

system obsługi banku Novum Bank Enterprise NOE

Internet Banking - generacja certyfikatu i obsługa karty Vasco Digipass KEY101

Instrukcja Użytkownika

Wersja 1.0

I. Obsługa certyfikatu dla pracownika firmy – karta KEY101

1. Przygotowanie karty do wydania klientowi

Klient banku powinien otrzymać:

- kartę kryptograficzną **Vasco Digipass KEY101**
- oprogramowanie **SafeSign**



Programy dostępne są na FTP:/support/install/IB podpis cyfrowy/vasco KEY101 i muszą być udostępnione klientowi wraz z kartą kryptograficzną.

2. Karta już jest sformatowana.



Uwaga! – Powtórne formatowanie zmienia predefiniowany PIN użytkownika i administratora.

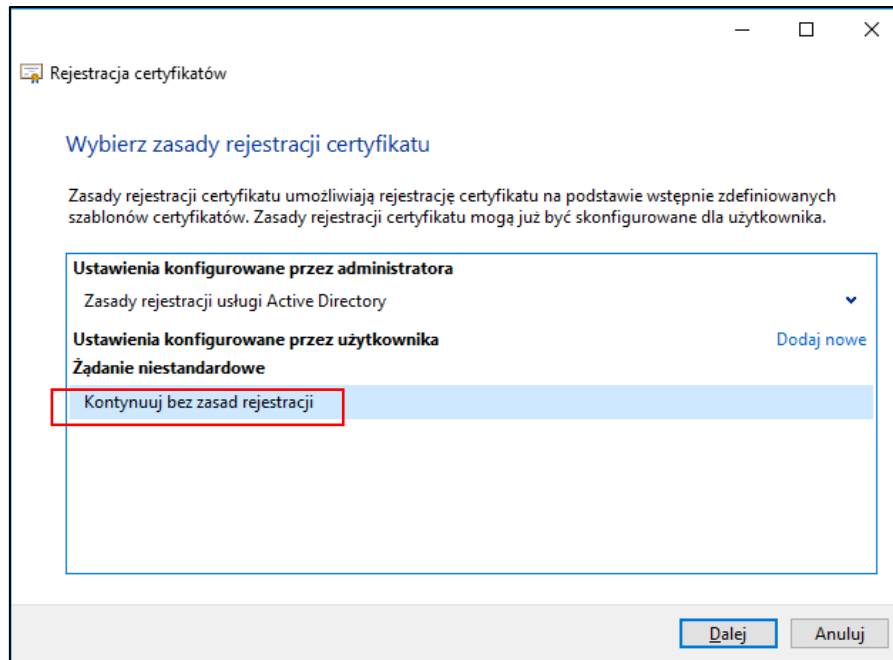
Klient banku musi u siebie w komputerze:

- zainstalować dostarczone oprogramowanie (**SafeSign**)
- zmienić **PIN** karty, predefiniowany PIN użytkownika to 1111, jeśli pozostanie bez zmian to aplikacja podpisu może nie działać prawidłowo. Zmieniony **PIN** ma być znany tylko osobie podpisującej nim przelewy.

