Рекомендації для налаштувань використання ЕЦП

Загальна рекомендація:

Якщо виникають в системі помилки, слід очистити кеш браузера, затиснувши Ctrl та натиснувши F5.

Кеш може зберігати застарілі дані, які впливають на роботу ЦС Майно негативним чином.

А) Помилка при пошуку сертифіката ("Сертифікат не знайдено")

Причини помилки:

Причина 1. Невірно встановлено параметри роботи програми.

Причина 2. Відсутні сертифікати користувача.

Причина 3. Відсутні сертифікати надавача ЕДП (центру сертифікації ключів).

Причина 4. Відсутні сертифікати ЦЗО (Центрального засвідчувального органу).

Причина 5. Особистий ключ було повторно перегенеровано вже після формування сертифіката (перезаписано на носієві ключа, а відповідно сертифіката для нового ключа не існує).



Для встановлення параметрів та перевірки наявності сертифікатів необхідно виконати наступні дії:

1) Натиснути у головному вікні програми пункт меню "Встановити параметри", або обрати підпункт "Встановити" у пункті меню "Параметри", або натиснути комбінацію

клавіш Ctrl+P.



2) Створити каталог для сертифікатів і СВС та вказати його у параметрах.



3) Скопіювати до каталогу сертифікати надавача ЕДП (ЦСК), ЦЗО, та власні, що відповідають особистому ключу.

Зробити це можна двома способами:

3.1) Вручну, завантаживши файл з сертифікатами всіх надавачів ЕДП (ЦСК) до

каталогу з сертифікатами. Також до цього каталогу необхідно скопіювати власні сертифікати користувача що відповідають особистому ключу.

3.2) Автоматично (Увага! Підтримують не всі надавачі (ЦСК)), за допомогою вибору підпункту "Отримати з ЦСК" пункту меню "Сертифікати та СВС".

😼 IT Користувач ЦСК-1					
ит Центр сертифікації ключів Користувач ЦСК					
🗧 Користувач ЦСК					
Файли 🕨	и Перевірити фа	йли			
Текст 🔸	собистому Перевірка підпису файлах	у на підписаних			
Особистий ключ		айли			
Сертифікати та СВС	Переглянути сертифікати F10	nis			
Лопомога	Переглянути СВС ГП	2			
(g=) перегляд сертич	Отримати з ЦСК	йловому			
фаиловому сл	Заблокувати власні сертифікати				
Встановити па Встановлення па	Скасувати власні сертифікати	ні запитами або			
користувача	Сформувати нові сертифікати	сертифікатів			
	L				
Допомога	Особистий ключ				
Про програму					
Перейти до web-сан	ту ЦСК				

4) Перевірити наявність необхідних сертифікатів у каталозі.

😨 IIT Користувач ЦСК-1		
Параметри роботи		
Файлове сховище	📃 Сертифікати та СВС	
Ргоху-сервер	Сертифікати та списн и відкликаних сертифікатів	
ТSP-сервер	Переглянути сертифікати Переглянути СВС	
ОСЅР-сервер		
LDAP-сервер		
р Сертифікати та СВС		
Ресстрація подій		
	ОК Відміна Застосувати	

Якщо помилка залишилась, необхідно перевірити відповідність особистого ключа, наявному сертифікату.

Для цього необхідно зчитати ключ за допомогою функції перевірки особистого ключа.

⊗ π ⊒	Користувач ЦСК-1 Параметри роботи Файлове сховище Ргоху-сервер ССУР-сервер LDAP-сервер CMP-сервер СМР-сервер СМР-сервер СМР-сервер СМР-сервер СМР-сервер Ресстрація подій	Собистий ключ Сообистий ключ Сообистий ключ Вкопортувати Веервне копіовання ч Змінити пароль захисту Зареестровані ноої особистого ключа Змінити список ч
		ОК Відміна Застосувати

Та співставити ідентифікатори відкритих ключів з особистого ключа та сертифіката.

