Інструкція по генерації особистого ключа користувача

Крок 1

Запустіть програму «ІІТ Користувач ЦСК» і виберіть пункт меню «Особистий ключ» / «Згенерувати ключі».

🚑 IIT Kopı	стувач ЦСК-1	
Файли	Особистий ключ Сертифікати та СВС Параметри Допомога	
🔊 🗄	Зчитати Ctrl+K	ШТ
K K	Переглянути власний сертифікат	
05	Згенерувати ключі]
. 00	Сформувати запит на сертифікат (зовнішній)	
	Резервне копіювання особистого ключа	
, <u></u>	Змінити пароль захисту особистого ключа	
9	Знищити особистий ключ на носієві ключової інформації	
	Зтерти особистий ключ з пам'яті програми F12	
	Перегляд сертифікатів у файловому сховищі Сковищі	
Дода	атково	
0	Перейти до web-сайту ЦСК	

Крок 2

В цьому вікні залиште вибраним перемикач «для державних алгоритмів і протоколів» і натисніть кнопку «Далі».

рація ключів				
Генеривати к	ція ключів			
Для держа	івних алгоритмів і прот	околів		
🔘 для міжна	родних алгоритмів і про	отоколів		
🔘 для держа	вних та міжнародних а	лгоритмів і пр	ютоколів	
			Далі >	Відміна

Крок З

В цьому вікні обов'язково переконайтесь, що відмічено «Використовувати окремий ключ для протоколу розподілу» і натисніть кнопку «Далі».

Тип криптографічних алго	ритмів та протоколів:
ДСТУ 4145-2002 та дифо Використовувати окре	мий ключ для протоколу розподілу
Ключі ЕЦП:	Ключі протоколу розподілу:
з файлу параметрів	🔹 🗴 файлу параметрів 🔹
Місце розміщення параме	трів (каталог, з'ємний чи оптичний диск):
C:\Program Files\Institute o	f Informational Technologies\Certificate Au 👻 🗌 Змін

Крок 4

У вікні «Запис особистого ключа»:

1. Виберіть тип носія, який буде використовуватися як носій ключової інформації (з'ємній диск, оптичний диск і т. д.). Наприклад, якщо особистий ключ планується зберігати на USB флеш-диску, то вибирається тип «з'ємній диск».

2. Виберіть назву носія (літеру). Наприклад, якщо в комп'ютер вставлено два USB флешдиска, і вони мають літерні позначення «G:\» і «H:\», то необхідно вказати той, на який потрібно записати ключ.

🔄 гнучкий диск		👝 Інформація про носій
👝 з'ємний диск		
- F:\		
🛃 оптичний диск		Harry EA
📾 е.ключ IIT Алмаз-1К		
е.ключ IIT Алмаз-1К (носій)	Ξ	Перезаписуємий, не потребує
е.ключ IIT Кристал-1		автентифікаці
💷 е.ключ IIT Кристал-1 (носій)		
🐙 файлова система (каталоги системи)		
🐙 файлова система (каталоги користувача)		
🦏 е.ключ Aladdin eToken (PKCS#11)		
🐙 е.ключ чи смарт-карта Автор (PKCS#11 носій)	
www.e.ключчи.c.карта G&D SafeSign (PKCS#11)		
www.e.ключ SafeNet iKey (PKCS#11 носій)	-	📀 Поновити
We a know when kapita (laddin lat ada (RK) STITT)		
ароль:	EN	
овтор:		

3. В полі «Пароль» введіть пароль для захисту особистого ключа. Пароль повинен задовольняти наступним вимогам:

- довжина пароля повинна бути не менше ніж 8 символів;
- символи повторюватися не повинні;
- не можна використовувати поспіль більше двох символів з розкладки клавіатури (по горизонталі);
- дозволені символи: «а» «z» , «А» «Z» , «0» «9» , «+» , «-».
- Наприклад, пароль «werobhfz8» не задовольняє вищевказаним вимогам.

4. В полі «Повтор» повторіть введений пароль для перевірки правильності попереднього введення.

5. Натисніть кнопку «Записати». Далі буде сгенеровано особистий ключ і записано його на носій. У разі виникнення будь-яких проблем, перевірте правильність вибору типу носія, його назви, пароля захисту особистого ключа.

Крок 5

Якщо складність пароля захисту особистого ключа не задовольняє вимогам, буде виданого відповідне попередження.

