Центр сертифікації ключів Державне підприємство «Українські спеціальні системи»

Інструкція з налаштування системи, генерації ключів та формування сертифікатів відкритих ключів

ДСТУ 4145-2002 ПБ eПідпис

Версія 1/2012

Ісмагілов Артур Ільясович

Digitally signed by Ісмагілов Артур Ільясович
DN: cn=Ісмагілов Артур Ільясович, o=ДП "УСС", ou=ДП "УСС", email=a.ismagilov@uss.gov.ua
Reason: Я одобряю данный документ
Location: м. Київ, вул. Мельникова , 83 Б
Date: 2012.10.05 09:47:45 +03'00'

Москаленко Ксенія Михайлівна

Digitally signed by Москаленко Ксенія Михайлівна
DN: cn=Москаленко Ксенія Михайлівна, ou=Main office, email=k.moskalenko@uss.gov.ua
Reason: Я выполнил рецензирование данного документа
Location: м. Київ, вул. Мельникова , 83 Б
Date: 2012.10.05 09:46:34 +03'00'

Глущенко Євген Олександрович

Digitally signed by Глущенко Євген Олександрович
DN: cn=Глущенко Євген Олександрович, ou=Main office, email=e.gluschenko@uss.gov.ua
Reason: Я автор документа
Location: м. Київ, вул. Мельникова , 83 Б
Date: 2012.10.05 09:45:59 +03'00'

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ *3*
ВСТУП *4*
МІНІМАЛЬНІ ТЕХНІЧНІ ВИМОГИ ДО СИСТЕМИ *4*
СУМІСНІСТЬ З ОПЕРАЦІЙНИМИ СИСТЕМАМИ *4*
НАЛАШТУВАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ *4*
Встановлення криптопровайдера **4**
Встановлення кореневих сертифікатів **8**
Налаштування браузера Internet Explorer **19**
Перевірка готовності системи **21**
ГЕНЕРАЦІЯ КЛЮЧОВОЇ ПАРИ ТА ОТРИМАННЯ СЕРТИФІКАТІВ *26*
Заміна стартового пароля **26**
Формування запиту на сертифікацію та одержання сертифікатів **29**
ПЕРЕВІРКА НАЯВНОСТІ КЛЮЧІВ ТА СЕРТИФІКАТІВ *31*
СТВОРЕННЯ РЕЗЕРВНОЇ КОПІЇ *33*

ПЕРЕЛІК СКОРОЧЕНЬ

IE	Internet Explorer
ЕЦП	Електронний цифровий підпис
КЗІ	Криптографічний захист інформації
ОС	Операційна система
ПК	Персональний комп’ютер
ПЗ	Програмне забезпечення
Криптопровайдер	Програмний виріб криптографічного захисту інформації “Криптографічний сервіс-провайдер “ЦСК-CSP”
ЦЗО	Центральний засвідчувальний орган
ЦСК	Акредитований центр сертифікації ключів Державного підприємства “Українські спеціальні системи”

ВСТУП

Даний документ містить опис послідовності дій користувача/заявника по налаштуванню персонального комп'ютера з метою подальшого використання/накладання ЕЦП, а також послідовність дій з генерації ключів та формування сертифікатів відкритих ключів на власному робочому місці.

МІНІМАЛЬНІ ТЕХНІЧНІ ВИМОГИ ДО СИСТЕМИ

Pentium 400 MHz, 128 MB RAM, 4000 MB hard disk space, Internet.

СУМІСНІСТЬ З ОПЕРАЦІЙНИМИ СИСТЕМАМИ

32-бітні ОС: Windows 2003/2008/XP/7 з наявним Internet Explorer 6 та вище (гарантовано)

64-бітні ОС: Windows 2008/7 з наявним Internet Explorer 6 та вище (гарантовано)

НАЛАШТУВАННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ

З метою успішного налаштування персонального комп'ютера та подальшої роботи з сертифікатами ЕЦП та КЗІ (далі – Сертифікати) необхідно:

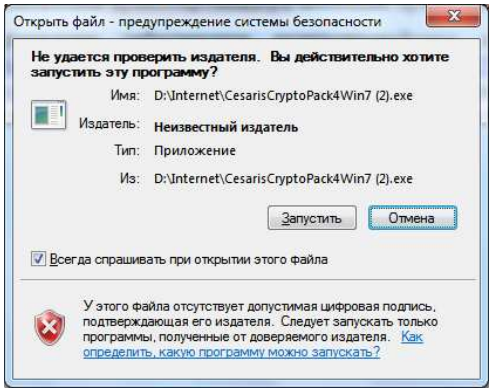
1. Встановити криптопровайдер для роботи з ключами та сертифікатами відкритих ключів за вітчизняними криптографічними алгоритмами.
2. Встановити кореневий сертифікат Центрального засвідчувального органу (далі – ЦЗО) та Акредитованого центру сертифікації ключів Державного підприємства «Українські спеціальні системи» (далі – ЦСК).
3. Налаштувати браузер IE.
4. Перевірити готовність системи.

Встановлення криптопровайдера

Примітка: Для встановлення криптопровайдера необхідні права адміністратора системи.

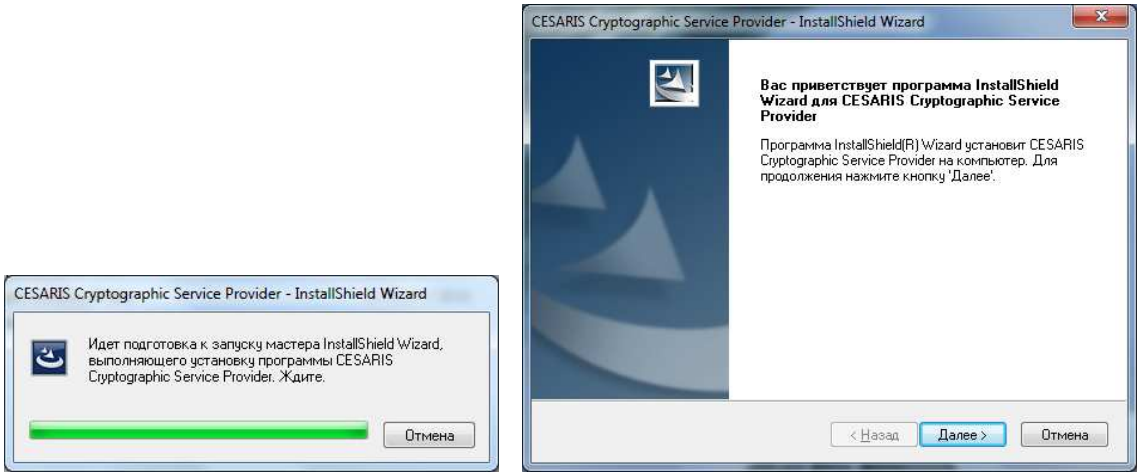
Завантажте програмне забезпечення криптопровайдера за прямим посиланням: http://acsk.uss.gov.ua/download/CSP/CSP4Win7/CesarisCryptoPack4Win7.exe або зі сторінки http://acsk.uss.gov.ua/software.htm та запустіть інсталяційний файл «CesarisCryptoPack4Win7.exe». Зверніть увагу на те, що у разі виникнення вікна «Предупреждение системы безопасности» необхідно натиснути кнопку «Запустить».

Примітка: В залежності від налаштування Вашої операційної системи вікно «Предупреждение системы безопасности» може не з'являтися.



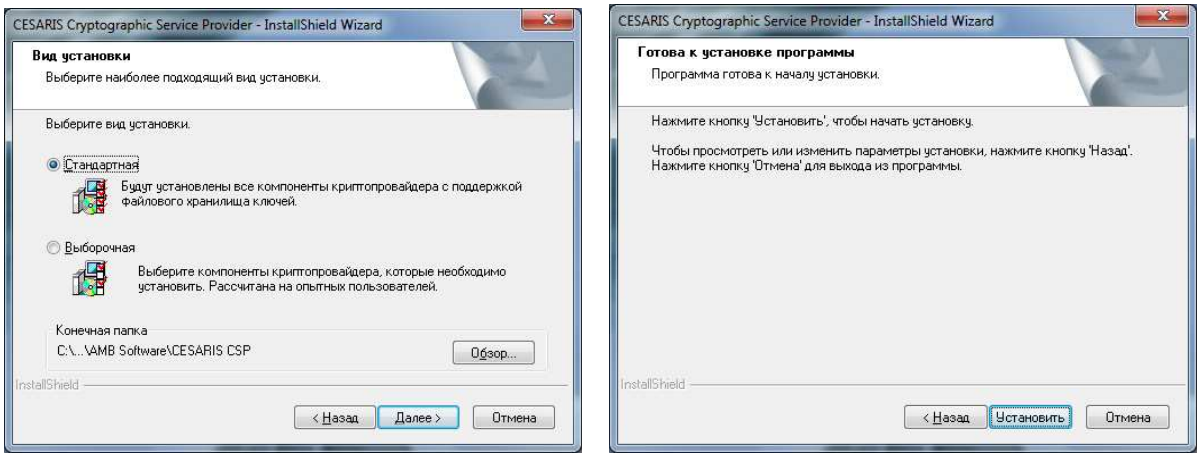
Пор. № зміни	Підпис відпов. особи	Дата внесення

Дочекайтеся завершення підготовки до інсталяції/встановлення програмного забезпечення та натисніть кнопку «Далее ».

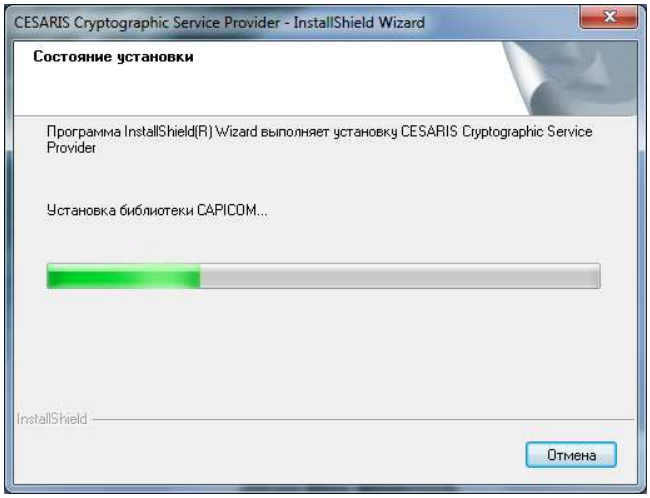


Оберіть вид встановлення програмного забезпечення «Стандартная» та натисніть кнопку «Далее», а у наступному вікні, яке з’явилося, натисніть кнопку «Установить».

Примітка: Ви маєте можливість обрати каталог для встановлення програми шляхом натискання на кнопку «Обзор», але **рекомендовано** використовувати каталог за замовчуванням (обраний самостійно програмним забезпеченням).

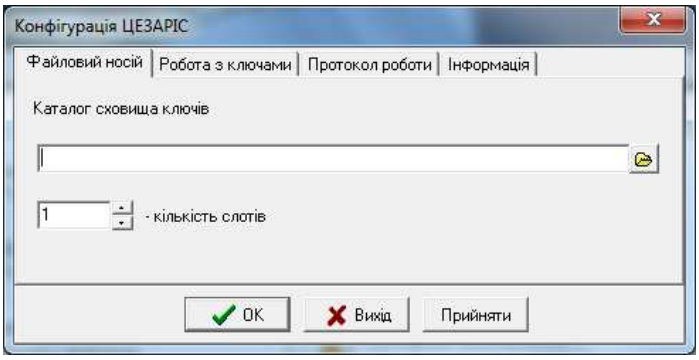


Дочекайтеся завершення процесу інсталяції (встановлення) програми.



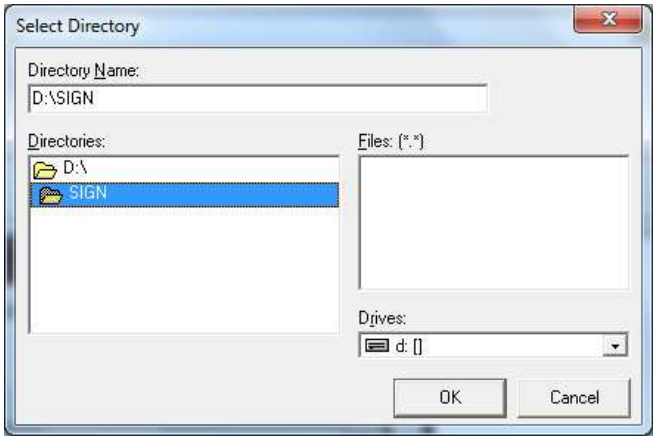
Приберіть прапорець «создать файловый носитель» та натисніть кнопку «Готово».

У вікні «Конфігурація ЦЕЗАРІС», натисніть на іконку  , для вибору місця розташування файлового токену.



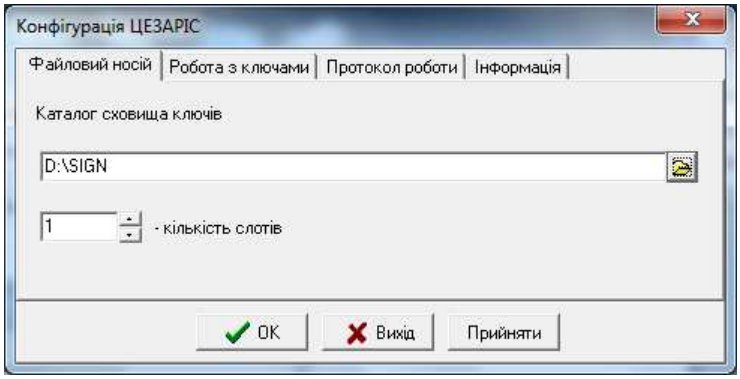
Рекомендовано створити каталог SIGN на локальному диску D:\ та обрати цей каталог через іконку  (Приклад: D:\SIGN). Для користувачів «тонких клієнтів» та користувачів, у яких відсутній локальний диск D:\, папку SIGN рекомендовано створити в папці «Мои документы» (Наприклад: C:\Users\Ivanov\SIGN).

<u>Примітка</u>: Назви та шляхи до папок рекомендовані, але Ви можете самостійно обрати папки та їх назви, зручні для Вас та вашої інфраструктури.



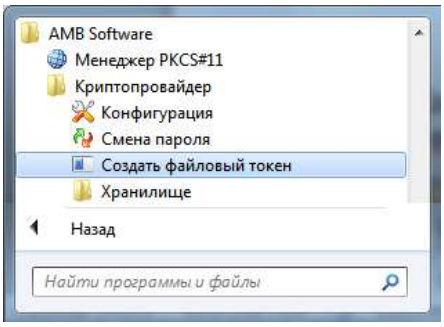
Пор. № зміни	Підпис відпов. особи	Дата внесення

Необхідно натиснути кнопку «Прийняти» та кнопку «ОК».



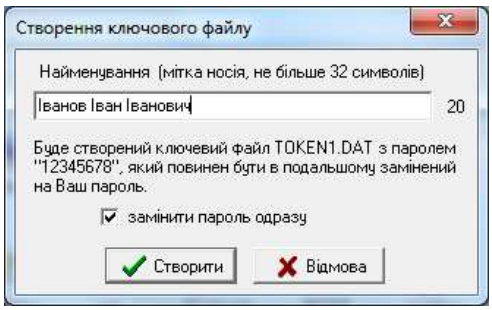
Програмне забезпечення криптопровайдера успішно встановлено. Натисніть «Готово».