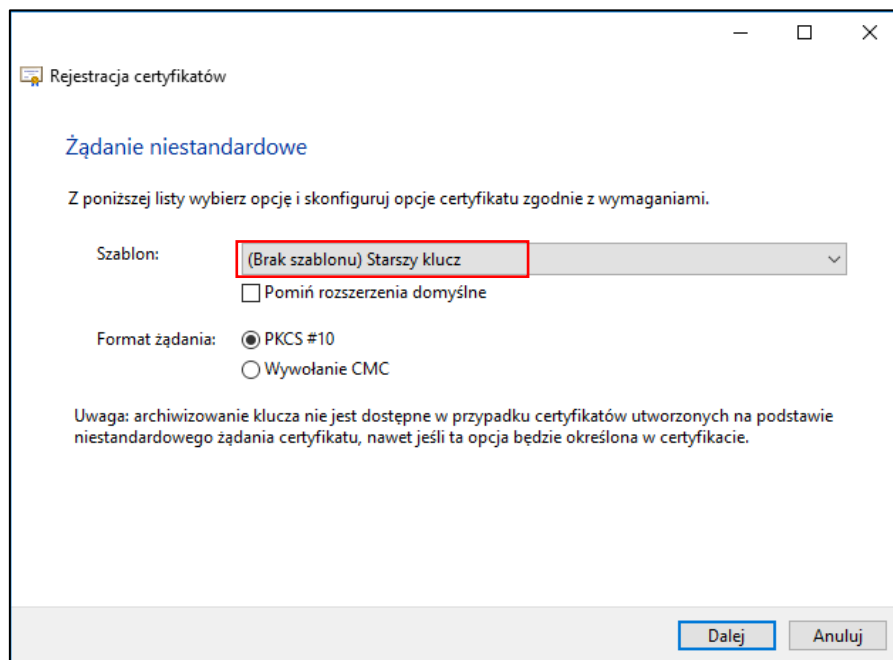
3. ETAP I - Generacja wniosku o certyfikację dla kart Vasco Digipass KEY101

Etap I powinien wykonać właściciel/pracownik firmy (klient banku – osoba używająca karty)

1. Zainstaluj program zarządzający kartami elektronicznymi – **SafeSign** (są to sterowniki urządzenia + zarządzanie PIN-ami i certyfikatami na karcie).
2. U uruchom certmgr.msc. W programie należy wybrać w kolejności:
 - Certyfikaty -> Bieżący użytkownik -> Osobisty -> Certyfikaty
 - Zakładka **Akcja** -> Wszystkie zadania -> Operacje zaawansowane -> Utwórz żądanie niestandardowe -> Dalej
 - należy wybrać: **Kontynuuj bez zasad rejestracji**

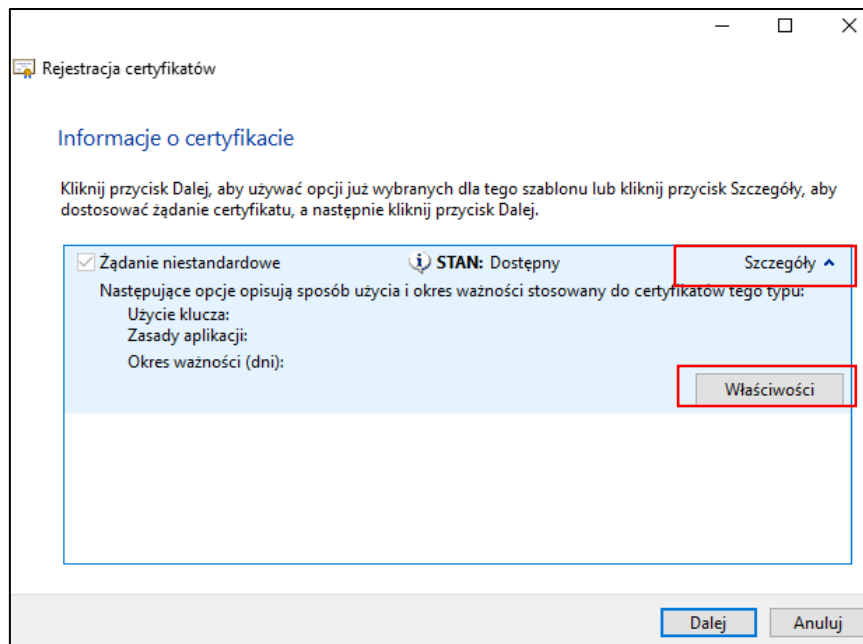


- W opcji Szablon należy wskazać: (Brak szablonu) Starszy klucz,
 - W opcji Format zadania: format zaznaczony domyślnie
- Potwierdzamy przyciskiem: Dalej