🔜 IIT Користувач	4 UCK-1	_ □	х
	Особистий ключ	J	IJΤ
Параметри	📍 Особистий ключ	×	
₽₽₽	Поля інформації про ключ:		
Lange and the second	 Параметри особистих ключів Державний алгорити ЕЦП ДСТУ 4145-2002 Розміщення ключа Носій Довжина ключа 256 біт(а) Ідентичейкатор відкритого ключа 8D C4 FC D3 AF 1A 8C D2 24 71 DF B1 Протокол розподілу ключів Д-Ге гр. точок ЕК Розміщення ключа Чосій Деле тичейкатор відкритого ключа 2D 69 2A 89 A8 05 DD 7B B1 41 3C C2 	щити азмсту с	
Pe 🔞	Ідентифікатор відкритого ключа:		
	2D 69 2A 89 A8 05 DD 7B B1 41 3C C2 AF 18 67 C2 8D 4F AF 7C C2 DB A4 7D D0 3D E4 B5 CF DA 21 3E		
	Особисті та відкриті ключі належать до однієї ключової пари, якщо ідентифікатори А відкритих ключів у цьому вікні співпадають з ідентифікаторами відкритих ключів у відповідних сертифікатах		
	• Друкувати ОК		



Ідентифікатори повинні співпадати.

Б) Помилка при використанні апаратного ключа ЕЦП

В разі виникнення повідомлень (наприклад 65535), чи помилок, перед відкриттям діалогового вікна підпису (значок з жовтим ключем), слід очистити кеш браузера, затиснувши Ctrl та натиснувши F5.

Необхідно спробувати вибрати інший тип носія (варіант без суфіксу «носій»). На скріншоті, червоним виділено правильні варіанти, при використанні токену Автор.

ЕЦП				
Файловий ключ Апаратний ключ				
📀 Оберіть носій з ос. ключем				
Оберіть ЦСК:				
КНЕДП ТОВ "Центр сертифікації ключів	"Україна" 🗸 🗸			
Тип носія:				
гнучкий диск	~			
е.ключ IIT Кристал-1 (PKCS#11, віртуальний) е.ключ SafeNet iKey (PKCS#11, RSA) е.ключ чи смарт-карта Avest (PKCS#11) е.ключ Ефіт Kev (PKCS#11)				
е.ключ чи смарт-карта Автор (PKCS#11) е.ключ чи смарт-карта Автор 338 (PKCS#11) смарт-карта Техноконс. TEllipse3 (PKCS#11) е.ключ DBO Soft iToken (PKCS#11) криптомод. IIT Гряда-61 (PKCS#11, носій) е.ключ IIT Алмаз-1К (PKCS#11, носій) е.ключ Aladdin eToken (PKCS#11, носій) е.ключ Aladdin JaCarta ASE (PKCS#11, носій) е.ключ SafeNet iKey (PKCS#11, носій) е.ключ Eфit Key (PKCS#11, носій) е.ключ Eфit Key (PKCS#11, носій) е.ключ чи скарта Aladdin JaCarta (PKCS#11, носій) е.ключ чи скарта G&D SafeSign (PKCS#11, носій) е.ключ чи скарта Avest (PKCS#11, носій)				

Для усунення помилок при зчитуванні ключа в першу чергу слід:

- перевірити правильність введення паролю, а саме: регістр вводу паролю, мову клавіатури тощо (створений пароль може містити особливі символи);

- перевірити чи вірно обрано носій ключової інформації, наприклад, файловий (USB-flash, CD(DVD)-R(RW) тощо), захищений (Алмаз-1К, Кристал-1, Гряда-301, ID-картка тощо), SIM-карта;

- спробувати зчитати особистий ключ електронного підпису в іншому програмному забезпеченні.

Для підпису «в іншому програмному забезпеченні» можна спробувати електронний підпис на <u>https://czo.gov.ua/sign</u> або <u>https://id.gov.ua/sign</u>