

Як замовити захищений апаратний носій

Захищений носій секретних ключів – надійний електронний пристрій, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на нього даних від несанкціонованого доступу, їх копіювання та використання.

Захищений носій, зазвичай, виконується у вигляді USB-пристрою, та може різнитися за модифікацією.

За допомогою програми **M.E.Doc** ви можете обрати модифікацію захищених носіїв, що пропонуються АЦСК "Україна", та сформувати необхідні документи для їх отримання.



Зверніть увагу! Для кожного особистого ключа використовується окремий носій.

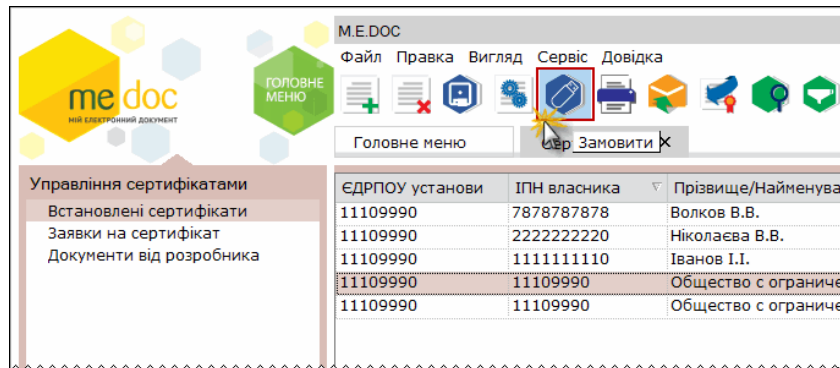
Щоб замовити захищені носії:

1. Перейдіть у розділ **Встановлені сертифікати**.

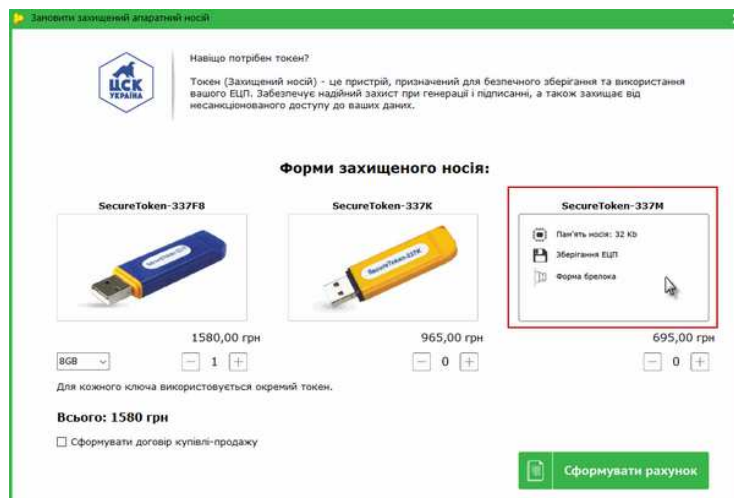
2. Скористайтесь одним із способів:



- на панелі інструментів натисніть кнопку  ;
- оберіть команду меню **Файл - Захищений носій (Token) - Замовити**;
- оберіть команду контекстного меню **Захищений носій (Token) - Замовити**;



3. Відкриється вікно **Замовити захищений апаратний носій**. У вікні наводиться зображення доступних носіїв та їх вартість. Щоб переглянути технічні характеристики, наведіть курсор миші на зображення носія:



Натисніть, щоб збільшити малюнок

4. Оберіть модифікацію захищеного носія. Для цього під описом носія вкажіть кількість, яку ви бажаєте замовити. Щоб збільшити або зменшити кількість натискайте кнопки  або .

Носій **SecureToken-337F** може використовуватись як флеш-накопичувач, при його замовленні у випадковому списку оберіть бажану ємність.

У вікні буде відображено вартість замовлення, залежно від обраної кількості носіїв та їх параметрів.

5. Якщо необхідно сформувати договір куплі продажу, встановіть відповідну відмітку у нижній частині вікна та оберіть тип вашої організації: бюджетна або госпрозрахункова.

Навіщо потрібен токен?

Токен (Захищений носій) - це пристрій, призначений для безпечного зберігання та використання вашого ЕЦП. Забезпечує надійний захист при генерації і підписанні, а також захищає від несанкціонованого доступу до ваших даних.

Форми захищеного носія:

SecureToken-337F16	SecureToken-337K	SecureToken-337M
16GB		
1640,00 грн	965,00 грн	695,00 грн
[-] 2 [+]	[-] 3 [+]	[-] 0 [+]

Для кожного ключа використовується окремий токен.

Всього: 6175 грн

☒ Сформувати договір купівлі-продажу
☐ Бюджетна організація
☐ Госп. розрахункова організація

Сформувати рахунок

Натисніть, щоб збільшити малюнок

6. Перевірте правильність замовлення та натисніть кнопку **Сформувати рахунок**.

7. У результаті обробки замовлення буде створено два документи: **PD010151** - рахунок та **PD010161** - довіреність. Якщо була встановлена відмітка **Сформувати договір куплі продажу**, додатково буде створений документ: **PD010171** - договір для госпрозрахункових організацій, або **PD010181** - договір для бюджетних організацій. Документи будуть відкриті на окремих вкладках. Перевірте дані, що були заповнені автоматично, та введіть дані у поля, що залишились незаповненими.

Товариство з обмеженою відповідальністю "АВС"
вулиця Прекрасна, буд. 10/20, корпус 30, оф. 40, ГОЛОСІВСЬКИЙ р-н,
м. КУЛІВ, М. КУЛІВ, М. КУЛІВ обл. 03185
(Підприємство-одержувач його адреса)

Ідентифікаційний код ЄДРПОУ 11109980

Банківські реквізити одержувача:
рахунок: 2800088888888888 МФО 300001
Національний банк України
(найменування банку)

Довіреність дійсна до _____ р.

ДОВІРЕНІСТЬ № _____

Дата видачі _____ р.

Видано _____
(посада, прізвище, ім'я, по батькові)

Документ, що засвідчує особу _____

Виданий _____
(нім виданий документ)

На отримання від ТОВ "ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ "УКРАЇНА"

Наступні дії: Принятка, Власності, Протокол перевірки

З питань супроводження «М.Е.ДоС» звертайтеся за телефоном: «До Розробника» - (044)206-72-10

Натисніть, щоб збільшити малюнок

Документи доступні для перегляду на редагування у розділі [Реєстр звітів](#).

8. Роздруковані та оформлені належним чином документи необхідно надати у АЦСК "Україна", або у одну з крамниць "Твій час". Отримати захищені носії ви зможете після оплати рахунку та надходження коштів за замовлення.

Заявки на сертифікати

В ЦЬОМУ РОЗДІЛІ:

- [Створення заявок на отримання нових сертифікатів](#)
- [Створення заявок на оновлення сертифікатів](#)



Адміністрування > Сертифікати > Заявки на сертифікат

Даний модуль призначений для формування заявок на отримання сертифікатів у сертифікаційному центрі АЦСК "Україна".

Формування заявки на отримання сертифікатів відкритих ключів відбувається на підставі самостійно згенерованих особистих секретних ключів керівників і установи (аналог печатки), а також для особи, яка підписуватиме Податкові накладні та Додаток № 2 до податкової накладної.

Секретні ключі не надаються до сертифікаційного центру, вони зберігаються безпосередньо у посадові особи. До АЦСК "Україна" надаються сформовані у програмному комплексі файли заявок: відправляються електронною поштою або записуються на будь-який електронний носій та надаються до центру. На основі заявок будуть сформовані відповідні сертифікати ЕЦП.



У програмі реалізована можливість оновлення користувачем існуючих сертифікатів (продовження терміну дії сертифікатів). Оновлення можливе для тих сертифікатів, до кінця терміну дії яких залишилось 45 або менше днів, та в яких не відбулось змін у даних сертифікату.

Але:

Користувач програмного комплексу **М.Е.ДоС** не може самостійно відправити електронною поштою заявки на нові сертифікати (ті, які отримуються вперше, або ж у випадку зміни посадових осіб установи). Для відправлення таких заявок електронною поштою необхідний електронний підпис адміністратора реєстрації (уповноваженого співробітника сертифікаційного центру).

За додатковими поясненнями та подальшого надання допомоги звертайтеся до представника продавця.

Для отримання нових сертифікатів

В ЦЬОМУ РОЗДІЛІ:

[Створення електронного бланку заявки на отримання нового сертифікату в АЦСК "Україна"](#)
[Генерація файлу заявки на отримання сертифікату для надання в АЦСК "Україна"](#)
[Що потрібно зробити далі?](#)
[Експорт заявок на сертифікати](#)
[Друк заявок на сертифікати](#)

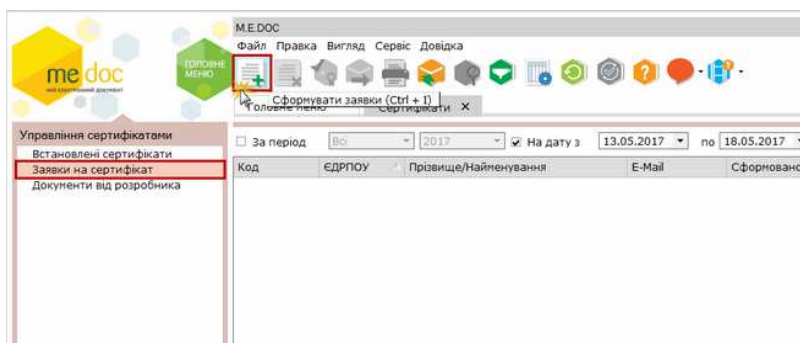
Крок 1 Створення заявки на отримання нового сертифікату



Важливо! Заявки на отримання нових сертифікатів ЕЦП створюються на підставі даних, внесених у [картку підприємства](#). Перед початком формування заявок на отримання сертифікатів переконайтесь, що [картку підприємства](#) заповнена в повному обсязі.

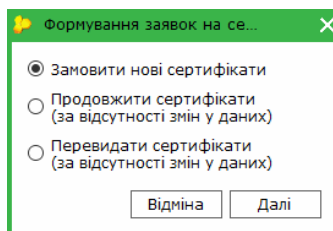
1. Для створення заявки на сертифікат скористайтесь одним із наступних способів:

- на панелі інструментів натисніть кнопку **Сформувати заявки**;
- виберіть команду **Файл/Сформувати заявки**;
- у контекстному меню оберіть команду **Сформувати заявки**;
- натисніть комбінацію клавіш **Ctrl+I**.

