Зміст

Інструкція по підключенню SSL-сертифіката

В мережевому варіанті FREDO для шифрування каналу зв'язку між серверною частиною і станцією передбачено можливість підключити SSL-сертифікат.

Досвідчені користувачі, які усвідомлюють ризики самопідписаних сертифікатів, можуть використати самопідписаний SSL-сертифікат.

Користувачам, що ще не мають досвіду в області IT безпеки, для отримання SSL-сертифіката рекомендується звернутися до кваліфікованого надавача електронних довірчих послуг (КНЕДП).

У інструкції описані наступні варіанти отримання SSL-сертифіката з подальшим його підключенням:

1. Створення самопідписаного сертифіката з параметрами вашого сервера за допомогою утиліти **ConnectionSetup** в складі FREDO.
2. Створення самопідписаного сертифіката за допомогою безкоштовної утиліти OpenSSL з відкритим кодом.
3. Створення сертифіката і ключа у КНЕДП за допомогою запиту на сертифікат.

Для створення та підключення SSL-сертифіката необхідно виконати кроки:

1. Створити самопідписаний SSL-сертифікат або замовити SSL-сертифікат у КНЕДП (для замовлення сертифіката необхідно створити запит на сертифікат).
2. Імпортувати сертифікат у сховище. У разі потреби, (якщо видавець передав сертифікат в форматі *.cer, *.crt) перед імпортом у сховище необхідно експортувати сертифікат в форматі *.pfx.
3. Підключити сертифікат за допомогою утиліти ConnectionSetup.exe.

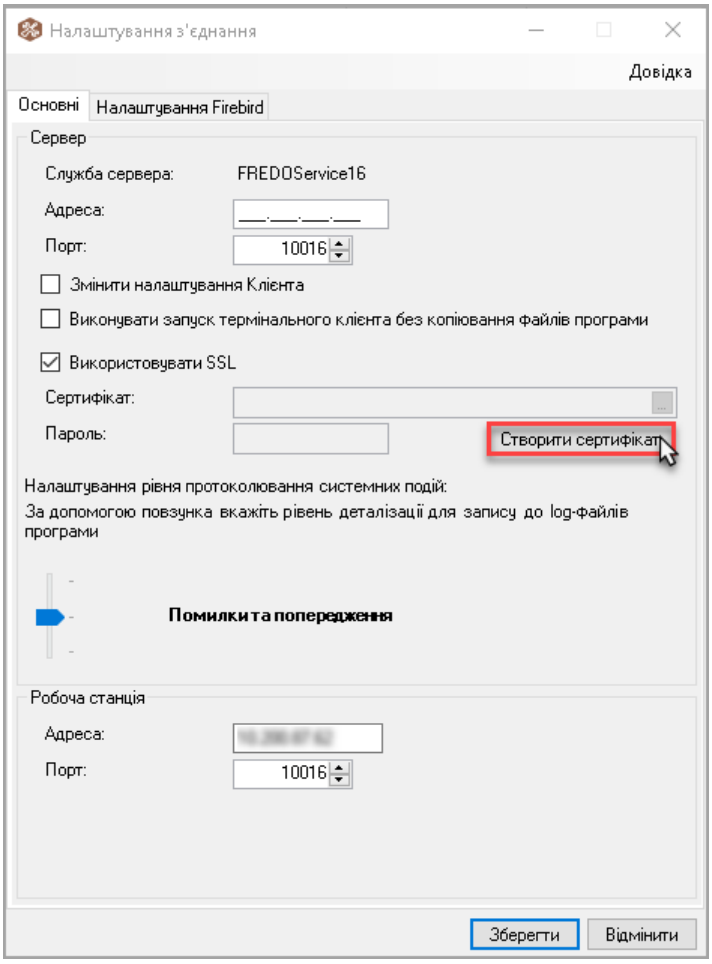
Важливо

- Самопідписані сертифікати не є визнаними довіреними сертифікатами і не можуть бути відкликані КНЕДП. Якщо ви не впевнені в своїх діях, рекомендовано отримати сертифікат від КНЕДП.
- Для підключення SSL-сертифікат повинен бути наданий у вигляді контейнера *.pfx, який містить секретний ключ та сертифікат.
- Сертифікат створюється для сервера.
- Сертифікат необхідно додати в сховище довірених кореневих сертифікатів сервера і всіх станцій.
- Назва сервера і домена в сертифікаті мають співпадати.
- Звернення до сервера зі станції відбувається по імені сервера, не допускається використання тільки IP-адреси сервера.
- В сертифікаті мають бути вказані:
    - в якості (альтернативних) доменних імен DNS: повне ім'я пристрою сервера, localhost, 127.0.0.1, IP адреса сервера;
    - призначення сертифіката: для шифрування даних, авторизації сервера і клієнта.

Створення самопідписаного сертифіката за допомогою утиліти ConnectionSetup

В утиліті **ConnectionSetup** реалізовано функцію створення самопідписаного сертифіката з параметрами, необхідними для коректної роботи.

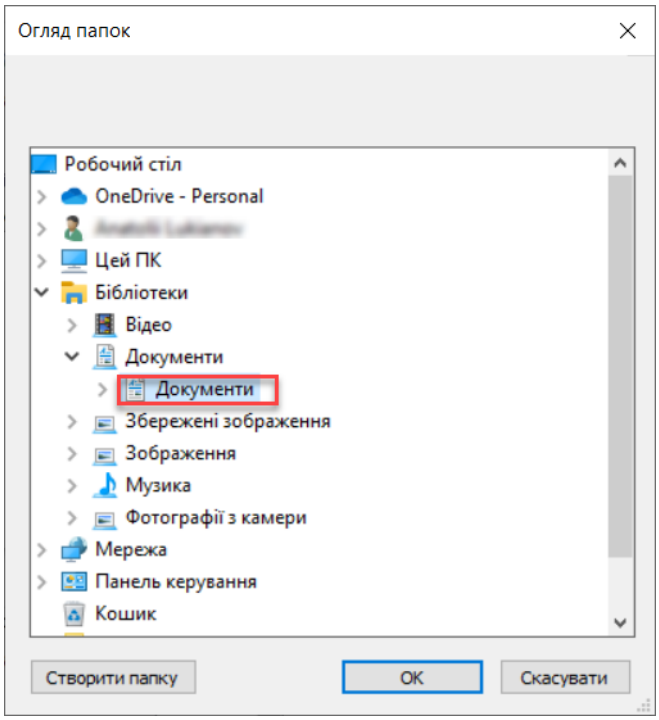
1. Відкрийте утиліту **ConnectionSetup**.
2. Натисніть кнопку **Створити сертифікат**.



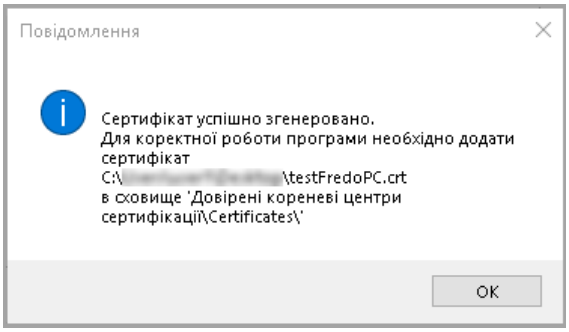
3. Перевірте і, у разі потреби, відкоригуйте поле **Ім'я сервера**. Поле повинно містити ім’я ПК, на якому встановлено сервер.
   Якщо сертифікат створюється на сервері, ім'я сервера співпадає з іменем ПК та заповнюється у полі за замовчуванням.
   Якщо сертифікат створюється для сервера, що розташований на іншому ПК, у полі **Ім'я сервера** введіть ім'я ПК, на якому встановлено сервер.
4. Введіть секретний пароль довжиною до 32 символів.

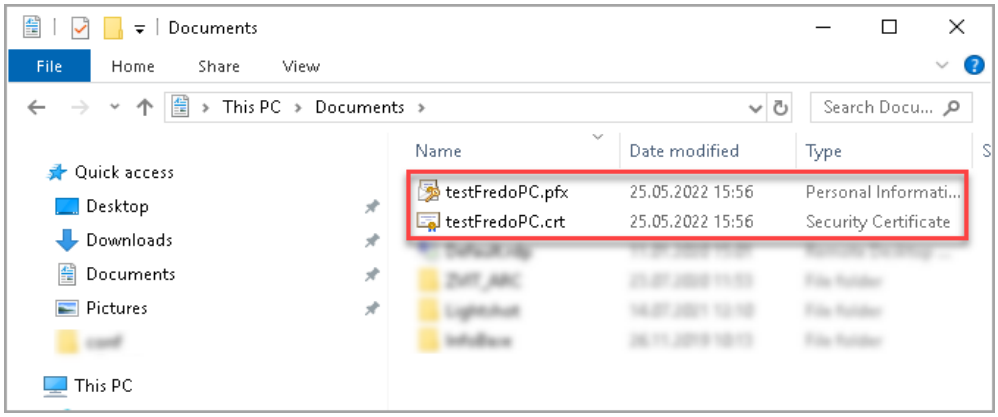
5. Натисніть кнопку **Згенерувати**.

6. Для збереження файлів сертифіката вкажіть папку розташування.