Далі пройдіть по ланцюжку «Пуск» → «Все программы» → «AMB Software» → «Криптопровайдер» → «Создать файловый токен».



У вікні «Створення ключового файлу» введіть бажане ім’я для файлового токену (бажано латиницею) та натисніть кнопку «Создать»

Примітка: Пташка «Замінити пароль одразу» повинна бути обов’язково встановлена.

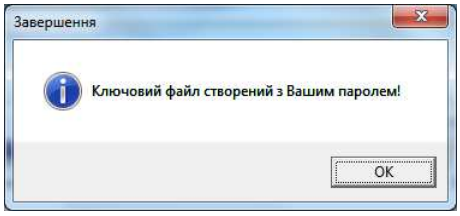


Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

У вікні «Введіть новий PIN» введіть та підтвердіть пароль, яким Ви будете користуватись при накладанні електронного цифрового підпису (довжина паролю повинен бути не менше 8 символів і пароль не повинен містити повтори двох і більше символів підряд) та натиснути кнопку «ОК».

Примітка: У разі, якщо введений Вами пароль не відповідає вимогам безпеки, програма видасть Вам відповідне повідомлення, і Вам необхідно буде ввести більш складний пароль, який буде відповідати вимогам безпеки щодо паролів.

У разі успішного введення пароля, який відповідає вимогам безпеки з’явиться повідомлення про успішне створення файлового токену, Вам необхідно натиснути кнопку «ОК».



Примітка: Пароль, який був введений Вами у подальшому, буде Вами використовуватися в процесі накладання Вашого власного електронного цифрового підпису (підписання електронних документів), який у відповідності до законодавства України прирівнюється до Вашого власноручного підпису. У зв’язку з викладеним вище, застерігаємо не розголошувати та не передавати пароль третім особам, а також рекомендуємо не забувати цей пароль. Звертаємо Вашу увагу на те, що пароль, який Ви ввели, невідомий співробітникам Державного підприємства «Українські спеціальні системи» та у разі, якщо Вами буде його втрачено, сприяти його відновленню співробітники Державного підприємства «Українські спеціальні системи» не мають можливості.

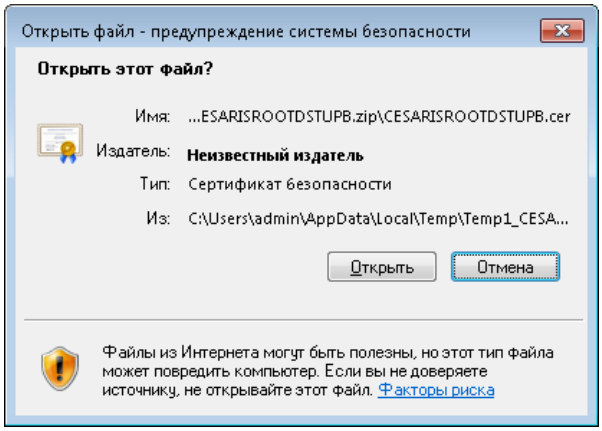
Встановлення кореневих сертифікатів

Встановлення кореневого сертифікату ЦСК

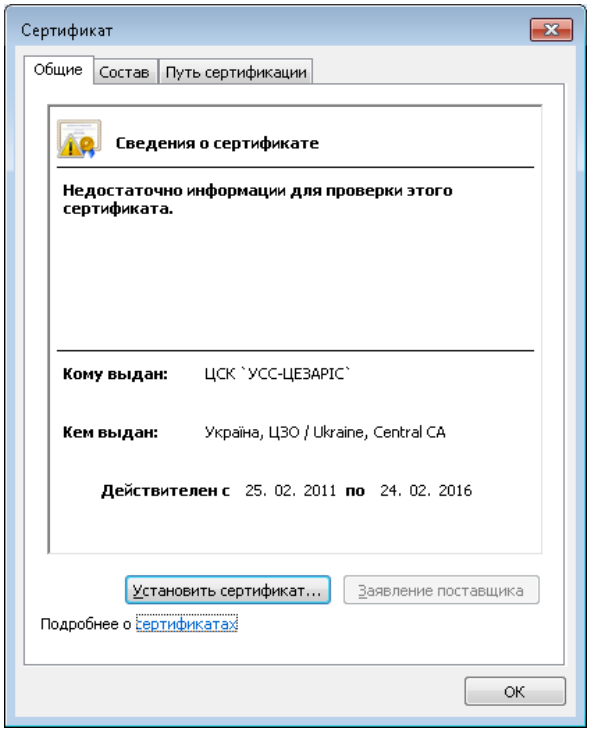
Завантажте кореневий сертифікат ЦСК за прямим посиланням: http://acsk.uss.gov.ua/download/rootcer/CESARISROOTDSTUPB.zip або зі сторінки http://acsk.uss.gov.ua/rootcertificate.htm (в таблиці «КОРЕНЕВІ СЕРИФІКАТИ ЦСК "УСС-ЦЕЗАРИС" під другим номером). Розпакуйте завантажений архів та запустіть файл **CESARISROOTDSTUPB.cer** шляхом подвійного натиснення лівої кнопки миші або виділення його і натиснення кнопки «Enter».

Звертаємо Вашу увагу на те, що у разі виникнення вікна «Предупреждение системы безопасности» необхідно натиснути кнопку «Открыть».

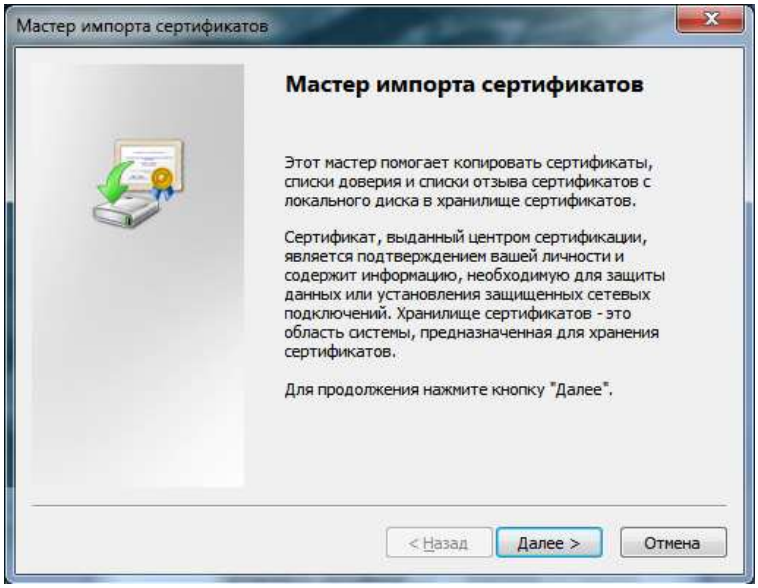
Примітка: В залежності від налаштування Вашої операційної системи вікно «Предупреждение системы безопасности» може не з’являтися.



З’явиться вікно сертифікату відкритого ключа ЦСК, де Вам необхідно натисніть кнопку «Установить сертификат».

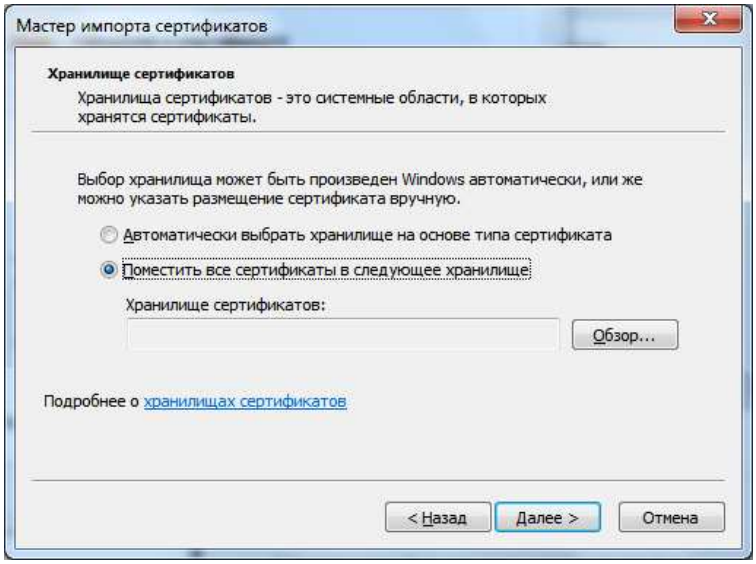


Відкриється вікно «Мастер импорта сертификатов», натисніть кнопку «Далее ».

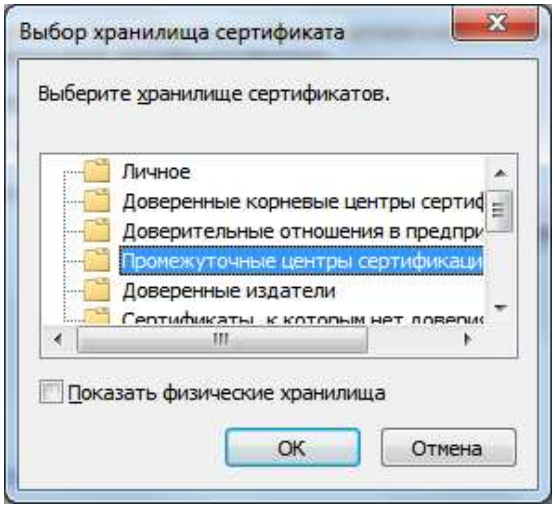


Пор. № зміни	Підпис відпов. особи	Дата внесення

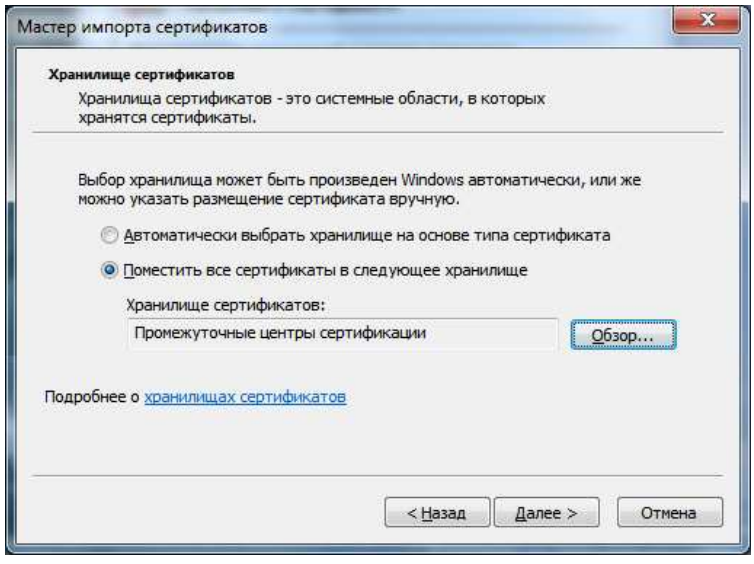
У вікні, яке відкрилося, відмітьте пункт «Поместить все сертификаты в следующее хранилище» и натисніть кнопку «Обзор…».



У вікні «Выбор хранилища сертификата» оберіть «Промежуточные центры сертификации» шляхом одноразового натиснення на цьому пункті лівою кнопкою миші та натисніть кнопку «ОК». Вікно «Выбор хранилища сертификата» закриється.

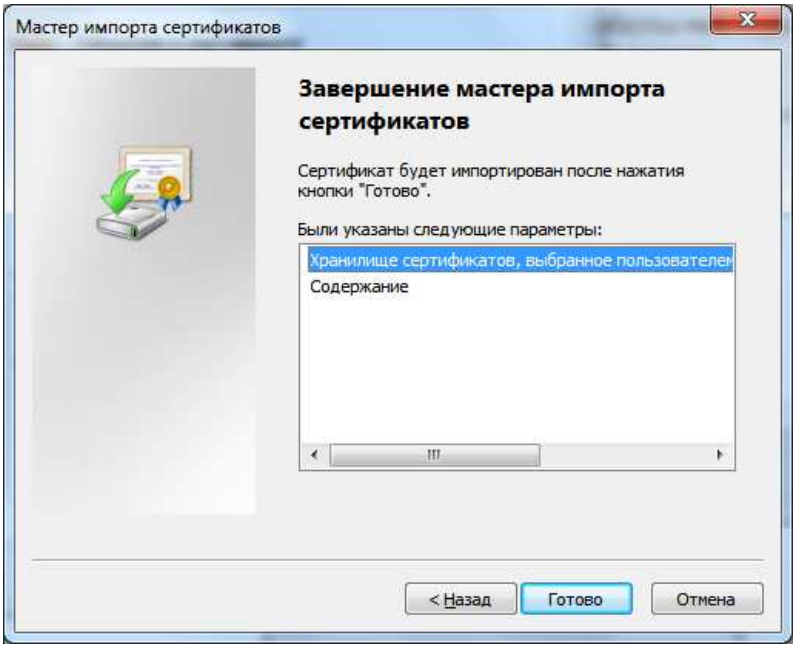


У вікні «Мастер импорта сертификатов» натисніть кнопку «Далее ».

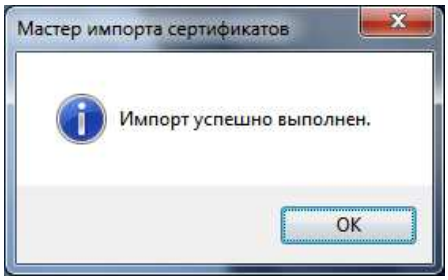


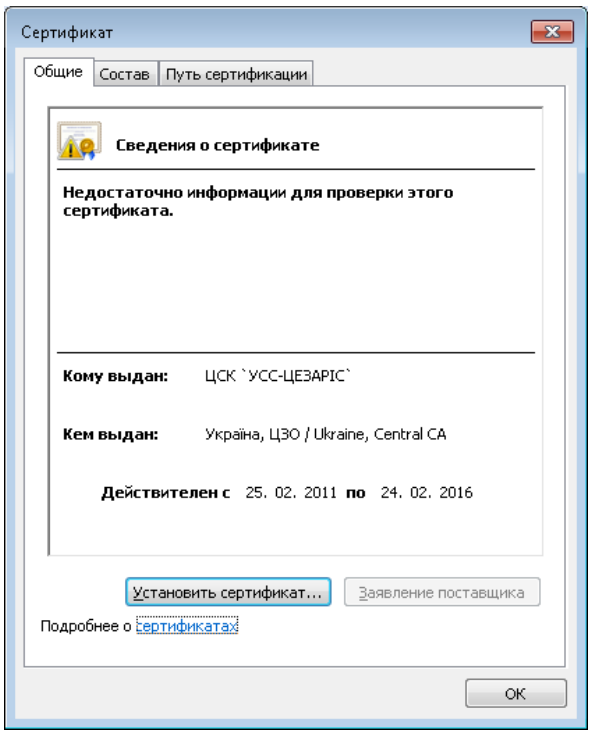
Пор. № зміни	Підпис відпов. особи	Дата внесення

У вікні «Мастер импорта сертификатов» натисніть кнопку «Готово».



У вікні «Мастер импорта сертификатов» натисніть кнопку «ОК», також натисніть кнопку «ОК» у вікні «Сертификат».