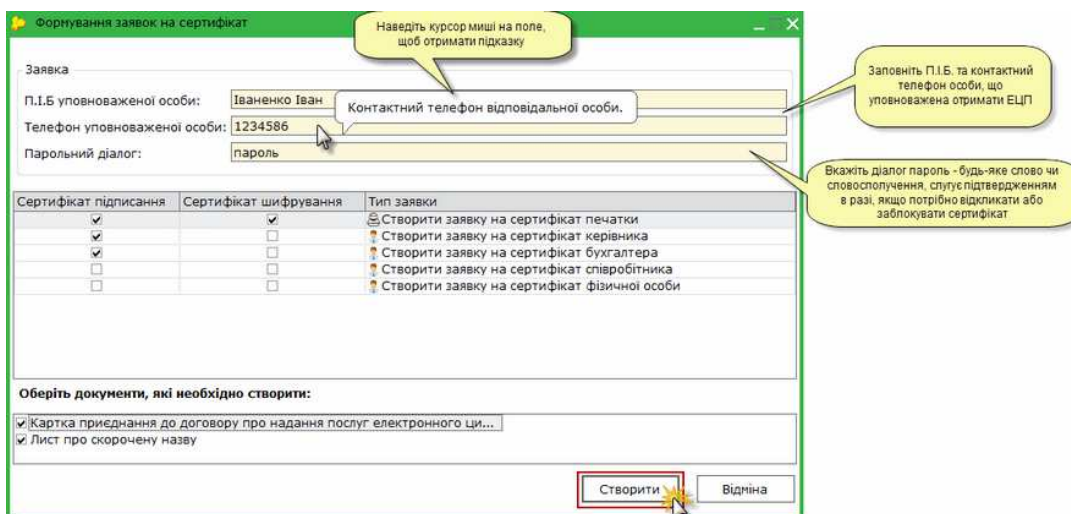


Натисніть, щоб збільшити малюнок

2. У вікні, що відкриється, встановіть опцію **Замовити нові сертифікати**. Натисніть **Далі**.



3. Відкриється вікно **Формування заявок на сертифікат** в АЦСК "Україна".



Натисніть, щоб збільшити малюнок

4. Вкажіть прізвище, ім'я та по-батькові особи, яка уповноважена отримати сертифікати для установи, та її контактний телефон. Це будь-яка особа, до якої можна звернутись в разі виникнення питань, пов'язаних з сертифікатами ЕЦП. Ці відомості автоматично додадуться в поля електронної заявки на отримання сертифікатів.

В полі **Парольний діалог** необхідно вказати діалог-пароль. Це будь-яке слово чи словосполучення слугує підтвердженням в разі, якщо потрібно відкликати або заблокувати даний сертифікат.

Далі слід вказати, які саме заявки формувати: на отримання сертифікатів підписання та сертифікатів шифрування.

Для шифрування звітності, яка відправляється в контролюючі органи, використовується сертифікат шифрування печатки установи. Відповідна галочка встановлена за замовчанням (див. малюнок).

Сертифікати шифрування інших типів використовуються для довільного підписання документів.

Сертифікати фізичної особи не використовуються в програмі **М.Е.Дос.**

Вони призначені для використання в проектах **Декларування доходів громадян, СОТА, Твій Час.**

М.Е.Дос надає лише можливість сформувати заявки на отримання цих типів сертифікатів. При виборі даного типу заявоч програма видасть попередження користувачу.

Для фізичних осіб **Заявки на сертифікат** завжди створюються в повному комплекті: Заявка на сертифікат підписання та Заявка на сертифікат шифрування.

Встановіть галочку напроти потрібних заявок і натисніть **Створити**.

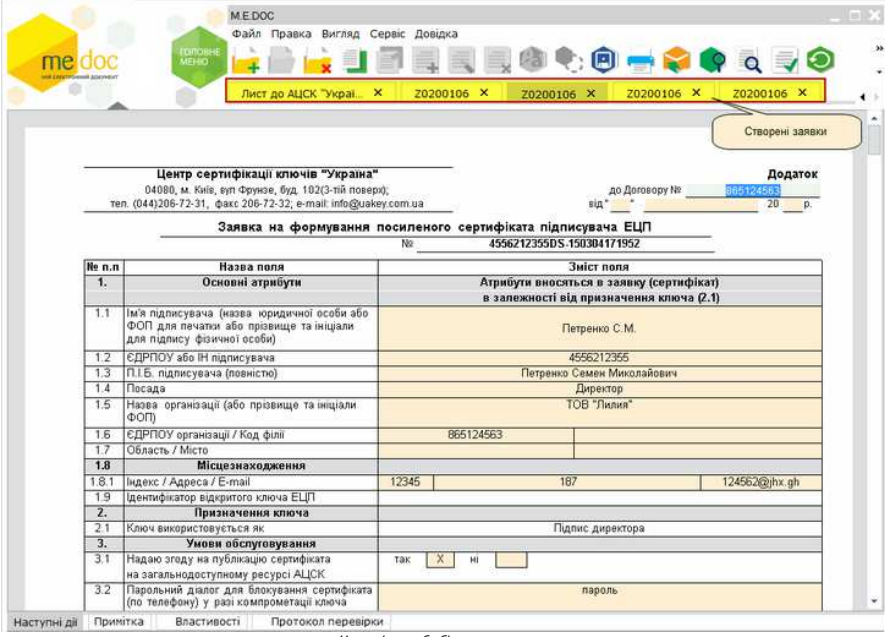
Примітка: ЕЦП співробітника - надає право певному співробітнику підприємства (окрім керівника та бухгалтера) підписувати **Податкові накладні** та **Додаток № 2** до податкової накладної

Якщо було відредаговано дані в групі **Організація**, то нові значення будуть додаватись лише у документи, що були створені після редагування.

5. Вказані на попередньому кроці заявки автоматично відкриваються в окремих закладках. (Записи сформованих заявок з'являться у таблиці на вкладці **Заявки на сертифікат**.)

Більшість полів заявок заповнюються автоматично даними із картки підприємства. Якщо у картці підприємства відсутні дані, що необхідні для заявки, заповніть ці поля вручну.

 Поля, що підсвічені жовтим кольором, доступні для заповнення та редагування.



М.Е.ДОС
Файл Правка Вигляд Сервіс Довідка

Лист до АЦСК "Україна" X Z0200106 X Z0200106 X Z0200106 X Z0200106 X

Створені заявки

Центр сертифікації ключів "Україна"
04080, м. Київ, вул. Фрунзе, буд. 102(3-тій поверх),
тел. (044)206-72-31, факс 206-72-32, e-mail: info@uakey.com.ua

Додаток
до Договору № 105124563
від " " " 20 р.

Заявка на формування посиленого сертифіката підписувача ЕЦП
№ 4556212355DS.150304171952

№ п.п.	Назва поля	Зміст поля
1.	Основні атрибути	Атрибути вносяться в заявку (сертифікат) в залежності від призначення ключа (2.1)
1.1	Ім'я підписувача (назва юридичної особи або ФОП для печатки або прізвище та ініціали для підпису фізичної особи)	Петренко С.М.
1.2	ЄДРПОУ або ІН підписувача	4556212355
1.3	П.І.Б. підписувача (повністю)	Петренко Семен Михайлович
1.4	Посада	Директор
1.5	Назва організації (або прізвище та ініціали ФОП)	ТОВ "Лілія"
1.6	ЄДРПОУ організації / Код філії	865124563
1.7	Область / Місто	
1.8	Місцезнаходження	
1.8.1	Індекс / Адреса / E-mail	12345 187 124562@lilya.gk
1.9	Ідентифікатор відкритого ключа ЕЦП	
2.	Призначення ключа	
2.1	Ключ використовується як	Підпис директора
3.	Умови обслуговування	
3.1	Надаю згоду на публікацію сертифіката на загальнодоступному ресурсі АЦСК	так ☒ ні ☐
3.2	Парольний діалог для блокування сертифіката (по телефону) у разі компрометації ключа	пароль

Наступні дії Примітка Властивості Протокол перевірки

Натисніть, щоб збільшити малюнок

Пояснення до заповнення деяких полів Заявки

- При генерації Заявки наступні поля заповнюються автоматично даними з картки підприємства:

поле 1.1 "Ім'я підписувача (назва юридичної особи або ФОП для печатки або прізвище та ініціали для підпису фізичної особи)":

- для юр. особи - в заявці на підпис директора, в заявці на підпис бухгалтера;
- для ФОП - в заявці на підпис директора, в заявці на підпис бухгалтера;
- для фіз. особи - в заявці на підпис фізичної особи.

поле 1.5 «Назва організації (або прізвище та ініціали ФОП)»:

- для ФОП - в заявці на печатку, в заявці на підпис директора, в заявці на підпис бухгалтера.

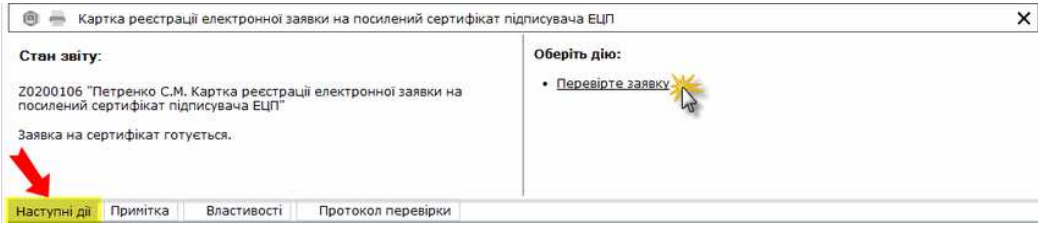


Зверніть увагу! Якщо в картці підприємства в полях **ПІБ керівника** та **ПІБ бухгалтера** 2 слова (прізвище та ім'я; ім'я та по-батькові), або більше 3, поле Заявки на сертифікат автоматично не заповнюється.

- Для ФОП в Заявці на підпис директора **поле 1.4** «Посада» не заповнюється. Поле заповнюється тільки для адвокатів та приватних нотаріусів.

- Якщо у **полі 3.1** "Надаю згоду на публікацію" вказано "Так", сертифікат ЕЦП буде опублікований на сайті АЦСК "Україна" <http://www.uakey.com.ua/>, де його можна отримати через мережу Інтернет, якщо "Ні" - сертифікат надається особисто відповідальною особою у сертифікаційному центрі.

6. На панелі стану документу виберіть закладку **Наступні дії** і натисніть **Перевірте заявку**.



Картка реєстрації електронної заявки на посилений сертифікат підписувача ЕЦП

Стан звіту:

Z0200106 "Петренко С.М. Картка реєстрації електронної заявки на посилений сертифікат підписувача ЕЦП"

Заявка на сертифікат готується.

Оберіть дію:

- Перевірте заявку

Наступні дії Примітка Властивості Протокол перевірки

Перевіряється заповнення обов'язкових полів у заявці. У випадку, якщо обов'язкові дані відсутні, система підсвітить червоним кольором поля, що необхідно заповнити.

Виправте помилки та знову виконайте перевірку.

7. Збережіть заявку, натиснувши кнопку  або комбінацію клавіш **Ctrl+S**.

Крок 2 Генерація файлу заявки на отримання сертифікату для надання в центр АЦСК "Україна"

1. Файл заявки на отримання сертифікатів, що надається в сертифікаційний центр, можна згенерувати:

- безпосередньо із бланку заявки;
- з таблиці заявок.

1.1. Щоб згенерувати заявку на отримання сертифікатів із бланку, на панелі стану документу виберіть закладку **Наступні дії** і натисніть **Згенеруйте заявку і секретний ключ**.

❗ Бланк заявки, на підставі якого генеруються файл заявки, має бути перевіреном та збереженим.

1.2. У таблиці виберіть потрібну заявку (або декілька заявок) та натисніть на панелі інструментів кнопку **Згенерувати заявки**.

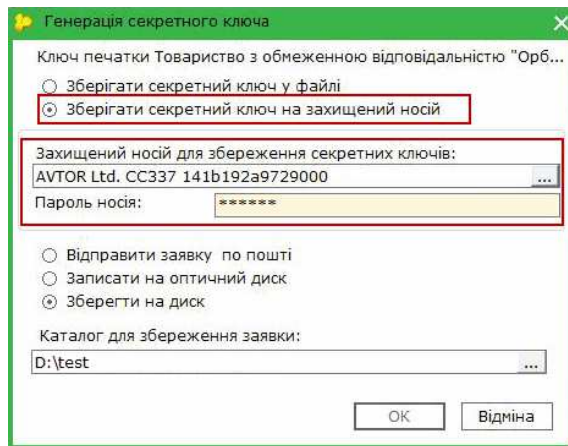
Натисніть, щоб збільшити малюнок

2. Відкриється вікно генерації файлу заявки та секретних ключів.

