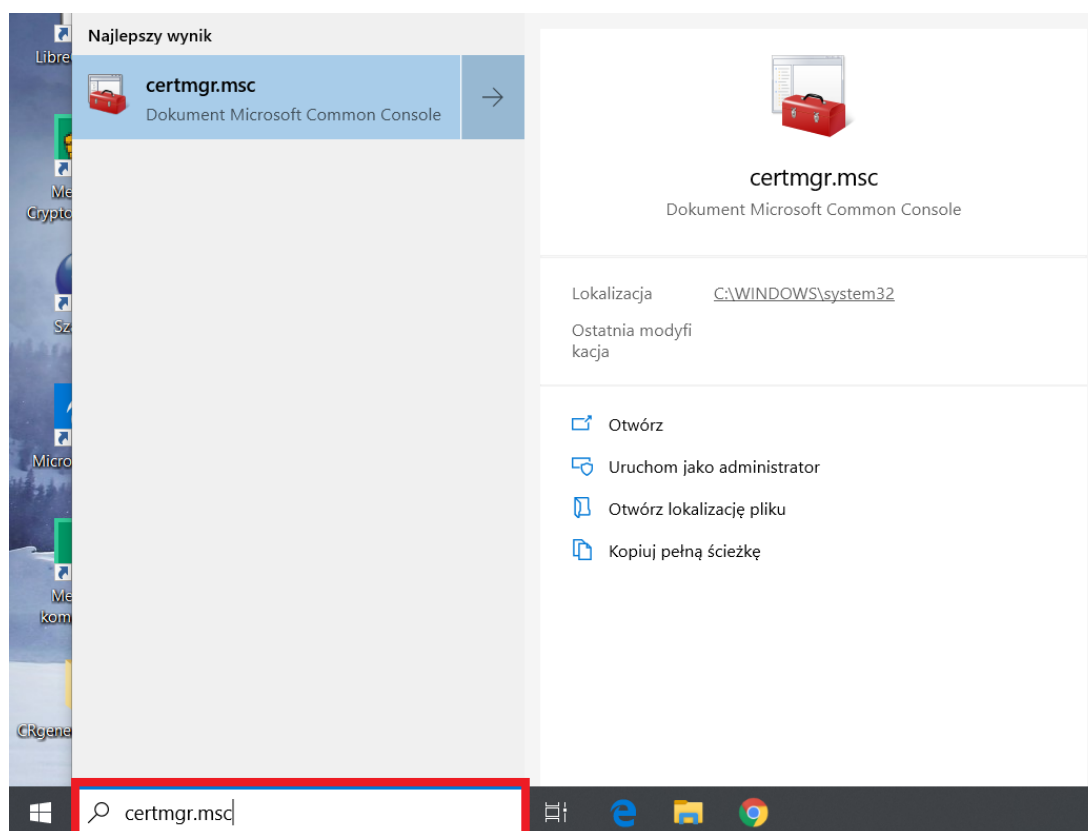


INTERNET BANKING DLA FIRM – OPIS ODNOWIENIA CERTYFIKATU OSOBISTEGO

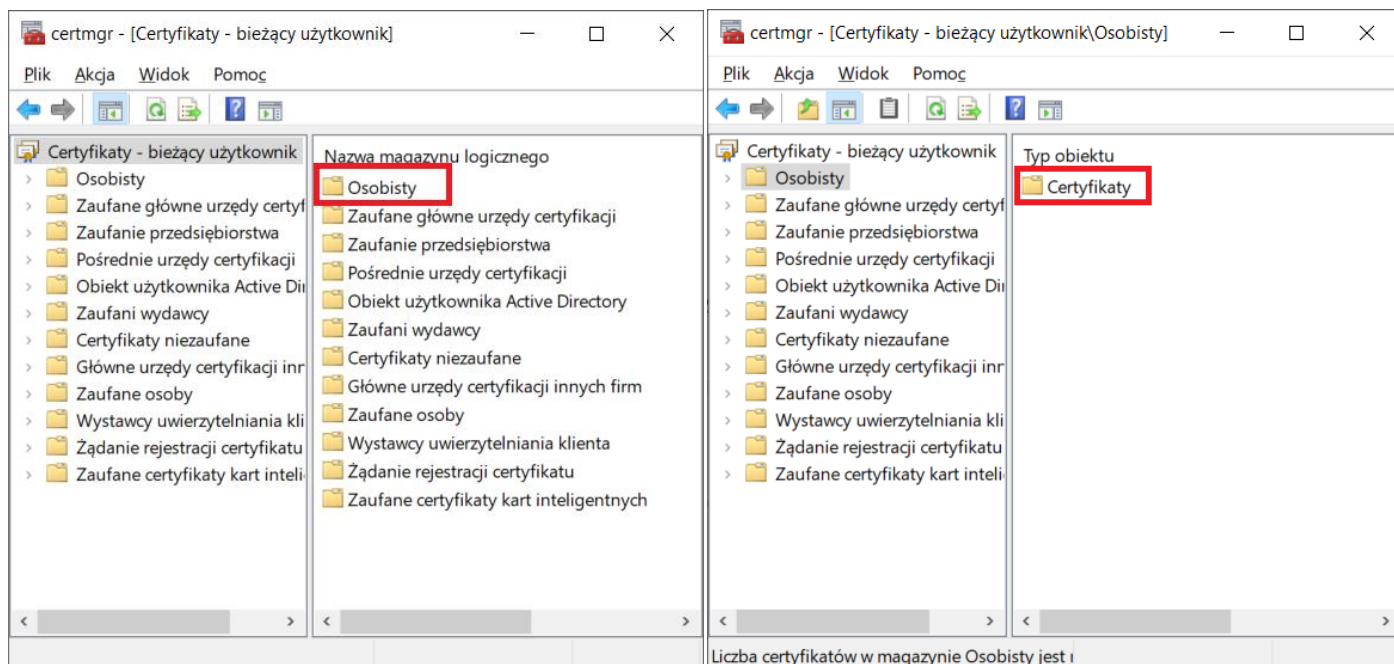
SPRAWDZENIE POPRAWNOŚCI INSTALACJI ODNOWIONEGO CERTYFIKATU

Pierwszym krokiem do weryfikacji poprawności instalacji naszego odnowionego certyfikatu będzie