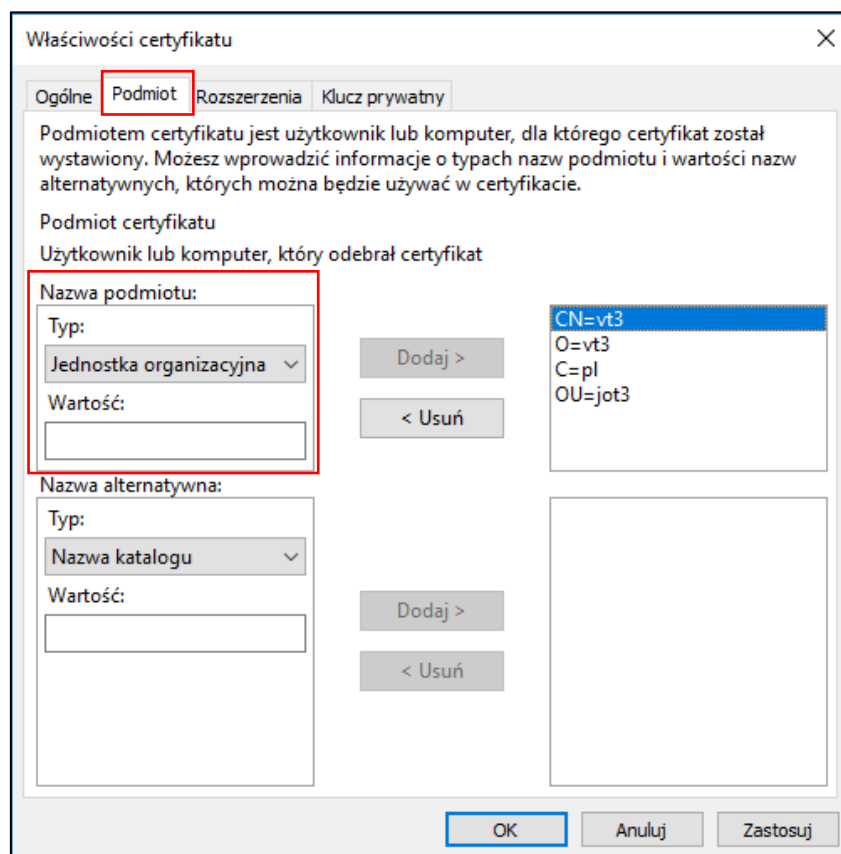


- W opcji Szczegóły:

Właściwości certyfikatu → Zakładka Podmiot

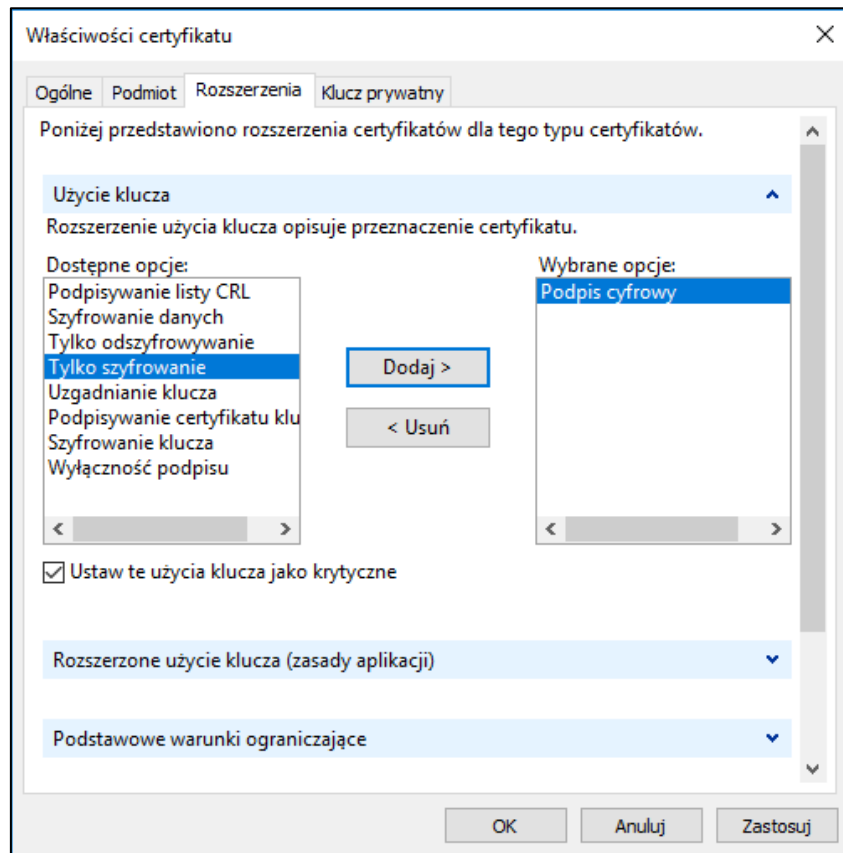


W oknie Właściwości certyfikatu należy uzupełnić dane **Nazwa podmiotu** wybieramy: Jednostka organizacyjna, Nazwa pospolita, Kraj, Organizacja, i wpisujemy **Wartość** – nazwę – >zatwierdzamy Dodaj->Zastosuj



W opcji Szczegóły:

Właściwości certyfikatu -> Zakładka Rozszerzenia -> Użycie klucza -> należy wybrać jn:



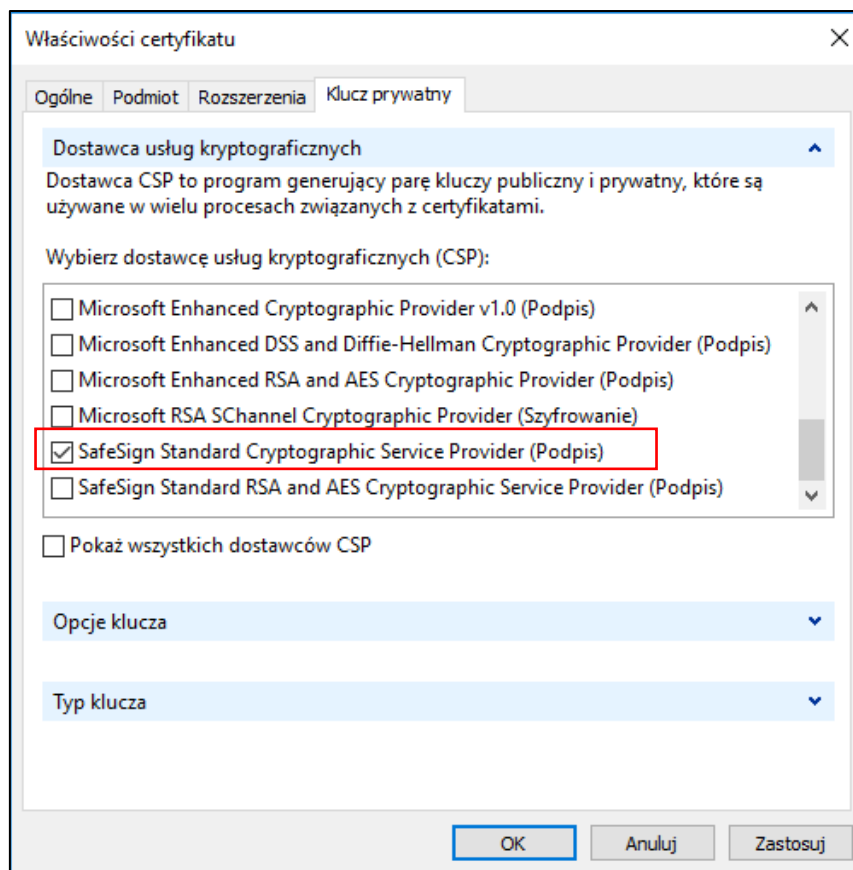
W opcji Szczegóły:

Właściwości certyfikatu -> Klucz prywatny -> Dostawca usług kryptograficznych -> należy odznaczyć opcję domyślną

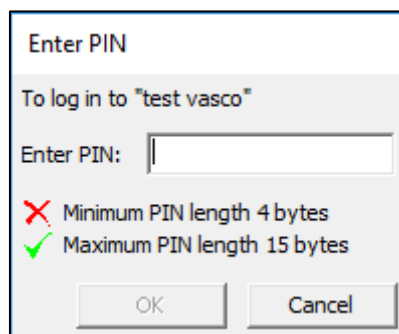
Microsoft Strong Cryptographic Provider (Podpis)

a zaznaczyć opcję

SafeSign Standard Cryptographic Service Provider (Podpis)



Należy potwierdzić Zastosuj, OK, Dalej.
Pojawi się okno wpisania PINU: domyślnie to 1111



- otrzymuję plik żądania xxx.req. W pliku zmieniamy rozszerzenie na *.p10. Zapisujemy.

Tak utworzony plik z rozszerzeniem *.p10 (wniosek o certyfikację) należy dostarczyć do Banku, gdzie zostanie wygenerowany certyfikat w systemie NOE.

4. ETAP II - Generacja certyfikatu w systemie Novum Bank

W module INTERNET BANKING – administracja należy otworzyć okno szczegółowych danych pracownika (tego, dla którego generowany jest certyfikat): **USTAWIENIA...** nazwisko imię (Id = ...), (FIRMY → EDYTUJ → EDYCJA OSOBY)

Kowalska Eliza Ident: 10222512 (ID = 799)

Król sp. z o.o. (ID = 27690) Zwykły użytkownik

Certyfikat nr: 633 Ważny do: 2022-08-16 Założony: 2016-03-17

Blokada od dnia: Udane logowanie: 2019-08-19 14:36:10

Wyłącz powiadomienia o naruszeniu CSP Nieudane logowanie: 2019-06-18 09:04:11

Błędne próby logowania: 0

Klient	Konto	Subkonto	Wkład	Opis konta
3259	27013	101	0	RACHUNKI BIEŻĄCE PRZEDSIĘBIORSTW INDYWIDUALNYCH
3259	27016	101	0	RACHUNKI BIEŻĄCE PODMIOTÓW NIEFINANSOWYCH
3259	27016	101-9	0	Rachunki VAT dla 27016-101

Produkt: dla firm 44 8747 1018 0000 3259 2000 0010 Limit poj. oper. 999,999,999,999.00

Nazwa klienta: DMC spółka z o.o. Limit dzienny

Nazwa kliencka: Rachunek Firmy DMC Limit miesięczny

Nazwa bankowa: RACHUNKI BIEŻĄCE PRZEDSIĘBIORSTW INDYWIDUALNYCH 27013-101 Limit w sklepie 700.00

Certyfikaty Hasło Poczta Limity Rachunek Uprawnienia Domyślne

Listy haseł Formularze Historia Przelewy Statystyka Ustawienia Esc zamknij

W wyświetlonym powyżej oknie wybieramy przycisk **Certyfikaty**, a w następnym oknie LISTA CERTYFIKATÓW KLIENTA wybieramy przycisk **Dopisz**.

