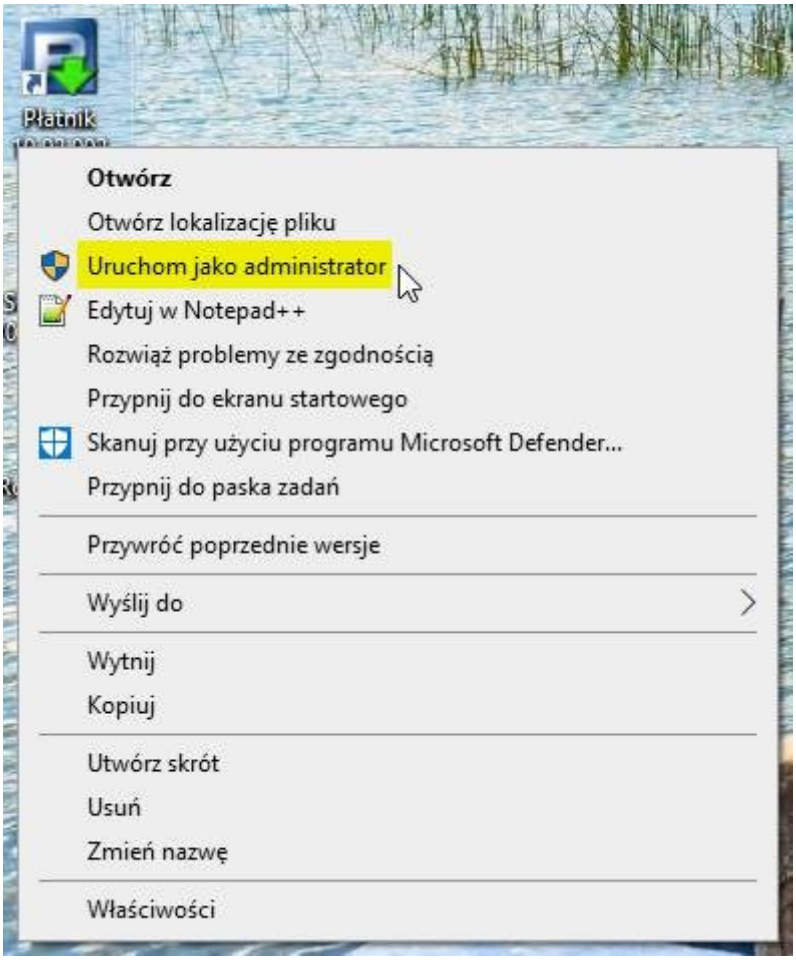
# Pierwsze uruchomienie programu Płatnik po aktualizacji do najnowszej wersji (metryka 334)

## Krok 1

W pierwszej kolejności uruchom program ***Płatnik*** jako administrator (na komputerze administrator lokalny).

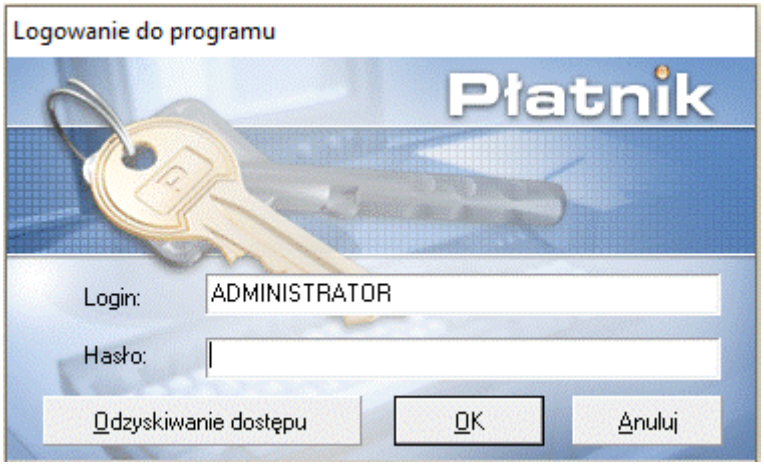



Kliknij prawym przyciskiem myszy na ikonie programu ***Płatnik*** i wybierz polecenie ***Uruchom jako administrator***.

## Krok 2

Podczas pierwszego logowania do zaktualizowanej wersji programu ***Płatnik*** wpisz **dotychczasowe hasło** do programu.

W tym etapie nie używaj nowego przycisku *Odzyskiwanie dostępu*.