sprawdzenie, czy został on poprawnie zarejestrowany w *Systemowym Magazynie Certyfikatów*. W tym celu:

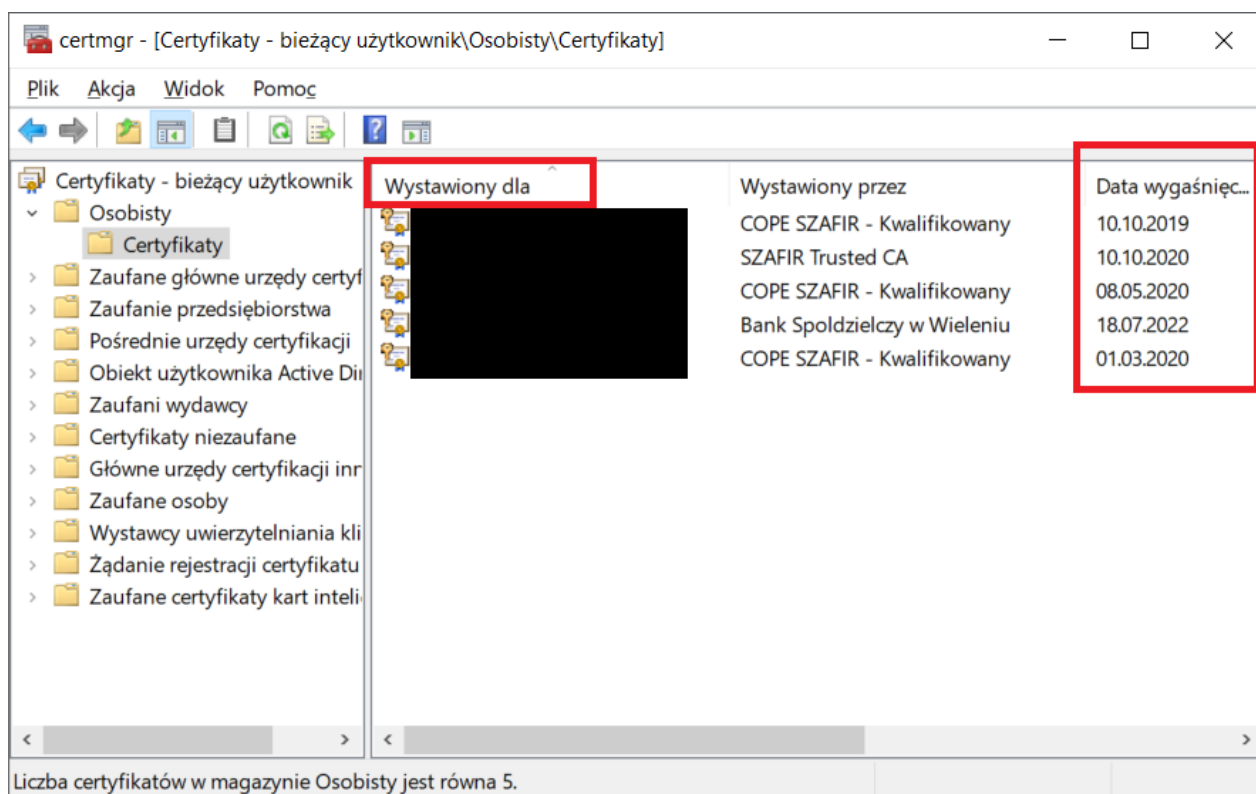
1. W lewym dolnym rogu ekranu klikamy na biały pasek oznaczony lupą (Windows 10) lub flagę (Windows 7), wpisujemy frazę „*certmgr.msc*”, a następnie wciskamy klawisz *Enter*