3. Для збереження секретного ключа на диску комп'ютера, встановіть опцію **Зберігати секретний ключ у файлі**.

У відповідні поля введіть пароль до секретного ключа та повторіть його для підтвердження правильності введення. **Зверніть увагу:** в паролі враховується регістр. Пароль повинен складатися мінімум з **3**, максимум з **64** символів та може складатися з будь-яких комбінацій букв, цифр, інших символів (' ~ ! @ # \$ % ^ & * () _ - + = { } [] \ | : ; ' < > , . ? /).

Якщо ви використовуєте для збереження секретного ключа захищений носій, під'єднайте носій до комп'ютера та встановіть опцію **Зберігати секретний ключ на захищеному носії**. У полі **Захищений носій для збереження секретних ключів** натисніть кнопку **...** та оберіть потрібний носій. У полі **Пароль носія** введіть пароль доступу до носія:



Будьте уважними! Кількість спроб вводу пароля обмежено виробником носія. У разі перевищення ліміту спроб захищений носій буде очищено.

Якщо на захищеному носії зберігається секретний ключ, виданий на інший номер ЕДРПОУ або ДРФО, та який більше не використовується, перед записом нового ключа необхідно виконати операцію [очищення захищеного носія](#).

На одному носії для певної особи (підприємства) можливо зберегти набір секретних ключів - підпис та шифрування.

Докладно про збереження секретного ключа на захищеному носії дивіться у розділі [Як зберегти секретний ключ на захищеному носії](#). Також, зберегти секретний ключ на токен можна при [перевіданні сертифікату](#).

Примітка: Якщо для генерації ключів ви одночасно обрали в таблиці кілька заявок, дії по генерації секретного ключа потрібно буде виконати для кожної заявки (сертифікату) окремо.

Якщо ви зберігаєте ключи на захищеному носії, перед генерацією наступного ключа необхідно підключити до комп'ютера відповідний носій.

Поради щодо створення надійних паролів

Пароль повинен бути відомим лише підписувачу, його потрібно запам'ятати та додатково подбати про захист!

Щоб забезпечити безпеку вашого цифрового підпису, рекомендується завжди використовувати надійні паролі. Якщо адміністратор встановив [використання посиленого захисту ЕЦП](#), то у вікні відобразяться вимоги до пароля в залежності від встановлених налаштувань (мінімальна довжина та/або складність пароля).

Пароль повинен відповідати трьом основним вимогам:

- він повинен бути відомий тільки вам;
- вам повинно бути легко його згадати;
- його має бути складно підібрати.

- Складайте пароль як мінімум з восьми знаків.
- Не використовуйте в якості пароля загальновідомі дані - ім'я, день народження, номер паспорта або назви компанії.
- Використовуйте в паролі одночасно букви верхнього і нижнього регістрів, цифри, символи, пробіли.

Ніколи і ні за яких обставин нікому не повідомляйте свій пароль! Якщо все ж таки потрібно записати пароль, щоб не забути, переконайтесь, що він зберігається в надійному місці і не позначається фразами як «мій пароль».

5. Оберіть спосіб у який будуть збережені файли секретних ключів та заявок. Файли заявок необхідні для подальшого подання їх до сертифікаційного центру для отримання сертифікатів

- **записати на оптичний диск** - згенеровані секретні ключі записуються на оптичний диск, а файли заявок зберігаються у вказаний каталог. Даний варіант радимо використовувати, якщо секретні ключі генеруються на чужому комп'ютері. При записі ключів одразу на диск досягається максимальна їх захищеність, тобто виключається можливість відновлення видалених файлів. У разі збереження секретних ключів на захищеному носії на диск записуються лише файли заявок.
- **зберегти на диск** - в указаний каталог зберігаються, як файли секретних ключів, так і файли заявок.



Користувач програмного комплексу **М.Е.Doc** не може самостійно відправити заявку на отримання нового сертифікату електронною поштою. Для відправлення заявки електронною поштою необхідний електронний підпис адміністратора реєстрації (вповноваженого співробітника сертифікаційного центру). За додатковими поясненнями та подальшого надання допомоги зверніться до представника продавця.

6. Далі вкажіть шлях до каталогу для збереження файлів заявки та секретного ключа. Якщо ж ви обрали збереження секретного ключа на захищеному носії, у обраному каталозі збережено лише файл заявки. Підтвердьте вибір, натиснувши кнопку **ОК**.

Якщо у програмі ведеться звітність декількох установ, рекомендується в указаному каталозі створити папки для кожної установи, що містять у назві код ЕДРПОУ.

Примітка: Можна також записати ключі всіх установ в один каталог, але додатково подбати про захист інформації. Відповідальність за збереження інформації в обох випадках покладається на заявника.

Таким чином, якщо в програмі ведеться звітність декількох установ, при переході до іншої установи, не потрібно кожного разу обирати каталог з секретними ключами.

Якщо Ви обрали запис секретних ключів на оптичний диск

Після того, як Ви обрали **Записати на оптичний диск** та натиснули кнопку **ОК**, система розпочне пошук оптичного приводу для запису дисків, а також наявного в ньому оптичного диску. Відкриється вікно **Запис на оптичний диск**, що містить інформацію про доступний пристрій та інформацію про диск.

У вікні повідомлення натисніть **ОК** для того, щоб розпочати запис на диск.

Результатом буде записаний на оптичний диск секретний ключ та створений файл заявки, збережений за вказаним шляхом, про що система оповістить користувача.

Під час запису диск не фіналізується. При повторному записі дані з диску не видаляються, а дозаписуються.

Якщо у Вас Windows XP

В операційній системі Windows XP можуть бути відсутні необхідні для виконання запису бібліотеки.

Порада: в разі отримання попередження про відсутність бібліотек зверніться до вашого системного адміністратора.

У вікні повідомлення натисніть **ТАК** для переходу за посиланням <http://support.microsoft.com/kb/932716> та виконайте вказані на сайті настанови.

Після встановлення компонентів виконайте запис на оптичний диск.

7. Результатом генерації буде створення файлів заявки та секретного ключа і збереження їх за вказаним шляхом, про що система оповістить користувача. Якщо ви обрали зберегти секретного ключа на захищеному носії, секретний ключ записується на обраний носій.

Розширення в назвах файлів особистих ключів, заявок та сертифікатів мають спеціальне призначення і змінювати їх не можна.

Нижче наведені формати розширень файлів та пояснення до них:

***.zs2** – особистий (секретний) ключ цифрового підпису в АЦСК "Україна".

Файли з таким розширенням до сертифікаційного центру не надаються, вони зберігаються безпосередньо у посадові особи. Потрібно додатково подбати про захист цієї інформації.

Відповідальність за збереження секретних ключів та паролів до них покладається на заявника;

***.рск** – файл, який містить електронну заявку на отримання сертифікату відкритого ключа цифрового підпису в сертифікаційному центрі "Україна" та Картку реєстрації електронної заявки на посилений сертифікат підписувача ЕЦП.

Файли з таким розширенням надаються до сертифікаційного центру на зовнішньому електронному носії.

Картка реєстрації електронної заявки поміщається також і у **Реєстр звітів** у тому звітному періоді, коли у програмі формувалась заявка, її **потрібно роздрукувати, підписати та поставити мокру печатку установи.**

Важливо! Роздрукувати заявку на отримання сертифікату ЕЦП можна тільки після генерації секретного ключа.

Що потрібно зробити далі?

1. Скопіювати на будь який зовнішній електронний носій файли заявок (файли з розширенням ***.рск**) для подання в АЦСК "Україна".

❗ Файли секретних ключів (***.zs2**) залишаються у заявника. Потрібно додатково подбати про захист цієї інформації (скопіювати її вміст на інший носій: CD-диск, флеш-диск, в інший каталог). **Відповідальність за збереження секретних ключів та паролів до них покладається на заявника!**

❗ У випадку пошкодження секретного ключа необхідно отримати новий сертифікат (тобто сплатити рахунок, повторно згенерувати цей ключ та надати до сертифікаційного центру заявку на сертифікат).

2. Ознайомитись із порядком отримання сертифікатів ЕЦП на сайті АЦСК "Україна" <http://www.uakey.com.ua/>. Підготувати комплект документів.

3. Роздрукувати, підписати та завірити печаткою установи Картки реєстрації електронних заявок.

4. Надати всі документи в АЦСК "Україна".

Експорт заявок на сертифікати

У випадку втрати файлу заявки (файли з розширенням ***.рск**) передбачена можливість його експорту.

Зверніть увагу! Експортуються лише згенеровані заявки на сертифікат.

1. Виділіть файл заявки, який необхідно вивантажити.

2. У меню **Файл** оберіть команду **Експорт/Експорт**, або у контекстному меню оберіть команду **Експорт**

3. Відкриється вікно **Експорт**. Вкажіть шлях для збереження файлу та натисніть кнопку **ОК**.

Друк заявок на сертифікати

1. Виділіть файл заявки, який необхідно друкувати.

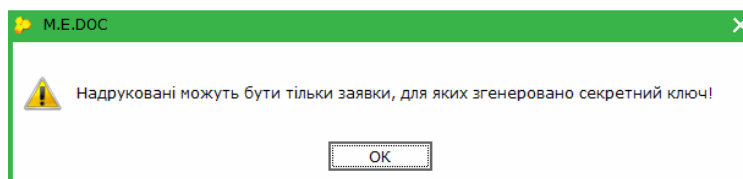
2. Оберіть один з способів:

- оберіть команду меню **Файл/Друк**;
- з контекстного меню оберіть команду **Друк**;
- натисніть комбінацію клавіш **Ctrl+P**.

3. Відкриється вікно налаштування друку. Вкажіть необхідні параметри та натисніть кнопку **Печать**.

Також друк можливий з вікна відкритого документу по команді меню **Файл/Друк**.

Зверніть увагу! Друкуються лише згенеровані заявки на сертифікат. При спробі друкувати незгенеровану заявку, виводиться вікно попередження:



Після попередження функція друку стає недоступною.

Для продовження сертифікатів користувачем

В ЦЬОМУ РОЗДІЛІ:

- [Коли можливе оновлення сертифікатів](#)
- [Виклик функції продовження сертифікатів](#)
- [Автоматичне створення електронних заявок на оновлення сертифікатів](#)
- [Отримання сертифікату із сайту АЦСК "Україна"](#)
- [Доопрацювання заявок у разі скасування автоматичного створення](#)

Функція автоматичного оновлення сертифікатів дозволяє користувачу самостійно продовжити термін дії існуючих сертифікатів. Оновлення виконується шляхом створення заявок на основі чинних сертифікатів. Автоматичне оновлення сертифікатів можливе за умови, що в базі даних АЦСК присутні документи на ці сертифікати.

Функція оновлення доступна для сертифікатів АЦСК, робота з якими [підтримується у програмі](#), та до кінця терміну дії яких залишилось 45 або менше днів.