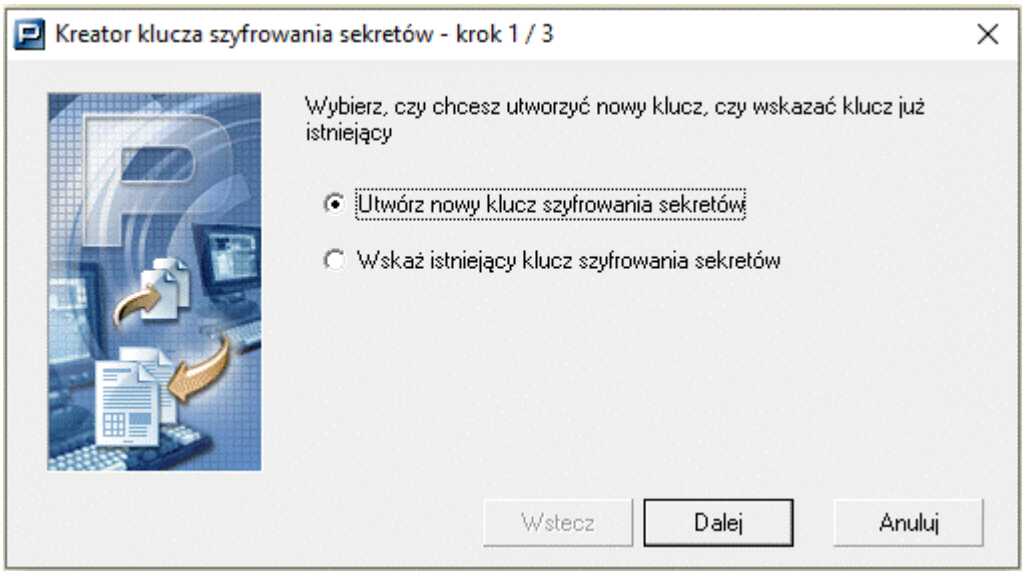

## Krok 3

Po zalogowaniu automatycznie uruchamiany jest **Kreator klucza szyfrowania sekretów**.

Aby użytkownik programu ***Płatnik*** miał możliwość pracy w programie (miał dostęp do bazy danych programu ***Płatnik***), musi zostać dodany do użytkowników certyfikatu.

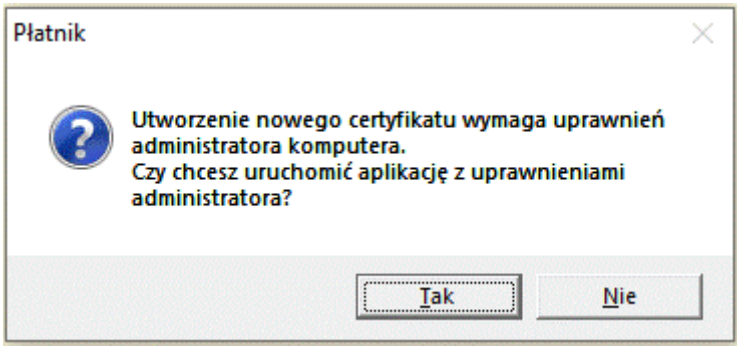
☞ Do pracy w kreatorze certyfikatu konieczne jest uprawienie administratora systemu Windows. Pojęcia administratorzy, grupy i użytkownicy występujące w kreatorze certyfikatu odnoszą się do uprawnień systemu Windows.

W pierwszym kroku **Kreatora klucza szyfrowania sekretów** wskaż opcję *Utwórz nowy klucz szyfrowania sekretów*



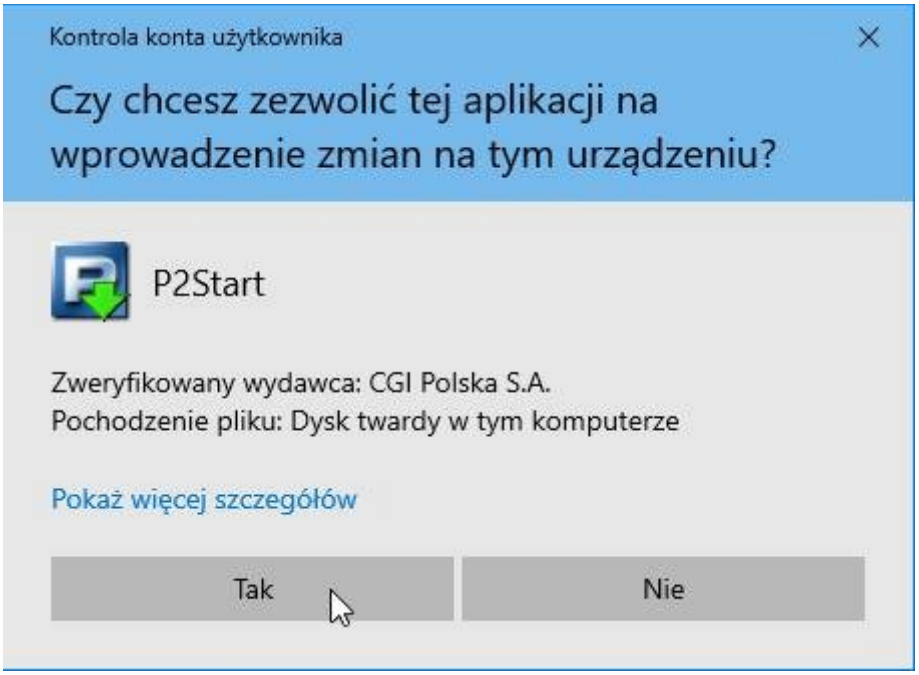

i wybierz przycisk **Dalej**.