2. W nowo otwartym oknie wchodzimy w folder „Osobisty”, a następnie „Certyfikaty”

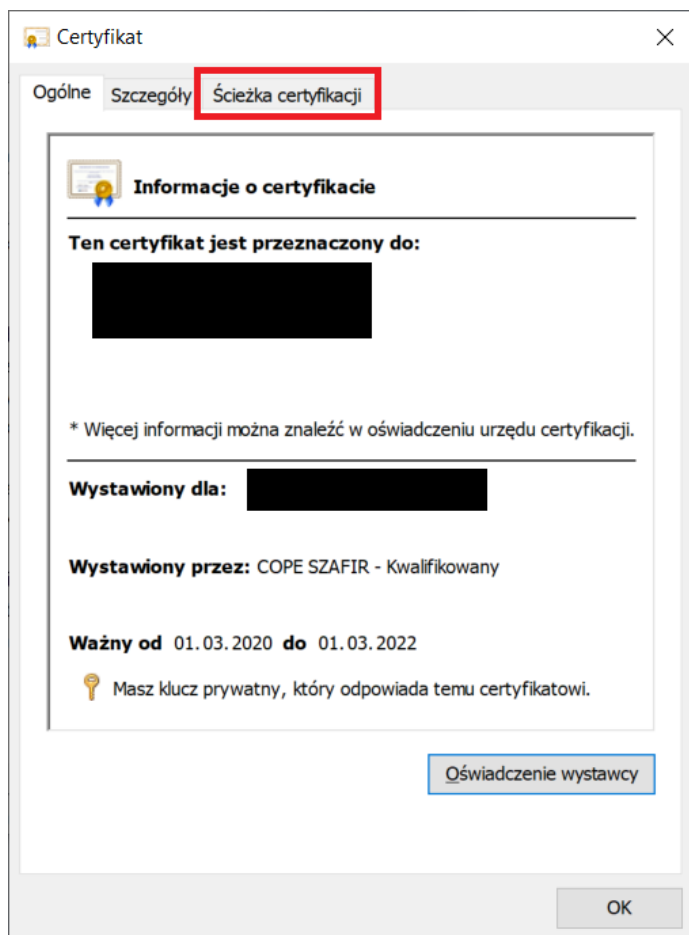


3. Następnie na widocznej liście wyszukujemy nasz odnowiony certyfikat i wchodzimy w niego. Aby przypadkowo nie wybrać jakiegoś przestarzałego, oprócz samego imienia i nazwiska sprawdzamy również datę wygaśnięcia w odpowiedniej kolumnie



Jeżeli na powyższej liście nie możemy odnaleźć certyfikatu, który nas interesuje, oznacza to, że nie został on poprawnie zarejestrowany w *Systemowym Magazynie Certyfikatów* i należy to zrobić za pomocą odpowiedniego narzędzia, w zależności od pochodzenia certyfikatu np. CryptoCard Monitor lub proCertumCardManager.

4. W nowo wyświetlonym oknie przechodzimy do zakładki „Ścieżka certyfikacji”



The screenshot shows a window titled "Certyfikat" with three tabs: "Ogólne", "Szczegóły", and "Ścieżka certyfikacji". The "Ścieżka certyfikacji" tab is selected and highlighted with a red rectangle. The main content area is titled "Informacje o certyfikacie" and contains the following text:

Ten certyfikat jest przeznaczony do:


[Redacted]

* Więcej informacji można znaleźć w oświadczeniu urzędu certyfikacji.

Wystawiony dla: [Redacted]