Пор. № зміни	Підпис відпов. особи	Дата внесення

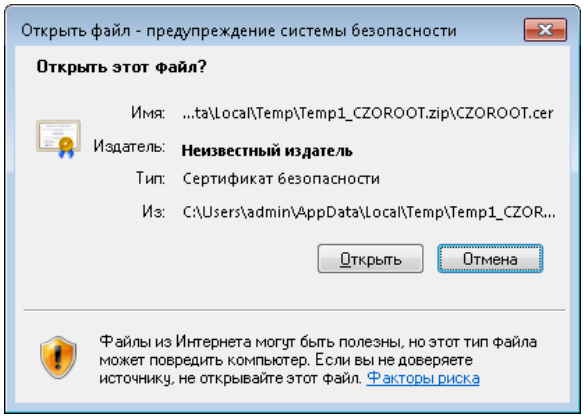
Встановлення кореневого сертифікату ЦЗО

Завантажте кореневий сертифікат ЦЗО за прямим посиланням: http://acsk.uss.gov.ua/download/rootcer/CZOROOT.zip або зі сторінки http://acsk.uss.gov.ua/rootcertificate.htm (в таблиці «КОРЕНЕВІ СЕРИФІКАТИ ЦСК "УСС-ЦЕЗАРИС"» під першим номером). Розпакуйте завантажений архів та запустіть файл **CZOROOT.cer** шляхом подвійного натиснення лівої кнопки миші або виділення його і натиснення кнопки «Enter». З'явиться вікно сертифікату відкритого ключа ЦЗО:

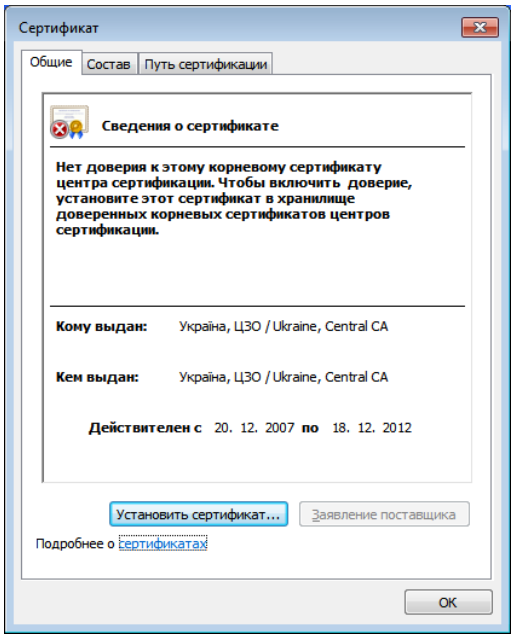
Примітка: Завантаження кореневого сертифікату ЦЗО доступне с офіційного Інтернет-ресурсу Центрального засвідчувального органу: http://czo.gov.ua/

Звертаємо Вашу увагу на те, що у разі виникнення вікна «Предупреждение системы безопасности» необхідно натиснути кнопку «Открыть».

Примітка: В залежності від налаштування Вашої операційної системи вікно «Предупреждение системы безопасности» може не з'являтися.

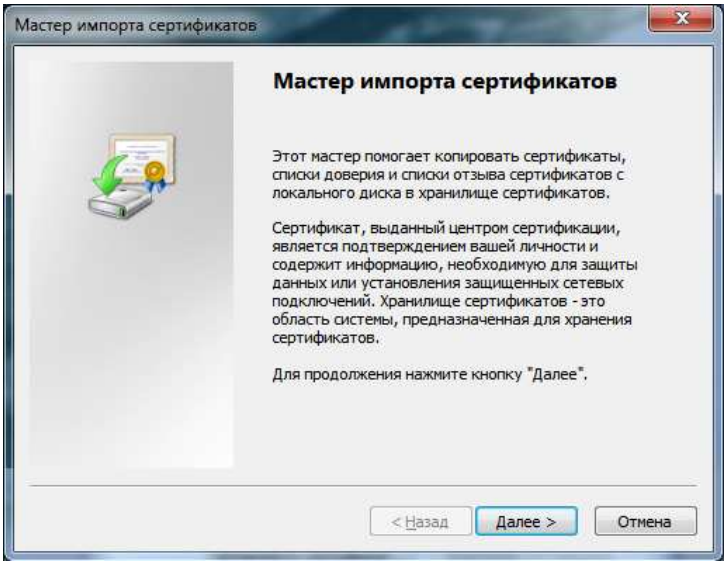


З'явиться вікно сертифікату відкритого ключа ЦЗО. Натисніть кнопку «Установить сертификат».

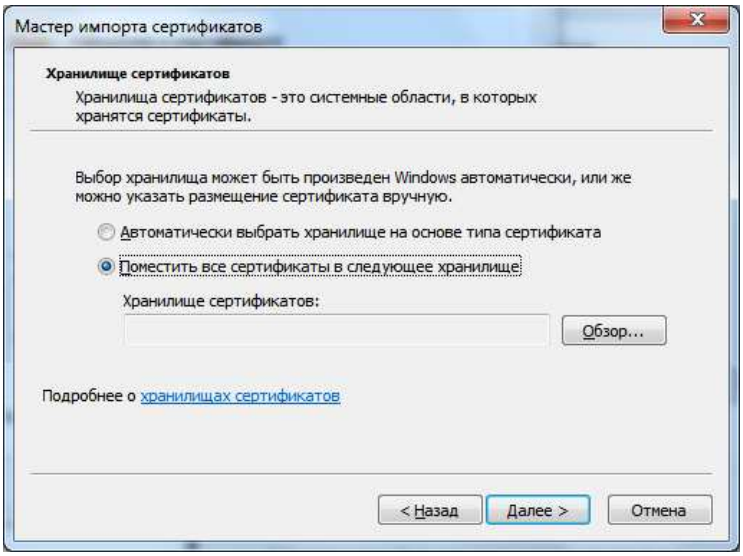


Пор. № зміни	Підпис відпов. особи	Дата внесення

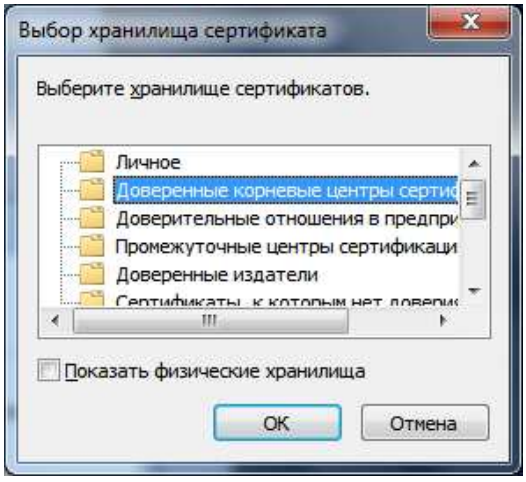
Відкриється вікно «Мастер импорта сертификатов», натисніть кнопку «Далее».



У вікні, яке відкрилося, відмітьте пункт «Поместить все сертификаты в следующее хранилище» и натисніть кнопку «Обзор…».

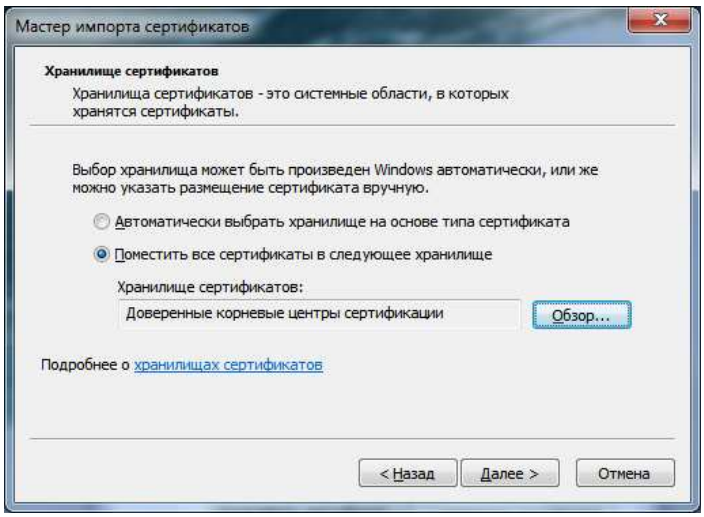


У вікні «Выбор хранилища сертификата» оберіть «Доверенные корневые центры сертификации» шляхом одноразового натиснення на цьому пункті лівою кнопкою миші та натисніть кнопку «ОК». Вікно «Выбор хранилища сертификата» закриється.

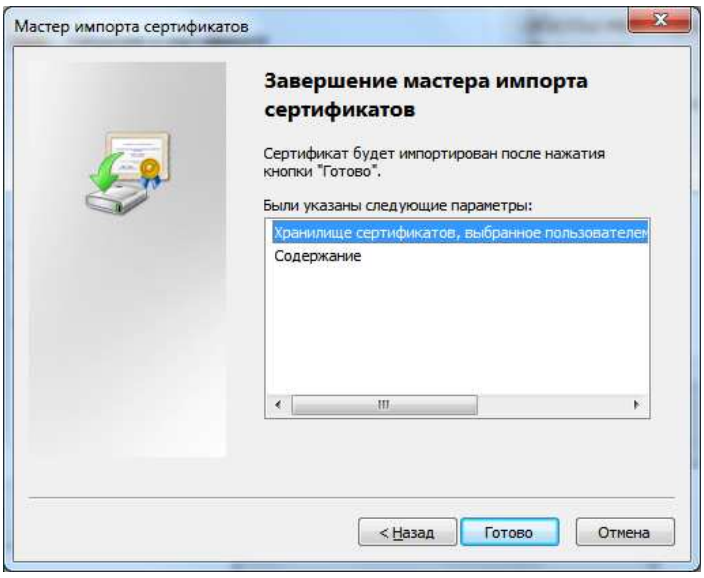


Пор. № зміни	Підпис відпов. особи	Дата внесення

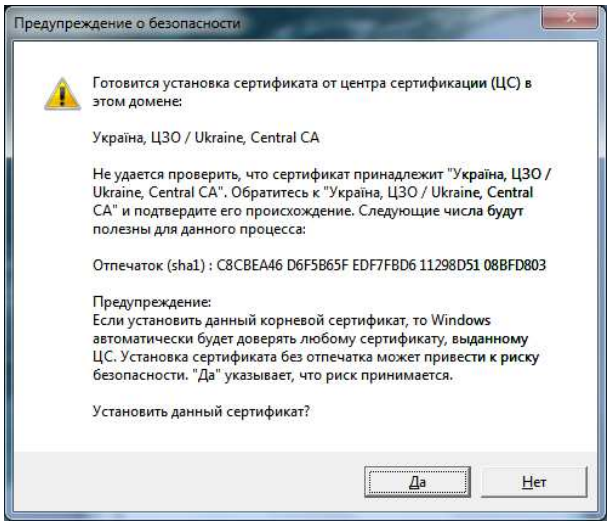
У вікні «Мастер импорта сертификатов» натисніть кнопку «Далее».



У вікні «Мастер импорта сертификатов» натисніть кнопку «Готово».

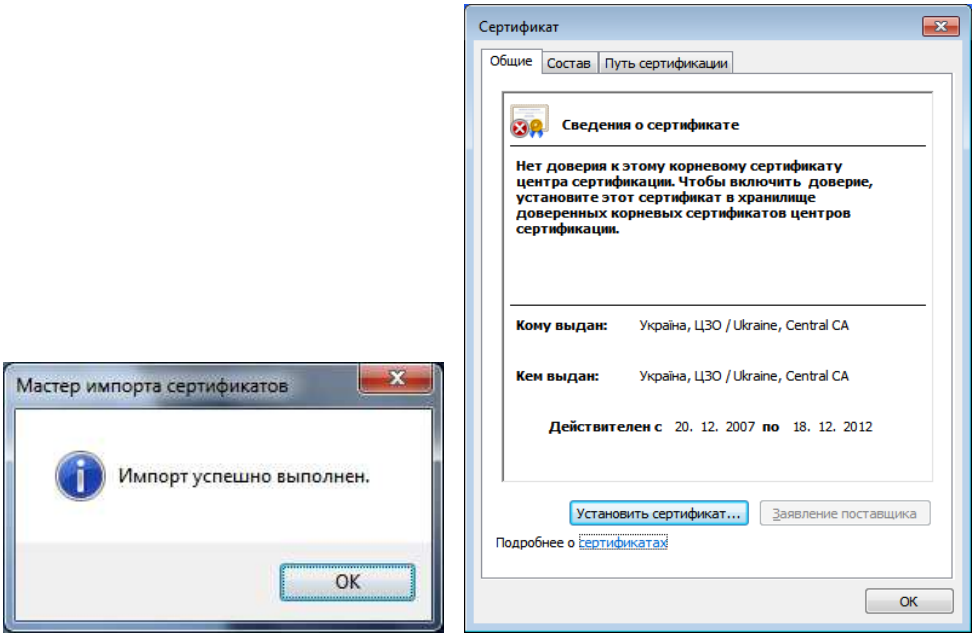


У вікні «Предупреждение о безопасности» обов’язково необхідно натиснути кнопку «Да» та встановити кореневий сертифікат ЦЗО.

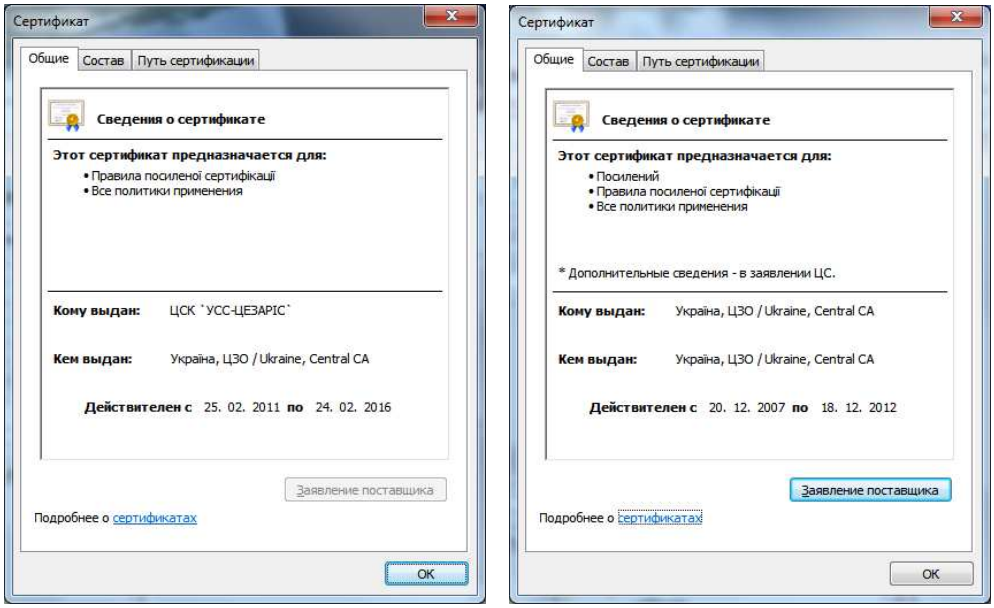


Пор. № зміни	Підпис відпов. особи	Дата внесення

У вікні «Мастер импорта сертификатов» натисніть кнопку «ОК», а також натисніть кнопку «ОК» у вікні «Сертификат».



