nAxiom

Współpraca nAxiom z usługą eSign

Wersja nAxiom: 1.13.1.0

Spis treści

1. Wstęp

W celu złożenia podpisu elektronicznego na dokumencie przetwarzanym w nAxiom należy wysłać ten dokument w formacie XML lub PDF do serwisu eSign. Służy do tego akcja *Podpis dokumentu (eSign)*. Podpis złożony na dokumencie można zweryfikować za pomocą akcji *Weryfikacja podpisu (eSign)*. Dodatkowo, akcja *Status zlecenia (eSign)* umożliwia sprawdzenie statusu zlecenia podpisu dla wysłanego dokumentu.

> Uwaga: Z uwagi na ciągłą rozbudowę usługi *eSign*, przedstawiony tutaj opis konfiguracji funkcji podpisu elektronicznego należy traktować poglądowo. Z chwilą publikacji stabilnej wersji ten opis zostanie zaktualizowany.

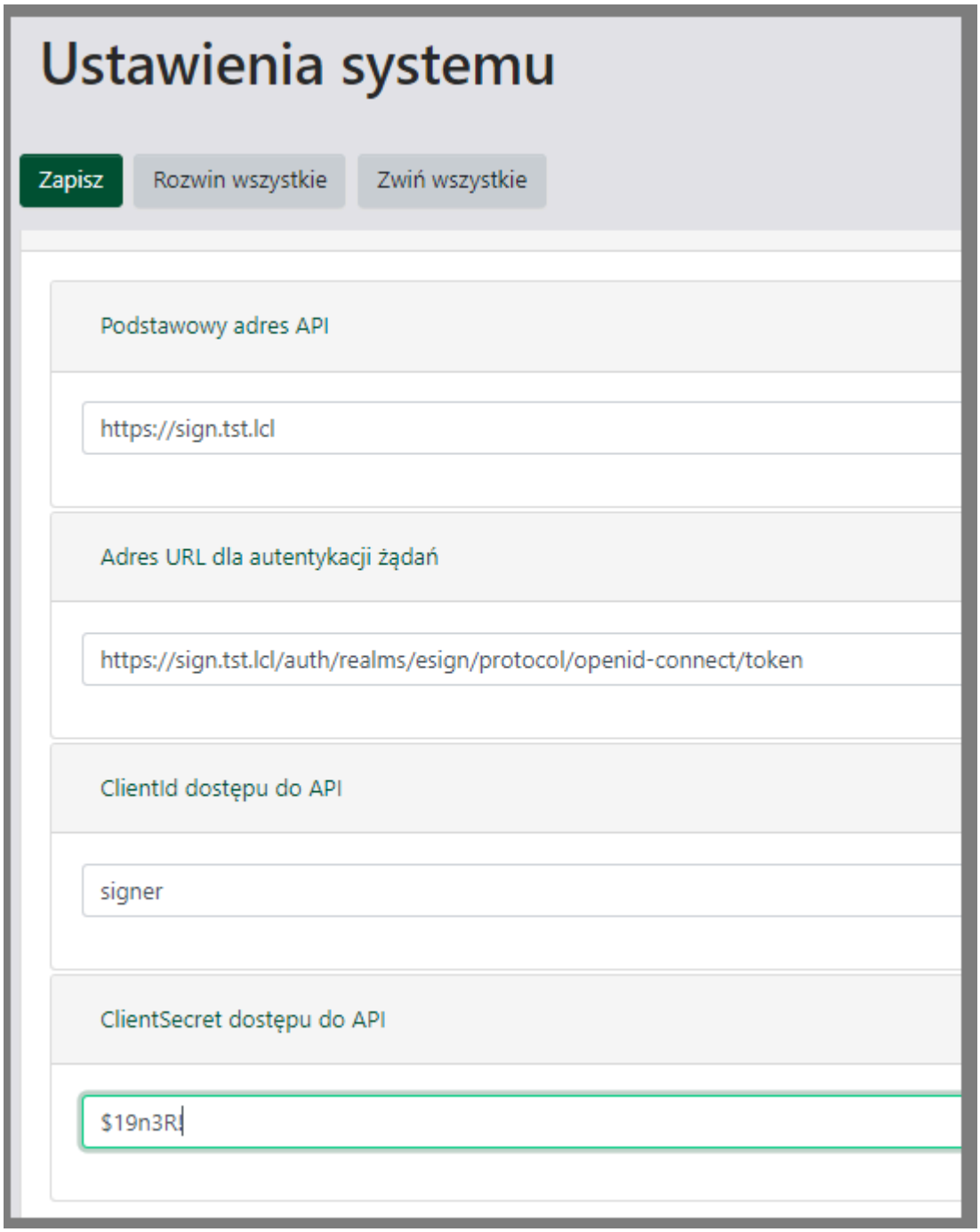
2. Konfiguracja usługi eSign

Aby umożliwić wysyłanie dokumentów z aplikacji nAxiom do usługi eSign, należy skonfigurować ustawienia usługi w ustawieniach systemowych nAxiom. W tym celu należy przejść do sekcji `eSign` na stronie ustawień (`ADMINISTRACJA` > `Ustawienia`) i skonfigurować następujące ustawienia:

- `Podstawowy adres API`: adres domeny, w której dostępna jest usługa *eSign*.
- `Adres URL dla autentykacji żądań`: pełny adres endpointu do uwierzytelniania w usłudze

eSign.