7. У вказану папку буде збережено сертифікат у форматах *.crt, *.pfx.





8. Якщо в утиліті ConnectionSetup перед створенням сертифіката не були заповнені поля **Сертифікат** і **Пароль**, в них копіюється вказаний шлях збереження сертифіката (п. 6), а також пароль, зазначений в генераторі сертифіката (п. 4). За потреби, значення у цих полях можна змінити.

Важливо. Для коректної роботи FREDO з створеним SSL-сертифікатом його необхідно імпортувати в сховище 'Довірені кореневі центри сертифікації\Certificates\' серверу і всіх станцій (див. Імпорт сертифіката в сховище).

Приклад створення самопідписаного сертифіката OpenSSL

Для генерації самопідписаного сертифіката можна скористатися ПЗ з відкритим кодом OpenSSL (https://wiki.openssl.org/index.php/Binaries).

Після встановлення OpenSSL, в командному рядку виконайте команду:

```
"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" req -x509 -v3 -newkey rsa:2048 -sha256 -
keyout MedocCert.key -out MedocCert.crt -days 600 -config  req.conf
```

з параметрами:

-keyout MedocCert.key – шлях збереження і ім'я ключа сертифіката;

-out MedocCert.crt – шлях збереження і ім'я сертифіката;

-days 600 – тривалість дії сертифіката;

-config req.conf - шлях збереження і ім'я файлу конфігурації;

Файл конфігурації (req.conf) містить такі рядки:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
x509_extensions = v3_ca
[req_distinguished_name]
C = UA
ST = Kyiv
L = Kyiv City
O = MedocOrganization
CN = MyWorkPC
[v3_req]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = XXX.XXX.XXX.XXX
DNS.2 = MyPC
DNS.3 = localhost
DNS.4 = 127.0.0.1
DNS.5 = MyWorkPC.FullName
[v3_ca]
basicConstraints = CA:FALSE
nsCertType = client, server
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
nsComment  = "OpenSSL Generated Test Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid, issuer
subjectAltName = @alt_names
```

Важливо. Необхідно вказати:

- у якості альтернативних імен (`subjectAltName`) DNS повне ім'я пристрою сервера, IP адресу сервера, localhost, 127.0.0.1;

- основне призначення сертифіката для шифрування даних (keyUsage);
- розширене призначення сертифіката для авторизації сервера і клієнта (nsCertType, extendedKeyUsage).

Для експорту сертифіката в форматі pfx виконайте команду:

```
"C:\Program Files\OpenSSL-Win64\bin\openssl.exe" pkcs12 -export -name "MedocCert" -out "MedocCert.pfx" -inkey MedocCert.key -in MedocCert.crt
```

з такими параметрами:

`-name "MedocCert"` – зрозуміле ім'я;

`-out "MedocCert.pfx"` – шлях збереження і ім'я сертифіката в форматі pfx;

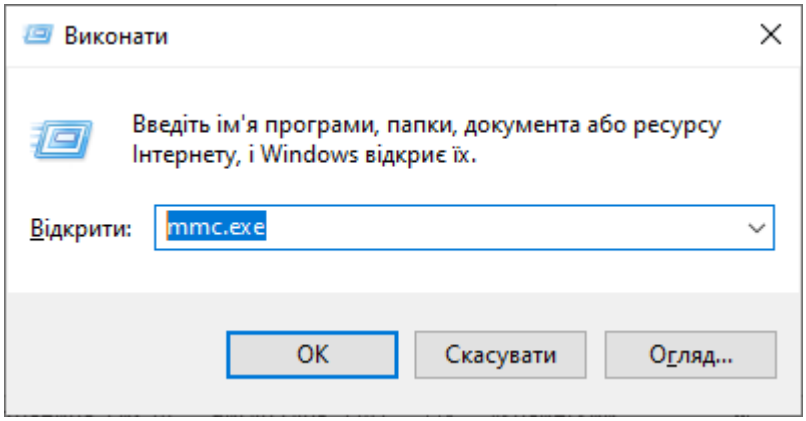
`-inkey MedocCert.key` – шлях до ключа згенерованого сертифіката;

`-in MedocCert.crt` – шлях до згенерованого сертифіката.

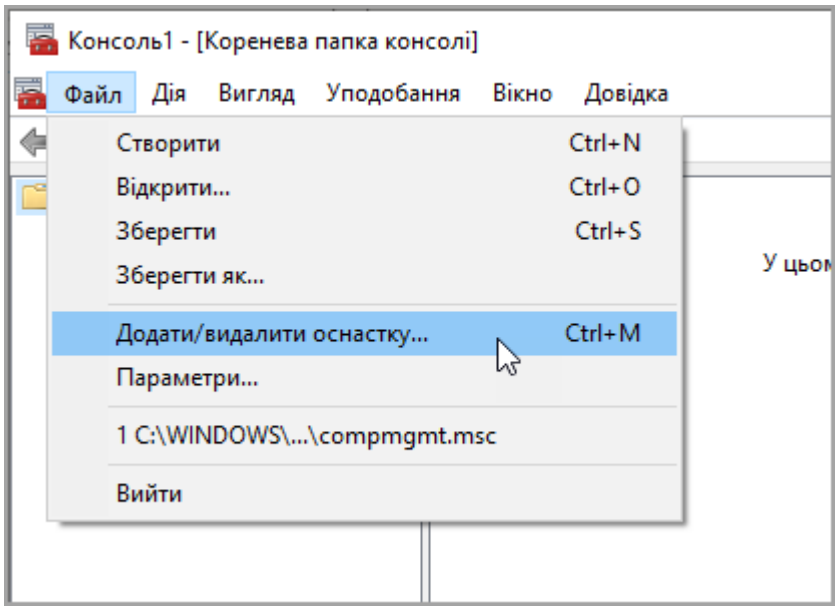
Створення запиту на сертифікат за допомогою Microsoft Management Console (MMC)

Запит на сертифікат потрібен для генерації сертифіката у КНЕДП.

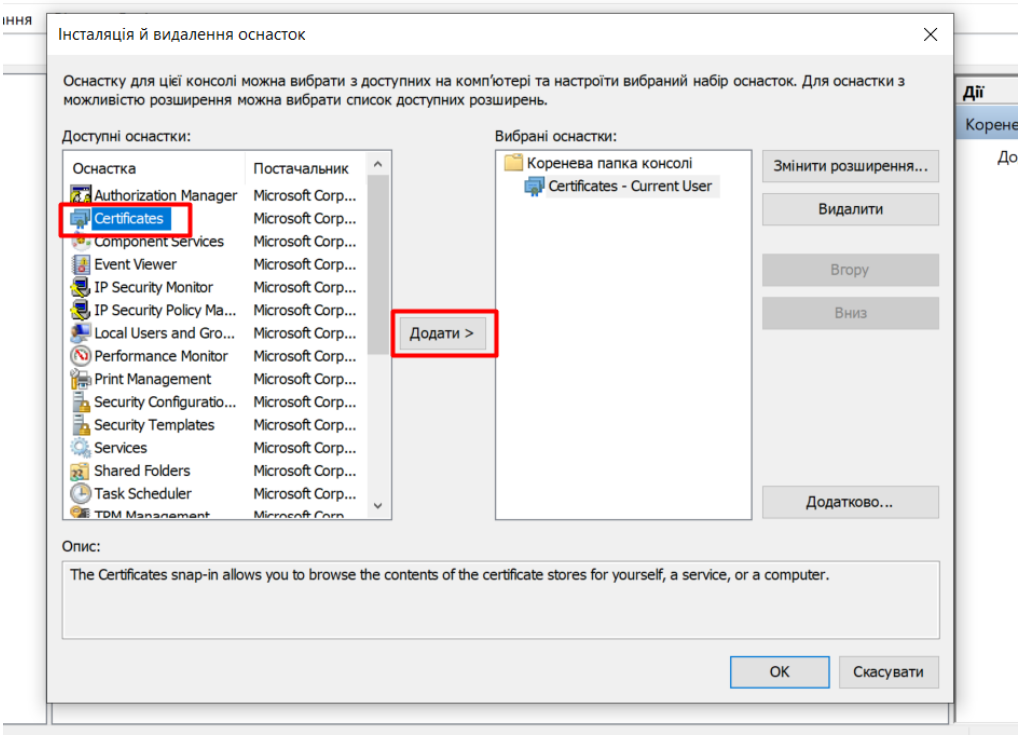
1. Запустіть mmc.exe в командному рядку Windows:



2. В меню **Файл** оберіть **Додати/видалити оснастку**:

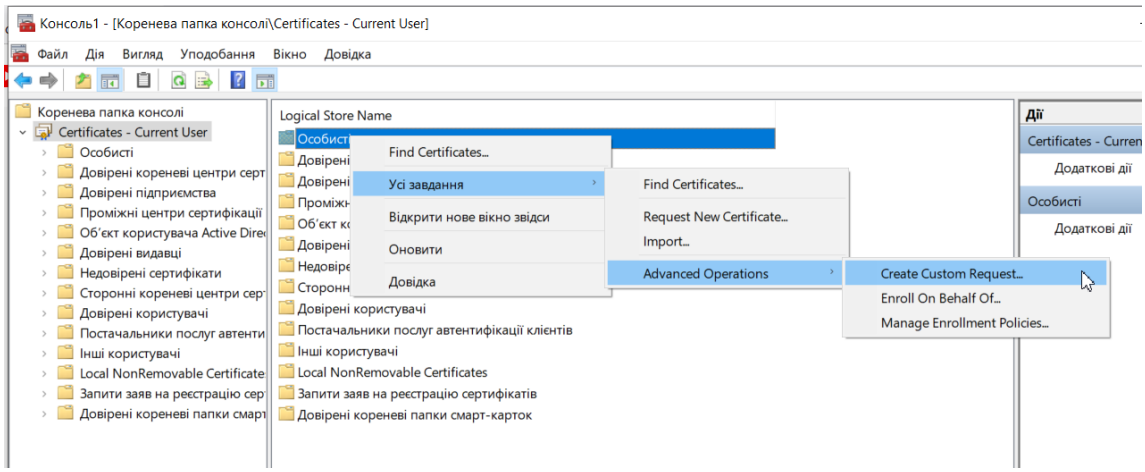


3. Додайте оснастку **Сертифікати**:

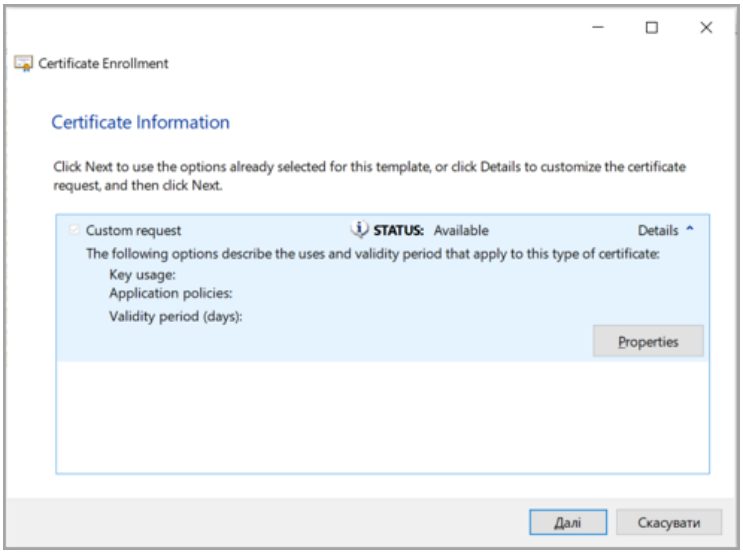


Якщо при інсталяції вимагається вказати користувача – оберіть поточного користувача.

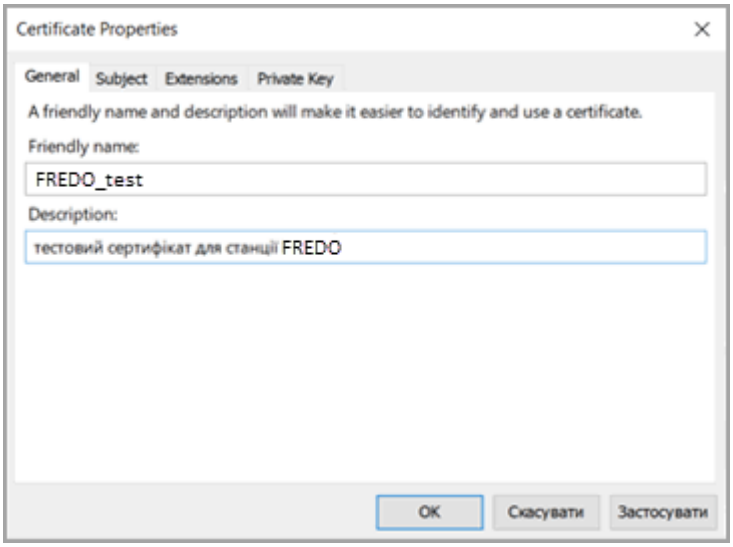