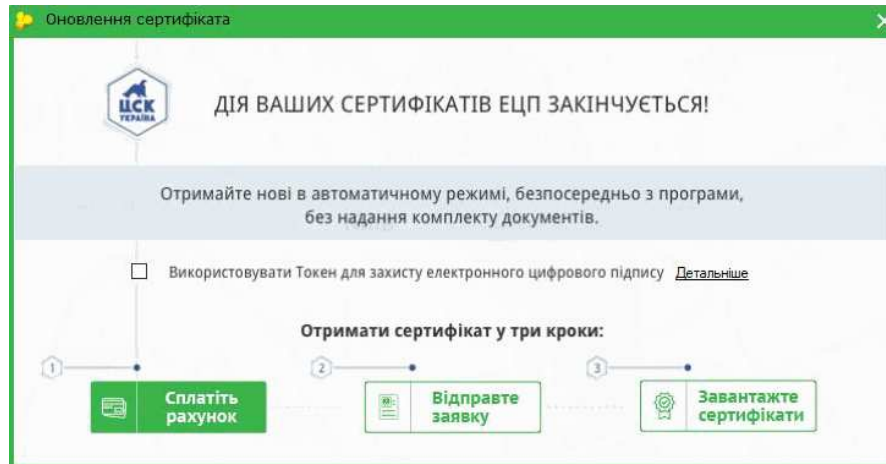
Продовження можливе для сертифікатів, [налаштованих у комплекті підписів](#), за відсутності змін у даних, які вносяться у сертифікати (ПІБ, адреса, назва організації тощо).

Якщо комплект підписів не налаштований, програма запропонує оновити завантажені сертифікати, що відповідають вказаним вище умовам.

Перевірка можливості оновлення (продовження терміну дії) сертифікатів

При вході в програму виконується перевірка можливості оновлення сертифікатів, що передбачає:

- перевірку наявності сертифікатів у комплекті підписів (налаштованих у [Параметрах системи > Підпис](#));
- якщо такі сертифікати знайдені, перевіряється їх термін дії (якщо комплект підписів не налаштований, перевіряється термін дії всіх завантажених сертифікатів). Якщо до кінця терміну дії залишилось 45 або менше днів, виконується наступний етап;
- за реєстраційним номером ДРФО посадових осіб із сертифікатів та ЄДРПОУ установи формується запит до АЦСК щодо наявності документів на чинні сертифікати;
- за позитивним результатом цієї перевірки програма запропонує користувачу оновити сертифікати:



У вікні ви можете виконати наступні операції:

Сформувати та оплатити рахунок

Натисніть кнопку **Сплатити рахунок** - відкриється вікно формування рахунку на продовження терміну дії сертифікатів:

Тип	Кількість
☒ Печатка підприємства	1
☒ Директор	2
☐ Бухгалтер	
☐ Співробітник	
Загальна кількість: 2	
СУМА: 349 грн.	
Термін дії: 2 роки (+ комісія 2.75%)	

Встановіть відмітки біля назв сертифікатів, які необхідно продовжити, та оберіть кількість сертифікатів.

Залежно від обраних параметрів у вікні відображається сума, яку необхідно сплатити за послугу.

Оберіть форму оплати та натисніть кнопку **ОК**:

- **Сформувати рахунок** - сформувати рахунок на оплату послуги, програма сформує рахунок-фактуру **PD010120** на сплату послуг, що може бути оплачений у будь-якій банківській установі;
- **Оплата онлайн** - оплатити послуги за допомогою платіжної системи онлайн, відкриється вікно платіжної системи, у якому вкажіть необхідні реквізити та виконайте оплату дотримуючись вказівок платіжної системи.

Створити та відправити заяву на продовження сертифікатів

Натисніть кнопку **Відправте заяву**. Запуститься [Майстер оновлення сертифікатів](#) та розпочнеться формування заявки. (Опція **Використовувати Токен для захисту електронного цифрового підпису** не встановлена).

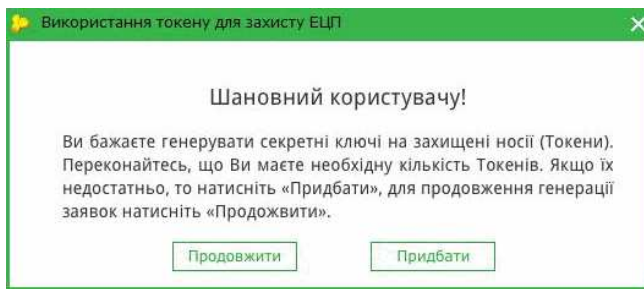
Завантажити оновлені сертифікати

Після оплати рахунку та опрацювання заявок адміністратором реєстрації отримаєте оновлені сертифікати та [завантажте](#) їх у програму.

Замовити захищений носій для зберігання сертифікатів ЕЦП

Дізнатися подробиці про замовлення та отримання захищених носіїв можна, натиснувши посилання [Детальніше](#).

Встановіть опцію **Використовувати Токен для захисту електронного цифрового підпису** та натисніть кнопку **Відправити заявку**. У вікні **Використання токена для захисту ЕЦП** натисніть **Придбати**:



Далі, [оберіть модифікацію токена та виконайте замовлення](#).

Якщо ви бажаєте відкласти замовлення захищених носіїв, у вікні **Використання токена для захисту ЕЦП** натисніть **Продовжити**. Запуститься [Майстер оновлення сертифікатів](#) розпочнеться формування заявок.

Сформувати рахунок та документи, що необхідні для отримання токенів, також можна у розділі [Адміністрування - Сертифікати](#). Про збереження секретного ключа на токени дивіться у розділі [Зберегти секретний ключ на захищеному носії](#).

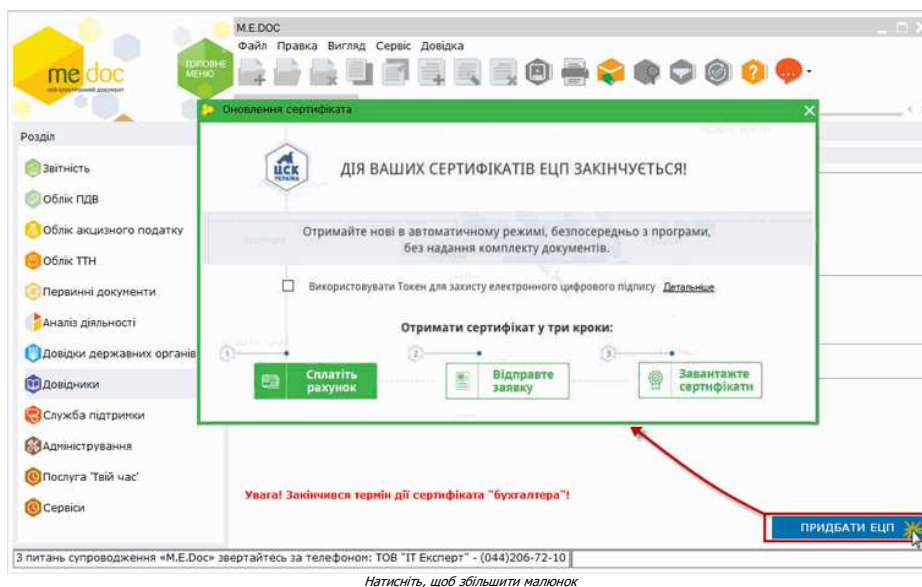


Оновлення сертифікатів можливе лише у випадку, якщо не відбулось змін у даних, внесених у сертифікат!

[До початку](#)

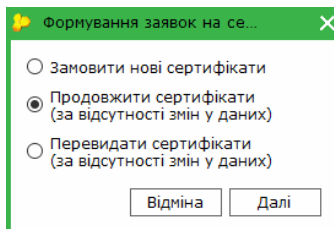
Виклик функції продовження сертифікатів

Якщо сертифікати відповідають [умовам](#), що необхідні для оновлення, ви можете оновити (продовжити термін дії) сертифікатів, натиснувши кнопку **Придбати ЕЦП** у головному програмі:



Майстер оновлення сертифікатів відкривається по натисканню кнопки **Відправте заявку** у вікні **Оновлення сертифіката**.

Також пропозиція щодо оновлення сертифікатів відображається в модулі **Сертифікати** при спробі користувача створити заявки:



- **Замовити нові сертифікати** - викликає вікно [створення заявок](#) на формування нових сертифікатів ЕЦП.
- **Продовжити сертифікати (за відсутності змін у даних)** - запускає [Майстер оновлення сертифікатів](#), який покроково допоможе сформувати рахунок-фактуру та заявку на оновлення, відправити їх в АЦСК, а після формування сертифікатів АЦСК Україна - завантажити їх у програму.
- **Перевидати сертифікати (за відсутності змін у даних)** - створюється сертифікат ідентичний існуючому. У перевиданому сертифікаті змінюється лише дата початку дії сертифікату - дата початку дії замінюється датою перевидачі сертифіката. Деталі у розділі [Перевидача сертифікату](#).

Автоматичне створення електронних заявок на оновлення сертифікатів

У першому вікні **Майстра** виводиться список сертифікатів, які можливо оновити:

Оновіть сертифікати ЕЦП у «М.Е.Доc» - без візиту до офісу з пакетом документів!

Увага! Якщо у Вас відбулись зміни реєстраційних даних (ПІБ, адреса, назва тощо), після оплати рахунку зверніться до найближчої крамниці «Твій час» з пакетом документів. Якщо Ви не сплатили рахунок – зробіть це.

Перевірте актуальність адреси електронної пошти та відредагуйте за необхідності.

Заявка

П.І.Б. уповноваженої особи:

Телефон уповноваженої особи:

Парольний діалог:

☒	ЄДРПОУ/ІПН	ПІБ/Найменування	Діє до	Призначення	Електронна пошта	Тип	Поч
☒	1122334455	Вовченко А.Б.	30.05.2017	Підписання	mail@gmail.com	Підпис бухг...	12.0
☒	1133557799	Зайчук О.К.	30.05.2017	Підписання	mail@gmail.com	Підпис дире...	12.0
☐	1133557799	Капітошка	30.05.2017	Підписання	mail@gmail.com	Підпис співр...	12.0
☐	27051003	ТОВ "Капітошка-сер...	30.05.2017	Підписання	mail@gmail.com	Печатка ус...	12.0
☐	1122334455	Вовченко А.Б.	30.05.2017	Шифрування	hgfk	Підпис бухг...	12.0
☒	1133557799	Зайчук О.К.	30.05.2017	Шифрування	11@gmail.com	Підпис дире...	12.0
☐	1133557799	Капітошка	30.05.2017	Шифрування	11@gmail.com	Підпис співр...	12.0
☐	27051003	ТОВ "Капітошка-сер...	30.05.2017	Шифрування	11@gmail.com	Печатка ус...	12.0

Термін: **2 роки** Сума до сплати: 349 грн.

☒ Надаю згоду на публікацію сертифікатів на загальнодоступному ресурсі АЦСК

1. Заповніть обов'язкові поля заявки (позначені жовтим кольором), використовуючи [довідкову інформацію попереднього розділу](#). В полі **Парольний діалог** вкажіть діалог-пароль. Це слово чи словосполучення, яке слугує підтвердженням в разі, якщо потрібно заблокувати даний сертифікат.



Дати початку та закінчення терміну дії сертифікатів будуть автоматично перенесені у заявку на формування сертифікатів. За замовчуванням, встановлений термін 2 роки.



Якщо оновлюється сертифікат підписання, програма автоматично запропонує створити заявку на оновлення сертифікату шифрування (позначка у рядку сертифіката шифрування встановлюється автоматично). Але ви можете створити заявку на оновлення лише сертифікату підписання або лише сертифікату шифрування, видаливши відповідну позначку вручну.

