99.236)-encr (encr)				

ПОДРОБИЦІ ГЕНЕРУВАТИ КЛЮЧ ГЕНЕРУВАТИ CSR ВІДКЛЮЧИТИ ЗАРЕЄСТРУВАТИ ВИДАЛИТИ ДОДАТИ ФАЙЛ ТОКЕНУ ІМПОРТ СЕРТИФІКАТУ

ВВЕДІТЬ PIN-КОД

ВИХІД

Після натискання на кнопку відкриється діалог «Запит на реєстрацію», в якому необхідно вказати загальнодоступну (публічну/білу) IP-адресу ШБО або відповідне DNS-ім'я та натиснути на кнопку «ОК».

9. Скасувати реєстрацію сертифікату аутентифікації. Для скасування реєстрації сертифікату необхідно виділити його (шляхом натискання) і натиснути на кнопку «Скасувати реєстрацію» в нижній частині вікна, після чого – натиснути на кнопку «Підтвердити» в наступному діалоговому вікні.

Ключ: authKey1 (auth) 1 || UXP Class3 CA 376750702783673873 | дійсний | 2028-11-29 | зареєстровано |
Ключ: authkey1100 (auth)				
Запит				
Токен: uacToken-файлова система (каталоги системи)-1				
Ключ: UaToken1-encr (encr)				
Адміністратор ІТС ЦЗО (CA T...		дійсний	2024-12-01	зареєстровано
Ключ: UaToken1-sign (sign)				
Адміністратор ІТС ЦЗО (CA T... GOV : 00000088		дійсний	2024-12-01	зареєстровано

ПОДРОБИЦІ ГЕНЕРУВАТИ КЛЮЧ ГЕНЕРУВАТИ CSR ВІДКЛЮЧИТИ СКАСУВАТИ РЕЄСТРАЦІЮ ВИДАЛИТИ ДОДАТИ ФАЙЛ ТОКЕНУ ІМПОРТ СЕРТИФІКАТУ

10. Видалити ключ аутентифікації. Для цього необхідно виділити ключ аутентифікації, який треба видалити (шляхом натискання) та натиснути на кнопку «Видалити» в нижній частині вікна.

Примітка. Дана дія виконується при необхідності перевипуску ключа аутентифікації.

Ключ: authKey1 (auth)				
UXP Class3 CA 376750702783...	1	дійсний	2028-11-29	zareestrovano
Ключ: authkey1100 (auth)				
Запит				
Токен: uaToken-файлова система (каталоги системи)-1				ВИХІД
Ключ: UaToken1-encr (encr)				
Адміністратор ІТС ЦЗО (CA Т...		дійсний	2024-12-01	zareestrovano
Ключ: UaToken1-sign (sign)				
Адміністратор ІТС ЦЗО (CA Т...	GOV : 00000088	дійсний	2024-12-01	zareestrovano
<p>ПОДРОБИЦІ ГЕНЕРУВАТИ КЛЮЧ ГЕНЕРУВАТИ CSR ВІДКЛЮЧИТИ ВИДАЛИТИ ДОДАТИ ФАЙЛ ТОКЕНУ ІМПОРТ СЕРТИФІКАТУ</p>				