4. Оберіть рядок **Сертифікати – Поточний користувач**, і в контекстному меню виберіть **Усі завдання – Розширені операції – Створити користувацький запит**.



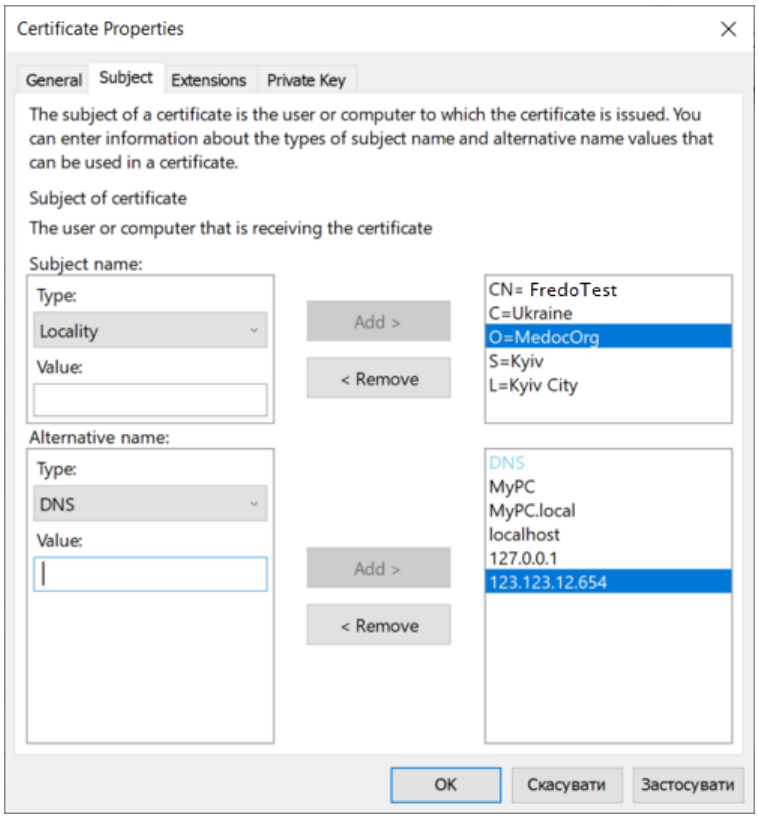
5. В майстрі запиту на сертифікат натисніть **Властивості** для заповнення властивостей сертифіката



6. У вкладці **General** (Загальні) заповніть назву і опис сертифіката:



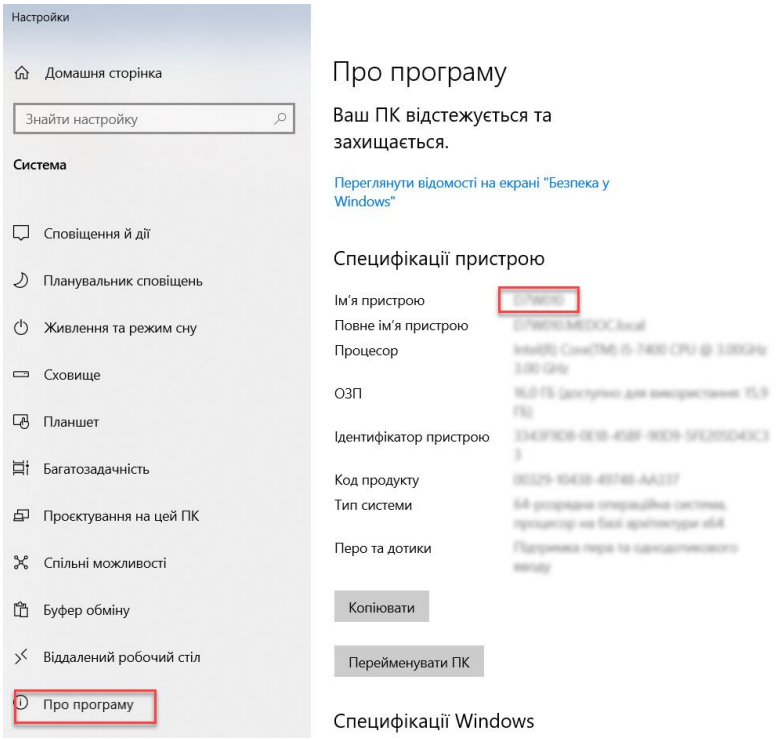
7. В вкладці **Subject** заповніть:



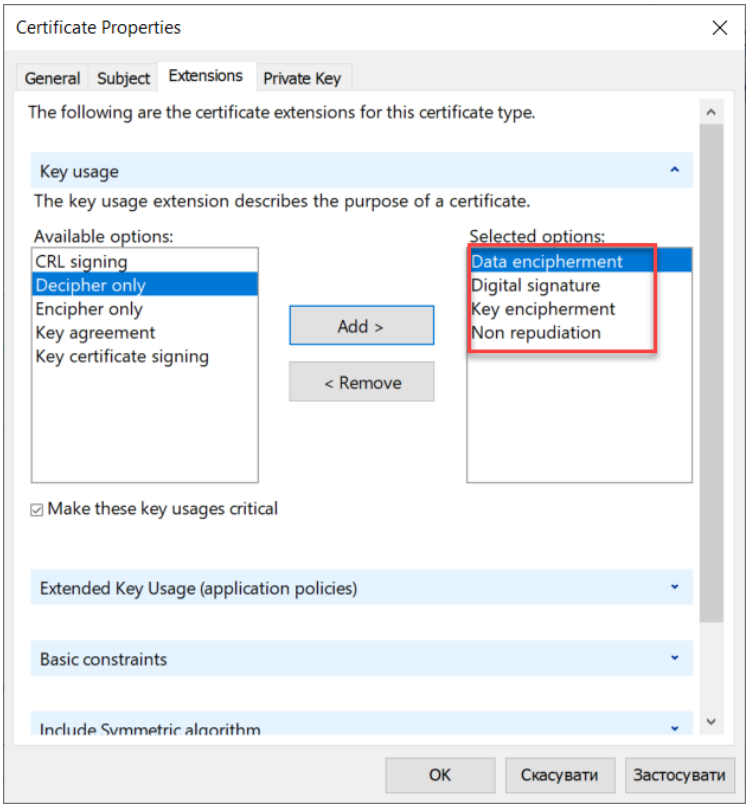
- Країна Country C = Ukraine;
- Основне ім'я ПК Common names CN;
- Додайте у розділі альтернативних імен параметри DNS-імен (тип - DNS), в яких також вкажіть ім'я комп'ютера (Common names, так само, як вказали параметри CN вище), IP-адресу сервера, localhost, "127.0.0.1".

За потреби вкажіть інші параметри.

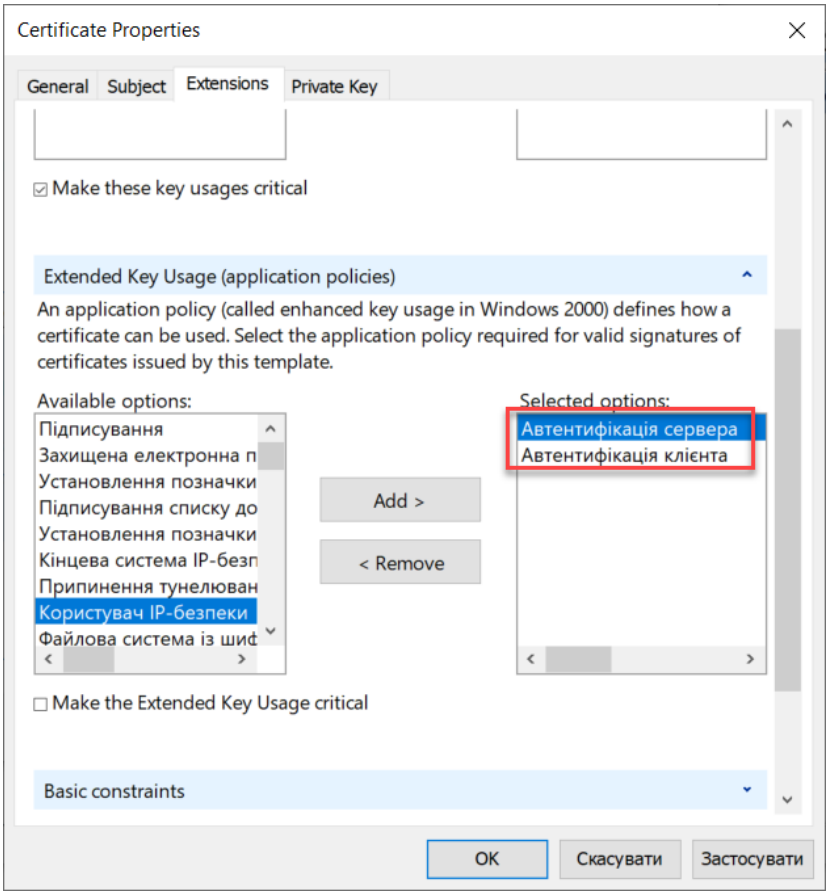
Ім’я ПК можна перевірити у розділі **Налаштування Windows – Система – Про програму – Ім'я пристрою**:



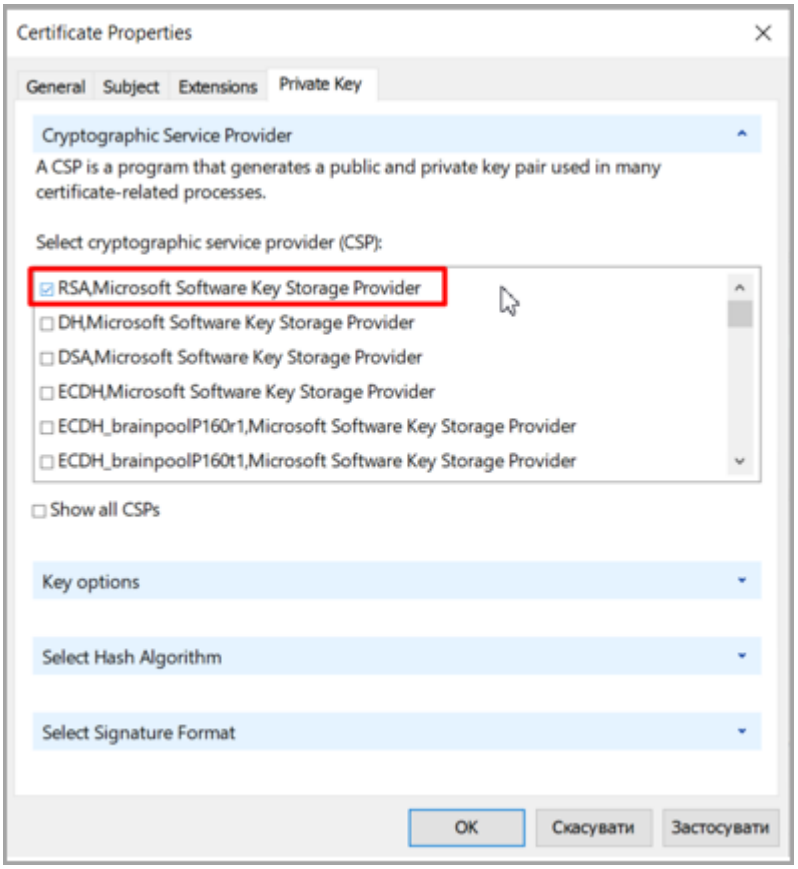
8. У вкладці **Extensions** (**Розширення**) переконайтеся, що в розділі використання ключа вказано шифрування ключів, шифрування даних, цифровий підпис:



9. В розділі розширених налаштувань переконайтеся, що вказано автентифікацію сервера і клієнта:

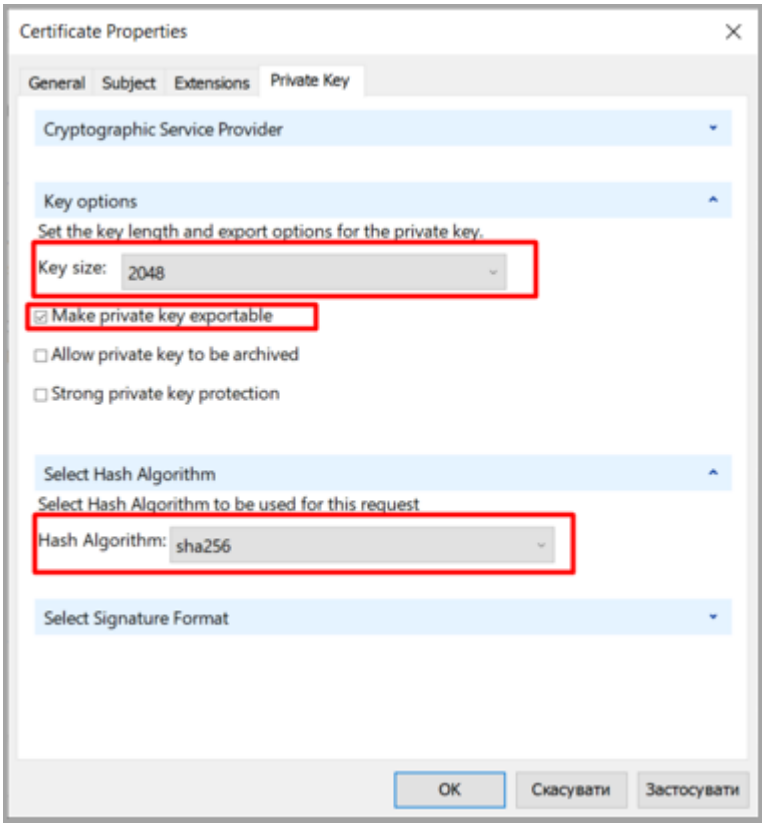


10. У вкладці **Private Key** (Приватний ключ) переконайтесь, що обрано RSA ключ:

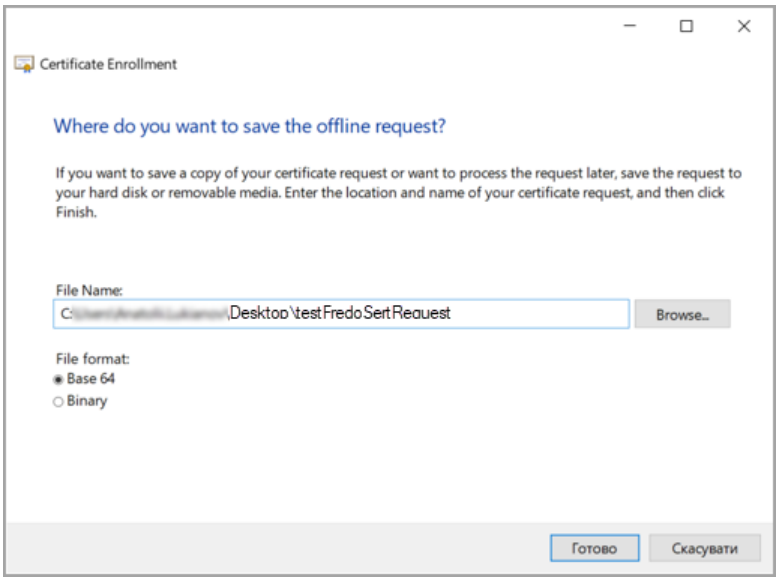


11. В розділі параметрів ключа встановіть довжину ключа (рекомендовано 2048). За потреби, встановіть прапорець **Make private key exportable** – додати можливість експортувати ключ.

12. В розділі Хеш-алгоритму оберіть алгоритм (рекомендовано sha256):



13. Застосуйте обрані властивості і натисніть **ОК**.
14. У наступному вікні натисніть **Далі**.
15. Вкажіть ім'я і розташування файлу ключа, переконайтеся, що обрано **Base64**:



16. Натисніть **Готово**.

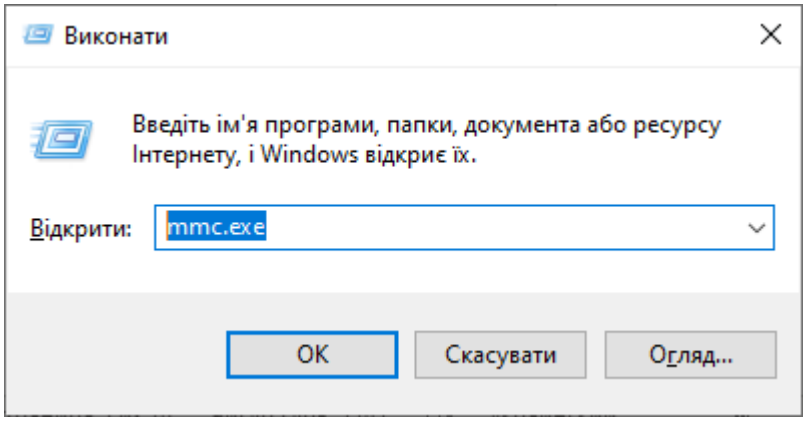
Отриманий файл необхідно відправити вашому КНЕДП для створення сертифіката.

Подбайте, щоб довірений видавець передав вам сертифікат у форматі pfx.

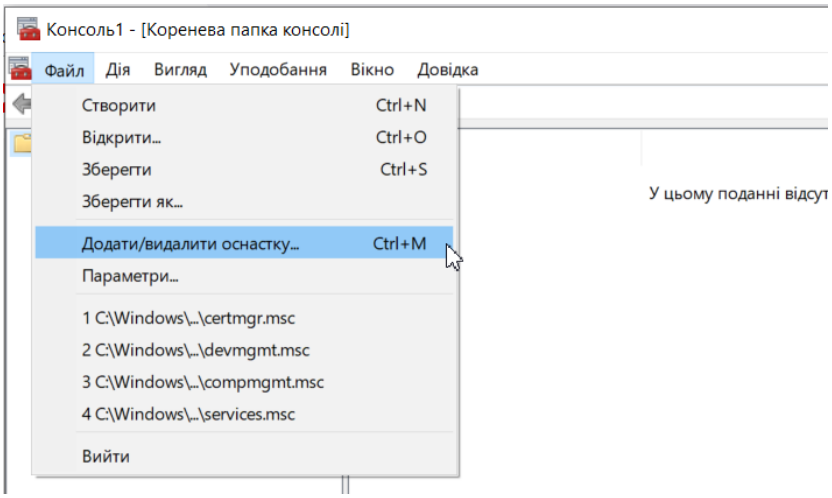
Імпорт сертифіката в сховище