Щоб сертифікати були доступні для завантаження, встановіть позначку **Надаю згоду на публікацію сертифікатів на загальнодоступному ресурсі АЦСК**. Сертифікат опублікований на сайті АЦСК "Україна" <http://www.uakey.com.ua/>, де його можна отримати через мережу Інтернет. Опубліковані сертифікати можуть бути завантажені за допомогою автоматичної перевірки змінення статусів сертифікатів.



Якщо ви бажаєте отримати рахунок на продовження терміну дії сертифікатів, натисніть кнопку **Отримати рахунок** - відкриється вікно формування рахунку. Поля вікна заповнюються автоматично, відповідно до даних, введених у вікні **Сертифікати для продовження**. Залежно від обраних параметрів у вікні відображається сума, яку необхідно сплатити за послугу. Перевірте, чи правильно заповнені поля, оберіть форму оплати та натисніть кнопку **ОК**.

Зверніть увагу! По натисканню кнопки **Отримати рахунок** формування заявки на продовження сертифікатів відміняється.

2. Перевірте та підтвердіть вибрані дані для переходу до наступного кроку. Натисніть кнопку **Далі**.

Якщо ви відмовились від публікації сертифікатів на ресурсі АЦСК, відкриється вікно повідомлення:

M.E.DOC

Ви дійсно бажаєте відмовитись від публікації сертифікатів на загальнодоступному ресурсі АЦСК?

Щоб продовжити формування заявки, натисніть **Так**.

3. Відкриється вікно **Генерація секретного ключа...** У заголовку вікна відображено порядковий номер сертифікату та загальна кількість сертифікатів, що повинні бути опрацьовані:

Якщо ви зберігаєте секретні ключі на диску комп'ютера, встановіть позначку **Зберегти секретний ключ у файл**. У відповідні поля введіть пароль до секретного ключа та повторіть для підтвердження правильності введення.

Якщо ви використовуєте для збереження секретного ключа захищений носій, під'єднайте носій до комп'ютера та встановіть опцію **Зберігати секретний ключ на захищеному носії**. У полі **Захищений носій для збереження секретних ключів** натисніть кнопку та оберіть потрібний носій. У полі **Пароль носія** введіть пароль доступу до носія:

Будьте уважними! Кількість спроб вводу пароля обмежено виробником носія. У разі перевищення ліміту спроб захищений носій буде очищено.

Якщо на захищеному носії зберігається секретний ключ, виданий на інший номер ЕДРПОУ або ДРФО, та який більше не використовується, перед записом нового ключа необхідно виконати операцію [очищення захищеного носія](#).

На одному носії для певної особи (підприємства) можливо зберегти набір секретних ключів - підпис та шифрування.

Докладно про збереження секретного ключа на захищеному носії дивіться у розділі [Як зберегти секретний ключ на захищеному носії](#). Також, зберегти секретний ключ на токени можна при [перевіданні сертифікату](#).

4. Оберіть каталог на комп'ютері, в який будуть записані файл заявки та файли секретних ключів.

5. Результатом генерації буде створення файлу секретного ключа. Файл ключа буде збережений за вказаним шляхом, про що система оповістить користувача:

Якщо ви обрали збереження секретного ключа на захищеному носії, секретний ключ записується на обраний носій. За вказаним шляхом буде збережено лише файл заявки.

Будьте уважні! Секретний ключ використовується для підпису звітності, тому подбайте про його безпеку. Для продовження натисніть **ОК**.

6. Запуститься процедура підпису заявки. Введіть пароль секретного ключа. Кожна заявка **підписується ключем сертифікату, який оновлюється**.

Підпис

Тип підпису: Співробітник

Вибраний сертифікат

ЄДРПОУ: 32323322 ДРФО: 1111111111

Діє з: 20.12.2016 Діє по: 19.12.2017

Видавець: АЦСК ТОВ "Центр сертифікації ключів "Україна" ПІБ: Кириленко О.І.

Каталог з секретними ключами: Z:\kvn\Заявки

Пароль секретного ключа: *** ☐ Зберігати пароль протягом сеансу

OK Відміна

Операції, описані у пунктах 3 - 6, будуть автоматично повторені для всіх обраних сертифікатів. Якщо ви зберігаєте ключи на захищеному носії, перед генерацією наступного ключа необхідно підключити до комп'ютера відповідний носій.

7. Відправте заявку на адресу сервера АЦСК Україна, який буде запропоновано програмою:

Вибір адресата

Найменування	Дата закінчення дії сертифіката
Документи АЦСК "Україна"	17.07.2018

OK Відмінити

8. Якщо оплата не здійснювалась, або кошти ще не надійшли до АЦСК, відкриється вікно, у якому оберіть форму оплати послуги:

Форма оплати

☐ Оплата онлайн (+ комісія 2.75%)

☐ Сформувати рахунок

☐ Оплату вже здійснено

OK

- Оплата онлайн** - оплатити послуги за допомогою платіжної системи онлайн, відкриється вікно платіжної системи, у якому вкажіть необхідні реквізити та виконайте оплату, дотримуючись вказівок платіжної системи;
- Сформувати рахунок** - сформувати рахунок на оплату послуги, програма сформує рахунок-фактуру **PD010120** на сплату послуг, що може бути оплачений у будь-якій банківській установі;
- Оплату вже здійснено** - оплату здійснено, але кошти ще не надійшли у АЦСК, заявка буде опрацьована після надходження коштів.

Натисніть **OK**.

9. Якщо оновлення сертифікатів було заздалегідь оплачене, та кошти надійшли до АЦСК, відкриється вікно повідомлення про успішне відправлення заявки:

M.E.DOC

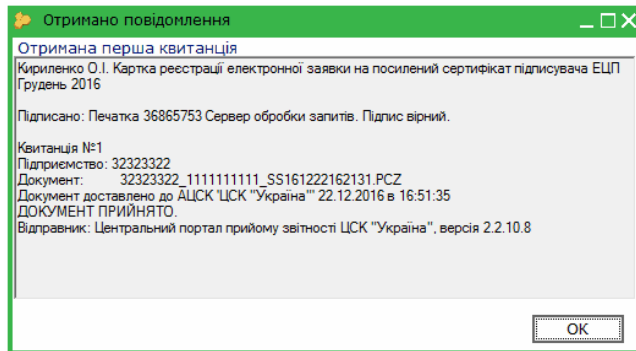
Вітаємо! Ви успішно відправили заявки. Очікуйте генерацію сертифікатів

OK

Зверніть увагу! Обробка заявки виконується після надходження оплати.

Отримання сертифікату із сайту АЦСК "Україна"

Після обробки заявок на шлюзі АЦСК Україна при перевірці поштових повідомлень надійде **квитанція № 1** з результатом прийняття/відхилення заявки, наприклад:



Причиною ж відхилення заявки може бути відсутність на шлюзі попередньої заявки на сертифікат, або ж випадок, коли заявка підписана некоректним ЕЦП.

Прийняті по першій квитанції заявки оброблюються адміністратором реєстрації. Результатом успішної обробки буде фінальна **квитанція № 2 "Документ прийнято"**.

 **Квитанція № 2** може містити й негативну відповідь з повідомленням про відхилення заявки адміністратором. У такому разі квитанція містить причину відхилення, вказану адміністратором реєстрації.

Якщо заявка успішно оброблена, користувач отримав **позитивну квитанцію № 2**, у модулі **Сертифікати > Заявки на сертифікат** стає доступною опція отримання сертифікату із сайту АЦСК.

Завантажте оновлені сертифікати одним із способів:

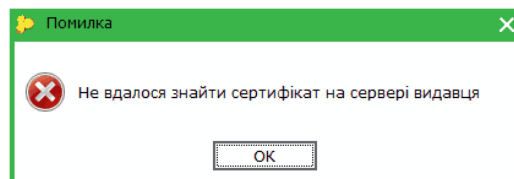
- вкладка **Наступні дії > Запит сертифікату**;
- меню **Правка > Запит сертифікату**;
- із контекстного меню > **Запит сертифікату**.

Якщо сертифікат сформований, він завантажується у базу даних програми та відображатиметься у модулі, про що буде сповіщено:



Натисніть, щоб збільшити малюнок

Якщо ж сертифікат не буде знайдено на сервері АЦСК, користувач отримає повідомлення:



Доопрацювання заявок у разі скасування автоматичного створення

У будь-який момент ви можете відмовитись від продовження автоматичного створення заявок на сертифікат.

Програма створить бланки заявок (**20200107**) на оновлення сертифікатів, що доступні у розділі **Заявки на сертифікат**.

 Заявка на оновлення буде створена на основі даних із сертифікату, який оновлюється. Ці дані недоступні для зміни. Якщо секретний ключ ще не згенеровано, ви можете виправити лише значення полів, що позначені жовтим кольором.

Ви можете доопрацювати створені заявки звичайним чином (за допомогою команд вкладки **Наступні дії**):

me.doc ГОЛОВНЕ МЕНЮ

Файл Правка Вигляд Сервіс Довідка

Головне меню Сертифікати X 20200107 X

Центр сертифікації ключів "Україна"
04080, м. Київ, вул. Кирилівська, 102;
тел. (044)206-72-31, факс 206-72-32, e-mail: info@uaakey.com.ua

Додаток
до Договору № 27051003
від " " " 20 " р.

Заявка на формування посиленого сертифіката підписувача ЕЦП
№ 27051003С-170515120134

№ п.п.	Назва поля	Зміст поля
1.	Основні атрибути	Атрибути вносяться в заявку (сертифікат) в залежності від призначення ключа (2.1)
1.1	Ім'я підписувача (назва юридичної особи або ФОП для печатки або прізвище та ініціали для підпису фізичної особи)	Тест
1.2	ЄДРПОУ або ІП підписувача	27051003
1.3	П.І.Б. підписувача (повністю)	
1.4	Посада	
1.5	Назва організації (або прізвище та ініціали ФОП)	Тест
1.6	ЄДРПОУ організації / Код філії	27051003
1.7	Область / Місто	ЗАКАРПАТСЬКА село БАРИ
1.8	Місцезнаходження	
1.8.1	Індекс / Адреса / E-mail	12345 набережна Найграща, буд. 9 potrivayev@intelserv.com
1.9	Ідентифікатор відкритого ключа ЕЦП	
2.	Призначення ключа	
2.1	Ключ використовується як:	Ключ шифрування печатки
3.	Умови обслуговування	
3.1	Надаю згоду на публікацію сертифіката на загальнодоступному ресурсі АЦСК:	так ☒ ні ☐
3.2	Парольний діалог для блокування сертифіката (по телефону) у разі компрометації ключа	пароль
3.3	Дата початку терміну дії сертифіката	15.05.2017
3.4	Дата закінчення терміну дії сертифіката	15.05.2019

Тест Картка реєстрації електронної заявки на посилений сертифікат підписувача ЕЦП

Стан заявки:
20200107 "Тест Картка реєстрації електронної заявки на посилений сертифікат підписувача ЕЦП"
Заявка на сертифікат не містить помилок.

Оберіть дію:
Згенерувати заявку і секретний ключ або змінити та Перевірте заявку

Наступні дії: Принятка Властивості Протокол перевірки

3 питань супроводження «М.Е.Доc» звертайтесь за телефоном: «До Розробника» - (044)206-72-15

59%

Натисніть, щоб збільшити малюнок

Доступні команди визначаються етапом, на якому було зупинено автоматичне формування заявки.