Jeżeli nie zalogowałeś się jako administrator pojawi się poniższy komunikat




Kliknij przycisk **Tak.**

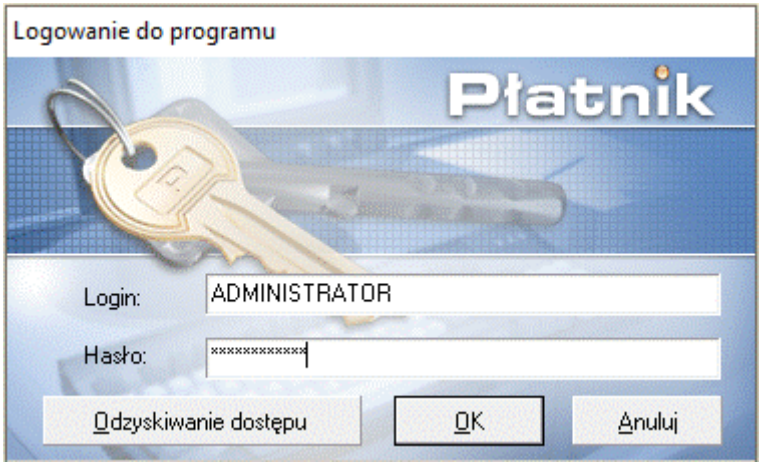
Wyświetlony zostanie systemowy ekran, w którym należy zezwolić na uruchomienie programu ***Płatnik*** z uprawnieniami administratora.



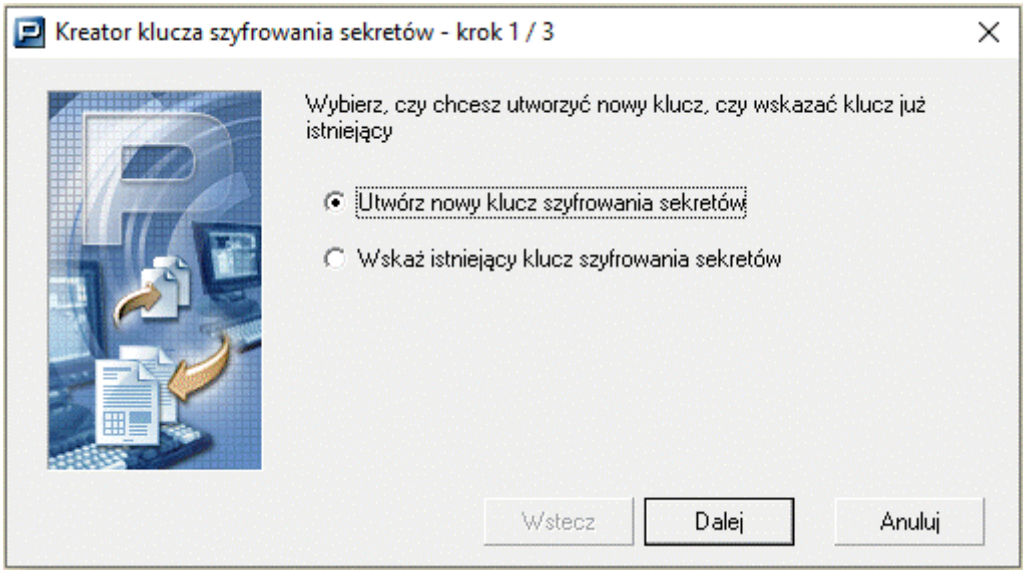

Kliknij przycisk **Tak.**

Program ***Płatnik*** uruchomi się ponownie z uprawnieniami administratora.

Ponownie zaloguj się do programu ***Płatnik*** dotychczasowym hasłem.