Ustawienia Kowalska Eliza

Długość klucza: 1,024

Hasło do klucza banku: ●●●●

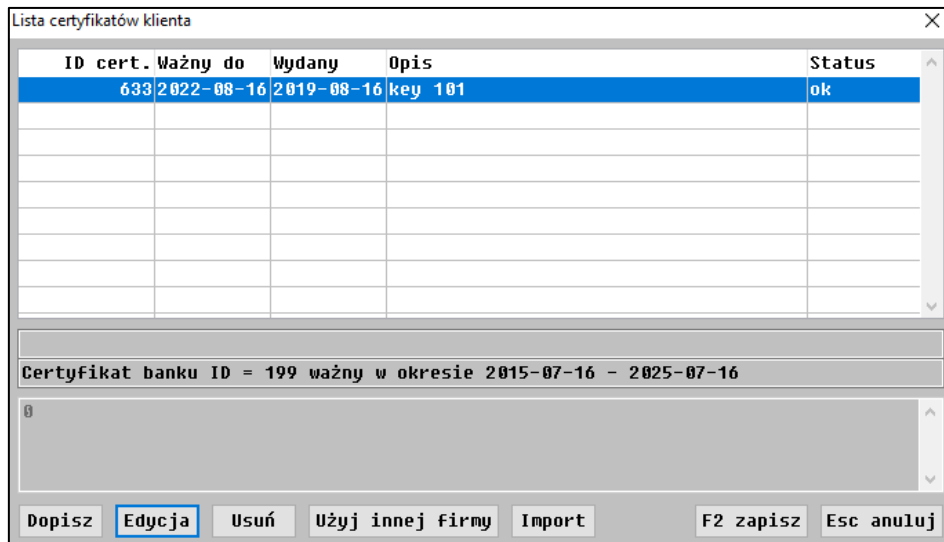
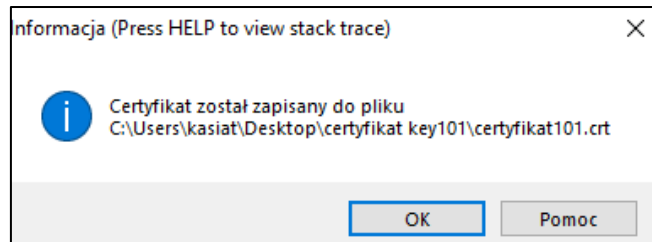
Ważny miesięcy: 36 Do dnia: 2022-08-21

Opis, numer seryjny karty:
key101

Wczytaj request, generuj certyfikat Esc anuluj

W oknie **USTAWIENIA...(IMIĘ I NAZWISKO)**, przykład powyżej, wprowadzić należy ustawienia dla tej osoby (wpisujemy hasło do klucza banku, okres ważności klucza – domyślnie 36 miesięcy, podajemy opis - zalecany nr seryjny karty), następnie klikamy **Wczytaj request, generuj certyfikat** i kojarzymy go z odpowiednim plikiem z żądaniem certyfikatu - *.p10. Potwierdzamy dane certyfikatu. Plik z certyfikatem zabezpieczającym o nazwie z wniosku o certyfikację i rozszerzeniu **crt** powstanie w tym samym katalogu, co plik *.p10.

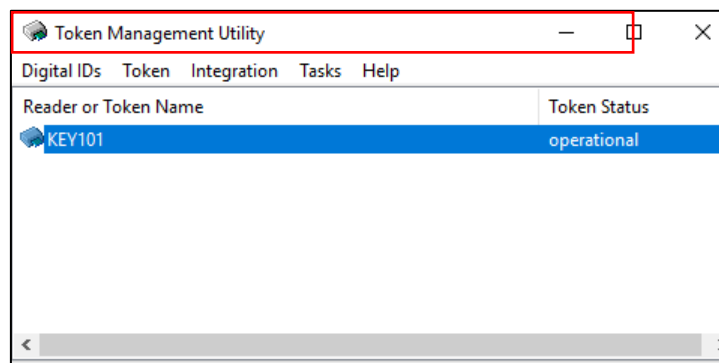
Certyfikat pracownika zostanie dopisany do listy jego certyfikatów, widoczny w oknie ustawień pracownika pod przyciskiem **Certyfikaty**.