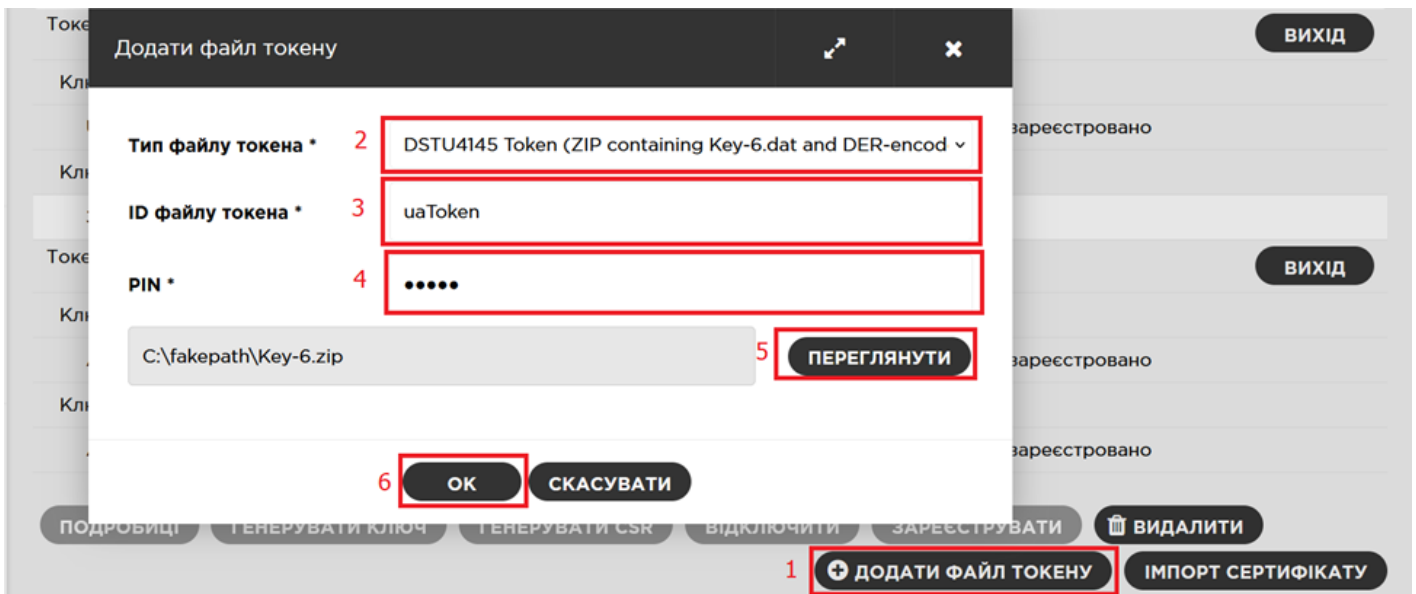
11. Додати нові файлові токени.

Примітка. Файлові токени використовуються в тестовому середовищі системи «Трембіта». Додавання файлових токенів здійснюється при ініціалізації ШБО або при необхідності заміни (перевипуску) особистого ключа.

Примітка. Перед додаванням токена необхідно 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 у найменуванні лише латинські літери та цифри, а файли сертифікатів повинні мати розширення *.CER.

Для того, щоб додати файловий токен необхідно:

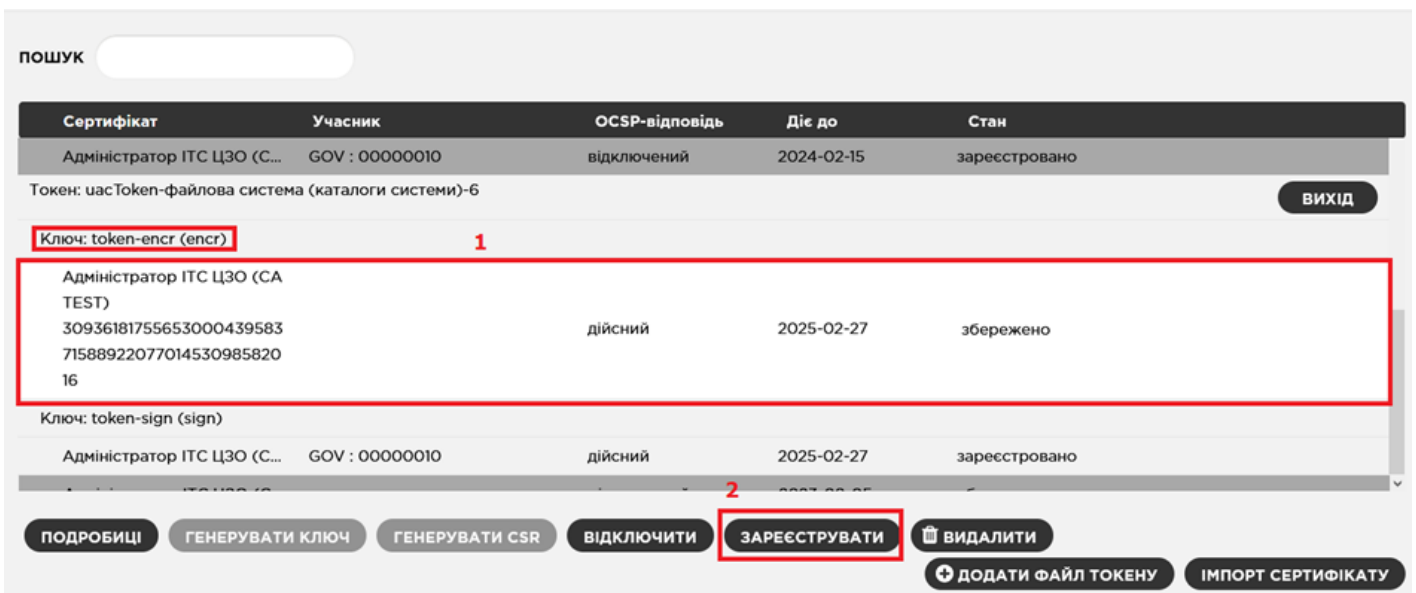
- Натиснути на кнопку «Додати файл токена» в нижній частині вікна.
- У діалоговому вікні «Додати файл токена» обрати значення параметру «Тип файлу токена» - DSTU4145 Token (ZIP containing Key-6.dat and DER-encoded certificates).
- У поле «ID файлу токена» ввести зрозумілий ідентифікатор, наприклад, uaToken.
- Натиснути на кнопку «Переглянути» та обрати з файлової системи робочої станції адміністратора 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».