Після підписання заявки на панелі стану документа стає доступною функція **Відправити заявку на сервер ЦСК**:

Кириленко О.І. Картка реєстрації електронної заявки на посилений сертифікат підписувача ЕЦП

Стан звіту:
20200107 "Кириленко О.І. Картка реєстрації електронної заявки на посилений сертифікат підписувача ЕЦП"

Оберіть дію:
Відправити заявку на сервер ЦСК.

Наступні дії: Принятка Властивості Вкладені документи Протокол перевірки

Натисніть, щоб збільшити малюнок



Зверніть увагу! Експорт, импорт та копіювання заявок на оновлення сертифікатів (20200107) НЕМОЖЛИВЕ.

[До початку](#)

Перевидача сертифікату



За допомогою перевидачі створюється сертифікат ідентичний існуючому. У перевиданому сертифікаті змінюється лише дата початку дії сертифікату - дата початку дії замінюється датою перевидачі сертифіката. Функція доступна лише для сертифікатів, що не підпадають під [умови продовження терміну дії](#).

Цей спосіб буде зручним у випадку, коли на захищеному носії необхідно зберегти секретний ключ існуючого сертифіката, термін дії якого ще не скінчився.

1. Перейдіть у розділ **Адміністрування - Сертифікати - Заявки на сертифікат**.

2. Скористайтесь одним із наступних способів:

- натисніть кнопку панелі інструментів
- виберіть команду контекстного меню **Файл - Сформувати заявку**.

3. У вікні, що відкриється на виконання команди, встановіть опцію **Перевидати сертифікати (за відсутності змін у даних)**:

Формування заявок на се...

☐ Замовити нові сертифікати

☐ Продовжити сертифікати (за відсутності змін у даних)

☒ Перевидати сертифікати (за відсутності змін у даних)

Відміна Далі

4. У наступному вікні заповніть необхідні поля та оберіть сертифікати, які потрібно перевидати. В полі **Парольний діалог** вкажіть будь-яке слово чи словосполучення, яке слугує підтвердженням в разі, якщо потрібно заблокувати даний сертифікат:

Перевидача сертифікатів

Новий сертифікат буде містити дані з Вашого попереднього сертифіката, крім дати початку дії. Дата зміниться на поточну

Заявка

П.І.Б. уповноваженої особи:

Телефон уповноваженої особи:

Парольний діалог:

☒	ЄДРПОУ/ІПН	ПІБ/Найменування	Діє до	Призначення	Електронна пошта	Тип	Початок дії
☒	2520012520	Токен ін Мій Юсби Т...	17.09.2018	Шифрування	2520012@ukr.net	Підпис дире..	20.10.2017
☒	2520012520	Токен ін Мій Юсби Т...	17.09.2018	Підписання	2520012@ukr.net	Підпис дире..	20.10.2017

Сума до сплати: 62 грн.

☒ Надаю згоду на публікацію сертифікатів на загальнодоступному ресурсі АЦСК

Якщо перевидается сертифікат підписання, програма автоматично запропонує створити заявку на перевидачу сертифікату шифрування (позначка у рядку сертифіката шифрування встановлюється автоматично). Але ви можете створити заявку на перевидачу лише сертифікату підписання або лише сертифікату шифрування, видаливши відповідну позначку вручну.

Щоб сертифікати були доступні для завантаження, встановіть позначку **Надаю згоду на публікацію сертифікатів на загальнодоступному ресурсі АЦСК**. Сертифікат б опублікований на сайті АЦСК "Україна" <http://www.uakey.com.ua/>, де його можна отримати через мережу Інтернет. Опубліковані сертифікати можуть бути завантажені за допомогою автоматичної перевірки зміни статусів сертифікатів.

Якщо ви бажаєте отримати рахунок на перевидачу сертифікатів, натисніть кнопку **Отримати рахунок** - відкриється вікно формування рахунку. Поля вікна заповнюються автоматично, відповідно до даних введених у вікні **Перевидача сертифікату**. Залежно від обраних параметрів у вікні відображається сума, яку необхідно сплатити за послугу Перевірте, чи правильно заповнені поля, оберіть форму оплати та натисніть кнопку **ОК**. Рахунок відкриється на окремій вкладці.

Зверніть увагу! По натисканню кнопки **Отримати рахунок** формування заявки на перевидачу сертифікатів відміняється.

5. Перевірте та підтвердіть вибрані дані для переходу до наступного кроку. Натисніть кнопку **Далі**.

6. Відкриється вікно **Генерація секретного ключа**. Якщо необхідно зберегти секретний ключ на токені, підключіть до комп'ютера захищений носій, та встановіть опцію **Збер секретний ключ на захищений носій**.

Генерація секретного ключа (1 з 2)

Ключ печатки Товариство з обмеженою відповідальністю "Орб..."

☐ Зберігати секретний ключ у файлі

☒ Зберігати секретний ключ на захищений носій

Захищений носій для збереження секретних ключів:

Пароль носія:

☒ Відправити заявку по пошті

☐ Записати на оптичний диск

☐ Зберегти на диск

Каталог для збереження заявки і секретних ключів:

У полі **Захищений носій для збереження секретних ключів** натисніть **...**, у вікні що відкриється оберіть назву потрібного захищеного носія:

Оберіть пристрій

Встановлені носії

AVTOR Ltd. CC337 141b192a9729000
KM AFD1
d8d5c1b1109f4ccb1ba85eca51c2c8f9c97907580f7152e38fa68

KM AFD2
AVTOR Ltd. CC337 143937c29629000
Токен ін М.Ю. (Директор) Ключ підписання
Токен ін М.Ю. (Директор) Ключ шифрування

7. У полі **Пароль носія** введіть пароль, який використовується для доступу до захищеного носія.

Будьте уважними! Кількість спроб вводу пароля обмежено виробником носія. У разі перевищення ліміту спроб захищений носій буде очищено.

Ви також можете зберегти секретні ключі перевиданого сертифікату на диску комп'ютера. Для цього, у вікні **Генерація секретного ключа** встановіть позначку **Зберегти секретний ключ у файл**. У відповідні поля введіть пароль до секретного ключа та повторіть його для підтвердження правильності введення.

8. Оберіть каталог на комп'ютері, в який будуть записані файл заявки та файли секретних ключів (якщо ви обрали збереження ключа у файл). Якщо ж ви обрали збереження секретного ключа на захищеному носії, у обраний каталог буде збережено лише файл заявки.
9. Для продовження натисніть **ОК**. Результатом генерації буде створення файлу секретного ключа. Файл ключа буде збережений на захищеному носії або за вказаним шляхом, про що система оповістить користувача.
10. Запуститься процедура підпису заявки. Введіть пароль секретного ключа. Заявка **підписується ключем сертифікату, який перевидається**.
11. Відправте заявку на адресу сервера **АЦСК Україна**, який буде запропоновано програмою.
12. Якщо оплата не здійснювалась, або кошти ще не надійшли до АЦСК, відкриється вікно, у якому оберіть форму оплати послуги:

- **Оплата онлайн** - оплатити послуги за допомогою платіжної системи онлайн, відкриється вікно платіжної системи, у якому вкажіть необхідні реквізити та виконайте оплату, дотримуючись вказівок платіжної системи;
 - **Сформувати рахунок** - сформувати рахунок на оплату послуги, програма сформує рахунок-фактуру **PD010190** на сплату послуг, що може бути оплачений у будь-якій банківській установі;
 - **Оплату вже здійснено** - оплату здійснено, але кошти ще не надійшли у АЦСК, заявка буде опрацьована після надходження коштів.
- Натисніть **ОК**.

13. Якщо оновлення сертифікатів було заздалегідь оплачене, та кошти надійшли до АЦСК, відкриється вікно повідомлення про успішне відправлення заявки.



Після завершення операції перевидачі, сертифікат, що був перевиданий, скасовується.

Як зберегти секретний ключ на захищеному носії

В ЦЬОМУ РОЗДІЛІ:
Збереження ключа при створенні нового сертифікату
Збереження ключа при продовженні терміну дії сертифікату

За допомогою програми **M.E.Doc** можливо зберегти секретний ключ на захищеному носії кількома способами:

- при створенні нового сертифікату;
- при продовженні терміну дії сертифікату;
- при [перевидачі сертифікату](#).



Зверніть увагу! Для кожного особистого ключа використовується окремий носій.



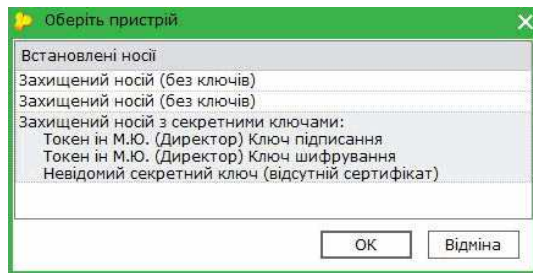
Якщо на захищеному носії зберігається секретний ключ, виданий на інший номер ЕДРПОУ або ДРФО, та який більше не використовується, перед записом нового ключа необхідно виконати операцію [очищення захищеного носія](#).

На одному носії для певної особи (підприємства) можливо зберегти набір секретних ключів - підпис та шифрування.

Збереження ключа при створенні нового сертифікату

1. Підключіть до комп'ютера захищений носій, на якому необхідно зберегти секретний ключ.
2. Перейдіть у розділ **Адміністрування - Сертифікати - Встановлені сертифікати**
3. Створіть заявку на новий сертифікат, як описано у розділі [Для отримання нових сертифікатів](#).
4. Згенеруйте файл заявки на отримання сертифікатів, виконавши команду **Згенерувати заявку** безпосередньо із бланку заявки або з таблиці заявок.
5. У вікні **Генерація секретного ключа** оберіть опцію **Зберегти секретний ключ на захищений носій**:

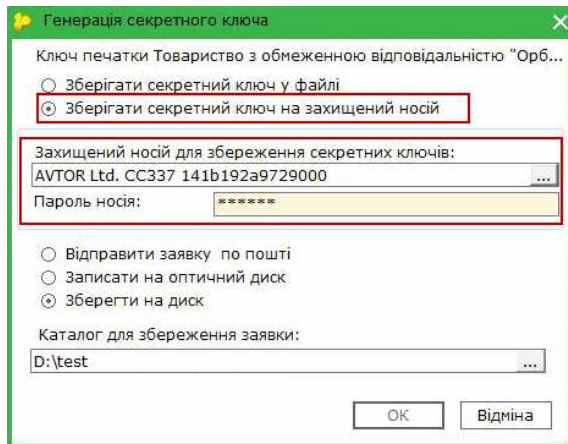
6. У полі **Захищений носій для збереження секретних ключів** натисніть **...**, у вікні що відкриється оберіть назву потрібного захищеного носія:



У вікні відображено інформацію про ключі на підключених носіях. Повідомлення **Невідомий секретний ключ (відсутній сертифікат)** означає, що у програму не завантажено сертифікати, що відповідають знайденому секретному ключу.

7. У полі **Пароль носія** введіть пароль, який використовується для доступу до захищеного носія.

Будьте уважними! Кількість спроб вводу пароля обмежено виробником носія. У разі перевищення ліміту спроб захищений носій буде очищено.