Wystawiony przez: COPE SZAFIR - Kwalifikowany

Ważny od 01.03.2020 **do** 01.03.2022

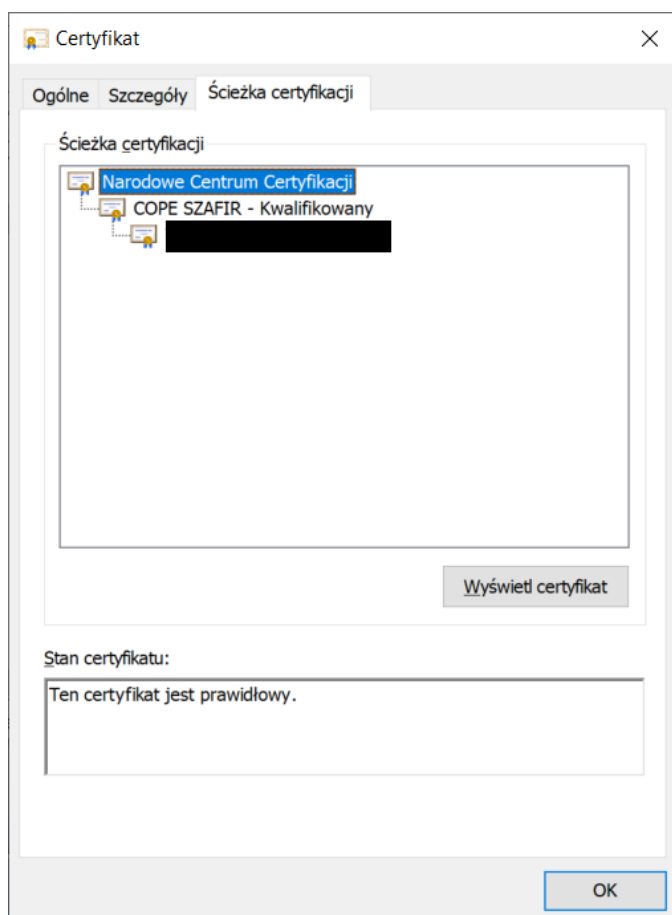
 Masz klucz prywatny, który odpowiada temu certyfikatowi.

At the bottom right of the main content area is a button labeled "Oświadczenie wystawcy". At the very bottom right of the window is an "OK" button.

5. W tym kroku sprawdzamy, czy nasza ścieżka certyfikacji wygląda podobnie do tej przedstawionej na grafice poniżej (powinna składać się z trzech części). Sprawdzamy zatem, czy przy żadnej z pozycji nie pojawia się ikona żółtego wykrzyknika. Najczęstszym problemem, występującym na tym etapie, jest brak certyfikatów pochodzących z *Narodowego Centrum Certyfikacji*. Można je pobrać tutaj (zalecamy pobranie i zainstalowanie obu):

<https://www.nccert.pl/files/nccert2016.crt>

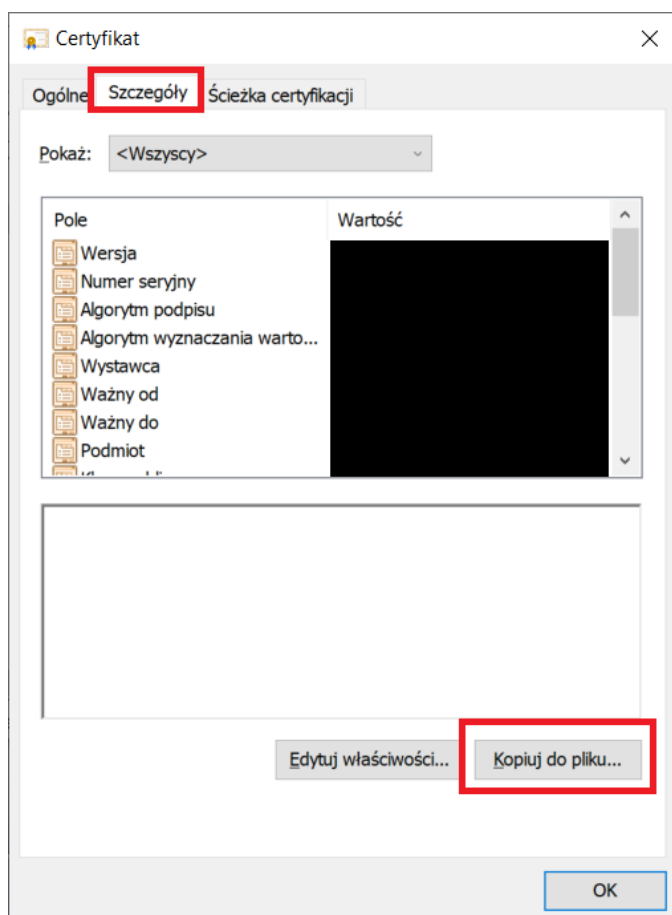
<https://www.nccert.pl/files/nccert.crt>



EKSPORT ODNOWIONEGO CERTYFIKATU DO PLIKU

Kolejnym krokiem jest wyeksportowanie naszego odnowionego certyfikatu z *Systemowego Magazynu Certyfikatów* do pliku w formacie .cer. W tym celu:

1. Będąc w tym samym oknie, przechodzimy do zakładki „Szczegóły”, a następnie klikamy w opcję „Kopiuj do pliku”



2. W nowo otwartym oknie klikamy przycisk „Dalej”

←  Kreator eksportu certyfikatów



Kreator eksportu certyfikatów — Zapraszamy!

Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z magazynu certyfikatów na dysk.

Certyfikat, wystawiany przez urząd certyfikacji, stanowi potwierdzenie tożsamości użytkownika i zawiera informacje używane do ochrony danych lub do ustanawiania bezpiecznych połączeń sieciowych. Magazyn certyfikatów jest obszarem systemowym, w którym przechowywane są certyfikaty.



Aby kontynuować, kliknij przycisk Dalej.

Dalej

Anuluj

3. Następnie upewniamy się, czy zaznaczona jest opcja „*Nie eksportuj klucza prywatnego*” (jeżeli nie, to ją zaznaczamy) i klikamy „*Dalej*”

✕

  Kreator eksportu certyfikatów

Eksportowanie klucza prywatnego

Możesz wybrać eksport klucza prywatnego razem z certyfikatem.

Klucze prywatne są chronione hasłem. Aby wyeksportować klucz prywatny z certyfikatem, musisz wpisać hasło na jednej z kolejnych stron.

Czy chcesz wyeksportować klucz prywatny wraz z certyfikatem?

☐ Tak, eksportuj klucz prywatny

☒ Nie eksportuj klucza prywatnego


Uwaga: nie można odnaleźć skojarzonego klucza prywatnego. Można wyeksportować jedynie certyfikat.

Dalej

Anuluj

4. Zgodnie z obrazkiem poniżej, zaznaczamy format „*Certyfikat X.509 szyfrowany algorytmem Base-64 (CER)*” i klikamy „*Dalej*”

×

←  Kreator eksportu certyfikatów

Format pliku eksportu
Certyfikaty mogą być eksportowane w wielu różnych formatach plików.

Wybierz format, którego chcesz użyć:

- ☐ Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER)
- ☒ Certyfikat X.509 szyfrowany algorytmem Base-64 (CER)
- ☐ Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B)
 - ☐ Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji
- ☐ Wymiana informacji osobistych — PKCS #12 (PFX)
 - ☐ Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji
 - ☐ Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie
 - ☐ Eksportuj wszystkie właściwości rozszerzone
 - ☐ Włącz funkcję prywatności certyfikatu
- ☐ Magazyn certyfikatów seryjnych firmy Microsoft (SST)

Dalej

Anuluj



5. Następnie klikamy w przycisk „Przeglądaj”

Kreator eksportu certyfikatów

Eksport pliku
Określ nazwę pliku, który chcesz wyeksportować

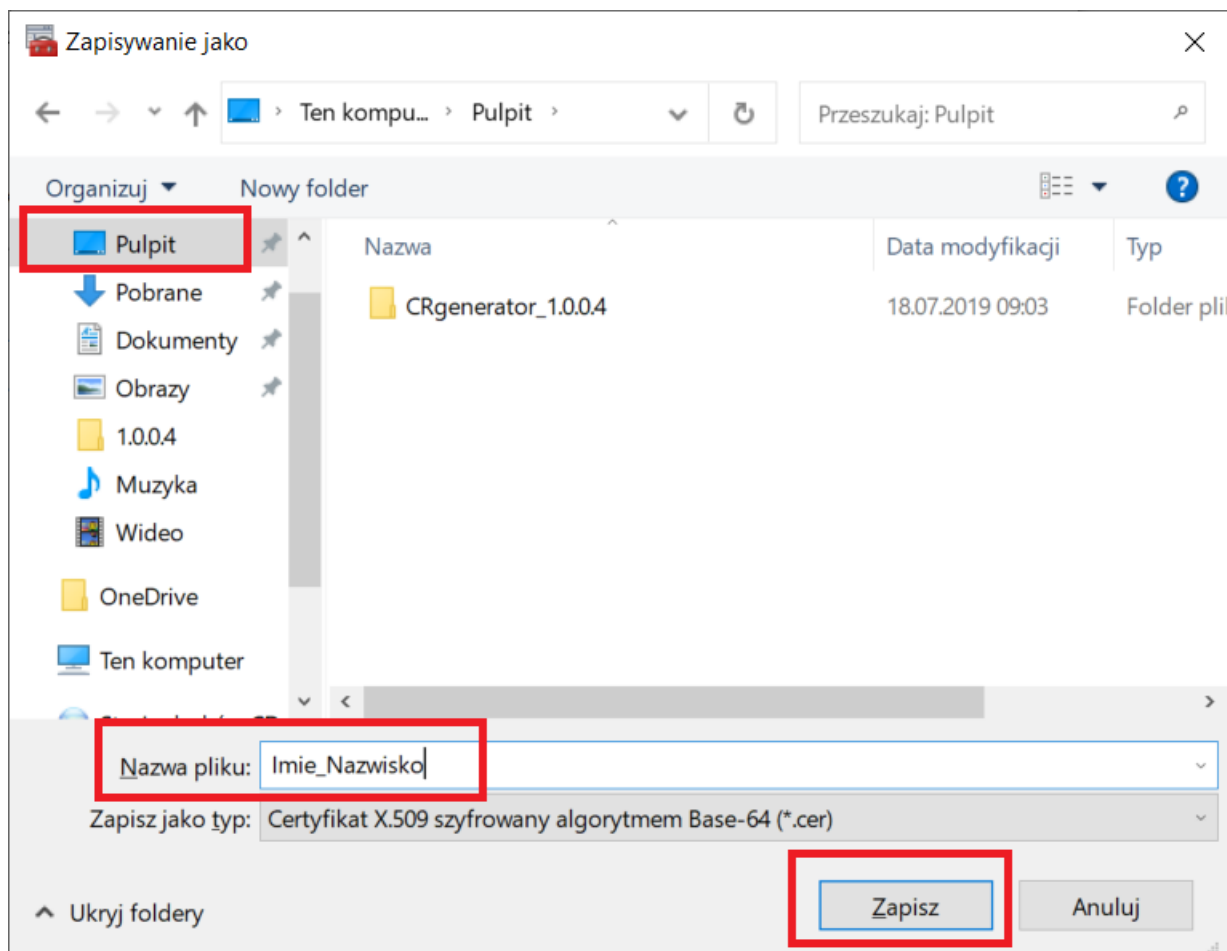
Nazwa pliku:

Przeglądaj...


Dalej



Anuluj

6. Wskazujemy miejsce, do którego chcemy wyeksportować nasz plik certyfikatu (zalecamy pulpit) oraz w polu „Nazwa pliku” wpisujemy imię i nazwisko właściciela certyfikatu (bez polskich znaków diakrytycznych) wg. poniższego schematu np. Jan_Kowalski. Następnie klikamy w przycisk „Zapisz”



7. W polu „Nazwa pliku” pojawiła się nazwa pliku naszego certyfikatu oraz ścieżka, do której zostanie on wyeksportowany. Jeżeli wszystko się zgadza, klikamy w przycisk „Dalej”



  Kreator eksportu certyfikatów

Eksport pliku
Określ nazwę pliku, który chcesz wyeksportować

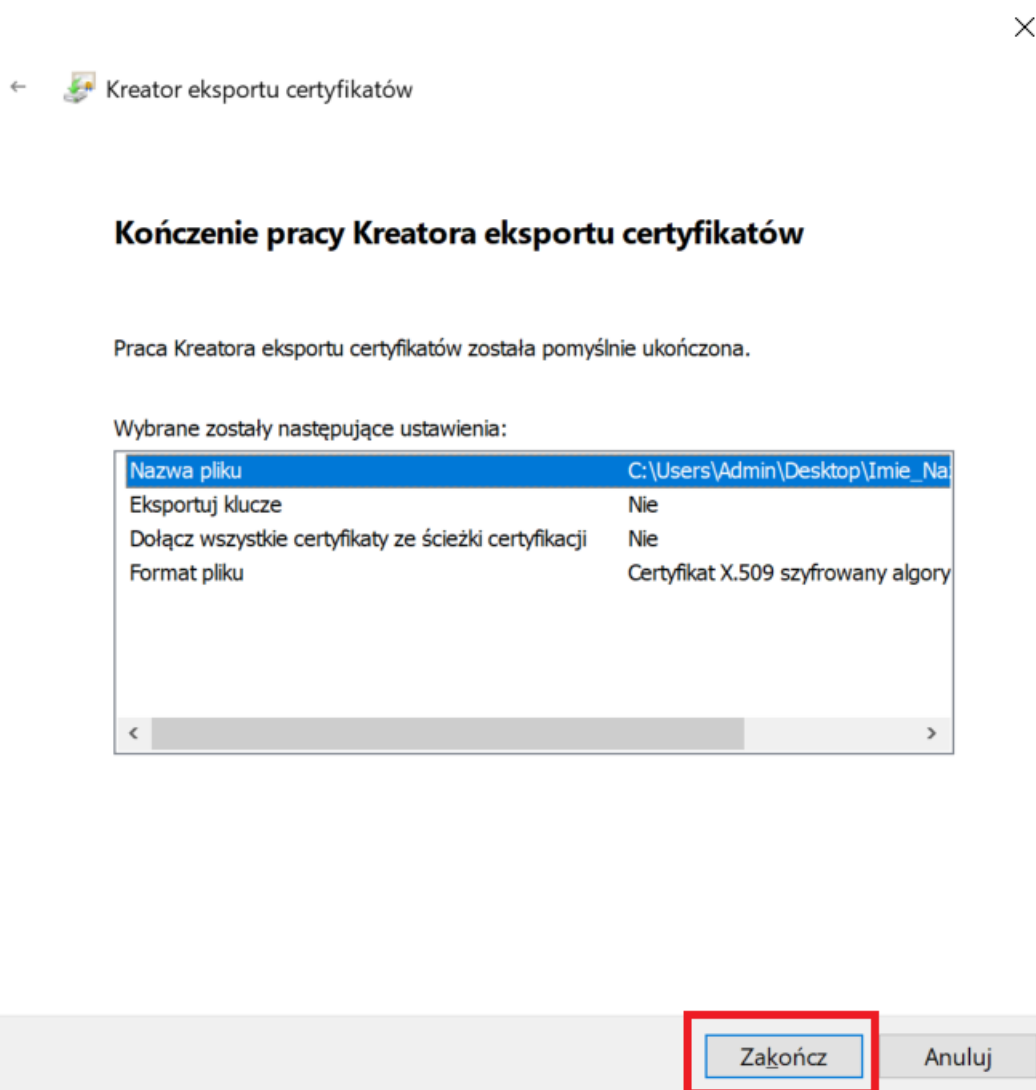
Nazwa pliku:
C:\Users\Admin\Desktop\Imie_Nazwisko.cer