Після виконання зазначених вище дій необхідно імпортувати ключі електронної печатки та шифрування на ШБО. Для цього треба натиснути на кнопку «Імпортувати» праворуч від доданих ключів.

12. Зареєструвати сертифікат шифрування.

Для реєстрації сертифікату шифрування необхідно виділити його (шляхом натискання на відповідний рядок під відповідним ключем з позначкою «encr», з числовим серійним номером) і натиснути на кнопку «Зареєструвати» в нижній частині вікна.



Після натискання на кнопку буде відображено повідомлення зеленого кольору про те, що запит надіслано успішно.

Після подачі заявки засобами ШБО, необхідно подати заявку на реєстрацію шлюзу безпечного обміну засобами Особистого кабінету Каталогу системи «Трембіта» (**Реєстрація ШБО в ядрі системи**). Порядок подання зазначеної заявки вказаний п. 7.3.4 Регламенту роботи системи «Трембіта».

Адміністратор системи «Трембіта» повинен обробити дану заявку та підтвердити запит. Коли запит на реєстрацію буде схвалено, статус сертифікату шифрування зміниться на «Зареєстровано».

13. Скасувати реєстрацію сертифікату шифрування. Для скасування реєстрації сертифікату шифрування необхідно виділити його (шляхом натискання) і натиснути на кнопку «Скасувати реєстрацію» в нижній частині вікна, після чого – натиснути на кнопку «Підтвердити» в наступному вікні.

пошук

Сертифікат	Учасник	OSCP- відповідь	Діє до	Стан	
Токен: softToken-0 ВИХІД					
Ключ: authKey1 (auth)					
UXP Class3 CA 376750702783673873		дійсний	2028-11-29	зареєстровано	
Токен: uasToken-файлова система (каталоги системи)-1 ВИХІД					
Ключ: UaToken1-encr (encr) 1					
Адміністратор ІТС ЦЗО (CA TEST) 30936181755653000439583715890784 3636409876545536		дійсний	2024-12-01	зареєстровано	
Ключ: UaToken1-sign (sign)					
Адміністратор ІТС ЦЗО (CA TEST) 3...		GOV : 00000088	дійсний	2024-12-01	зареєстровано
2					
ПОДРОБИЦІ ГЕНЕРУВАТИ КЛЮЧ ГЕНЕРУВАТИ CSR ВІДКЛЮЧИТИ СКАСУВАТИ РЕЄСТРАЦІЮ ВИДАЛИТИ + ДОДАТИ ФАЙЛ ТОКЕНУ ІМПОРТ СЕРТИФІКАТУ					

14. Відключити токени (або окремі сертифікати). Для того, щоб відключити токен або окремий сертифікат необхідно виділити його (шляхом натискання) та натиснути на кнопку «Відключити» в нижній частині вікна. Після цього в колонці «OSCP відповідь» навпроти цього токена або окремого сертифікату з'явиться позначка «Відключений».

Ключ: UaToken1-encr (encr) 1

Адміністратор ІТС ЦЗО (CA TEST) 30936181755653000439583715890784 43636409876545536		дійсний	2024-12-01	зареєстровано	
Ключ: UaToken1-sign (sign)					
Адміністратор ІТС ЦЗО (CA TEST) 3...		GOV : 00000088	відключений	2024-12-01	зареєстровано
2					
ПОДРОБИЦІ ГЕНЕРУВАТИ КЛЮЧ ГЕНЕРУВАТИ CSR ВІДКЛЮЧИТИ СКАСУВАТИ РЕЄСТРАЦІЮ ВИДАЛИТИ + ДОДАТИ ФАЙЛ ТОКЕНУ ІМПОРТ СЕРТИФІКАТУ					

Версія #3

Admin створив 2024-09-23 10:50:08 UTC

Admin оновив 2024-09-25 09:57:56 UTC