ІНСТРУКЦІЯ З ЗАПОВНЕННЯ ТА ГЕНЕРАЦІЇ ЗАЯВОК НА ОТРИМАННЯ ПОСИЛЕНОГО СЕРТИФІКАТУ ЕЦП

Для того щоб стати власником сертифікатів ЕЦП, Вам необхідно пройти процедуру реєстрації, зокрема надати всі необхідні документів, затверджений перелік яких представлений на сайті АЦСК в розділі «Комплект документів».

Обов'язковою умовою є наявність сформованих у програмі «M.E.Doc» заявок на формування посилених сертифікатів підписантів ЕЦП.

Формування сертифікатів відкритих ключів відбувається на підставі самостійно згенерованих заявок та секретних ключів підписантів.

Секретні ключі **не надаються** до сертифікаційного центру, вони зберігаються безпосередньо у підписанта. До АЦСК «Україна» надаються сформовані у програмі файли заявок, попередньо записані на будь-який електронний носій. На підставі заявок будуть сформовані відповідні сертифікати ЕЦП.

Формування заявки на отримання сертифікату

Процес створення заявки на отримання сертифікату поділено на 2 етапи:

- Створення електронного бланку заявки на отримання сертифікату.
- Генерація файлу заявки на отримання сертифікату для надання в АЦСК «Україна».

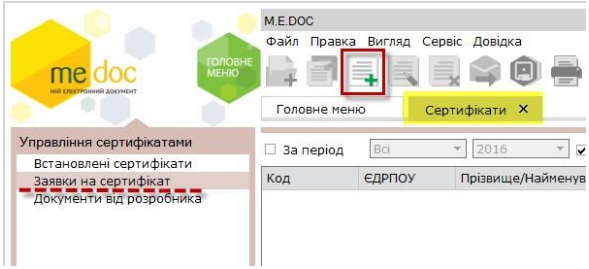
Зверніть увагу!!! *Заявки на отримання сертифікатів ЕЦП створюються на підставі даних, внесених у картку підприємства.*

Перед початком формування заявок на отримання сертифікатів переконайтесь, що картку підприємства заповнено в повному обсязі.

Крок 1. Створення заявки на отримання сертифікату.

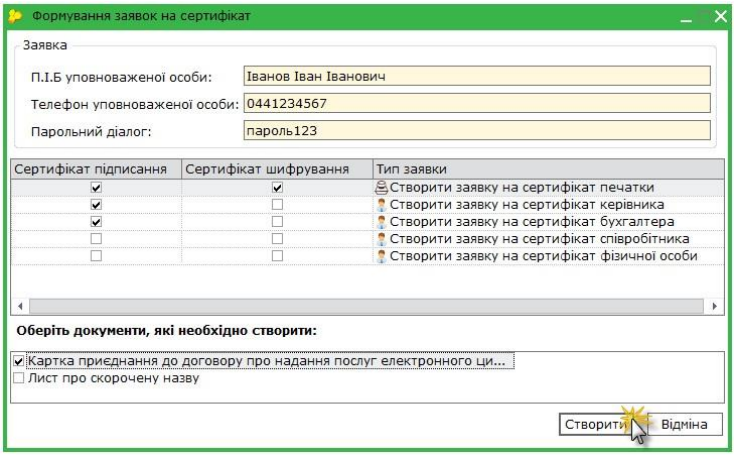
1. У головному меню оберіть **Адміністрування - Сертифікати - Заявки на сертифікат**.

2. На панелі інструментів оберіть команду *Сформувати заявку* (Ctrl+I) або *Файл – Сформувати заявку (Мал.1)*



Мал.1 Створення нової заявки

3. Вкажіть прізвище, ім'я та по-батькові особи, яка відповідає за використання сертифікатів в установі, та її контактний телефон. Ці дані автоматично додадуться у поля електронної заявки на отримання сертифікатів *(Мал.2).*



Мал.2 Вікно Формування заявок на сертифікат

В полі "**Парольний діалог**" необхідно вказати слово чи словосполучення, яке слугуватиме підтвердженням у разі необхідності заблокувати даний сертифікат.

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

Для шифрування звітності, яка відправляється до контролюючих органів, використовується сертифікат шифрування печатки установи. Відповідну галочку встановлено за замовчанням.

Сертифікати шифрування інших типів використовуються для довільного підписання документів.