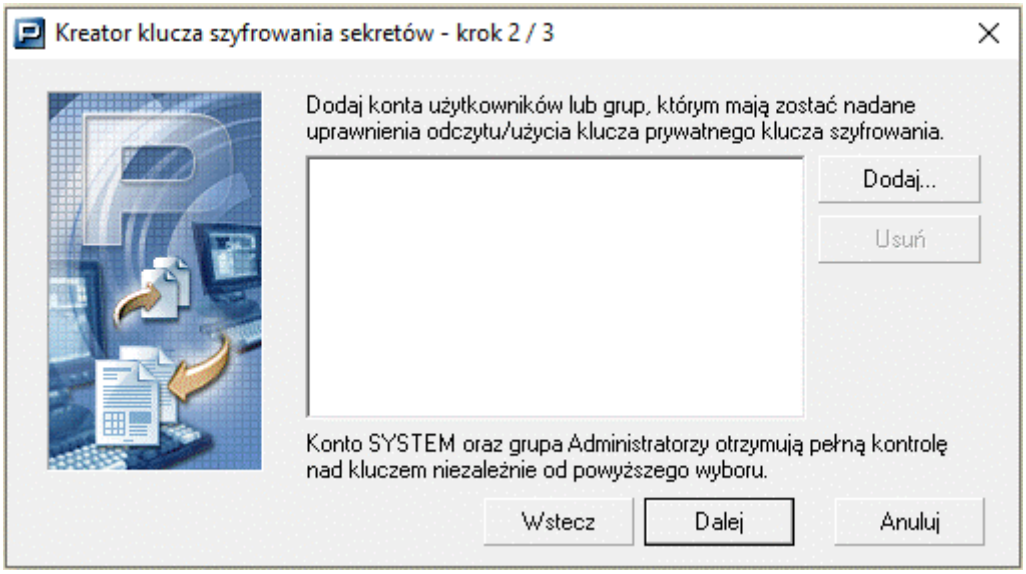



W Kreatorze wybierz ponownie opcję *Utwórz nowy klucz szyfrowania sekretów*




i wybierz przycisk **Dalej**.

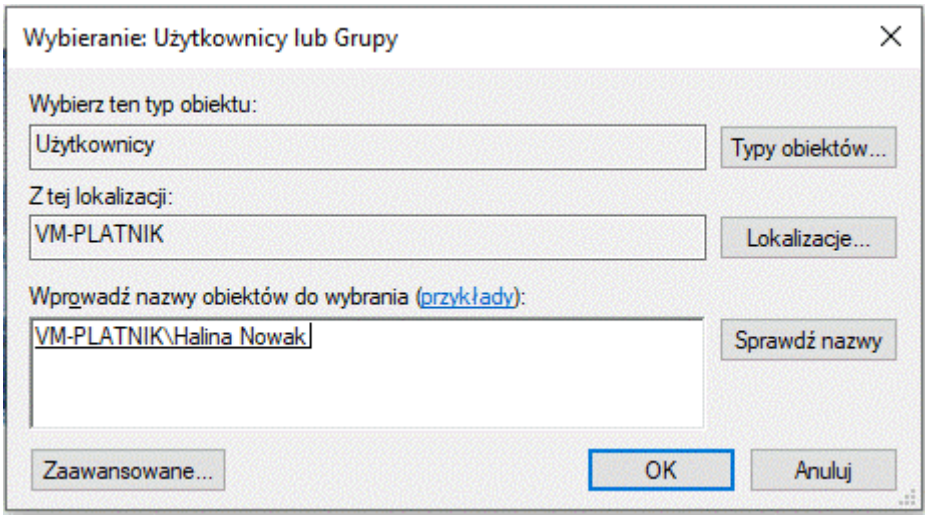
Dodaj do certyfikatu użytkowników systemowych klikając przycisk **Dodaj.**




☞ Zgodnie z informacją na formularzu, administratorzy systemu Windows są dodawani do certyfikatu automatycznie.

Dodaj pożądane obiekty (użytkownicy systemu, grupy użytkowników systemu) uprawnione do używania kluczy szyfrowania programu ***Płatnik***.

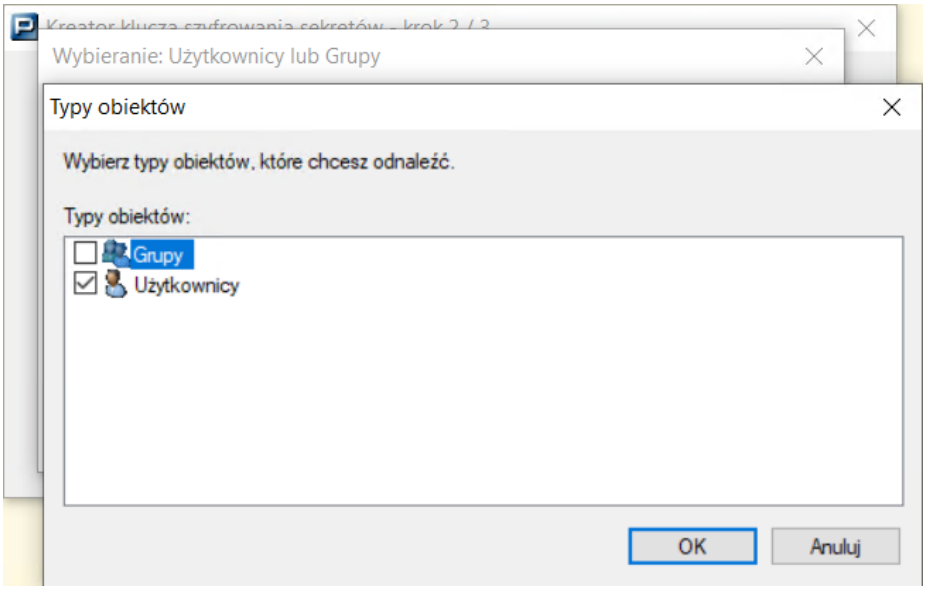
Dodawanie grup lub użytkowników odbywa się w standardowym trybie Windows.