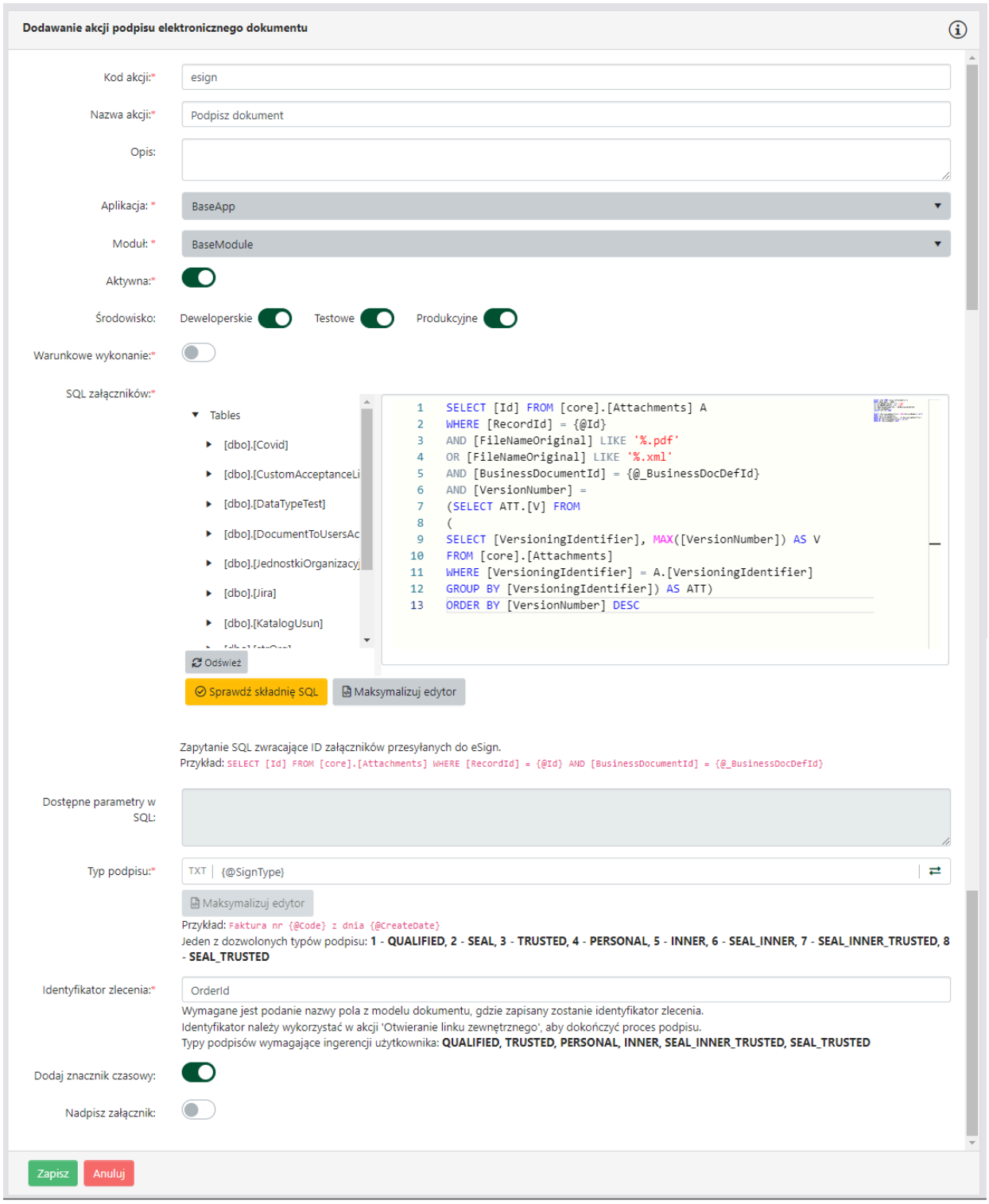
- `ClientId dostępu do API`: identyfikator użytkownika API używany do autoryzacji w usłudze *eSign*.
- `ClientSecret dostępu do API`: hasło użytkownika API używane do autoryzacji w usłudze *eSign*.