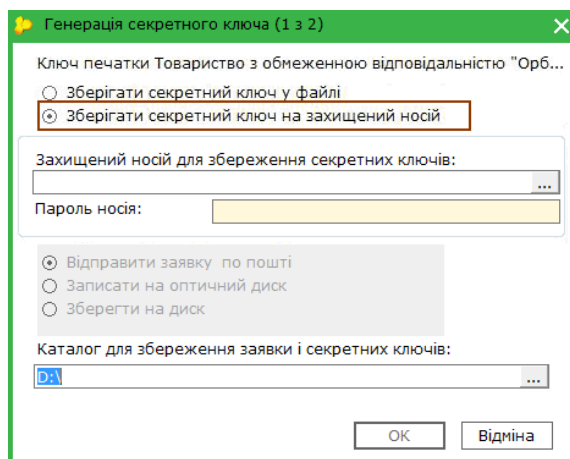


8. Оберіть спосіб у який будуть збережені файли заявок: **записати на оптичний диск** або **зберегти на диск**. Файли заявок необхідні для подальшого подання їх до сертифікаційного центру для отримання сертифікатів.
9. Далі вкажіть шлях до каталогу для збереження файлів заявки. Підтвердьте вибір, натиснувши кнопку **Ok**.
10. Файл секретного ключа буде збережено на захищеному носії. Створені файли заявок будуть збережені за вказаним шляхом.

Перед генерацією наступного ключа необхідно підключити до комп'ютера відповідний носій.

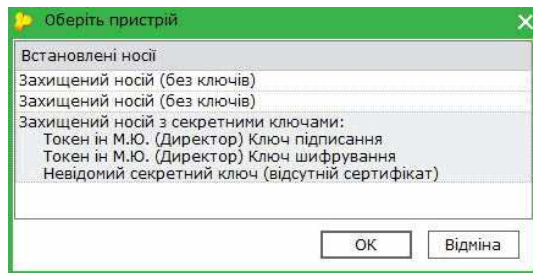
Збереження при продовженні сертифікату

- Підключіть до комп'ютера захищений носій, на якому необхідно зберегти секретний ключ.
- Створіть заявку на продовження терміну дії сертифіката як описано у розділі [Для оновлення сертифікатів користувачем](#).
- У вікні **Генерація секретного ключа...** оберіть опцію **Зберегти секретний ключ на захищений носій**:



У заголовку вікна відображено порядковий номер сертифікату та загальна кількість сертифікатів, що повинні бути опрацьовані.

4. У полі **Захищений носій для збереження секретних ключів** натисніть **...**, у вікні що відкриється оберіть назву потрібного захищеного носія:



5. У полі **Пароль носія** введіть пароль, який використовується для доступу до захищеного носія.

Будьте уважними! Кількість спроб вводу пароля обмежено виробником носія. У разі перевищення ліміту спроб захищений носій буде очищено.

6. Файл секретного ключа буде збережено на захищеному носії. Також створені файли заявки та секретного ключа будуть збережені за вказаним шляхом. Система повідомить вас про успішне збереження ключа.

Примітка: Якщо для продовження ви одночасно обрали кілька сертифікатів, дії по генерації секретного ключа потрібно буде виконати для кожної сертифікату окремо.
Якщо ви зберігаєте ключи на захищеному носії, перед генерацією наступного ключа необхідно підключити до комп'ютера відповідний йому носій.

Операції з ключем на захищеному носії

В ЦЬОМУ РОЗДІЛІ:
Змінення пароля доступу до захищеного носія
Очищення захищеного носія
Пошук секретного ключа

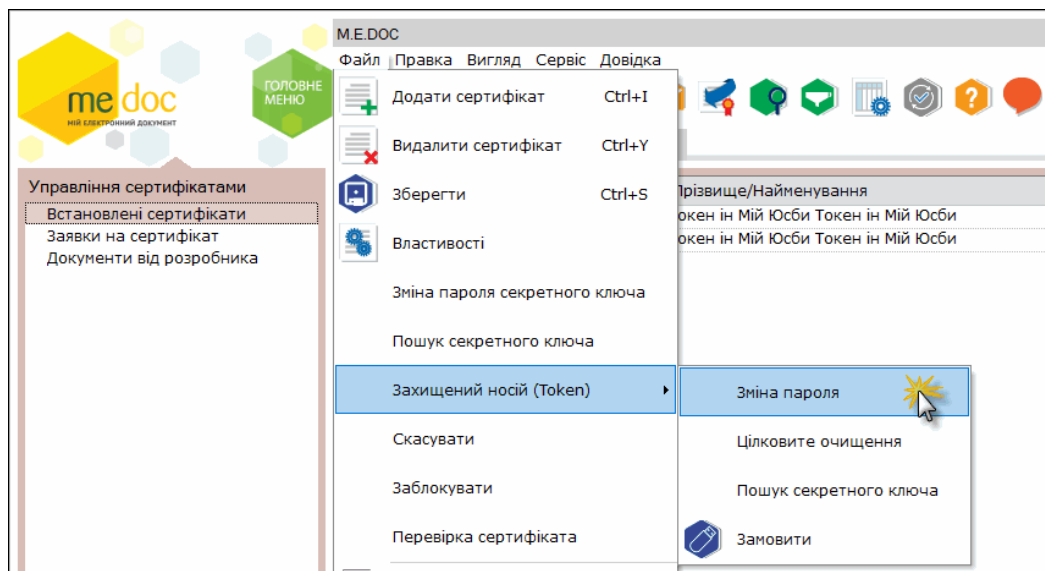
За допомогою програми **M.E.Doc** з секретним ключем, який збережено на захищеному носії, можливо виконувати наступні операції:

- змінювати пароль доступу до захищеного носія;
- видаляти секретний ключ захищеного носія;
- дізнатися назву захищеного носія, що зберігає секретний ключ певного сертифікату.

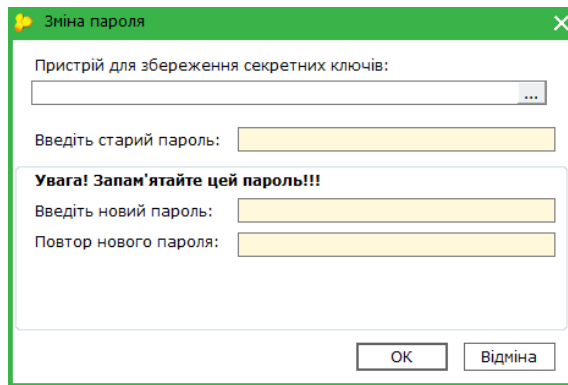
Операції з захищеним носієм виконуються у розділі **Адміністрування - Сертифікати - Встановленні сертифікати**.

Зміна пароля доступу до захищеного носія

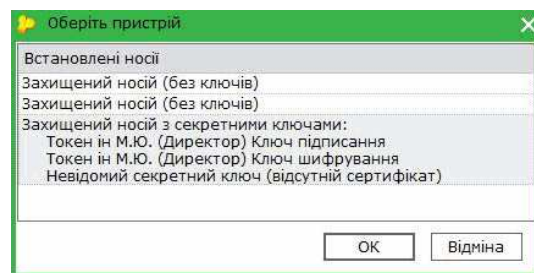
1. У таблиці розділу оберіть необхідний сертифікат.
2. Підключіть до комп'ютера захищений носій.
3. Виконайте команду меню **Файл - Захищений носій (Token) - Зміна пароля**, або оберіть команду контекстного меню **Захищений носій (Token) - Зміна пароля**.



4. Відкриється вікно **Зміна пароля**:



5. У полі **Пристрій для збереження секретних ключів** натисніть **...**, у вікні що відкриється оберіть назву потрібного захищеного носія:



Знайти назву потрібного захищеного носія можна за допомогою функції [пошук секретного ключа](#). Носій повинен бути підключений до комп'ютера

6. Введіть старий пароль до захищеного носія.

Будьте уважними! Кількість спроб вводу пароля обмежено виробником носія. У разі перевищення ліміту спроб захищений носій буде очищено.

6. У відповідні поля введіть новий пароль до захищеного носія та повторіть його для підтвердження правильності введення. Для продовження натисніть **OK**.

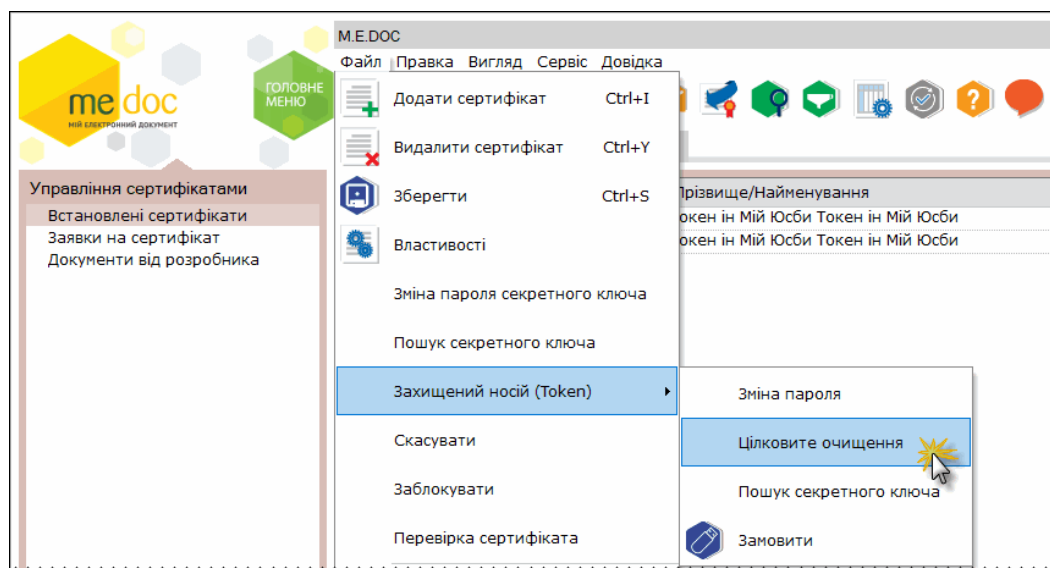
7. Система повідомить вас про успішне зміння пароля.

Очищення захищеного носія

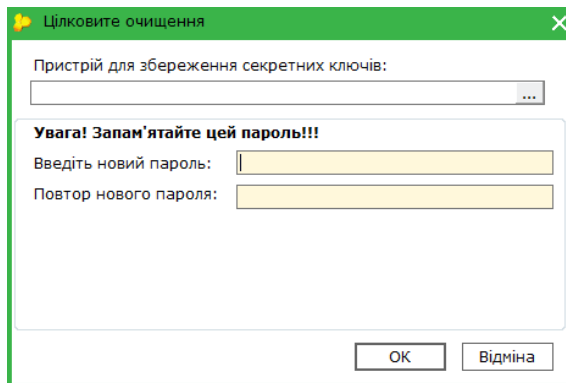
Будьте уважними! Після очищення захищеного носія відновити секретні ключі буде неможливо. Щоб отримати секретні ключі замість втрачених, необхідно замовити нові сертифікати (подати заявку, сплатити рахунок тощо).

1. Підключіть до комп'ютера захищений носій, який потрібно очистити.

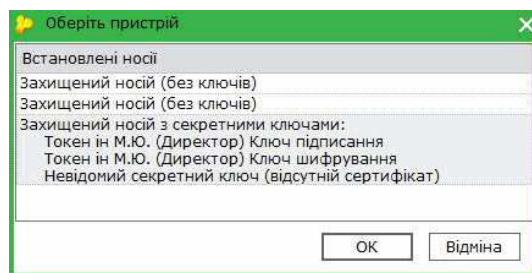
2. Виконайте команду меню **Файл - Захищений носій (Token) - Цілковите очищення**, або оберіть команду контекстного меню **Захищений носій (Token) - Цілковите очищення**:



3. Відкриється вікно **Цілковите очищення**:



4. У полі **Пристрій для збереження секретних ключів** натисніть **...**, у вікні що відкриється оберіть назву потрібного захищеного носія:



Перевірте чи правильно обрано захищений носій для очищення. **Будьте уважні! З токена видаляються всі секретні ключі. Видалені дані відновити неможливо.**

5. У відповідні поля введіть новий пароль до захищеного носія та повторіть його для підтвердження правильності введення.
6. Для продовження натисніть **ОК**.
7. У вікні повідомлення, що відкриється, підтвердіть намір очистити захищений носій.
8. Система повідомить вас про успішне змінення пароля.