Повторно відкрийте обидва сертифікати і впевніться у тому, що червоні позначки та зауваження щодо довіри зникли, а сертифікати відображаються саме так, як зазначено нижче.

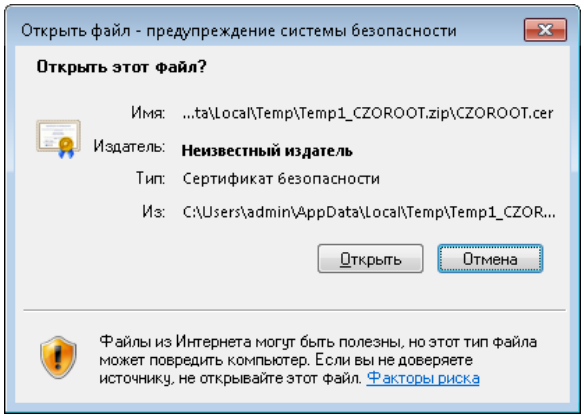


Кореневі сертифікати встановлені успішно.

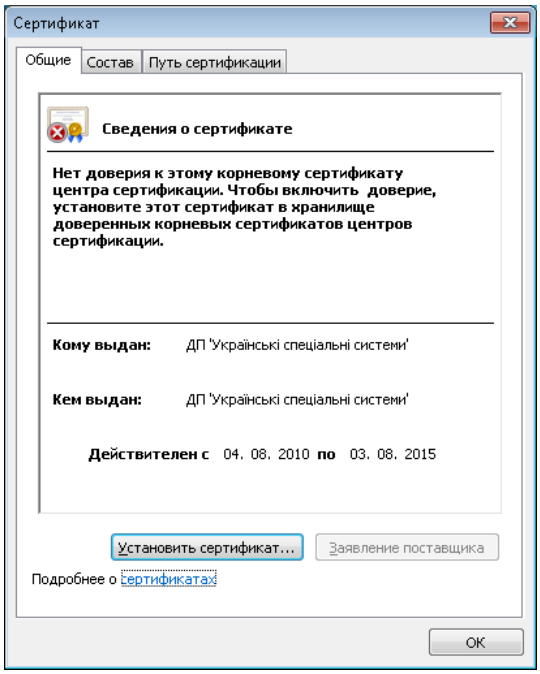
Завантажте кореневий сертифікат ЦСК, що необхідний для функціонування ресурсу за HTTPS протоколом (SSL - Secure Sockets Layer) використовуючи пряме посилання: http://acsk.uss.gov.ua/download/rootcer/CESARISROOTRSA.zip або зі сторінки http://acsk.uss.gov.ua/rootcertificate.htm в таблиці «КОРЕНЕВІ СЕРИФІКАТИ ЦСК "УСС-ЦЕЗАРИС"» під п’ятим номером). Розпакуйте завантажений архів та запустіть файл **CESARISROOTRSA.cer** шляхом подвійного натиснення лівої кнопки миші або виділення його і натиснення кнопки «Enter».

Звертаємо Вашу увагу на те, що у разі виникнення вікна «Предупреждение системы безопасности» необхідно натиснути кнопку «Открыть».

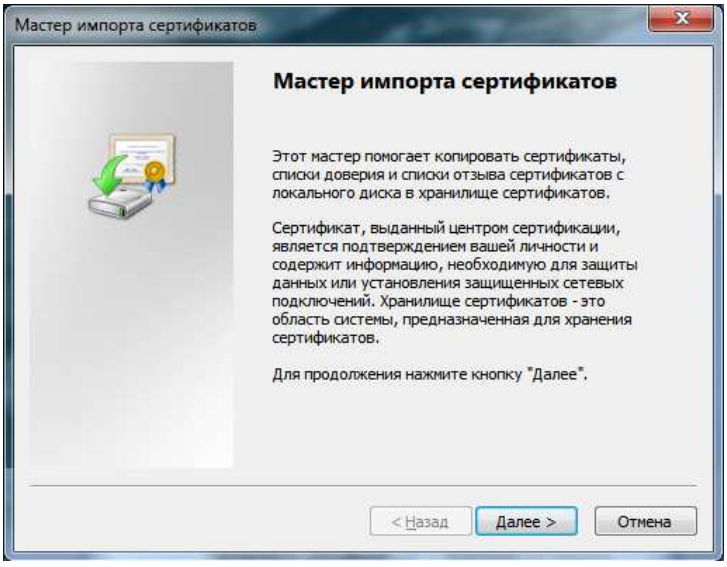
Примітка: В залежності від налаштування Вашої операційної системи вікно «Предупреждение системы безопасности» може не з'являтися.



З'явиться вікно сертифікату відкритого ключа ЦСК, необхідного для коректної роботи SSL. Натисніть кнопку «Установить сертификат».

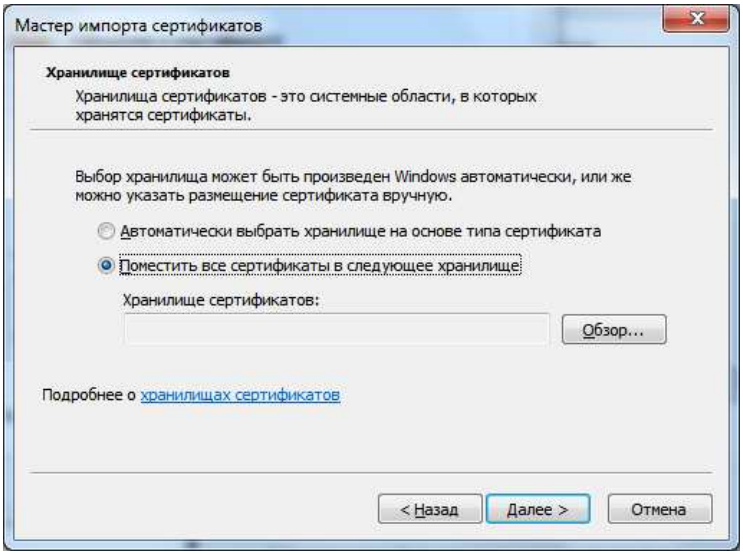


Відкриється вікно «Мастер импорта сертификатов», натисніть кнопку «Далее».

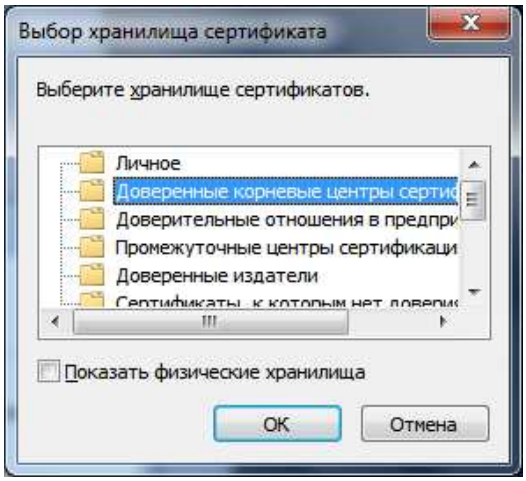


Пор. № зміни	Підпис відпов. особи	Дата внесення

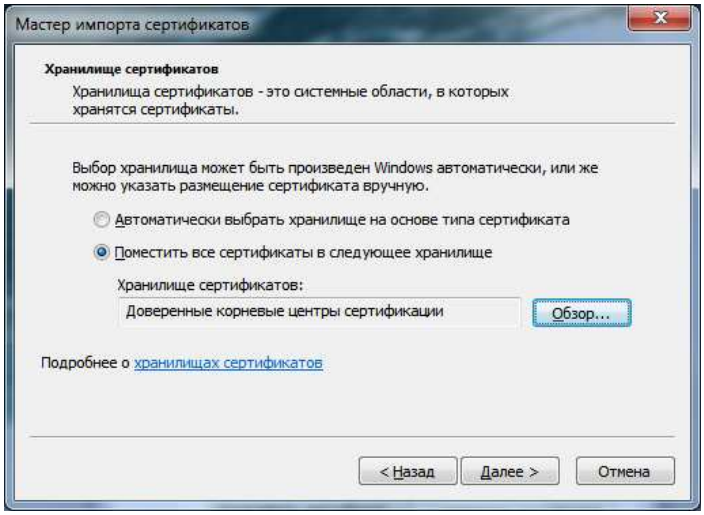
У вікні, яке відкрилося, відмітьте пункт «Поместить все сертификаты в следующее хранилище» і натисніть кнопку «Обзор…».



У вікні «Выбор хранилища сертификата» оберіть «Доверенные корневые центры сертификации» шляхом одноразового натиснення на цьому пункті лівою кнопкою миші та натисніть кнопку «ОК». Вікно «Выбор хранилища сертификата» закриється.

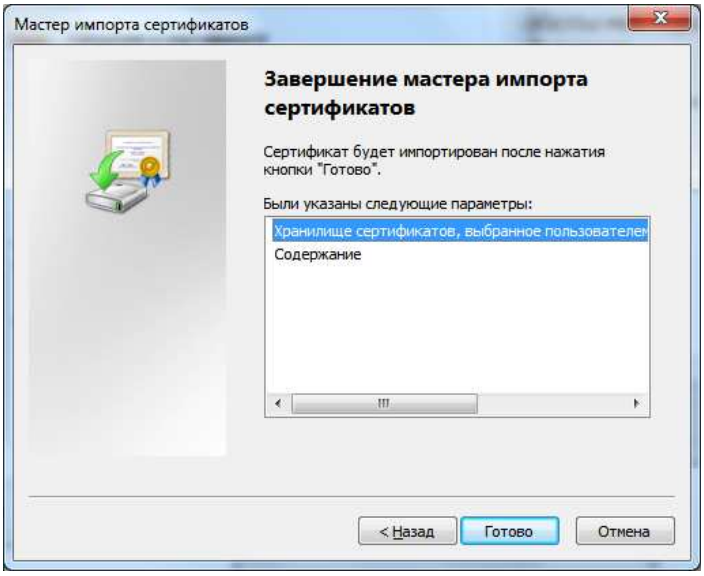


У вікні «Мастер импорта сертификатов» натисніть кнопку «Далее».

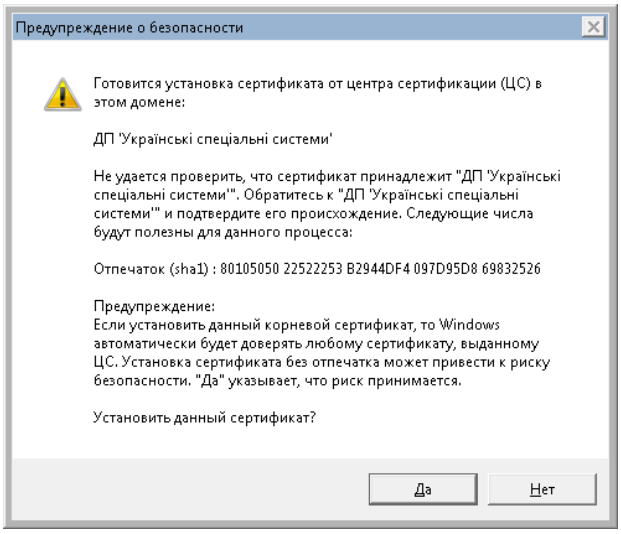


Пор. № зміни	Підпис відпов. особи	Дата внесення

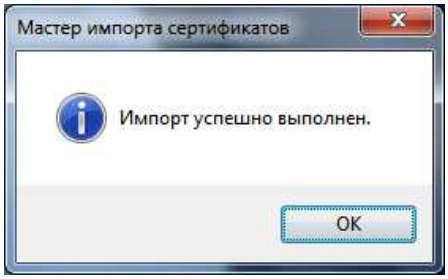
У вікні «Мастер импорта сертификатов» натисніть кнопку «Готово».

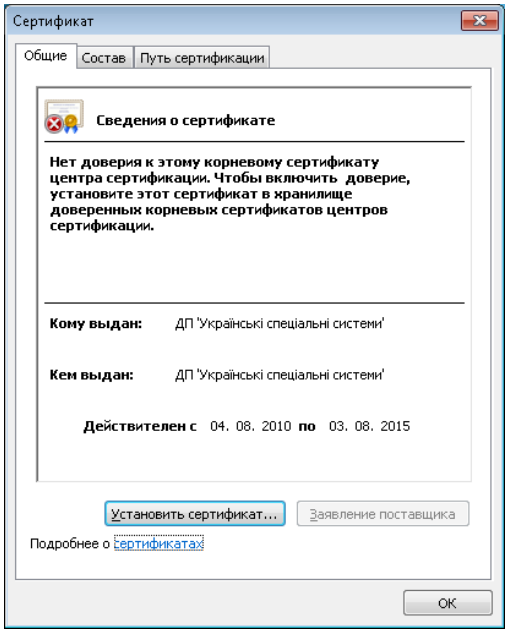


У вікні «Предкпреждение о безопасности» обов’язково необхідно натиснути кнопку «Да» та встановити кореневий сертифікат ЦСК.



У вікні «Мастер импорта сертификатов» натисніть кнопку «ОК», а також натисніть кнопку «ОК» у вікні «Сертификат».



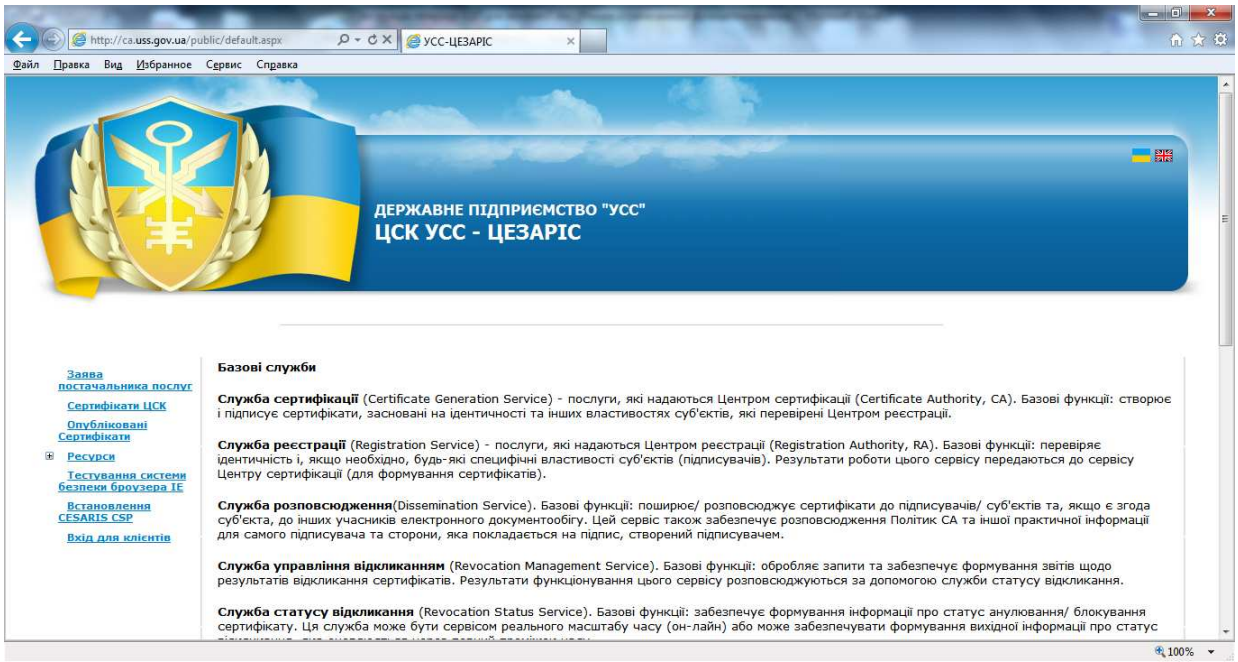


Сертифікат відкритого ключа ЦСК, необхідний для коректної роботи SSL, було успішно встановлено.