Przeglądaj...

Dalej

Anuluj

8. Następnie klikamy w przycisk „Zakończ”

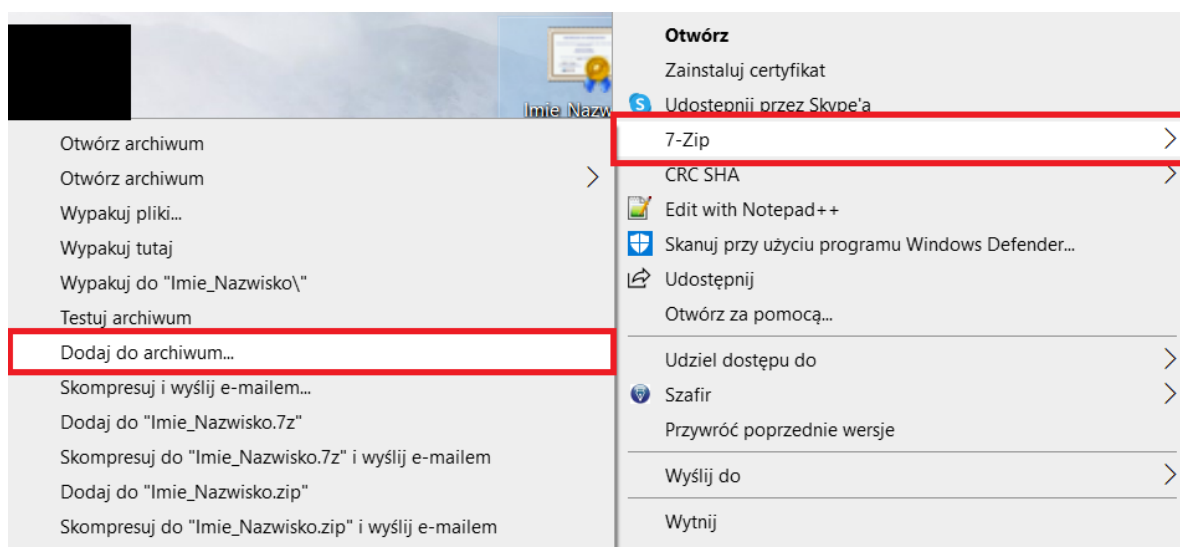


Komunikat o treści: „Eksport zakończył się pomyślnie”, powiadamia nas, że wszystkie czynności wykonaliśmy poprawnie i możemy przejść do kolejnego etapu.