W pole tekstowe ***Wprowadź nazwy obiektów do wybrania*** wpisz dokładną nazwę użytkownika (tak jak widoczna na przykładzie: VM-PLATNIK\Halina Nowak lub po prostu nazwę konta, np. Halina Nowak).

Kliknij przycisk ***Sprawdź nazwy*** znajdujący się po prawej stronie. System zweryfikuje, czy wpisany użytkownik istnieje w wybranej lokalizacji i podkreśli nazwę (lub zmieni ją na pełną ścieżku sieciową/lokalną).

Przycisk ***Typy obiektów...*** (widocznym w prawym górnym rogu okna) pozwala określić, jakich dokładnie rodzajów obiektów system ma szukać podczas wpisywania nazw lub korzystania z wyszukiwania zaawansowanego.



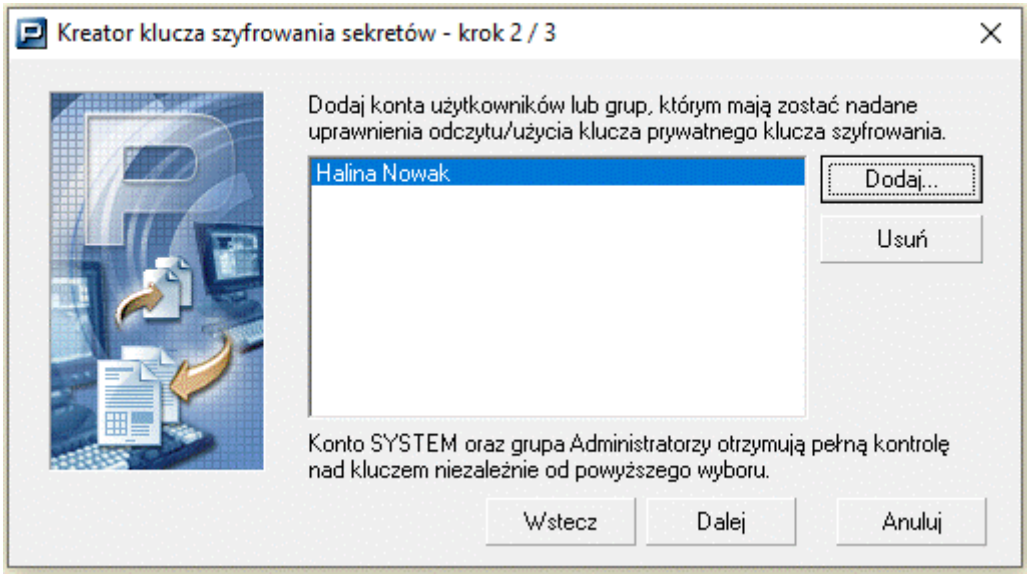

Po kliknięciu tego przycisku pojawia się małe okienko, w którym możesz zaznaczyć lub odznaczyć następujące kategorie:

**Użytkownicy** – standardowe konta osobiste użytkowników korzystających z systemu.

**Grupy** – grupy bezpieczeństwa lub dystrybucyjne skupiające wielu użytkowników (przypisanie uprawnień grupie nadaje je wszystkim jej członkom).

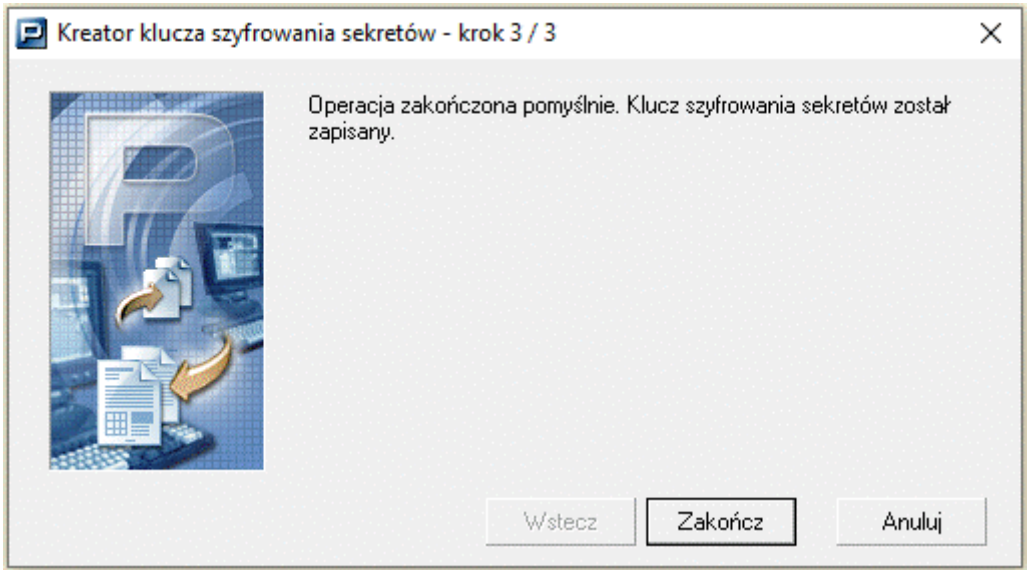
Przycisk ***Zaawansowane...*** (w lewym dolnym rogu ekranu **Wybieranie: Użytkownicy lub Grupy**) służy do rozbudowanego wyszukiwania użytkowników lub grup, gdy nie pamiętasz dokładnej nazwy konta lub pisowni.