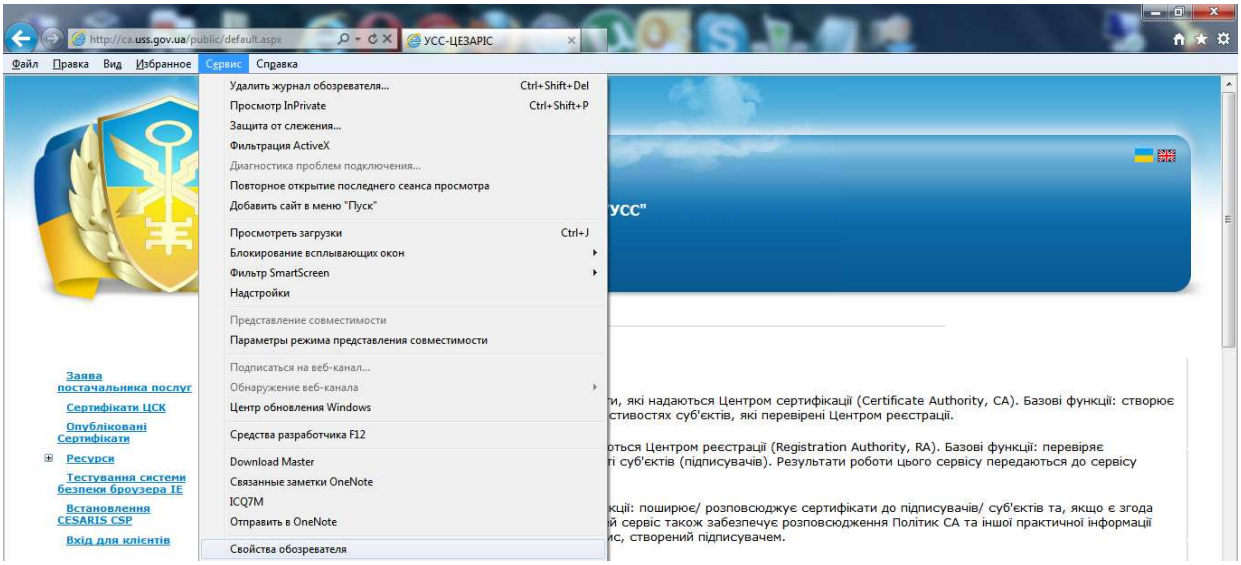
Налаштування браузера Internet Explorer

Примітка: Для отримання/формування сертифікатів відкритих ключів необхідно використовувати виключно браузер **Internet Explorer версії 6 та вище**. Отримання/формування сертифікатів відкритих ключів **в інших браузерах не підтримується**.

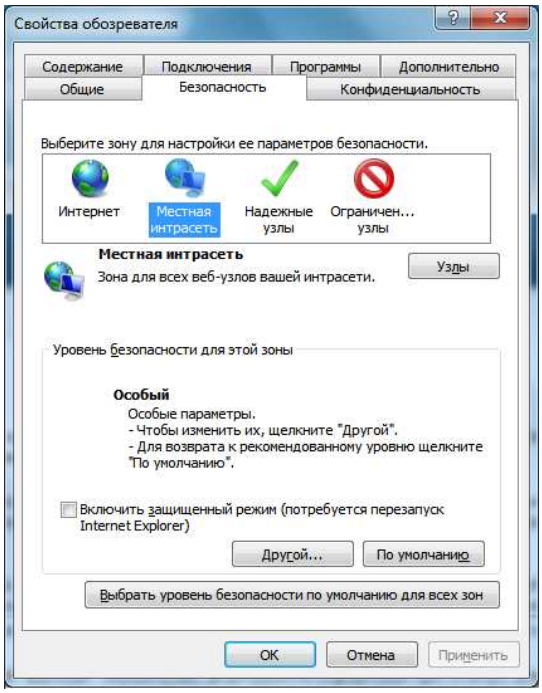
Відкрийте браузер Internet Explorer (IE) та перейдіть за наступним посиланням: http://ca.uss.gov.ua



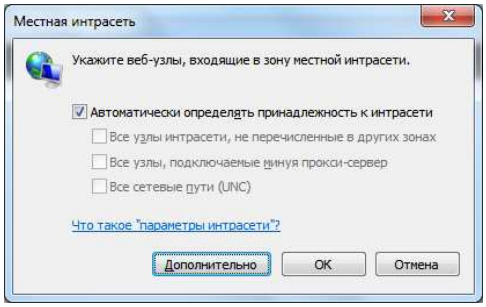
Зайдіть в меню IE «Сервис» (якщо строка меню відсутня, натисніть кнопку «alt» на клавіатурі, і вона з’явиться), оберіть пункт «Свойства обозревателя».



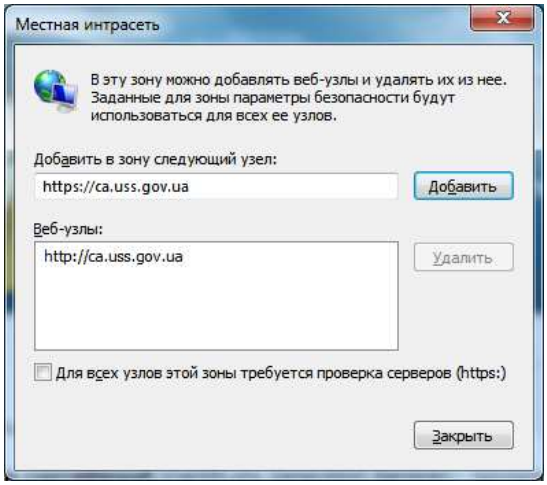
Перейдіть до вкладки «Безопасность», виділіть одним натисканням лівої кнопки миші пункт «Местная интрасеть» та натисніть кнопку «Узлы».



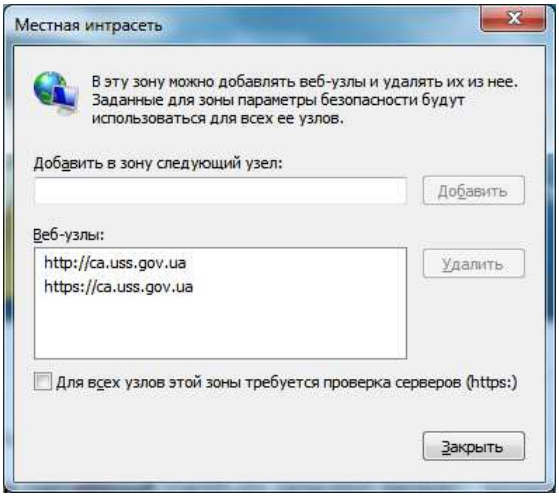
У вікні, яке з’явилося, натисніть кнопку «Дополнительно». У вікні, яке після цього відкрилося, зніміть пташку з пункту «Для всех узлов этой зоны требуется проверка серверов (https:)» (якщо вона встановлена) та в полі «Добавить в зону следующий узел:» введіть адресу вузла http://ca.uss.gov.ua та натисніть кнопку «Добавить», а потім введіть адресу сайту https://ca.uss.gov.ua та натисніть кнопку «Добавить».



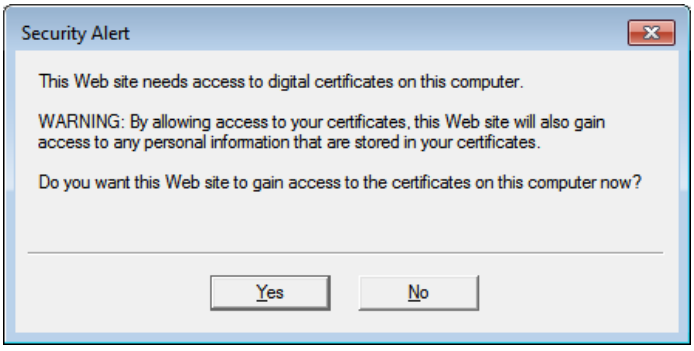
Пор. № зміни	Підпис відпов. особи	Дата внесення



Обидві введені Вами адреси вузлів повинні бути зазначені в полі «Веб-узлы»



Примітка: Під час роботи на вузлах http://ca.uss.gov.ua та https://ca.uss.gov.ua може з'являтися повідомлення безпеки у вікні «Security Alert», потрібно натискати «Yes» в усіх випадках, коли зазначене вікно буде з'являтися. Натискання кнопки «Yes» надає можливість доступу до сертифікатів відкритих ключів Вашого комп'ютера.

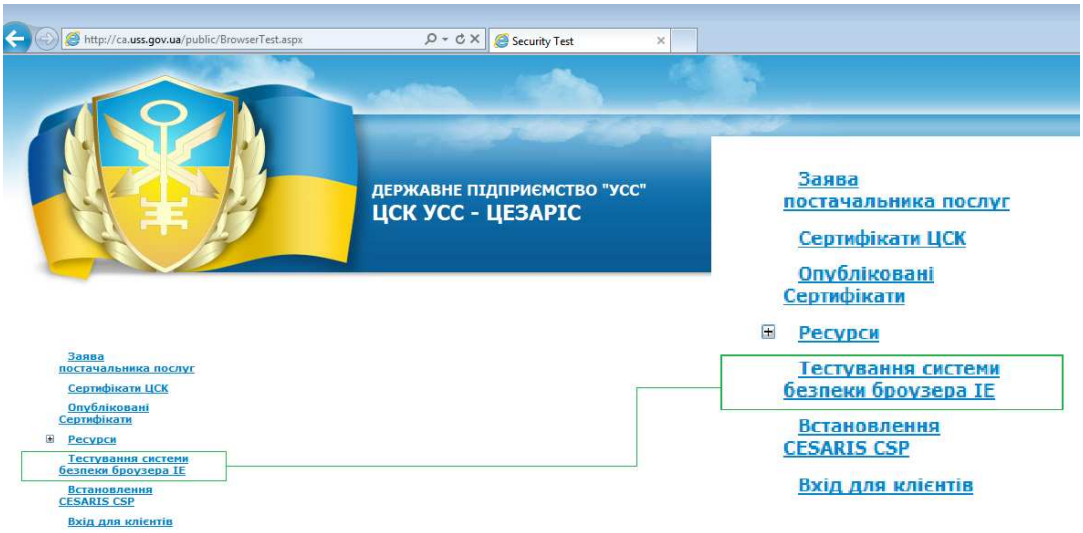


Перевірка готовності системи

Відкрийте браузер IE та перейдіть за наступним посиланням: http://ca.uss.gov.ua

Перейдіть на сторінку «Тестування системи безпеки браузера IE»

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*



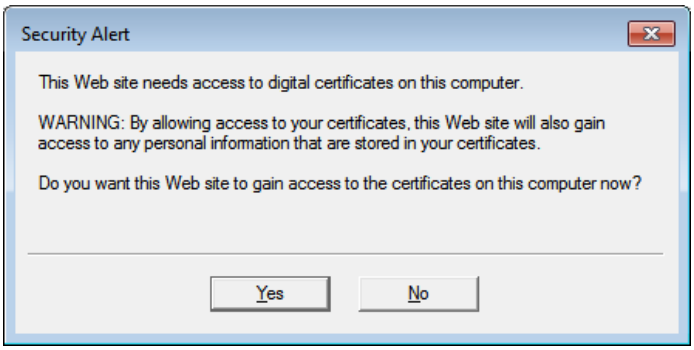
Натисніть кнопку «Виконати» загальну перевірку налаштування браузера.

Загальна перевірка налаштування броузера [Виконати]

Критерій	Стан	Подробиці	Допомога
Тип броузера	Готово	Броузер : **IE**. Тип - **IE7**. Версія - **7.0**. Платформа - **WinNT**. Модель -**Win32**.	
Дозвіл на використання модулів ActiveX	Готово	Дозволено	
Використання JavaScript	Готово	Версія - 1.2	
Використання VBScript	Готово	Підтримується	
Параметри броузера		Підтримка таблиць : True Підтримка Cookies : True	
Наявність CAPICOM [Перевірка]			Встановлення ActiveX CAPICOM v.2.1.
Криптографічні сховища [Перевірка]			
Наявність XEnroll [Перевірка]			Встановлення ActiveX XEnroll
Встановлені криптопровайдери [Список]			Встановлення модуля **Cesaris CryptoPack**

Зауваження. Звертайте увагу на діалоги та попередження системи безпеки броузера, що можуть з'являтися у верхній частині вікна в процесі виконання тестування та налагодження. Виконуйте рекомендації системи.

У вікні повідомлення безпеки «Security Alert» потрібно натискати «Yes».



Якщо в колонці «Стан» по всім пунктам «Готово», система налаштована вірно та готова для подальшої роботи.

Загальна перевірка налаштування броузера [Виконати]

Критерій	Стан	Подробиці	Допомога
Тип броузера	**Готово**	Броузер : **IE**. Тип - **IE7**. Версія - **7.0**. Платформа - **WinNT**. Модель -**Win32**.	
Дозвіл на використання модулів ActiveX	**Готово**	Дозволено	
Використання JavaScript	**Готово**	Версія - 1.2	
Використання VBScript	**Готово**	Підтримується	
Параметри броузера		Підтримка таблиць : True Підтримка Cookies : True	
Наявність CAPICOM [Перевірка]	**Готово**	Модуль CAPICOM встановлено	[Встановлення ActiveX CAPICOM v.2.1.]
Криптографічні сховища [Перевірка]	**Готово**	Персональне Сховище **My** доступне Сховище Smart card **My** доступне	
Наявність XEnroll [Перевірка]	**Готово**	Встановлено модуль Xenroll	[Встановлення ActiveX XEnroll]
Встановлені криптопровайдери [Список]	**Готово**	• **CESARIS DSTU 4145-2002(PB) and RSA Cryptographic Provider** • **CESARIS DSTU 4145-2002(PB) and ECDH Cryptographic Provider**	Встановлення модуля **Cesaris CryptoPack**

Зауваження. Звертайте увагу на діалоги та попередження системи безпеки броузера, що можуть з'являтися у верхній частині вікна в процесі виконання тестування та налагодження. Виконуйте рекомендації системи.