Щоб змінити пароль на складніший натисніть на кнопку «Ні», щоб використовувати введений пароль, натисніть на кнопку «Так».

Повідомл	ення оператору	23
<u>^</u>	Введений пароль доступу до носія ключової інформації не задовільняє вимогам. Пароль містить підряд більше ніж 2 символи з розкладинки клавіатури. Використати його?	
	Да Нет	

Крок 6

Якщо на вибраному носії вже є записаний особистий ключ (файли Key-6.dat та Key-11.dat) то буде показано вікно з попередженням.

Вставте інший носій або скопіюйте існуючі файли ключа і натисніть кнопку «Так».

Повідомле	ння оператору
<u> </u>	На носієві ключової інформації вже є особистий ключ. Перезаписати його?
	Да <u>Н</u> ет

Крок 7

У вікні «Запитів на формування сертифіката з відкритим ключем ЕЦП» відображається інформацію, що міститься у файлі-запиті на сертифікат ЕЦП (електронної печатки).

оля запиту: Реквізити заявника відсутні	
Додаткові дані відсутні	
🛱 Тип заявника	Не вказаний
Строк чинності сертифіката ві	
Строк дії особистого ключа ві	
Параметри відкритого ключа	
Тип ключа	ДСТУ 4145-2002
Довжина ключа	264 біт(а)
Відкритий <mark>к</mark> люч	13 68 F5 4B 5C A7 EF FB 82 3B AB 5A
Ідентифікатор відкритого ключа	EA 94 50 98 D7 C4 99 6A F2 0F 4B AE
Уточнене призначення ключів	
Запит самопідписаний	

Крок 8

У вікні «Запитів на формування сертифіката з відкритим ключем протоколу розподілу» відображається інформацію, що міститься у файлі-запиті на сертифікат шифрування.

Запит на формувани	ня сертифіката	
Толя запиту:		
🛱 Реквізити заявника відсутні		
🔄 Додаткові дані відсутні		
🔄 Тип заявника	Не вказаний	
Строк чинності сертифіката ві		
Строк дії особистого ключа ві		
🖕 Параметри відкритого ключа		
Тип ключа	ДСТУ 4145-2002	
Довжина ключа	432 біт(а)	
Відкритий ключ	16 53 29 75 04 4E 3C 1E C0 61 E7 DC	
Ідентифікатор відкритого ключа	70 CD BB 89 51 9A 87 84 BF DE 4F AD	
🔄 Уточнене призначення ключів		
🛱 Запит самопідлисаний		
22.5		
Друкувати	HO I	<

Крок 9

Виберіть опцію «Зберегти у файл» і натисніть кнопку «Далі».



Крок 10

Далі необхідно вказати каталог для збереження і назви файлів запитів на формування сертифікатів.

Файли запитів мають розширення р10.

Щоб змінити каталог для запису файлу натисніть кнопку «Змінити».

грація ключів	
Запити на формування сертифік	атів
C:\My Certificates and CRLs 13\EU-A1449CDE.p10	Змінити
м'я файлу для запису запиту з відкритим ключем протоколу р	озподілу:
C:\My Certificates and CRLs 13\EU-KEP-C2DB2FC4.p10	Змінити

Ім'я для файлу-запиту бажано задавати наступним чином:

- для запиту з відкритим ключем ЕЦП у форматі
- *ЕU-ЄДРПОУ-Прізвище.р10,* наприклад:
- EU-12345678-Петренко.р10
- для запиту з відкритим ключем протоколу розподілу у форматі
- ЕU-КЕР-ЄДРПОУ-Прізвище.p10, наприклад:
- EU-KEP-12345678-Петренко.p10

м я фаилу для запису запиту з C:\My Certificates and CRLs 13\E	ЕЦ-12345678-Петренко.р10	Змінит
м'я файлу для запису запиту з	Відкритим ключем протоколу розпо	ninv:
C:\Mv Certificates and CRLs 13\	EU-KEP-12345678-Петренкоlp10	Змінит

Після того, як ви вказали каталог та імена файлів, натисніть кнопку «Далі».

Крок 11.

Щоб завершити процес генерації нового ключа, натисніть кнопку «Завершити».

Генерація ключів	
Генерацію ключів завершено	
	Завершити

Отримані файли-запити на формування сертифікатів збережіть на окремий з'ємний носій (USB флеш-диск, оптичний диск) для передачі до ЦСК ТОВ «КС» (в найближчий до Вас пункт реєстрації).