Dla potwierdzenia poszczególnych wyborów wybierz przycisk **OK**



Po dodaniu wymaganych użytkowników wybierz przycisk **Dalej**

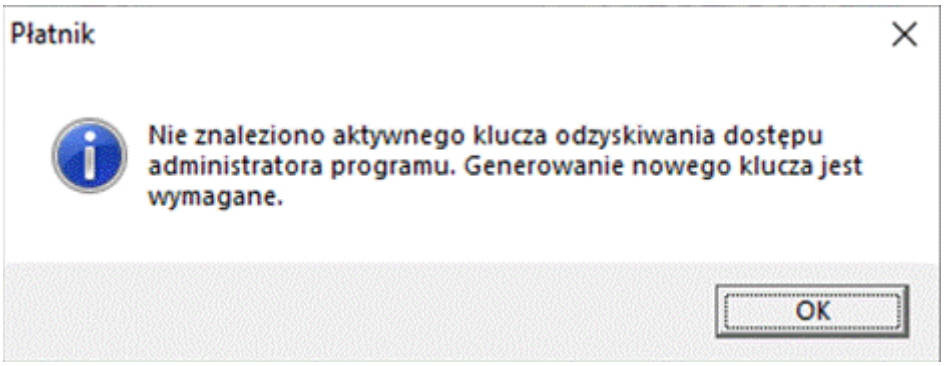
Wyświetlony zostanie komunikat o pomyślnym zakończeniu operacji.




Wybierz przycisk **Zakończ**

## Krok 4

Po zakończeniu działania Kreatora klucza szyfrowania sekretów wyświetlona zostanie informacja o potrzebie wygenerowania klucza odzyskiwania dostępu administratora.



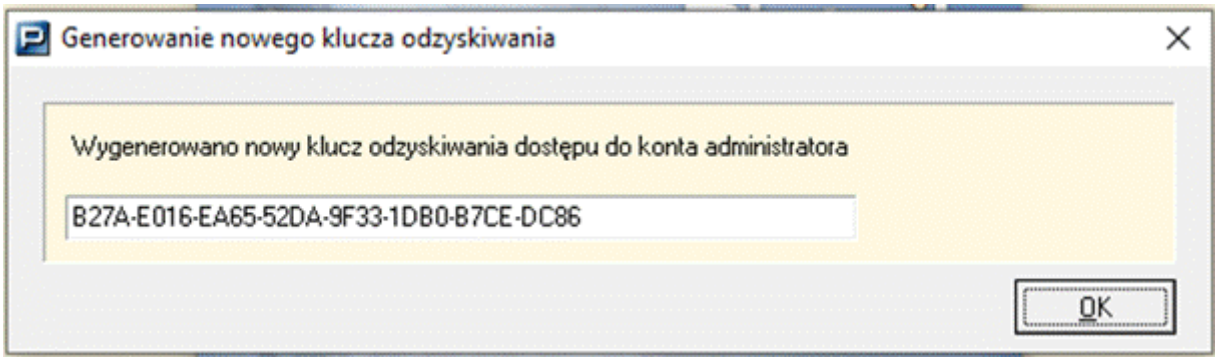

Kliknij przycisk **OK**

## Krok 5

**Ważne!**

Wygenerowany zostanie klucz, który **należy zapisać w bezpieczny sposób – zapisz w pliku na dysku lub pendrive.**