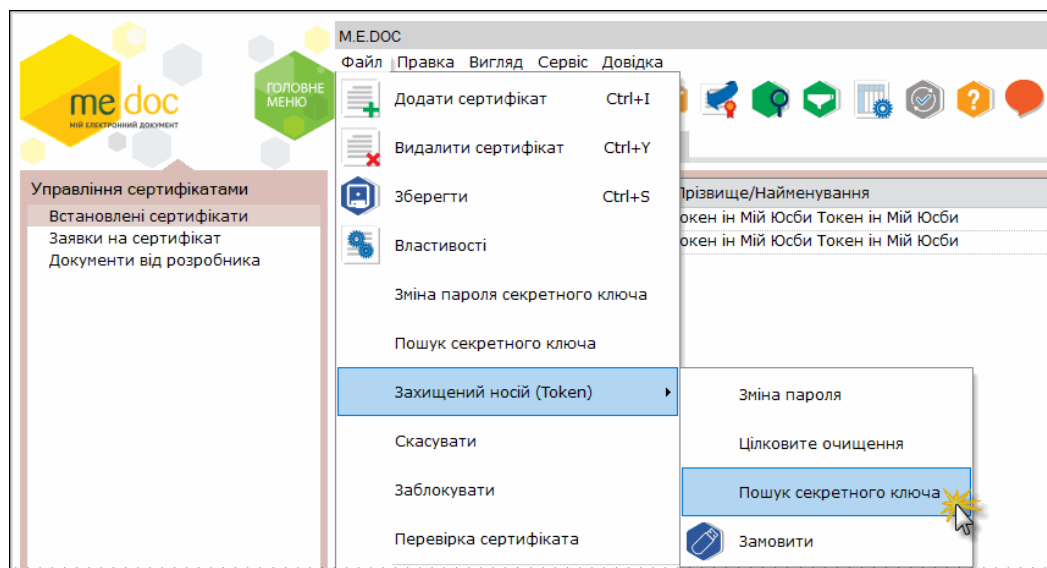
Якщо очищується захищений носій, що може використовуватись як флеш-накопичувач, видалені будуть лише дані секретного ключа. Інша інформація, збережена на накопичувачі, залишається неушкодженою.

Пошук секретного ключа

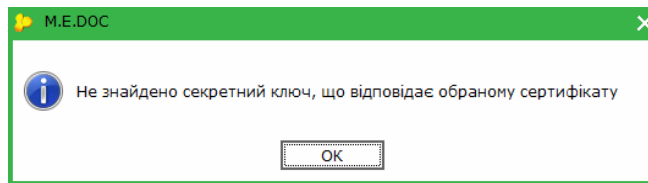
Ця функція буде корисна, якщо ви використовуєте декілька захищених носіїв одночасно. За допомогою функції пошуку секретного ключа ви швидко визначите, який саме носій, відповідає обраному сертифікату.

Захищені носії повинні бути підключені до комп'ютера.

1. У таблиці розділу оберіть сертифікат, для якого необхідно визначити носій секретного ключа.
2. Виконайте команду меню **Файл - Захищений носій (Token) - Пошук секретного ключа**, або оберіть команду контекстного меню **Захищений носій (Token) - Пошук секретного ключа**.



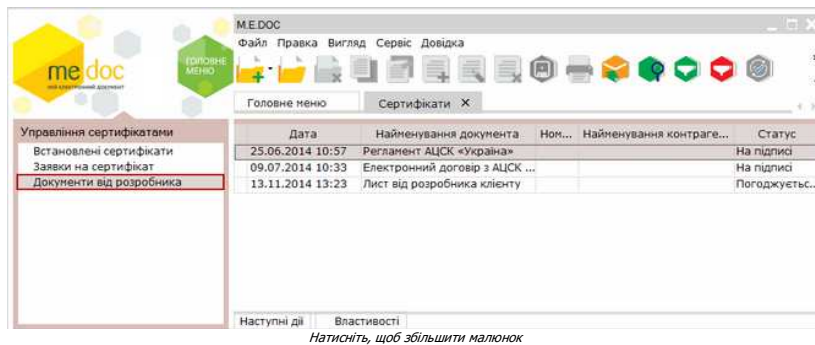
4. У вікні, що відкриється, буде відображено назва та код захищеного носія, який відповідає обраному сертифікату.
Якщо ж носій не знайдено, з'явиться відповідне повідомлення:



Документи від розробника

 [Адміністрування > Сертифікати > Документи від розробника](#)

У розділі знаходяться документи від сертифікаційного центру "Україна". Документи присутні у розділі за замовчуванням і надаються разом з дистрибутивом програми або черговим оновленням.



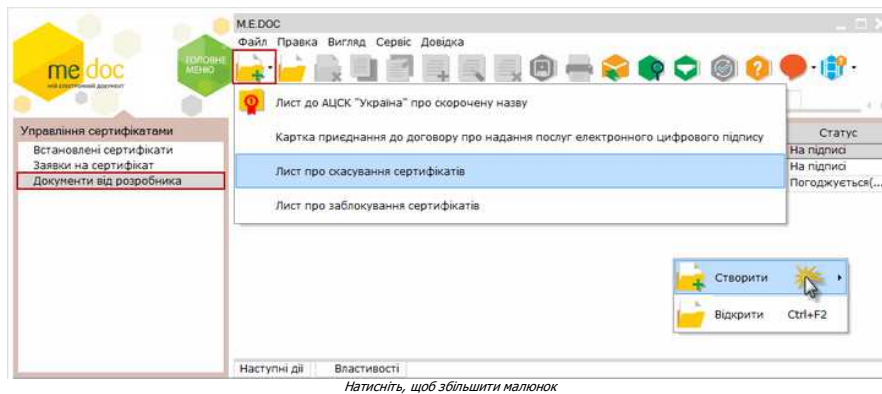
Також у розділі розміщуються документи від розробника програми, що містять офіційні повідомлення, наприклад, "Лист від розробника клієнту".

Ви можете самостійно створювати та відправляти офіційні документи, що адресовані АЦСК "Україна":

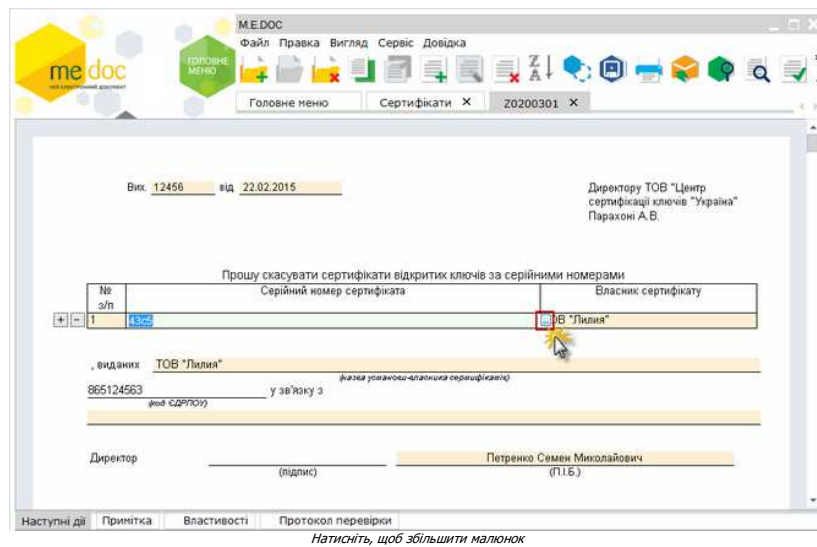
- Лист до АЦСК "Україна" про скорочену назву;
- Картка приєднання до договору про надання послуг електронного цифрового підпису;
- Лист про скасування сертифікатів;
- Лист про заблокування сертифікатів.

1. Для створення документу скористайтесь одним із наступних способів:

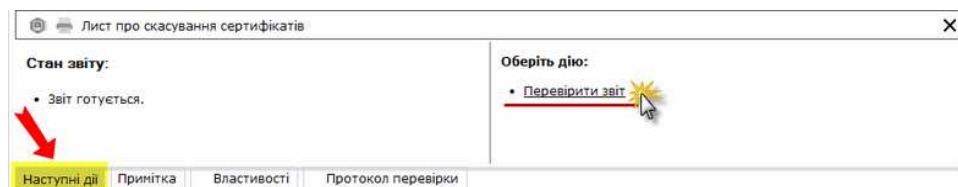
- на панелі інструментів натисніть кнопку **Створити**;
- у контекстному меню оберіть команду **Створити**;



2. Створюваний документ відкривається у окремій вкладці. Заповніть обов'язкові поля документу (підсвічені жовтим кольором).



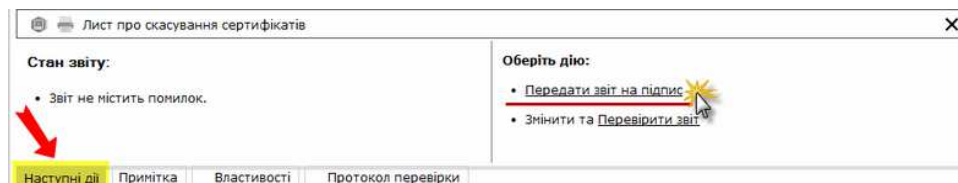
3. На панелі стану документу виберіть закладку **Наступні дії** і натисніть **Перевірити звіт**.



Перевіряється наявність заповнення обов'язкових полів у документі. Якщо обов'язкові дані відсутні, система підсвітить червоним кольором поля, що необхідно заповнити. Виправте помилки та знову виконайте перевірку.

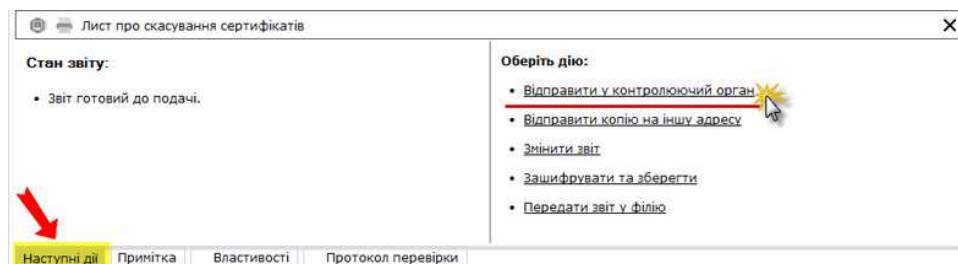
4. Збережіть документ, натиснувши кнопку  або комбінацію клавіш **Ctrl+S**.

5. На закладці **Наступні дії** натисніть **Передати звіт на підпис**.



6. Виконайте стандартну [процедуру підписання звітів електронним цифровим підписом](#).

7. На вкладці **Наступні дії** натисніть **Передати звіт на підпис**.



8. У вікні, що відкрилось, оберіть адресу АЦСК "Україна" та натисніть кнопку **ОК**.