Для коректної роботи сертифікат необхідно імпортувати в сховище сертифікатів як на сервері, так і на всіх станціях.

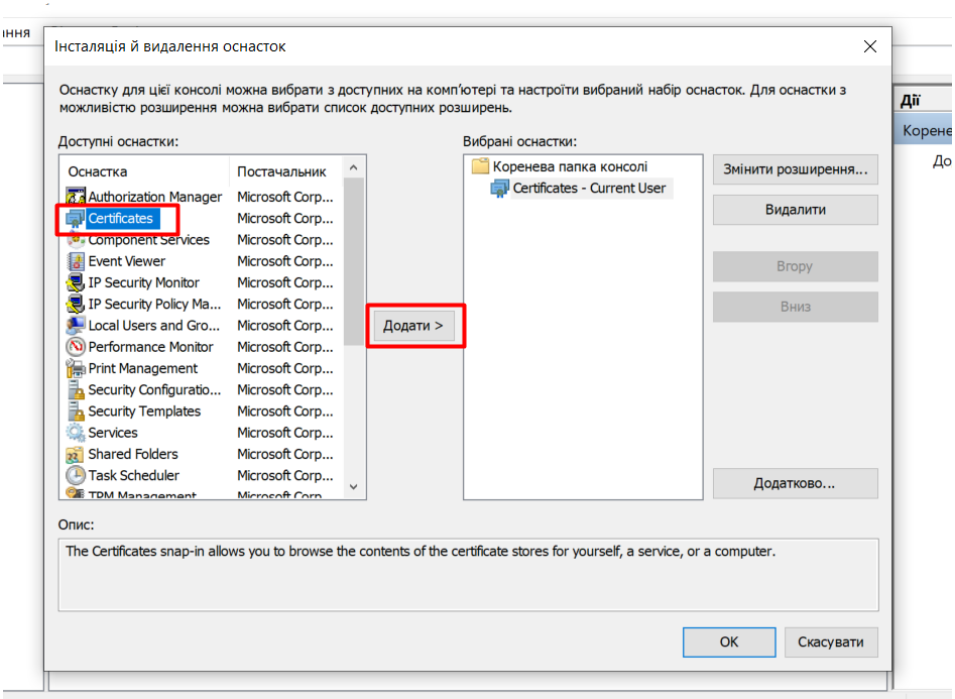
1. Імпортуйте отриманий сертифікат в утиліті MMC. Запустіть mmc.exe в командному рядку Windows:



2. В меню Файл виберіть **Додати/видалити оснастку**:

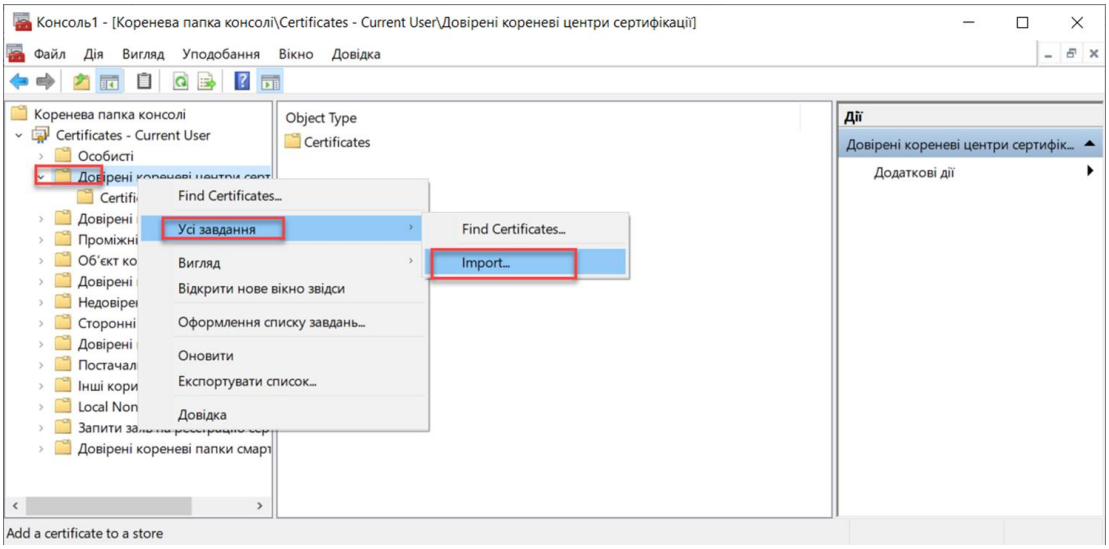


3. Додайте оснастку **Сертифікати**:

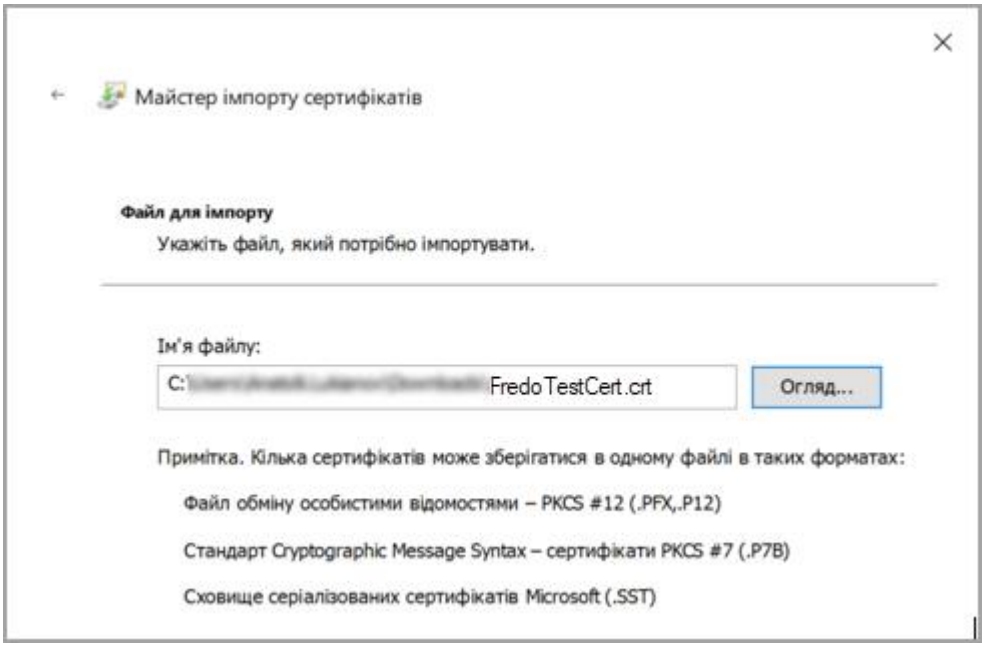


Якщо при інсталяції вимагається вказати користувача – оберіть поточного користувача.

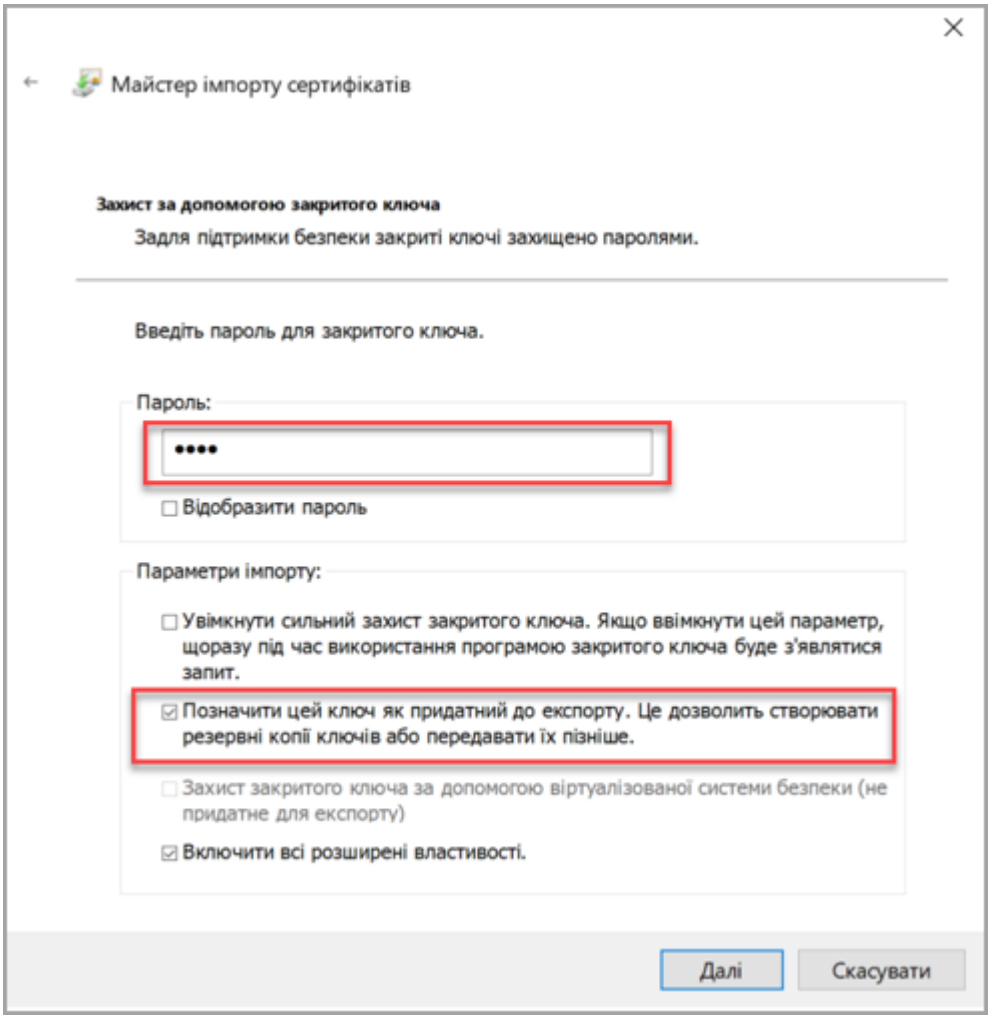
4. Для коректної роботи SSL-шифрування в M.E.Doc сертифікат необхідно додати в сховище довірених кореневих сертифікатів.



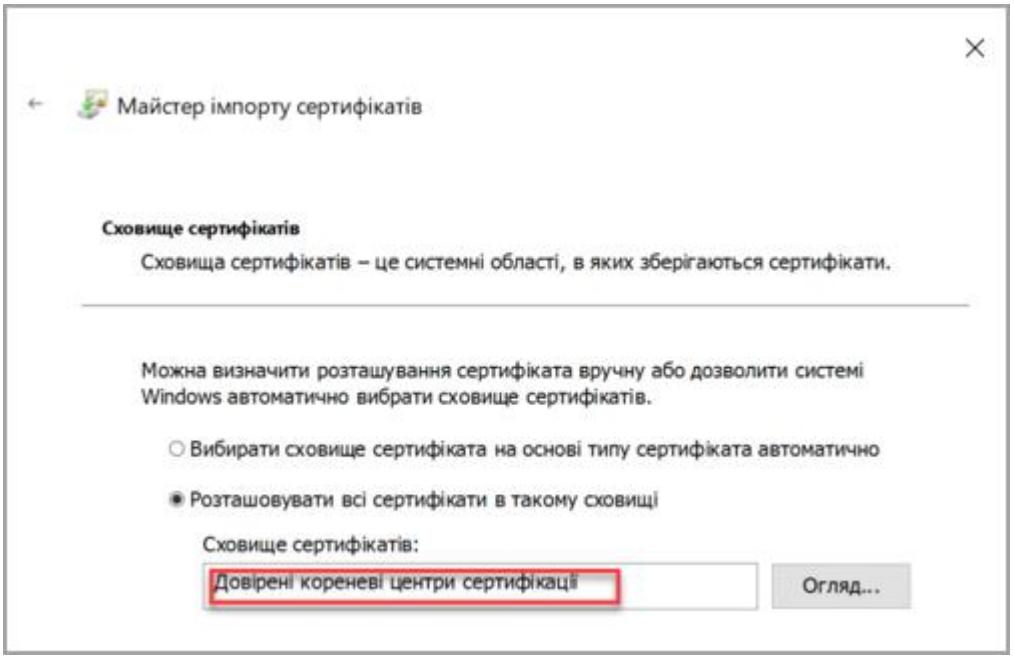
5. Вкажіть шлях до файлу сертифіката (в форматі *.cer, *.crt, *.pfx):



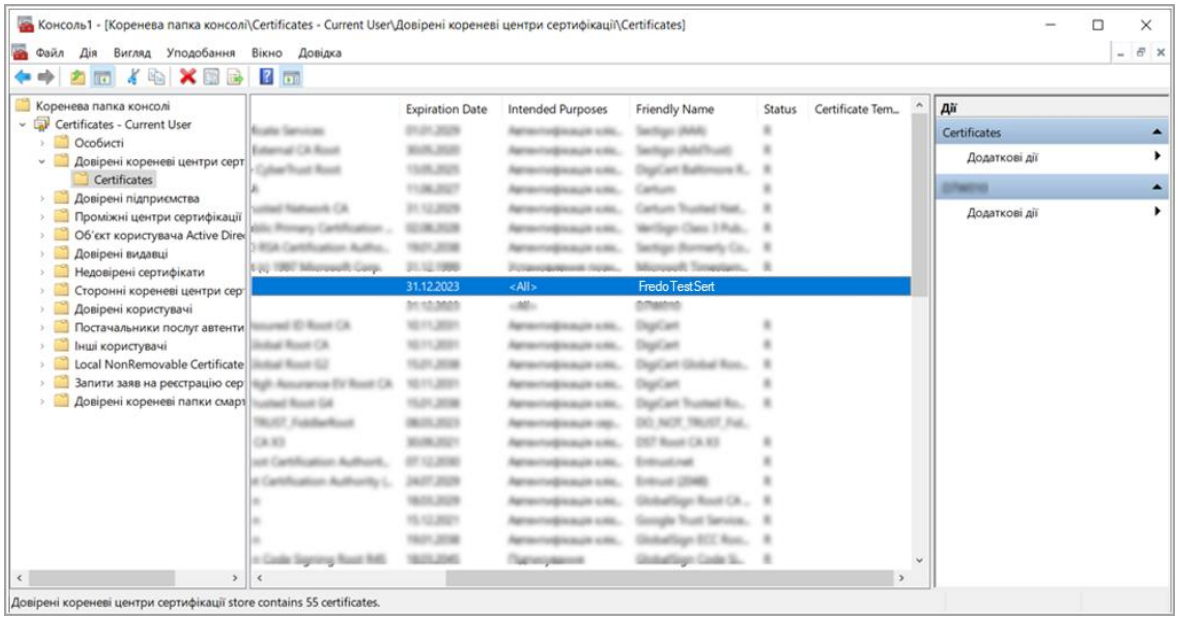
6. Для сертифікатів в форматі pfx необхідно ввести пароль. Також на цьому етапі можна позначити сертифікат придатним для експорту:



7. Оберіть розташування сертифіката – **Довірені кореневі центри сертифікації**:



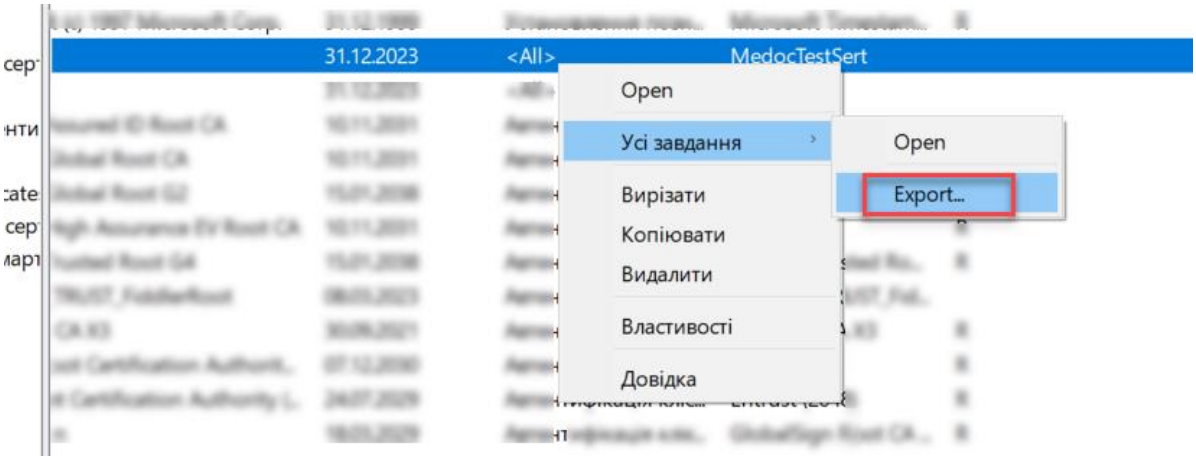