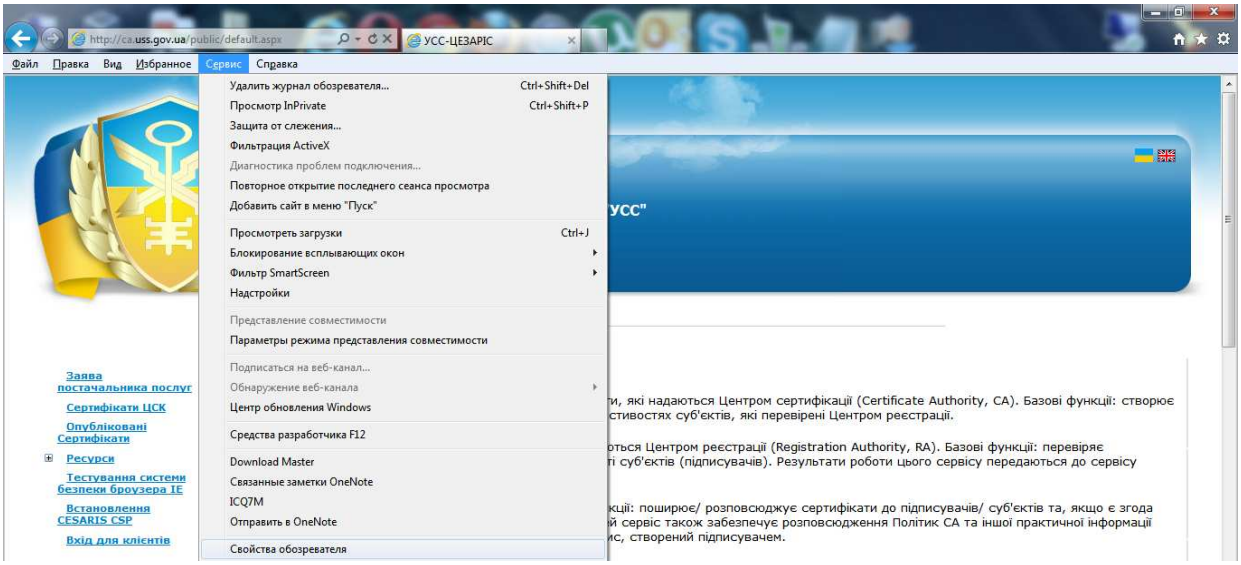
У разі, якщо в колонці «Критерій» по пункту «Наявність XEnroll» в колонці «Стан» виникла «Помилка», а по пункту «Встановлені криптопровайдери» в колонці «Стан» та «Подробиці» відображені пусті поля, необхідно дозволити виконання елементів ActiveX щодо зони місцевої інтромережі.

Загальна перевірка налаштування броузера [Виконати]

Критерій	Стан	Подробиці	Допомога
Тип броузера	**Готово**	Броузер : **IE**. Тип - **IE7**. Версія - **7.0**. Платформа - **WinNT**. Модель -**Win32**.	
Дозвіл на використання модулів ActiveX	**Готово**	Дозволено	
Використання JavaScript	**Готово**	Версія - 1.2	
Використання VBScript	**Готово**	Підтримується	
Параметри броузера		Підтримка таблиць : True Підтримка Cookies : True	
Наявність CAPICOM [Перевірка]	**Готово**	Модуль CAPICOM встановлено	[Встановлення ActiveX CAPICOM v.2.1.]
Криптографічні сховища [Перевірка]	**Готово**	Персональне Сховище **My** доступне Сховище Smart card не доступне	
Наявність XEnroll [Перевірка]	**Помилка**	Завантаження ...Модуль Xenroll відсутній	[Встановлення ActiveX XEnroll]
Встановлені криптопровайдери [Список]			Встановлення модуля **Cesaris CryptoPack**

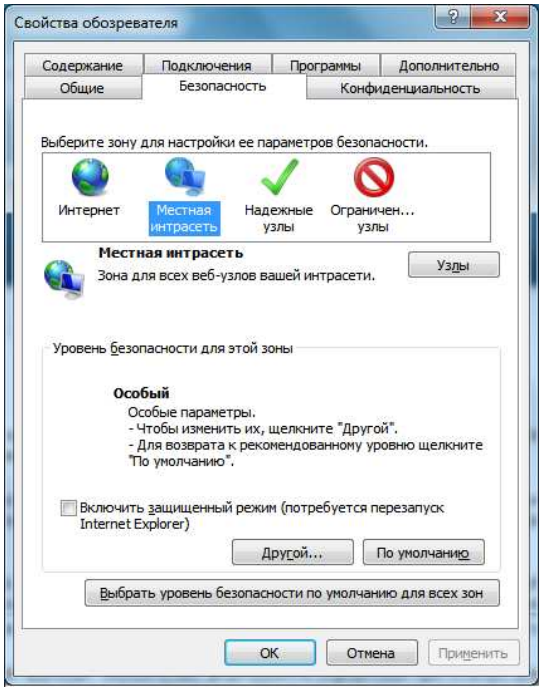
Зауваження. Звертайте увагу на діалоги та попередження системи безпеки броузера, що можуть з'являтися у верхній частині вікна в процесі виконання тестування та налагодження. Виконуйте рекомендації системи.

Зайдіть в меню IE «Сервис» (якщо строка меню відсутня натисніть кнопку «alt» на клавіатурі, і вона з’явиться), оберіть пункт «Свойства обозревателя».

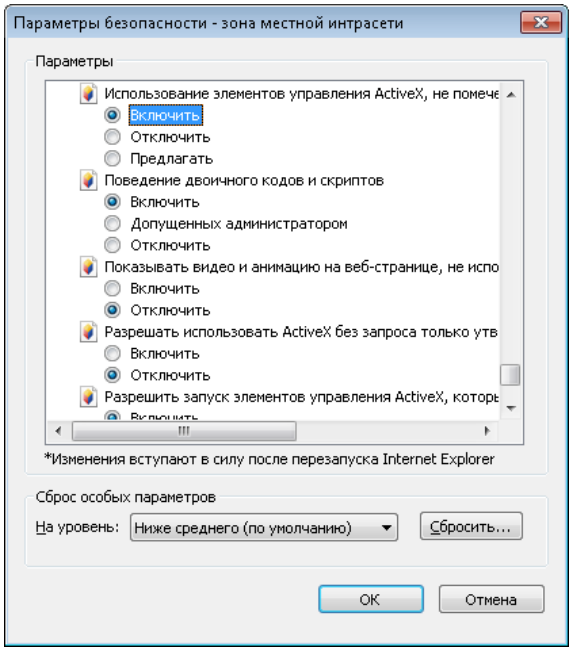


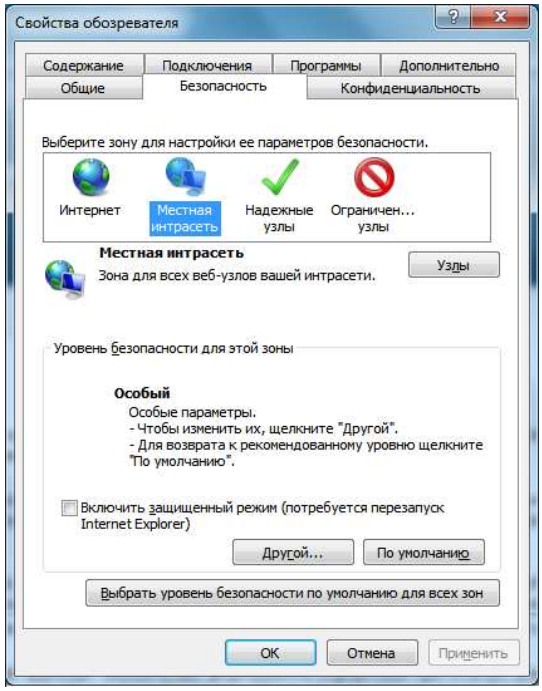
Пор. № зміни	Підпис відпов. особи	Дата внесення

Перейдіть до вкладки «Безопасность», виділіть пункт «Местная интрасеть» та натисніть кнопку «Другой…».



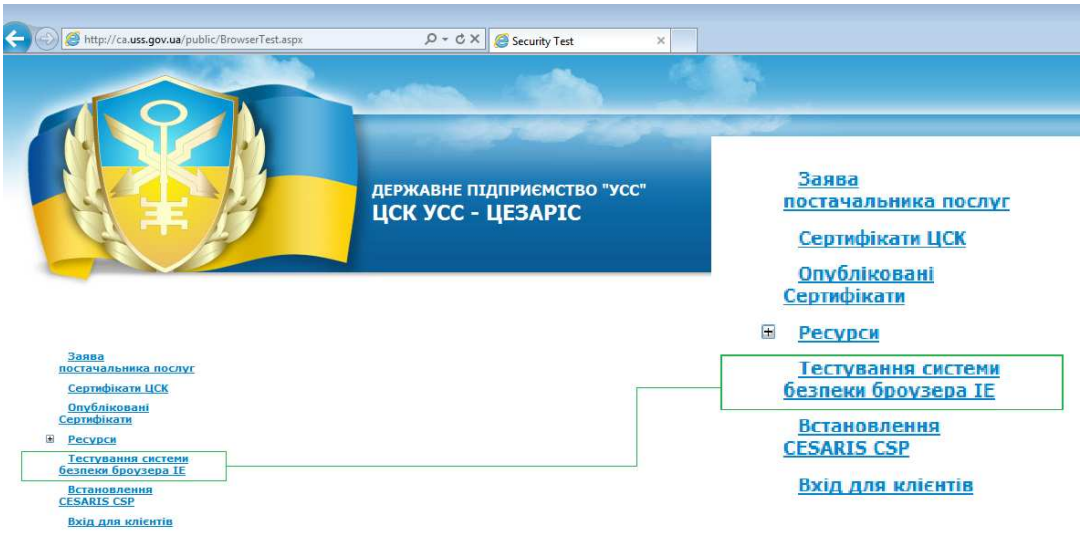
Знайдіть параметр «Использование элементов управления ActiveX, непомеченных как безопасные для использования» та поставте позначку у режим «Включить», нижче натисніть кнопку «ОК». У вікні «Свойства обозревателя» натисніть кнопку «Применить» та кнопку «ОК».





Повторно перевірте систему безпеки браузера IE, для чого знову перейдіть на сторінку «Тестування системи безпеки браузера IE»

Пор. № зміни	Підпис відпов. особи	Дата внесення



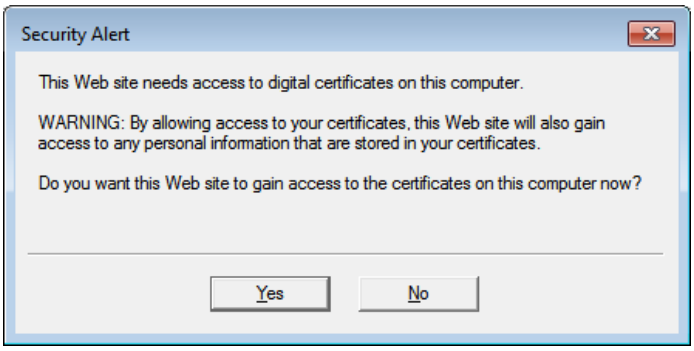
Натисніть кнопку «Виконати» загальну перевірку налаштування браузера.

Загальна перевірка налаштування броузера [Виконати]

Критерій	Стан	Подробиці	Допомога
Тип броузера	Готово	Броузер : **IE**. Тип - **IE7**. Версія - **7.0**. Платформа - **WinNT**. Модель -**Win32**.	
Дозвіл на використання модулів ActiveX	Готово	Дозволено	
Використання JavaScript	Готово	Версія - 1.2	
Використання VBScript	Готово	Підтримується	
Параметри броузера		Підтримка таблиць : True Підтримка Cookies : True	
Наявність CAPICOM [Перевірка]			Встановлення ActiveX CAPICOM v.2.1.
Криптографічні сховища [Перевірка]			
Наявність XEnroll [Перевірка]			Встановлення ActiveX XEnroll
Встановлені криптопровайдери [Список]			Встановлення модуля **Cesaris CryptoPack**

Зауваження. Звертайте увагу на діалоги та попередження системи безпеки броузера, що можуть з'являтися у верхній частині вікна в процесі виконання тестування та налагодження. Виконуйте рекомендації системи.

У вікні повідомлення безпеки «Security Alert», потрібно натискати «Yes».



В колонці «Стан» по всім пунктам повинно бути зазначено «Готово», що свідчить про правильне налаштування системи безпеки браузера IE та готовність до подальшої роботи.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

Загальна перевірка налаштування броузера Виконати

Критерій	Стан	Подробиці	Допомога
Тип броузера	Готово	Броузер : **IE**. Тип - **IE7**. Версія - **7.0**. Платформа - **WinNT**. Модель -**Win32**.	
Дозвіл на використання модулів ActiveX	Готово	Дозволено	
Використання JavaScript	Готово	Версія - 1.2	
Використання VBScript	Готово	Підтримується	
Параметри броузера		Підтримка таблиць : True Підтримка Cookies : True	
Наявність CAPICOM Перевірка	Готово	Модуль CAPICOM встановлено	Встановлення ActiveX CAPICOM v.2.1.
Криптографічні сховища Перевірка	Готово	Персональне Сховище **My** доступне Сховище Smart card **My** доступне	
Наявність XEnroll Перевірка	Готово	Встановлено модуль Xenroll	Встановлення ActiveX XEnroll
Встановлені криптопровайдери Список	Готово	• **CESARIS DSTU 4145-2002(PB) and RSA Cryptographic Provider** • **CESARIS DSTU 4145-2002(PB) and ECDH Cryptographic Provider**	Встановлення модуля **Cesaris CryptoPack**

Зауваження. Звертайте увагу на діалоги та попередження системи безпеки броузера, що можуть з'являтися у верхній частині вікна в процесі виконання тестування та налагодження. Виконуйте рекомендації системи.

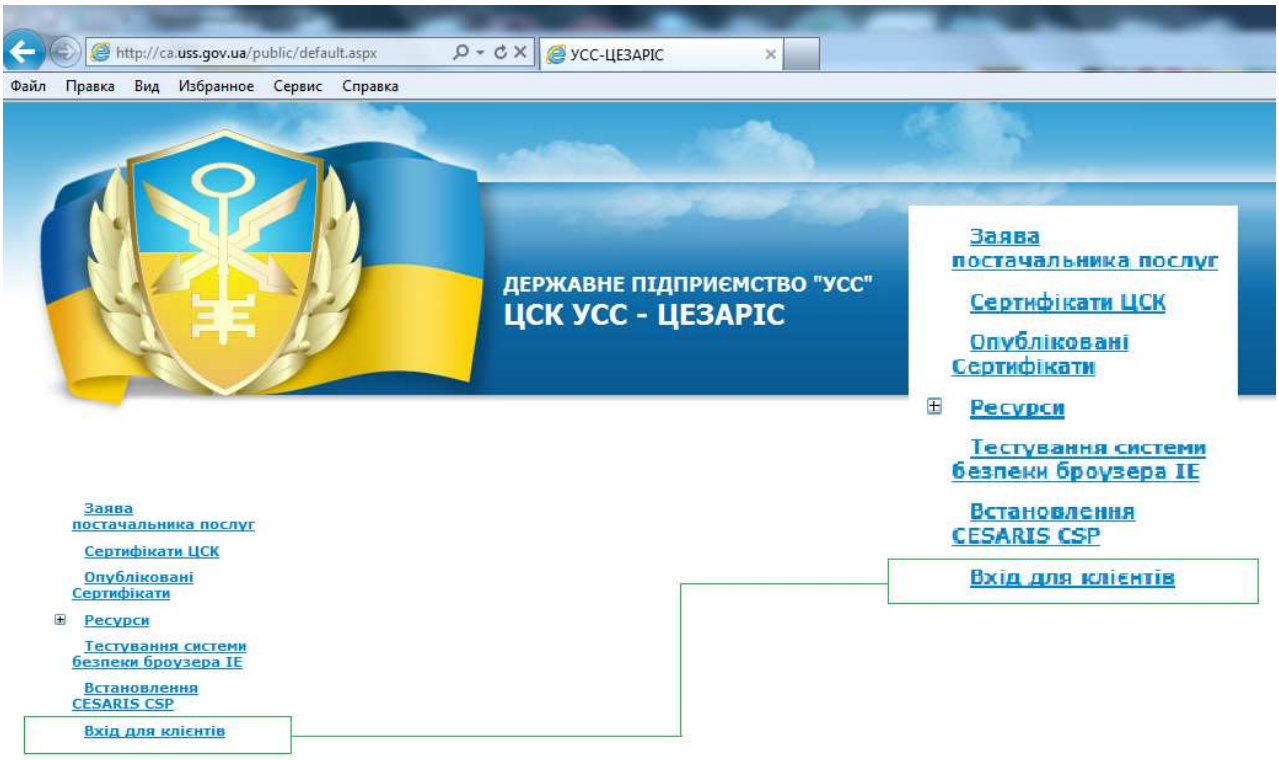
ГЕНЕРАЦІЯ КЛЮЧОВОЇ ПАРИ ТА ОТРИМАННЯ СЕРТИФІКАТІВ

Заміна стартового пароля

Примітка: Для отримання/формування сертифікатів відкритих ключів необхідно використовувати виключно браузер **Internet Explorer версії 6 та вище**. Отримання/формування сертифікатів відкритих ключів **в інших браузерах не підтримується**.

