## Інструкція по налаштуванню накладання КЕП з використанням апаратних носіїв для зберігання ключів

1. Завантажте файл з сертифікатами акредитованих центрів сертифікації ключів за посиланням: <u>https://ca.informjust.ua/download/Soft/CACertificates.p7b</u>. За потреби скопіюйте посилання у браузер та перейдіть за ним.

2. Створіть на диску С:\ папку з назвою «Cert» та скопіюйте туди файл з сертифікатами, що був завантажений у попередньому пункті.

Папка C:\Cert з файлом сертифікатів матиме наступний вигляд:

1200.00092			
> Этс	от компьютер 🔸 Локальный д	иск (C:) > cert	
	АМИ	Дата изменения Тип	Размер
* * * *	CACertificates	12.12.2018 12:31 Сертификаты	РКС 271 КБ
E_201			

3. Завантажте та встановіть агент підпису за посиланням: <u>http://iit.com.ua/download/productfiles/EUSignWebInstall.exe</u>.

На операційних системах Windows 7 та вище встановлювати програмне забезпечення потрібно від імені адміністратора системи.

4. Запустіть «**IIT Користувач ЦСК-1.3. Агент підпису**» та натисніть кнопку «Зупинити»:



5. Для налаштування параметрів натисніть кнопку «Встановити»:

🛃 IIT Користувач ЦСК-1. Управління агентом підпису	×
Користувач ЦСК Управління агентом підпису	"
Стан	Запустити
лараметри россти	Встановити

6. На вкладці «Агент підпису» додайте у довірені веб-сайти адреси ЄДЕБО (<u>http://www.edbo.gov.ua</u>) та тестової ЄДЕБО (<u>http://www.edbo.gov.ua</u>:9090).

Після цього натисніть кнопку «Застосувати»:

Криптографічна бібліотека	Параметри запуску НТТР-порт: 8081 НТТР(S)-порт: 8083 Запускати процес автоматично (додати в авто Довірені web-сайти	запуск)	Полати
	Web-сайт       ×         Довірений web-сайт         URL-адреса web-сайту:         http://www.edbo.gov.ua		Змінити Видалити
	ОК Відміна	Certificate Authority- Експортувати	1.3\End User\S Переглянути

7. На вкладці «**Криптографічна бібліотека**», оберіть «*фіксовані параметри»* та натисніть кнопку «**Встановити**»:

Параметри роботи	X
Агент підлису	🔊 Криптографічна бібліотека
Криптографічна бібліотека	Параметри криптографічної бібліотеки Параметри носія ключової інформації О запитувати у оператора
	<ul> <li>Фіксовані параметри</li> <li>Відображати повідомлення оператору</li> <li>Фіксовані параметри носія ключової інформації:</li> </ul>
	Встановити Перевірити

8. На вкладці «Файлове сховище» вкажіть «Каталог з сертифікатами та СВС», натиснувши кнопку «Змінити», - папку С:\Cert, яку створили у п.1:

	Каталог з сертифікатами та СВС	X	пифікатів та
Ргоху-сервер ТSP-сервер	Каталог з сертифікатами та СВС		
ОСЅР-сервер	> 📓 Видео > 🚊 Документы	^	н
СМР-сервер	<ul> <li>Загрузки</li> <li>Шображения</li> <li>Музыка</li> </ul>		, с: 3600
Особистий ключ	<ul> <li>Э Объемные объекты</li> <li>Рабочий стол</li> </ul>		
Реєстрація подій	<ul> <li>Докальный диск (С:)</li> <li>cert</li> </ul>	Ŷ	

Якщо для доступу до ІНТЕРНЕТ у вашій локальній мережі використовується 9. ПРОКСІ-СЕРВЕР, оберіть вкладку «**Proxy-сервер**» та вкажіть параметри підключення. В іншому випадку – перейдіть до наступного пункту.

Параметри роботи		×
🔎 Файлове сховище	<b></b> Ргоху-сервер	]
Ргоху-сервер	Підключатися через ргоху-сервер	
5 ТSP-сервер		
ССSР-сервер		
LDAP-сервер		
Ф СМР-сервер		
🧖 Особистий ключ		
📻 Сертифікати та СВС		
🔞 Реєстрація подій		
	ОК Відміна Застосувати	И

На вкладках «OCSP-сервер» та «СМР-сервер» зніміть позначки 10.