Сертифікат буде додано в сховище:



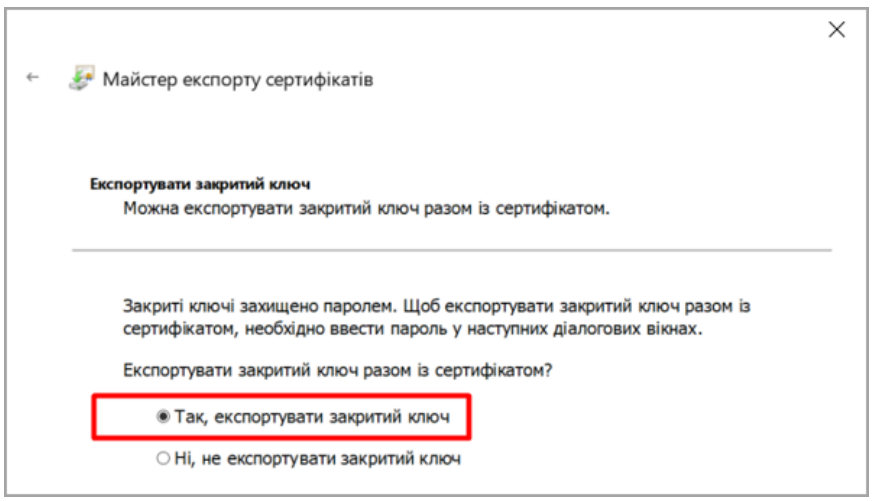
Експорт сертифіката в форматі pfx

Якщо КНЕДП передав сертифікат в форматі *.cer, *.crt, то його також потрібно імпортувати в сховище, як в попередньому розділі. Для підключення SSL-сертифіката в M.E.Doc такий сертифікат необхідно експортувати в форматі *.pfx.

1. Експортуйте імпортований сертифікат в форматі pfx.

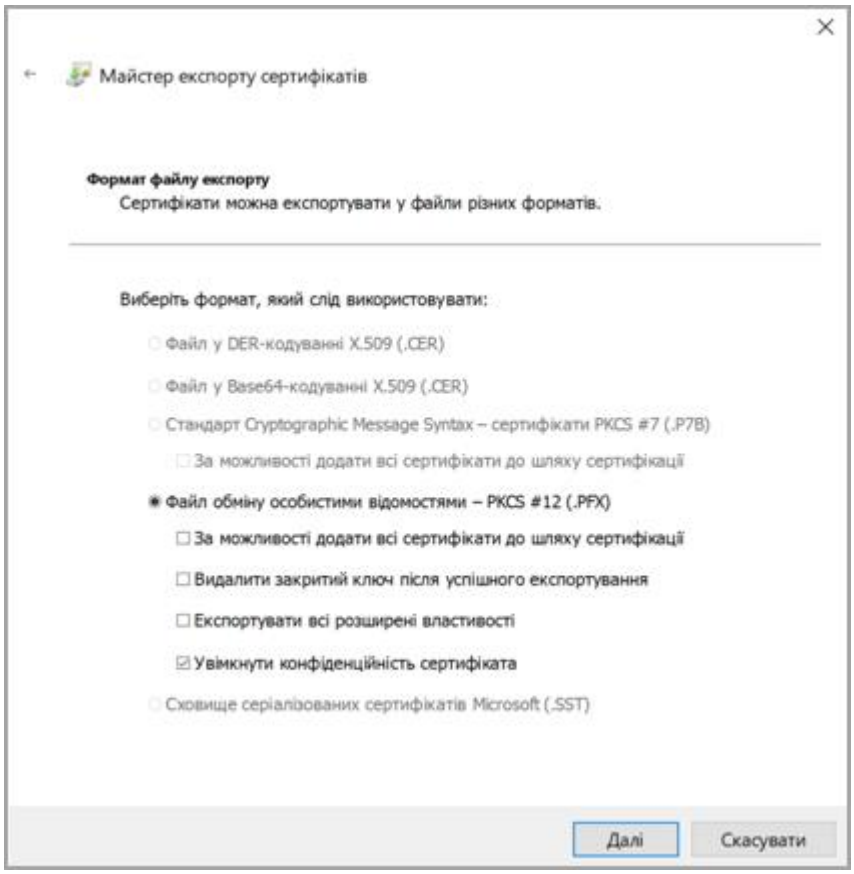


2. Оберіть **Експортувати закритий ключ**:

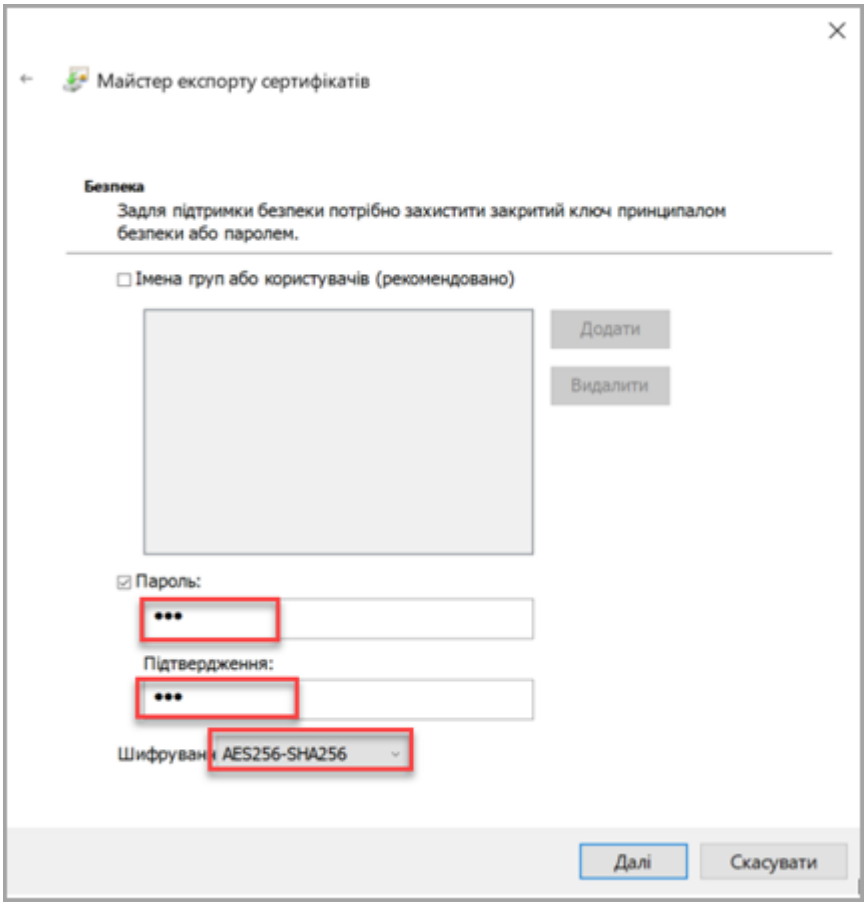


Зауваження. Якщо ця опція недоступна, зверніться до вашого КНЕДП для отримання сертифіката в форматі pfx (див. розділ Імпорт сертифіката в сховище).

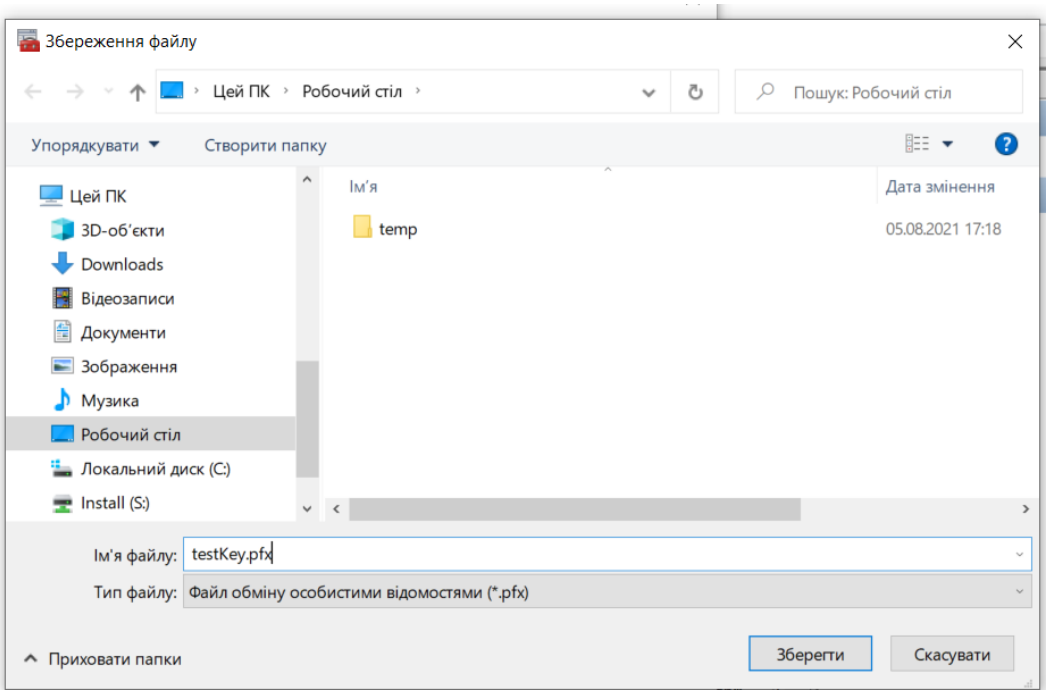
3. Для експорту в форматі pfx оберіть **Файл обміну особистими відомостями – PKCS #12**:



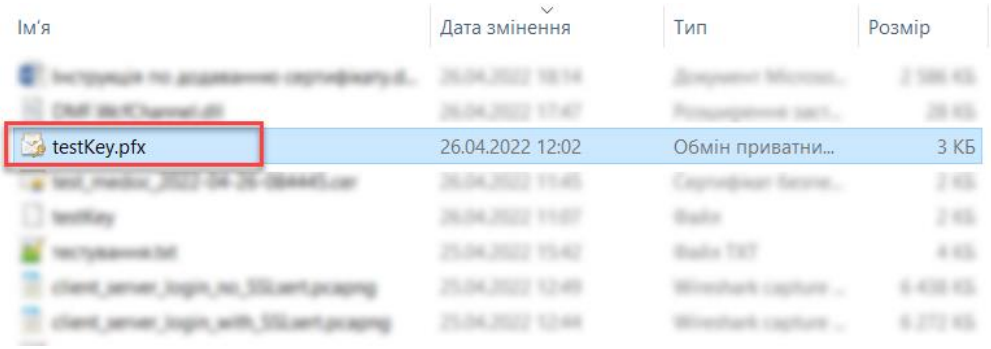
4. Введіть пароль з підтвердженням, оберіть тип шифрування



5. Вкажіть ім'я і шлях збереження файлу сертифіката:



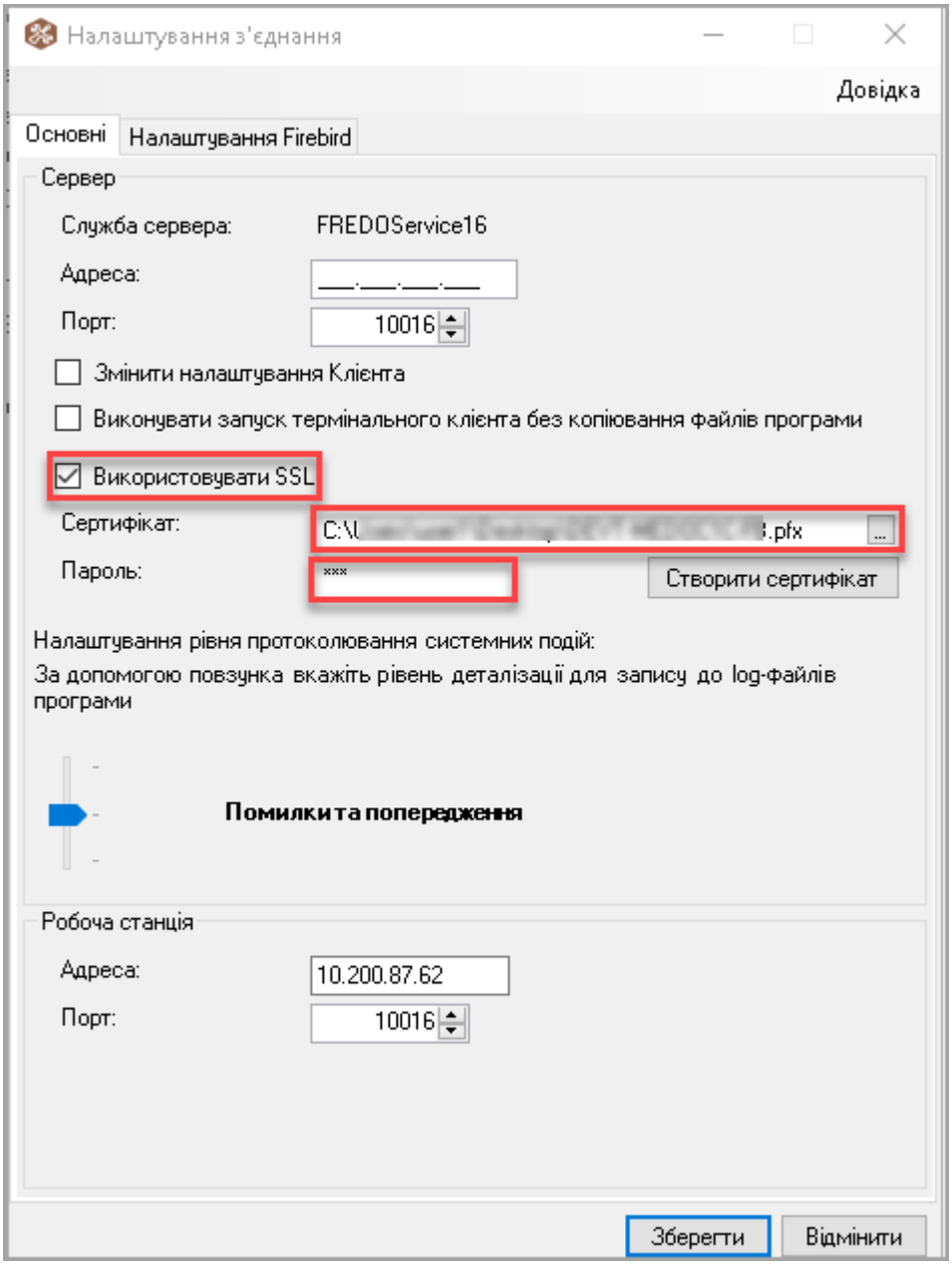
6. У вказаний каталог буде експортовано сертифікат у форматі pfx:



Підключення сертифіката

1. Запустіть з правами адміністратора утиліту **ConnectionSetup.exe**, яка знаходиться в кореневій папці встановленої програми FREDO.
   (наприклад, c:\Program Files\FREDO\FREDO \ConnectionSetup.exe)
2. Встановіть опцію **Використовувати SSL**.
3. В полі **Сертифікат** вкажіть шлях до сертифіката у форматі pfx.
4. В полі **Пароль** введіть пароль сертифіката.
5. Натисніть **Зберегти**".

При використанні функції **Створити сертифікат** шлях до сертифіката і пароль автоматично заповнюються вказаними в функції даними.


Налаштування з'єднання
Довідка
Основні
Налаштування Firebird
Сервер
Служба сервера:
FREDOService16
Адреса:
Порт:
10016
Змінити налаштування Клієнта
Виконувати запуск термінального клієнта без копіювання файлів програми
Використовувати SSL
Сертифікат:
.pfx
Пароль:
***
Створити сертифікат
Налаштування рівня протоколювання системних подій:
За допомогою повзунка вкажіть рівень деталізації для запису до log-файлів програми
Помилки та попередження
Робоча станція
Адреса:
10.200.87.62
Порт:
10016
Зберегти
Відмінити