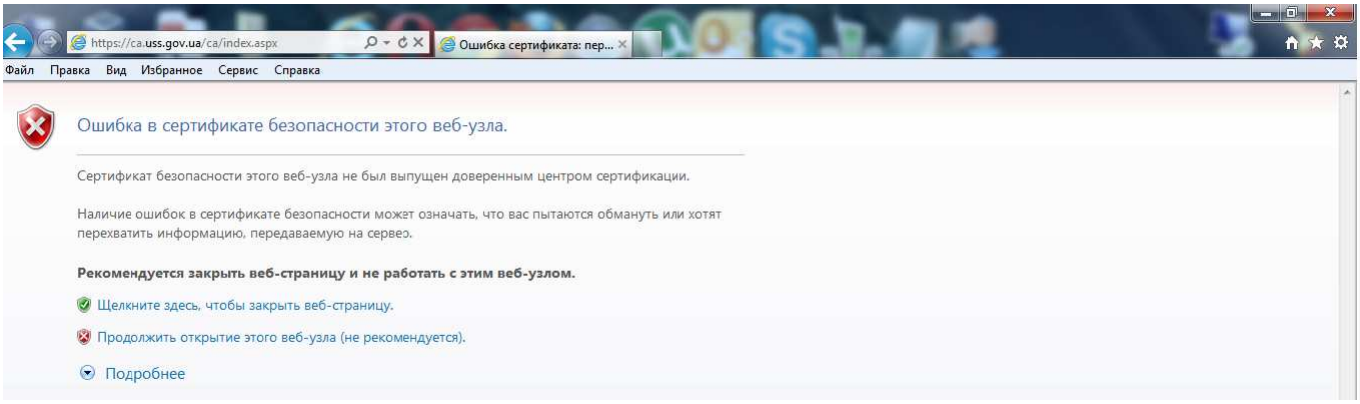
Примітка: Перед початком роботи рекомендує закрити Internet Explorer, а потім знову його відкрити (однозначно потрібно перезавантажувати Internet Explorer, якщо він був включений на момент створення файлового токену).

В Internet Explorer введіть адресу вузла http://ca.uss.gov.ua, а потім перейдіть за посиланням «Вхід для клієнтів».



Пор. № зміни	Підпис відпов. особи	Дата внесення

Примітка: Можливі попередження системи безпеки у зв'язку з переходом на безпечне з'єднання або з тим, що сертифікат серверу не є довіреним.



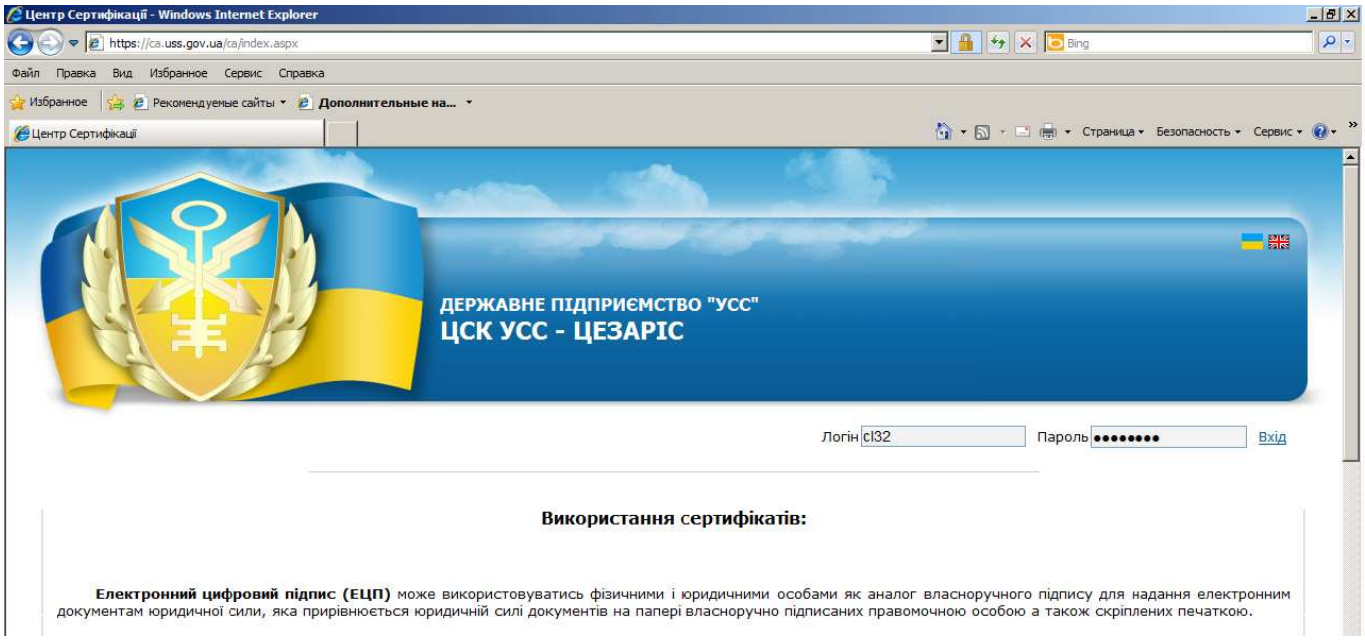
«Ошибка в сертификате безопасности этого веб-узла» свідчить про те, що сертифікат відкритого ключа ЦСК, який необхідний для коректної роботи SSL не було встановлено, або встановлено некоректно. Необхідно обрати «Продолжить открытие этого web-узла (не рекомендуется)» та перевірити термін дії SSL сертифікату.

Поновіть сторінку (натисніть клавішу F5 клавіатури) та скопіюйте в поля «Логін» та «Пароль» дані, які було отримано електронною поштою.

Центр сертифікації ключів "УСС-ЦЕЗАРІС" Державного підприємства "Українські спеціальні системи"
Іванов Іван Іванович Логін: cl32 Пароль: VddKVg6^

Перевірте, щоб довжина пароля була рівно 8 символів. Бажано копіювати логін та пароль з електронного листа та вставляти у веб-форму, у зв'язку з тим, що не завжди легко відрізнити символи стартового пароля, що сформовані системою (0 схожий на О, 1 схожа на l).

Після введення логіну та стартового пароля натисніть «Вхід».

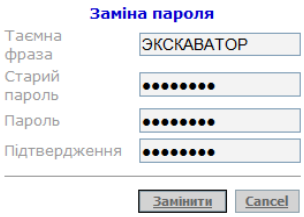


При першому вході до електронного персонального кабінету система автоматично запропонує змінити стартовий пароль, отриманий електронною поштою. Вам необхідно **великими** літерами ввести таємну фразу (яка була вказана Вами в заяві «Заява про реєстрацію юридичної (чи фізичної) особи»),

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

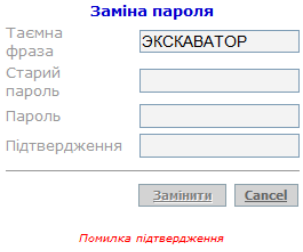
Таємна фраза, що використовується для зміни паролю до власного облікового запису сервера ЦСК "УСС-Цезаріс"										
Таємна фраза:	Э	К	С	К	А	В	А	Т	О	Р

старий пароль (отриманий електронною поштою) та двічі ввести новий пароль, який буде використовуватися у подальшому для входу до власного електронного кабінету. Мінімальна довжина пароля повинна становити 8 символів. Після введення зазначених вище парольних параметрів необхідно натиснути кнопку «Замінити».

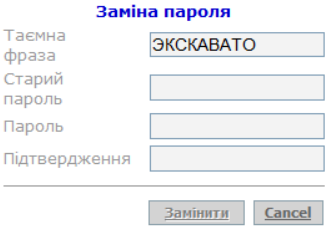


У разі некоректного введення одного з парольних параметрів система проінформує Вас про цей факт, після чого Вам необхідно буде ввести вірні параметри, спираючись на підказки системи.

Примітка: У разі, якщо Ви ввели пароль та невірно ввели його підтвердження, система видасть повідомлення «Помилка підтвердження».

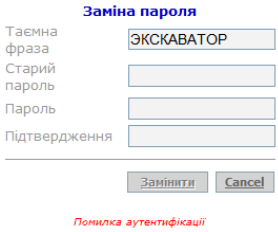


Примітка: У разі, якщо Ви невірно ввели таємну фразу, система видасть повідомлення «Невірна таємна фраза. Спробуйте ще».



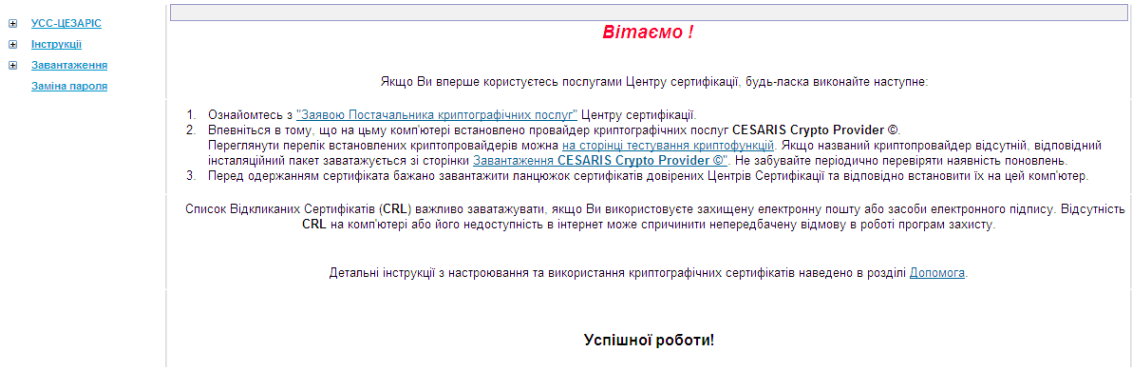
Пор. № зміни	Підпис відпов. особи	Дата внесення

Примітка: У разі, якщо Ви невірно ввели старий пароль (стартовий, який було надіслано електронною поштою), система видасть повідомлення «Помилка аутентифікації».



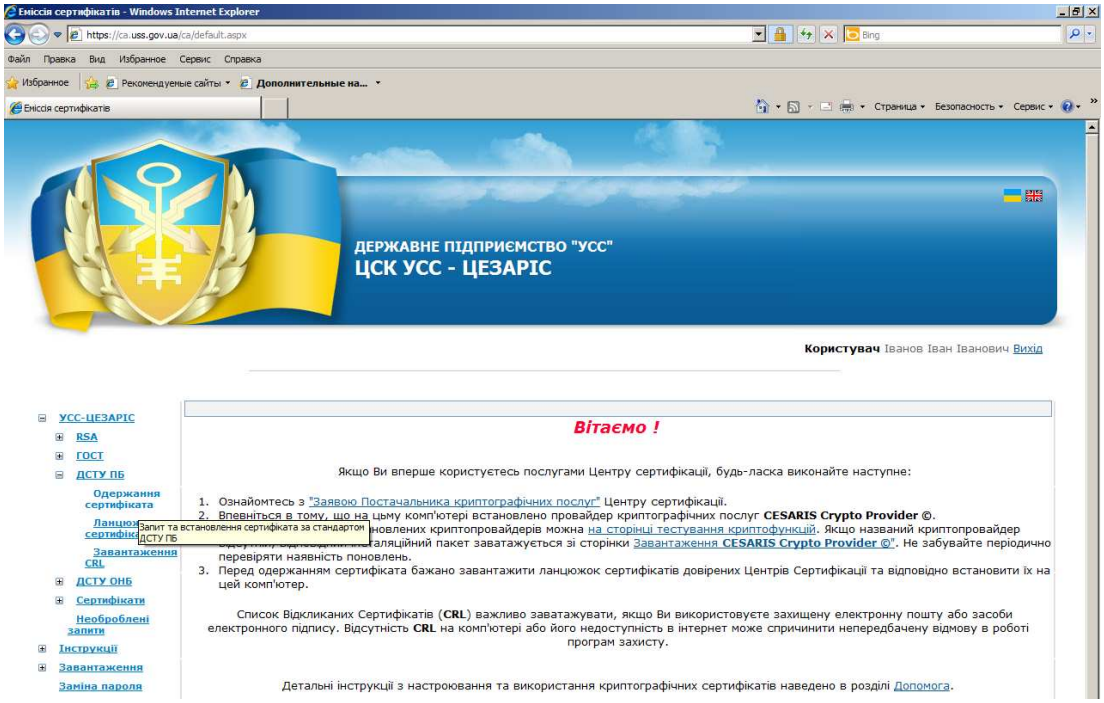
Примітка: У разі втрати зазначеного Вами пароля, у подальшому Ви не зможете зайти до електронного персонального кабінету з метою формування запитів на сертифікацію відкритих ключів та одержання сертифікатів відкритих ключів, якщо потрібно буде продовжити дію сертифікату відкритого ключа після його закінчення. Запишіть введене Вами значення «Логін» та «Пароль» у спеціальну пам'ятку (або інше зручне для вас місце), яка є в списку документів, і зберігайте у надійному місці протягом усієї дії договірних відносин з Державним підприємством «Українські спеціальні системи».

У разі успішного входу до електронного персонального кабінету відобразиться сторінка з привітання «Вітаємо! Якщо Ви вперше…».