Параметри роботи		Х
Файлове сховище	📙 ОСЅР-сервер ЦСК	
Ргоху-сервер	на використовувати OCSP-сервер	
5 ТSP-сервер		
ОСЅР-сервер		
LDAP-сервер		
СМР-сервер		
🍂 Особистий ключ		
сертифікати та СВС		
Реєстрація подій		
	ОК Відміна Застосує	зати

«Використовувати ОСЅР-сервер» та «Використовувати СМР-сервер»:

Параметри роботи	×	
Файлове сховище	📮 СМР-сервер ЦСК	
Ргоху-сервер	Використовувати СМР-сервер	
TSP-сервер		
ОСЅР-сервер		
LDAP-сервер		
СМР-сервер		
🧖 Особистий ключ		
Сертифікати та СВС		
🛚 Реєстрація подій		
	ОК Відміна Застосувати	

метри роботи Файлове сховище	• Файлове сховище сертифікатів та
	CBC
ТSP-сервер ОСSP-сервер LDAP-сервер СМР-сервер Особистий ключ Сертифікати та СВС Реестрація подій	Каталог з сертифікатами та СВС: С:\cett Автоматично перечитувати при виявленні змін Зберігати сертифікати, що отримані з ОСЅР-, LDAP- чи СМР-серверії Час зберігання стану перевіреного сертифіката, с: 3600 Перевіряти СВС

12. Встановіть в USB-порт комп'ютера апаратний носій з КЕП та натисніть «Встановити»:

Агент підпису	Криптографічна бібліотека
Криптографічна бібліотека	Параметри криптографічної бібліотеки Встановити Параметри носія ключової інформації Э запитувати у оператора Фіксовані параметри Рісовані параметри носія ключової інформації: Не встановлені Встановити Перевірити
	ОК Відміна Застосувати

У наступному вікні оберіть тип носія КЕП, сам носій (*автоматично вказується його номер, на скріншоті вказані дані ПРИКЛАДУ*), введіть пароль та натисніть «Зчитати» (або «Ок»):

С ГНУЧ	Встановіть носій ключової інформації чи г иодуль та вкажіть параметри чкий диск аний лиск	ідключіть криптографічний
опт сма сма екл екл екл екл екл екл екл екл екл рай По-к	ичний диск арт-карта Автор (318) арт-карта BIFIT Integra 1.0 люч BIFIT iToken пюч IIT Алмаз-1К 001314 пюч IIT Алмаз-1К (носій) пюч IIT Кристал-1 пюч IIT Кристал-1 пюч IIT Кристал-1 (носій) апова система (каталоги системи) апова система (каталоги користувача) сарта громадянина (БЕН) птомод. IIT Гряда-61 (PKCS#11)	Тип: е.ключ IIT Алмаз-1К Назва: 001314 Перезаписуемий, потребує автентифікації, тільки повна очистка, електронний ключ, апаратний ГВП Апаратний криптомодуль
ре.кл ре.кл ре.кл ре.кл	пюч IIT Алмаз-1К (PKCS#11) пюч IIT Кристал-1 (PKCS#11) птомодуль IIT Гряда-301 (PKCS#11) пюч IIT Алмаз-1К (PKCS#11, віртуальний)	<ul> <li>Поновити</li> <li>Ключ у файлі (на диску)</li> </ul>
роль:	••••••	

13. Якщо все вірно обрано та введено, будуть відображені «*Фіксовані параметри носія ключової інформації*». Для перевірки підпису натисніть кнопку «Перевірити»:

🙀 Криптографічна бібліотека	Криптографічна бібліотека	
	Параметри криптографічної оіоліотеки Параметри носія ключової інформації ○ запитувати у оператора ● фіксовані параметри ⊡ Відображати повідомлення оператору Фіксовані параметри носія ключової інформації: Тип носія: е.ключ IIT Алмаз-1К, назва носія: 001314 Встановити	Перевірити



Програма запропонує завантажити власний сертифікат. Натисніть «Да»:

Повідоі	илення оператору	×	
?	Завантажити власний сертифікат з СМР-с	сервера ЦСК?	тан
	Да	Нет	

15. У наступному вікні оберіть ЦСК, в якому отримано ключ підпису (*якщо у переліку* <u>декілька</u> записів щодо СМР-сервера, оберіть <u>перший</u> запис) та натисніть «**ОК**»:

Сертифікат СМР-сервера ЦСК Пошук за власни Килькість: 47		иком:	
3ласник 🔻	ЦСК	Серійний номер	Т
СМР-сервер АЦСК органів юстиції У	АЦСК органів юстиції України	1A15A67BC8E82F4C02000000100000A5BB00	Е
СМР-сервер АЦСК органів юстиції У	АЦСК органів юстиції України	1A15A67BC8E82F4C020000001000000A4BB00	Д
СМР-сервер АЦСК органів юстиції У	АЦСК органів юстиції України	12A1C72050EC6854020000001000002F910B00	Д
СМР-сервер АЦСК ринку електричн	АЦСК ринку електричної енергії	27F0CA960A257595020000001000000CB060000	Д
СМР-сервер АЦСК ринку електричн	АЦСК ринку електричної енергії	56C8165F7646BB26020000001000000F000000	Д
СМР-сервер АЦСК ринку електричн	АЦСК ринку електричної енергії	56C8165F7646BB26020000001000000E000000	Д
СМР-сервер АЦСК ринку електричн	АЦСК ринку електричної енергії	27F0CA960A257595020000001000000CA060000	Д
СМР-сервер Акредитований центр с	Акредитований центр сертифікації кли	2084E4ED0D30998C02000000100000060000	Д
СМР-сервер Акредитований центр с	Акредитований центр сертифікації	33B6CB7BF721B9CE020000002000003CB93	Д
СМР-сервер Акредитований центр с	Акредитований центр сертифікації	33B6CB7BF721B9CE020000002000003DB93	Д
СМР-сервер Акредитований центр с	Акредитований центр сертифікації	20B4E4ED0D30998C020000001000000050000	Д
СМР-сервер Акредитований центр с	Акредитований центр сертифікації	3EEE524F3BA9E8BB0200000020000089960F	L
СМР-сервер Акредитований центр с	Акредитований центр сертифікації	3EEE524F3BA9E8BB0200000020000088960F	L
СМР-сервер Акредитований центр с	Акредитований центр сертифікації	5FA2C5F8F37805D902000000200000E1DF04	Д
СМР-сервер Акредитований центр с	Акредитований центр сертифікації	5FA2C5F8F37805D902000000200000E0DF04	L
ЦСК. Служба СМР	Акредитований центр сертифікації	C397	Д
			>

16. У разі успішного завантаження сертифіката з сервера з'явиться повідомлення з пропозицією щодо імпортування сертифіката до файлового сховища. Натисніть «Да»:



17. Після імпортування з'являється наступне вікно з даними сертифіката. Перевірте дані та натисніть «Ок»:

ертифікат		×
📄 Сертиф	ыкат	
ЦCK:	Акредитований центр сертифікації ключів ІДД ДФС	
Користувач:		
Дійсний:	з 11.05.2018 до 11.05.2020	
Реєстраційний номер:	20B4E4ED0D30998C04000000	
Використання ключів:	ЕЦП, Неспростовність у державних алгоритмах і протоколах	
<ul> <li>Детальна інфо</li> <li>Наступний сер</li> </ul>	рмація ртифікат	
	ОК	

18. Після здійснення усіх необхідних налаштувань та перевірки підпису запустіть агент підпису для можливості <u>використання апаратного носія для накладання КЕП</u> в ЄДЕБО:

🛒 IIT Користувач ЦСК-1. Управління агентом підпису	×
Користувач ЦСК Управління агентом підпису	117
Стан	Запустити Встановити

У разі потреби у <u>додатковому налаштуванні</u> натисніть кнопку «**Зупинити**» та виконайте необхідні дії.

19. Для використання **КЕП на захищених носіях** (*наприклад*, *«Алмаз», «Кристал»*) у відповідних модулях ЄДЕБО, у вікні підпису встановіть позначку **«Використовувати** апаратний носій ключової інформації», оберіть необхідні параметри носія та натисніть **«Прийняти»**:

іс відповідальної особи	
Центр сертифікації, який видав ключ	
Акредитовании центр сертифікації ключів ІДД ДФС	•
Використовувати апаратний носій ключової інформації	
Тип носія	
е.ключ IIT Алмаз-1К	•
Носій	
002718	•
Пароль особистого ключа підпису	
£	
прийнати	ВИЛИН