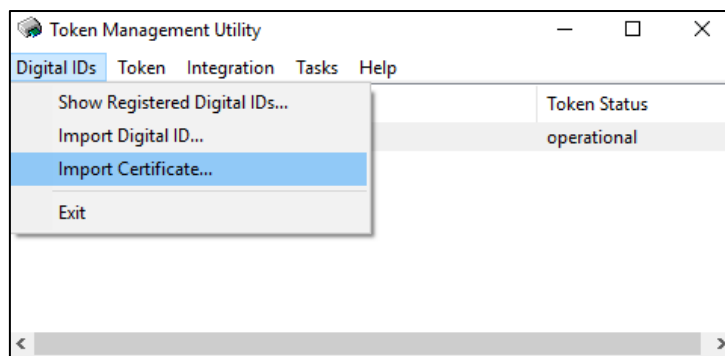


5. ETAP III - Zapis certyfikatu na kartę

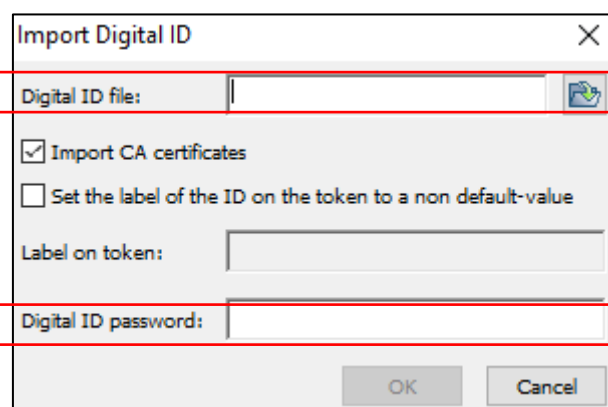
W celu zapisania certyfikatu na kartę należy uruchomić ponownie program SafeSign Token Management Utility i zaimportować certyfikat

Digital IDs -> Import Certificate...

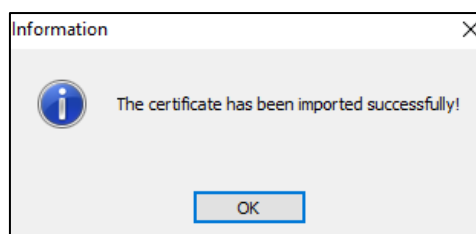




W momencie importu certyfikatu należy wskazać miejsce, z którego zostanie pobrany certyfikat oraz wpisać hasło certyfikatu

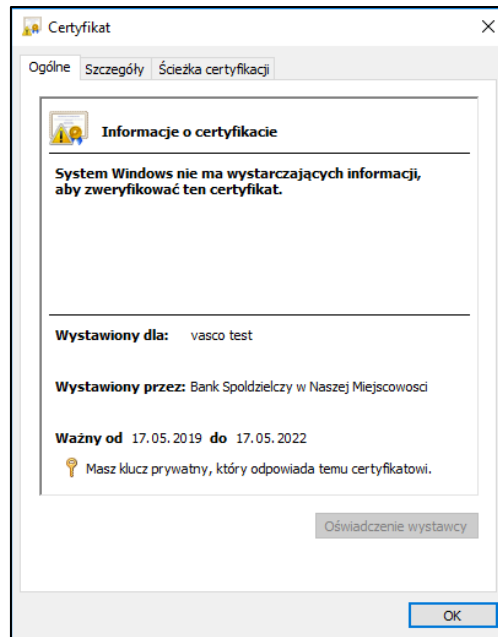


Proces poprawnego importu certyfikatu zakończy się komunikatem jn:



Tak wygenerowany certyfikat gotowy jest do podpisu przelewów przez pracownika firmy.

Po uruchomieniu certmgr.msc w folderze **Osobisty** -> **Certyfikaty** wygenerowany certyfikat powinien pojawić się na liście:



Spis treści

I.	Obsługa certyfikatu dla pracownika firmy – karta KEY101.....	1
1.	Przygotowanie karty do wydania klientowi	1
2.	Karta już jest sformatowana.....	1
3.	ETAP I - Generacja wniosku o certyfikację dla kart Vasco Digipass KEY101.....	1
4.	ETAP II - Generacja certyfikatu w systemie Novum Bank	6
5.	ETAP III - Zapis certyfikatu na kartę.....	7