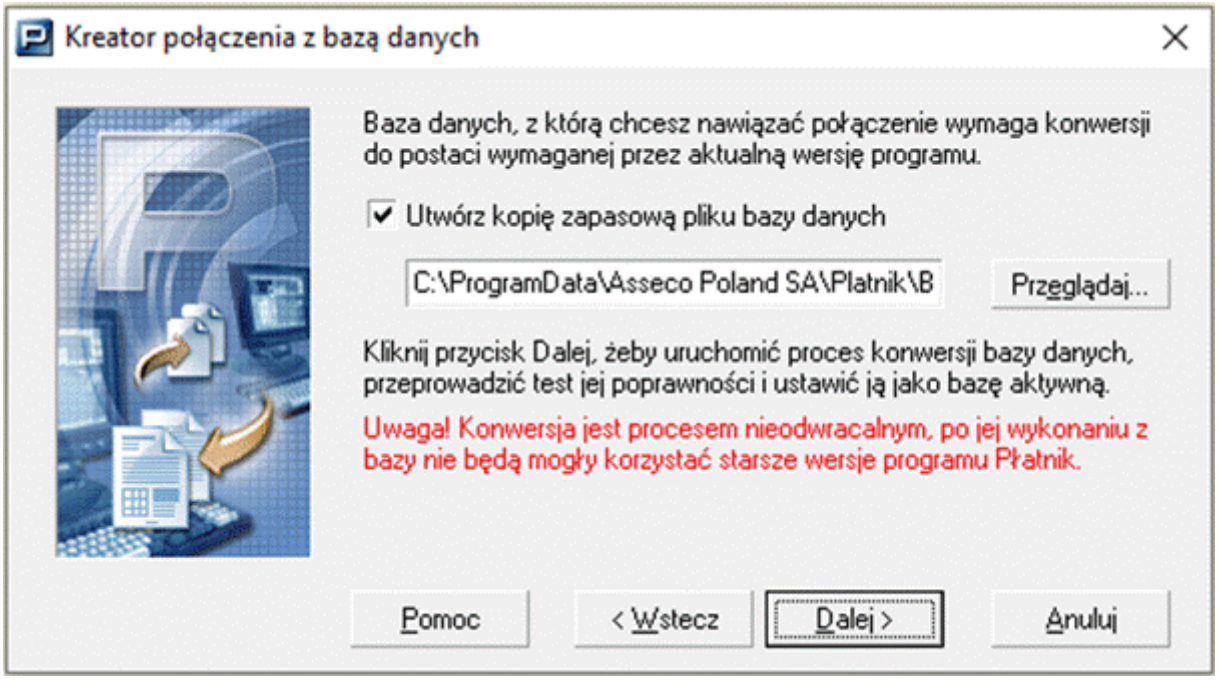
Posiadanie klucza odzyskiwania pozwala na zmianę hasła Administratora w przypadku utraty poprzedniego hasła.




Kliknij przycisk **OK**

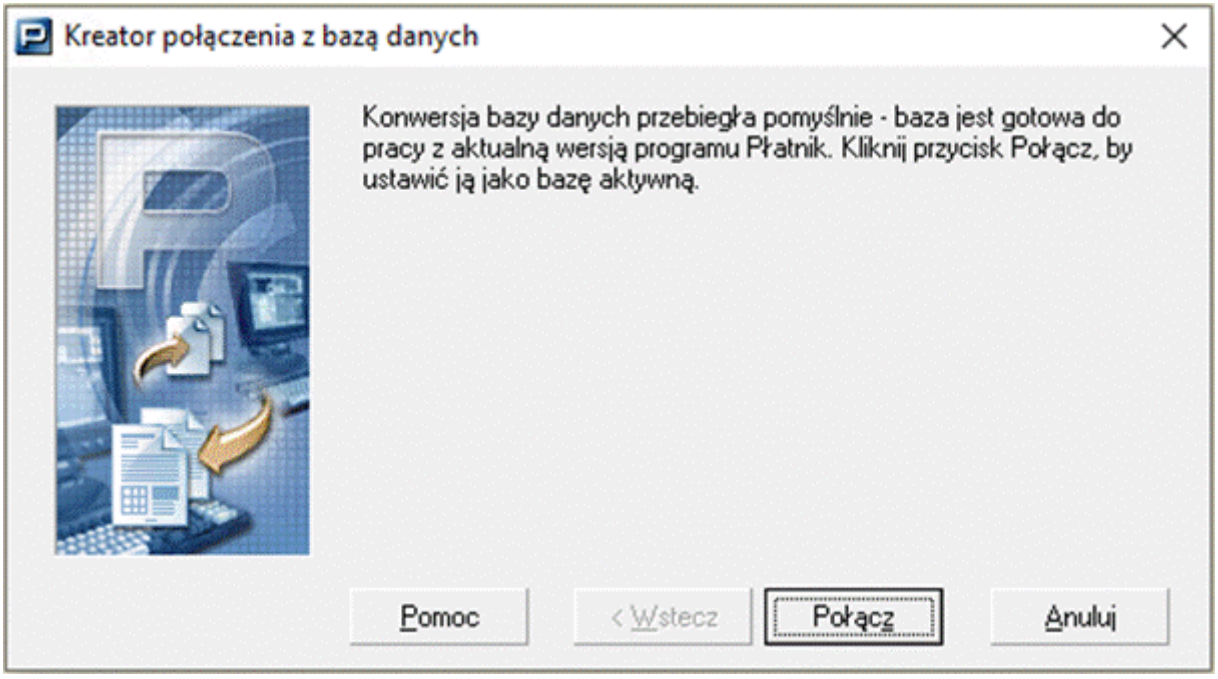
## Krok 6

Po wygenerowaniu klucza odzyskiwania uruchamiana jest konwersja bazy danych.