ZABEZPIECZENIE WYEKSPORTOWANEGO PLIKU ORAZ PRZESŁANIE POCZTĄ ELEKTRONICZNĄ DO BANKU

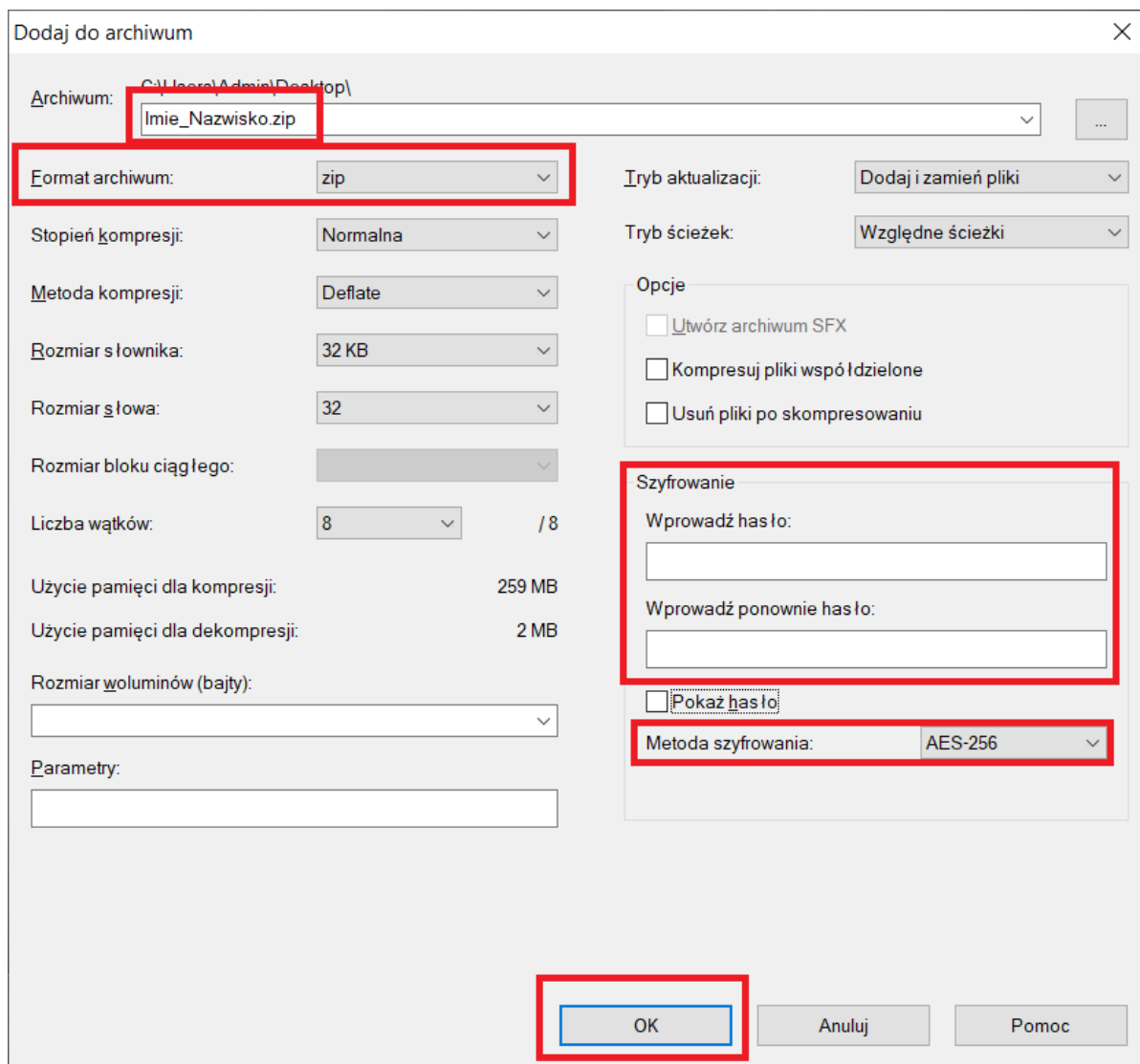
Ostatnim już krokiem procesu odnawiania certyfikatu kwalifikowanego jest spakowanie go do archiwum zabezpieczonym hasłem oraz przesłanie do Banku Spółdzielczego w Wieleniu w celu podjęcia dalszych czynności.

1. Upewniamy się, że na naszym komputerze zainstalowane jest oprogramowanie *7-Zip*. Link do pobrania tutaj:
<https://7-zip.org.pl/>
2. Odnajdujemy nasz wyeksportowany plik certyfikatu i klikamy na niego prawym przyciskiem myszy. Następnie wybieramy *7-Zip* -> *Dodaj do archiwum...*



3. W nowo otwartym oknie ustawiamy wszystko tak jak na poniższym obrazku:
 - Archiwum: *tutaj nazwa naszego pliku certyfikatu z dopiskiem .zip np. Jan_Kowalski.zip*
 - Format archiwum: *zip*
 - Metoda szyfrowania: *AES-256*

Zabezpieczamy nasze archiwum dowolnym hasłem, uzupełniając pole „Wprowadź hasło” oraz „Wprowadź ponownie hasło”. Następnie klikamy w przycisk „OK”



4. Nowo powstałe archiwum przesyłamy pocztą elektroniczną na adres m.milcarz@bswielen.pl. Hasło, które założyliśmy w poprzednim kroku, wysyłamy na ten sam adres dla bezpieczeństwa w oddzielnej wiadomości. W przeciągu kilku godzin powinniśmy otrzymać odpowiedź z potwierdzeniem pomyślnego odnowienia certyfikatu kwalifikowanego w Bankowości Elektronicznej Banku Spółdzielczego w Wieleniu.