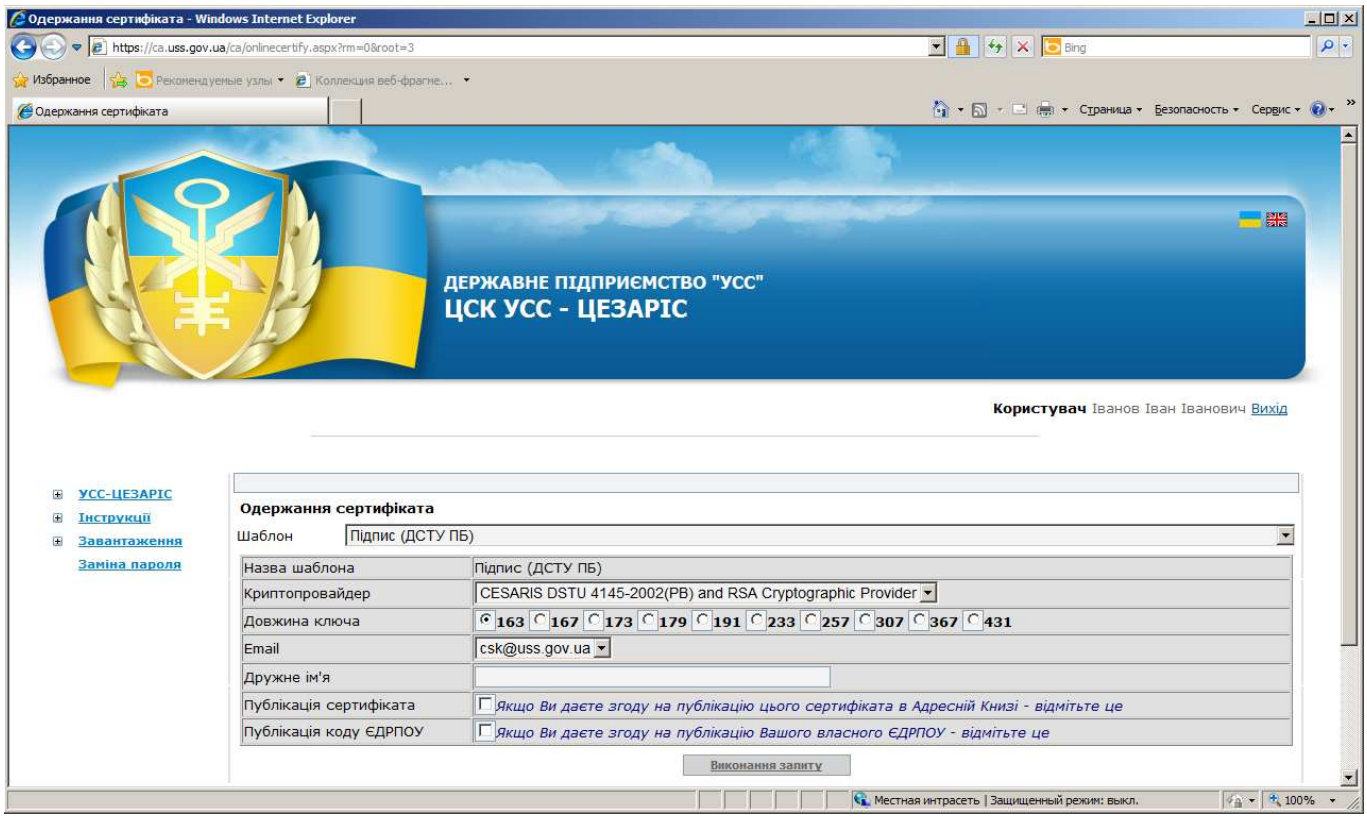
Формування запиту на сертифікацію та одержання сертифікатів

На тій же сторінці оберіть «УСС-ЦЕЗАРІС» → «ДСТУ ПБ» та перейдіть за посиланням «Одержання сертифіката».



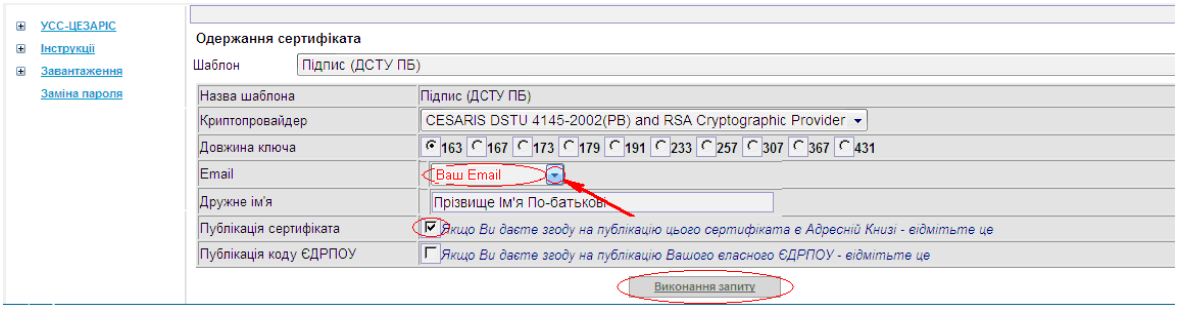
Примітка: Якщо такого посилання немає, необхідно звернутися за телефоном до Державного підприємства «Українські спеціальні системи» або відправити електронне поштове повідомлення за адресою csk@uss.gov.ua, вказавши інформацію про особу, для якої формується сертифікат, та примітку «Заблоковано шаблон сертифікату».

У формі, яка відкрилася, необхідно перевірити, щоб у позиції «Email» був зазначений достовірний адрес Вашої електронної поштової скриньки. Якщо в позиції «Email» знаходиться інша адреса, то потрібно обрати зі списку адресу Вашої електронної поштової скриньки.

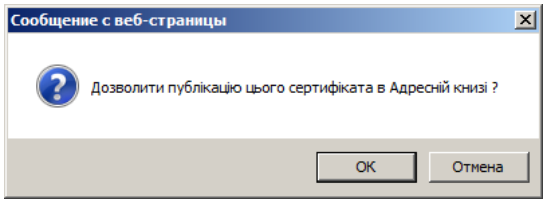


Встановити натисканням лівої кнопки миші пташку у позиції «Публікація сертифіката».

Примітка: У разі, якщо Ви бажаєте опублікувати Ваш сертифікат, який буде сформовано, на загальнодоступному Інтернет-ресурсі Центру сертифікації ключів, опублікований сертифікат буде доступний іншим Інтернет користувачам.



У вікні «Сообщение с веб-страницы» необхідно натиснути кнопку «ОК».

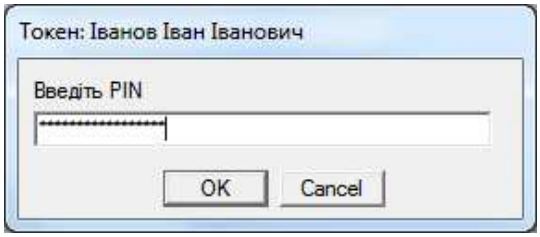


Пор. № зміни	Підпис відпов. особи	Дата внесення

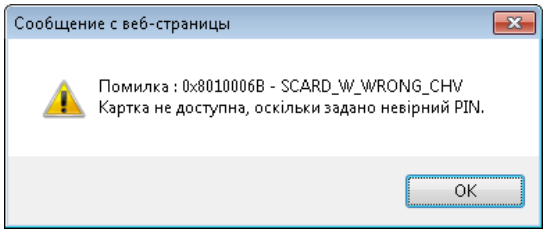
Поля «Дружне ім'я» довільні для заповнення, тобто Ви можете їх заповнювати інформацією на власний розсуд або залишити незаповненими, після чого необхідно натиснути кнопку «Виконання запиту».

Примітка: За Вашим бажанням Ви можете збільшити довжину ключа. Збільшення довжини ключа підвищує криптографічну стійкість, але, в свою чергу, вимагає більше ресурсів центрального процесора для обчислення криптографічних перетворень.

У вікні «Токен: …» введіть значення паролю, який використовувався при створенні файлового токену, та натисніть «ОК».



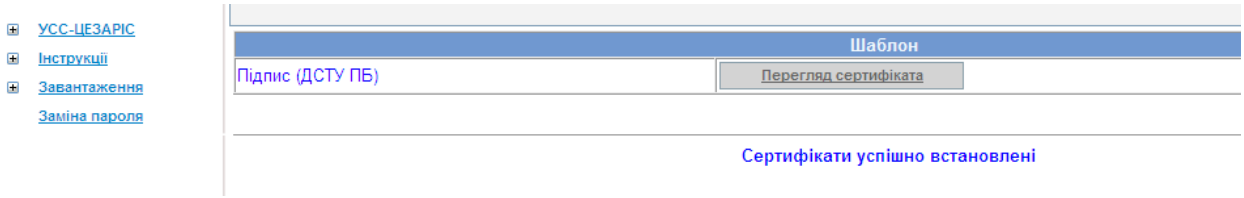
Примітка: У разі невірного введення паролю від файлового токену, система надасть Вам ще одну спробу. У разі, якщо кількість спроб буде вичерпано, з'явиться наступне повідомлення:



Примітка: Для усунення зазначеної проблеми необхідно оновити сторінку, повторно заповнити шаблон, натиснути кнопку «Виконання запиту» та вірно ввести значення пароля від файлового токену, звертаючи увагу на мовну розкладку клавіатури та на те, включений чи виключений Caps Lock.

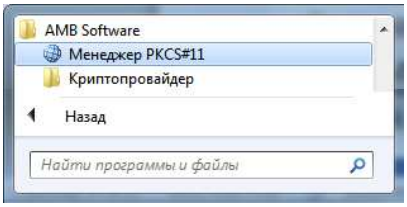
Примітка: Можлива помилка про неможливість доступу до файлового токену (потрібно закрити браузер та відкрити його знову – якщо файловий токен було створено після останнього запуску програми, то браузер не готовий до його використання).

У разі успішного введення паролю від файлового токену з'явиться інформація про успішне встановлення/отримання сертифікатів.



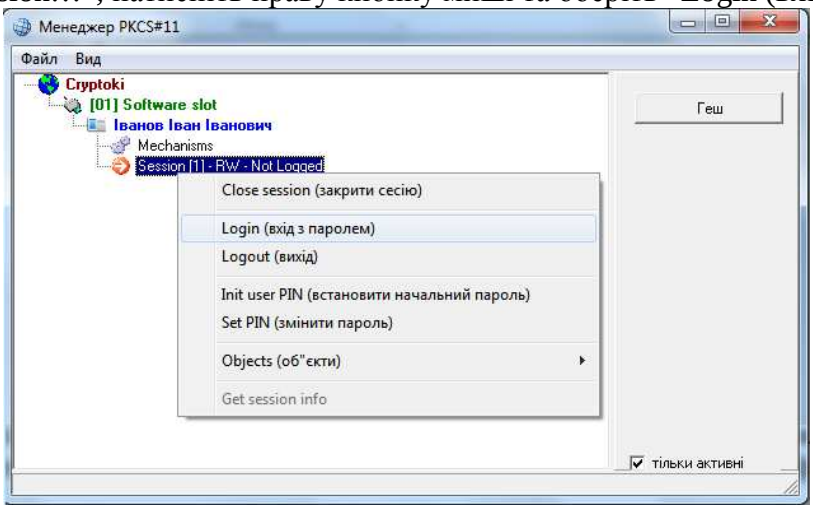
ПЕРЕВІРКА НАЯВНОСТІ КЛЮЧІВ ТА СЕРТИФІКАТІВ

Пройдіть по ланцюжку «Пуск» → «Все программы» → «AMB Software» → «Криптопровайдер» → «Менеджер PKCS#11».



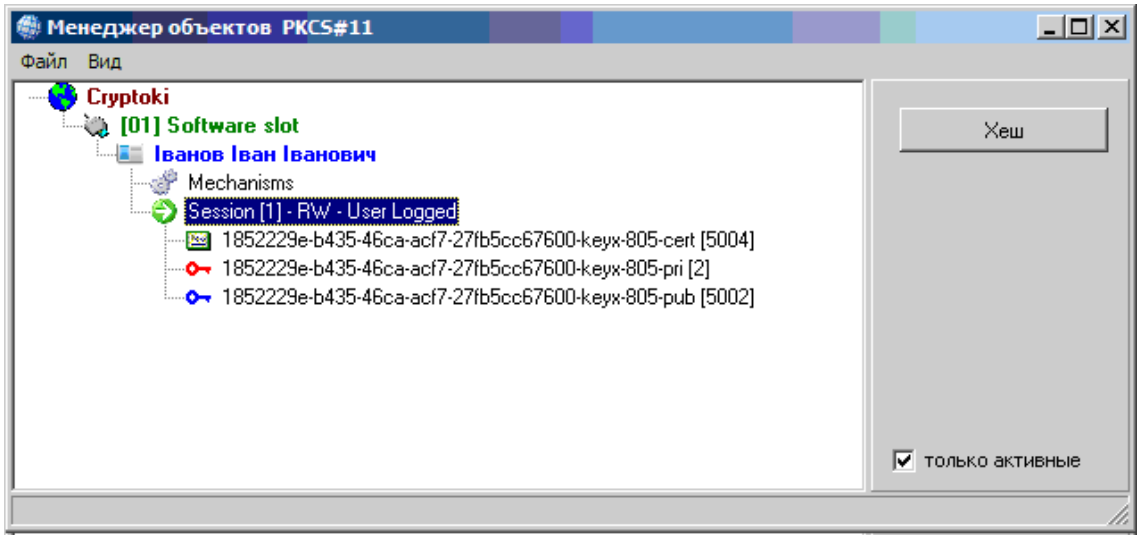
Пор. № зміни	Підпис відпов. особи	Дата внесення

Подвійним натисканням лівої кнопки миші відкрийте “Cryptoki”, оберіть свій файловий токен, виділіть “Session…”, натисніть праву кнопку миші та оберіть “Login (вхід з паролем)”



У вікні «Тип користувача» оберіть «Користувач» шляхом встановлення відповідної позначки та натисніть кнопку «ОК», після чого введіть свій власний пароль від файлового токену.

Натисніть на «Session [1]»



Сертифікат відкритого ключа ЕЦП або шифрування (КЗІ).

Закритий (особистий) ключ ЕЦП або шифрування (КЗІ).

Відкритий ключ ЕЦП або шифрування (КЗІ).

Якщо у файловому сховищі наявні закриті і відповідні їм відкриті ключі та сертифікати відкритих ключів, то це свідчить про те, що усе встановлено вірно і Ви маєте можливість здійснювати електронні правочини шляхом накладання електронного цифрового підпису.

Пор. № зміни	*Підпис відпов. особи*	*Дата внесення*

Примітка: На кожний сертифікат відкритого ключа наявна своя ключова пара. Можливий виняток: у разі, якщо під час проходження усіх зазначених вище етапів виникали помилки, то кількість особистих ключів та відповідних їм відкритих ключів буде більша за кількість сертифікатів. Перевищення кількості ніяким чином не впливає на роботу системи.

СТВОРЕННЯ РЕЗЕРВНОЇ КОПІЇ

У разі втрати файлового токену (файл: token1.dat) Ви втратите можливість здійснювати електронні правочини та накладати електронний цифровий підпис (підписувати електронні документи). За зберігання та використання файлового токену (файл: token1.dat) Ви несете персональну відповідальність. У разі втрати з тих чи інших причин файлового токену з особистими ключами та сертифікатами (файл: token1.dat) Державне підприємство «Українські спеціальні системи» не несе ніякої відповідальності та не в змозі відновити зазначений файл, тому рекомендовано створити резервну копію.

Для створення резервної копії необхідно файловий токен (файл: token1.dat) скопіювати на лазерний носій або флешку та зберігати в сейфі або в іншому надійному місці.