Wybierz przycisk **Dalej**

Po pomyślnej konwersji bazy danych wyświetli się ekran z informacją.

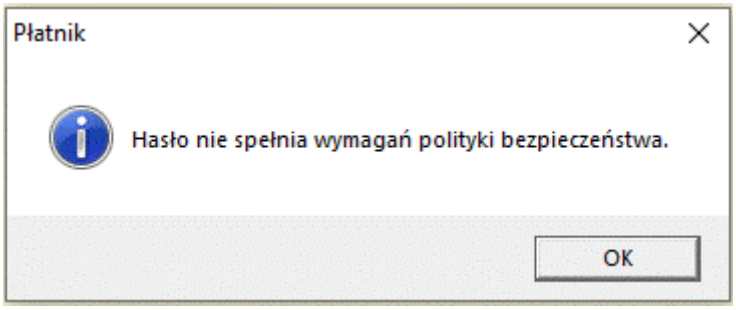



Wybierz przycisk **Połącz** żeby połączyć się z przekonwertowaną bazą danych.

## Krok 7

Po zakończeniu konwersji bazy danych, w przypadku gdy hasło Administratora nie spełnia domyślnych ustawień polityki haseł, program ***Płatnik*** wymusza zmianę hasła Administratora.

Wyświetlany jest komunikat o potrzebie zmiany hasła.



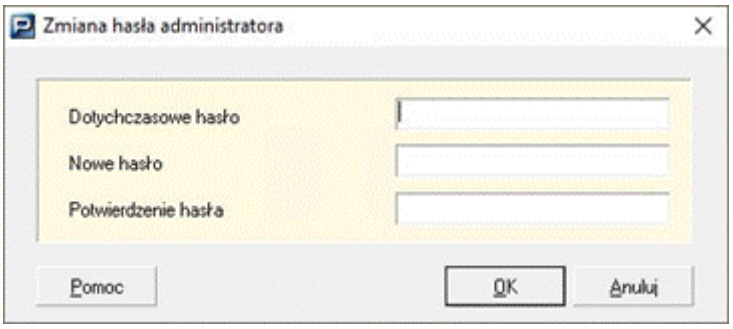

Kliknij przycisk **OK**

Domyślne wymagania polityki bezpieczeństwa dla haseł:

- Minimum 12 znaków w tym:
- Minimum jedna wielka litera,
- Minimum jedna mała litera,
- Minimum jeden znak specjalny,

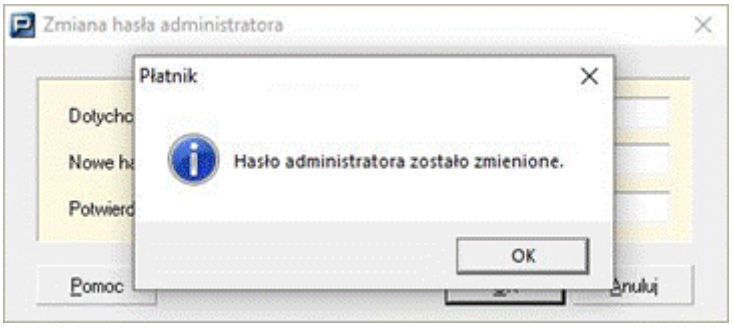
- Minimum jedna cyfra

W ekranie **Zmiana hasła administratora** wpisz dotychczasowe hasło oraz nowe hasło spełniające domyślne ustawienia polityki haseł.




Wybierz przycisk **OK**

Po prawidłowym wprowadzeniu wartości haseł, program ***Płatnik*** prezentuje komunikat o zmianie hasła Administratora.




## Przypadki szczególne

Domyślna konfiguracja dotyczy sytuacji, gdy program Płatnik działa na jednym stanowisku i jest uruchamiany z poziomu jednego użytkownika systemu Windows.

1. Konfiguracja przy pracy wielu użytkowników Windows na jednym komputerze (fizycznym lub wirtualnym) przebiega analogicznie jak domyślna konfiguracja.
2. Konfiguracja przy pracy rozproszonej – wielu użytkowników na różnych komputerach. Należy upewnić się, że administrator zaloguje się choć raz na każdy komputer (fizyczny lub maszynę wirtualną), żeby wygenerować na nim klucz szyfrowania. Klucz szyfrowania jest lokalny dla komputera, choć dostęp do tego klucza może być nadany dla użytkownika domenowego.