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

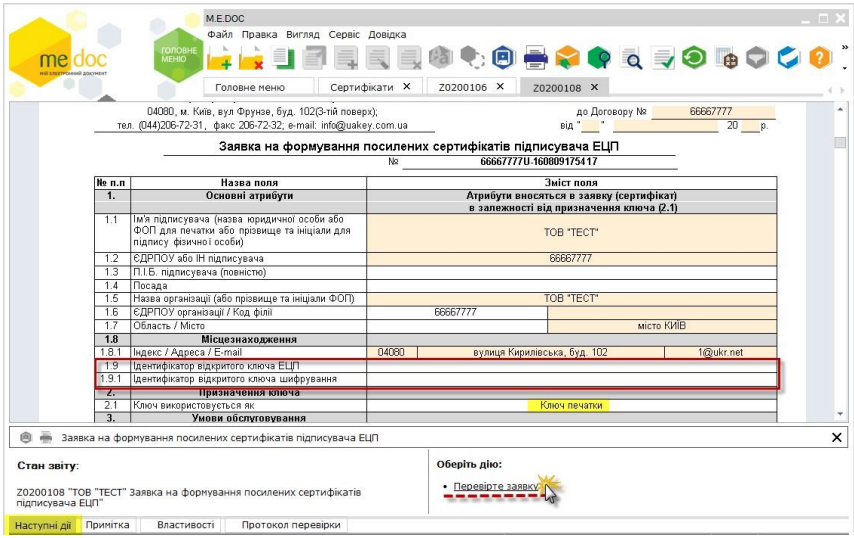
4. **Створено** (з'явилися записи сформованих заявок) та автоматично відкрито в окремих закладках всі вказані в попередньому кроці заявки *(Мал.3).*

Заявка на сертифікат підписання та шифрування печатки відкриється в одному вікні, оскільки при формуванні стояло дві галочки.

Більшість полів заявок заповнюються автоматично даними із картки підприємства. Якщо у картці підприємства відсутні данні, що є необхідними для заявки, заповніть їх власноруч.

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

5. На панелі стану документу оберіть закладку **Наступні дії** і натисніть **Перевірте заявку**. *(Мал.3).*



Мал.3 Перевірка заявки на заповнення обов'язкових полів

Перевіряється заповнення обов'язкових полів, і у випадку відсутності обов'язкових даних, програма виділить відповідні поля червоним кольором.

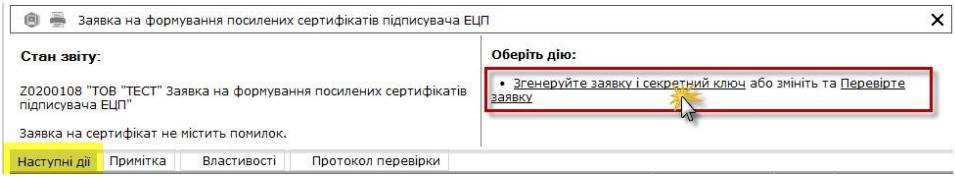
Виправте помилки та знову виконайте перевірку.

6. Збережіть заявку, натиснувши кнопку  або **Ctrl+S**.

Крок 2. Генерація файлу заявки для надання в АЦСК «Україна».

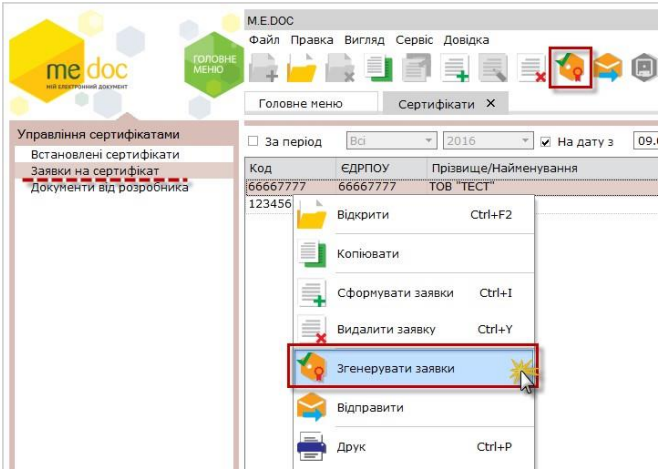
1. Файл заявки на отримання сертифікатів, що надається в сертифікаційний центр, можна згенерувати:

✓ безпосередньо з бланку заявки: оберіть на панелі стану документу закладку **Наступні дії** і натисніть **Згенеруйте заявку і секретний ключ**. *(Мал.4)*



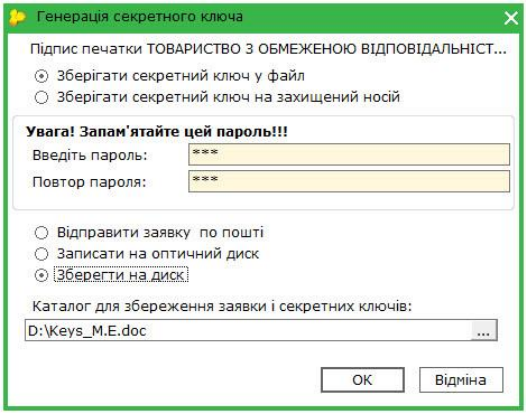
Мал.4 Генерування заявки і секретного ключа з вікна заявки на сертифікат

✓ з таблиці заявок оберіть потрібну заявку (або декілька заявок) та натисніть на панелі інструментів кнопку **Згенерувати заявки** *(Мал.5).*



Мал.5 Генерування заявки і секретного ключа з таблиці заявок на сертифікат

2. Відкриється вікно генерації файлу заявки та секретних ключів.



Мал.6 Генерація заявки

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

Пароль повинен складатись мінімум з **3** і максимум з **64** символів. Пароль може складатися з будь-яких комбінацій букв, цифр, інших символів (*Мал.6).*

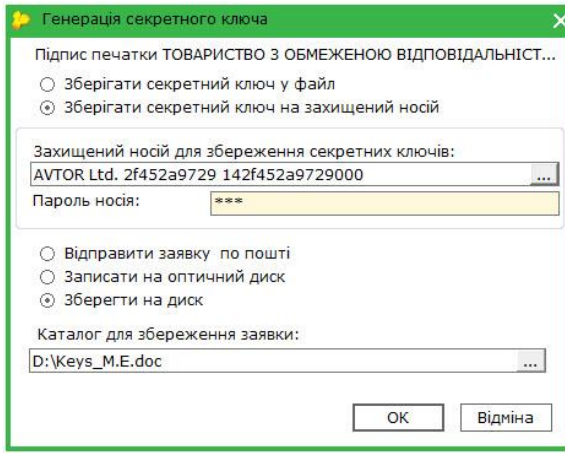
Оберіть спосіб, яким Ви збираєтесь зберегти файли секретних ключів та заявок, з метою надання заявки на отримання сертифікатів до сертифікаційного центру:

- *записати на оптичний диск* - згенеровані секретні ключі записуються на оптичний диск, а файли заявок зберігаються у вказаний каталог. При записі ключів одразу на диск досягається максимальна їх захищеність, тобто виключається можливість відновлення видалених файлів.

- *зберегти на диск* - в указаний каталог зберігаються як файли секретних ключів, так і файли заявок.

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.

Оберіть каталог, де будуть зберігатися файли заявок, з метою надання заявки на отримання сертифікатів до сертифікаційного центру (Мал. 6.1).



Мал.6.1 Генерація заявки на захищений носій

Будьте уважними!!!

✓ За замовчуванням пароль для захищених носіїв від виробника ТОВ«АВТОР» стандартний **12345678**. При генерації секретного ключа на новий носій необхідно вводити саме його. Стандартний пароль Ви можете змінити або після генерації секретних ключів, або до генерації. *У різних виробників можуть бути різні стандартні паролі до захищених носіїв.*

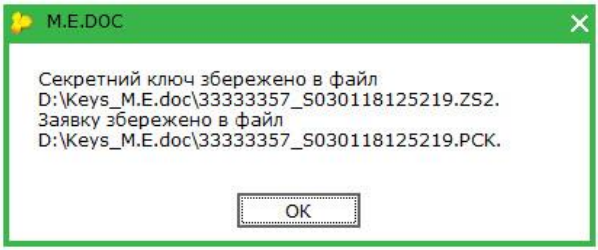
✓ Кількість спроб вводу пароля обмежено виробником носія. У разі перевищення ліміту спроб захищений носій буде заблоковано.

✓ Якщо на захищеному носії зберігається секретний ключ, виданий на інший код ЄДРПОУ або ДРФО, та який більше не використовується, перед генерацією нового ключа необхідно виконати операцію очищення захищеного носія.

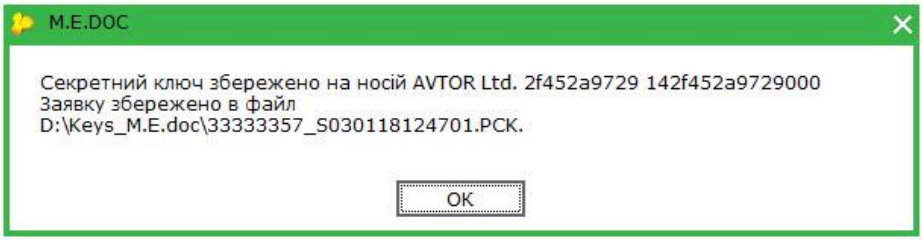
✓ На одному носії для певної особи (підприємства) можливо зберегти набір секретних ключів - підписання та шифрування.

Зверніть увагу!!! *Користувач програми «M.E.Doc» не може самостійно відправити заявку на отримання сертифікату електронною поштою. Для відправлення заявки електронною поштою необхідно мати електронний підпис адміністратора реєстрації (уповноваженого співробітника сертифікаційного центру).*

3. Результатом генерації буде створення файлів заявки та секретного ключа і збереження їх у вказаному каталозі, про що програма повідомить користувача *(Мал.7 та Мал.7.1).*



Мал.7 Шлях, за яким зберігаються заявки та секретний ключ у вказаний каталог.



Мал.7.1 Шлях, за яким зберігаються заявки та секретний ключ, якщо використовують захищений носій.

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

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

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

***.рск** – заява на формування посиленого сертифіката підписанта ЕЦП в електронному вигляді, необхідна для отримання сертифікату відкритого ключа цифрового підпису в АЦСК «Україна» .

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

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 підписанта. Відповідальність за збереження секретних ключів та паролів до них покладається на підписанта!

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" в розділі «Комплект документів».

3. Роздрукувати, підписати та завірити печаткою установи Заявки на формування посиленого сертифікату підписанта ЕЦП.

4. Надати всі документи в АЦСК "Україна".