3. Wysyłka dokumentu do podpisu

W celu wysłania dokumentu z aplikacji nAxiom do podpisu należy użyć akcji *Podpis dokumentu (eSign)*. W akcji, oprócz standardowych parametrów należy skonfigurować:

- `SQL załączników`: zapytanie zwracające identyfikatory załączników wysyłanych do podpisu; mogą to być wyłącznie pliki w formatach XML lub PDF (zależy od typu podpisu).
- `Typ podpisu`: rodzaju podpisu elektronicznego (numer), który ma zostać złożony na wysłanym dokumencie. Dostępne wartości:
    - `QUALIFIED (1)`: podpis kwalifikowany. Obecnie dostępna opcja podpisu za pomocą chmury oraz karty.
    - `SEAL (2)`: obecnie niewspierany typ podpisu.
    - `TRUSTED (3)`: podpis składany za pomocą usługi Profil Zaufany. Obsługuje wyłącznie dokumenty w formacie XML. W trakcie podpisu użytkownik musi zalogować się do usługi Profil Zaufany. Dokument po podpisie zostanie odesłany do formularza.
    - `PERSONAL (4)`: obecnie niewspierany typ podpisu.
    - `INNER (5)`: wykorzystuje dane osobowe osoby podpisującej; złożenie podpisu wymaga, aby użytkownik przeszedł na stronę usługi eSign. Przed pierwszym użyciem konieczne jest wygenerowanie certyfikatu z następującymi danymi: imię, nazwisko, numer PESEL. W poniższym przypadku źródłem tych danych jest serwis *KeyCloak*, a dokładnie *ActiveDirectory*. Źródłem numeru PESEL jest atrybut *serialNumber* z AD. Ten typ podpisu jest uznawany za mało znaczący. Proces składania podpisu opisano w kolejnym rozdziale.
    - `SEAL_INNER (6)`: podpis typu pieczęć; po przesłaniu do eSign, plik zostanie podpisany za pomocą pieczęci skonfigurowanej w eSign. Użytkownik nie musi w trakcie podpisywania przechodzić na stronę eSign.
    - `SEAL_INNER_TRUSTED (7)`: podpis typu pieczęć; po przesłaniu do eSign, plik zostanie podpisany za pomocą pieczęci skonfigurowanej w eSign. Użytkownik musi w trakcie podpisywania przejść na stronę eSign.
    - `SEAL_TRUSTED (8)`: podpis typu pieczęć; po przesłaniu do eSign, plik zostanie podpisany za pomocą pieczęci z chmury tj. zewnętrznego serwera skonfigurowanego w eSign. Użytkownik musi w trakcie podpisywania przejść na stronę eSign.
- `Dodaj znacznik czasowy`: flaga określająca, czy do podpisu ma zostać dodany znacznik czasu.
- `Nadpisz załącznik`: (domyślnie wyłączone) decyduje, czy podpisany plik ma nadpisać oryginalny załącznik, czy ma zostać dodany jako nowa wersja.



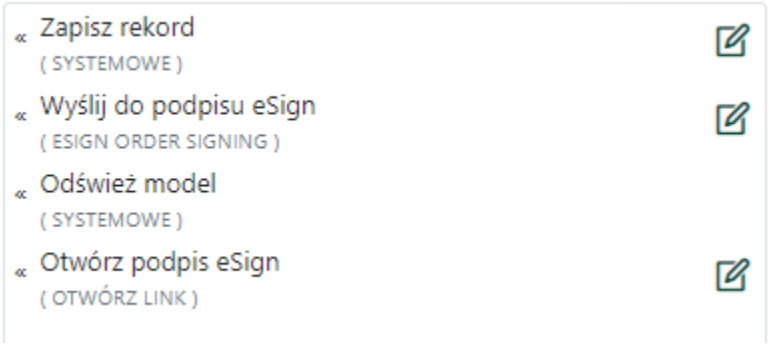
3.1. Przykład zapytania

Przykład zapytania zwracającego załączniki do podpisania dla bieżącej instancji dokumentu biznesowego.

```
SELECT [Id] FROM [core].[Attachments] A
WHERE [RecordId] = {@Id}
AND [FileNameOriginal] LIKE '%.pdf'
OR [FileNameOriginal] LIKE '%.xml'
AND [BusinessDocumentId] = {@_BusinessDocDefId}
AND [VersionNumber] =
(SELECT ATT.[V] FROM
(
SELECT [VersioningIdentifier], MAX([VersionNumber]) AS V
FROM [core].[Attachments]
WHERE [VersioningIdentifier] = A.[VersioningIdentifier]
GROUP BY [VersioningIdentifier]) AS ATT)
ORDER BY [VersionNumber] DESC
```

3.2. Przykład konfiguracji

Przykładowa konfiguracja sekwencji akcji dla przycisku podpisu dokumentu:



Pierwsza akcja zapisuje dane na formularzu. Następna akcja wysyła załączniki bieżącej instancji dokumentu do podpisu. Po poprawnym wykonaniu akcji w odpowiedzi zostanie zwrócony identyfikator zlecenia, który zostanie zapisany w odpowiednim polu na formularzu. Kolejna akcja odświeża model, aby ten identyfikator był dostępny jako parametr dla akcji otwierania linku zewnętrznego.
Ponieważ podpisy typu *SEAL_CLOUD* oraz *SEAL_INNER* nie wymagają, aby użytkownik przechodził na stronę podpisu, w akcji otwierania linku zewnętrznego należy skonfigurować warunkowe wykonanie.

```
SELECT
CASE {@SignType}
WHEN 4 THEN 0
WHEN 5 THEN 0
```

```
ELSE 1
END
```

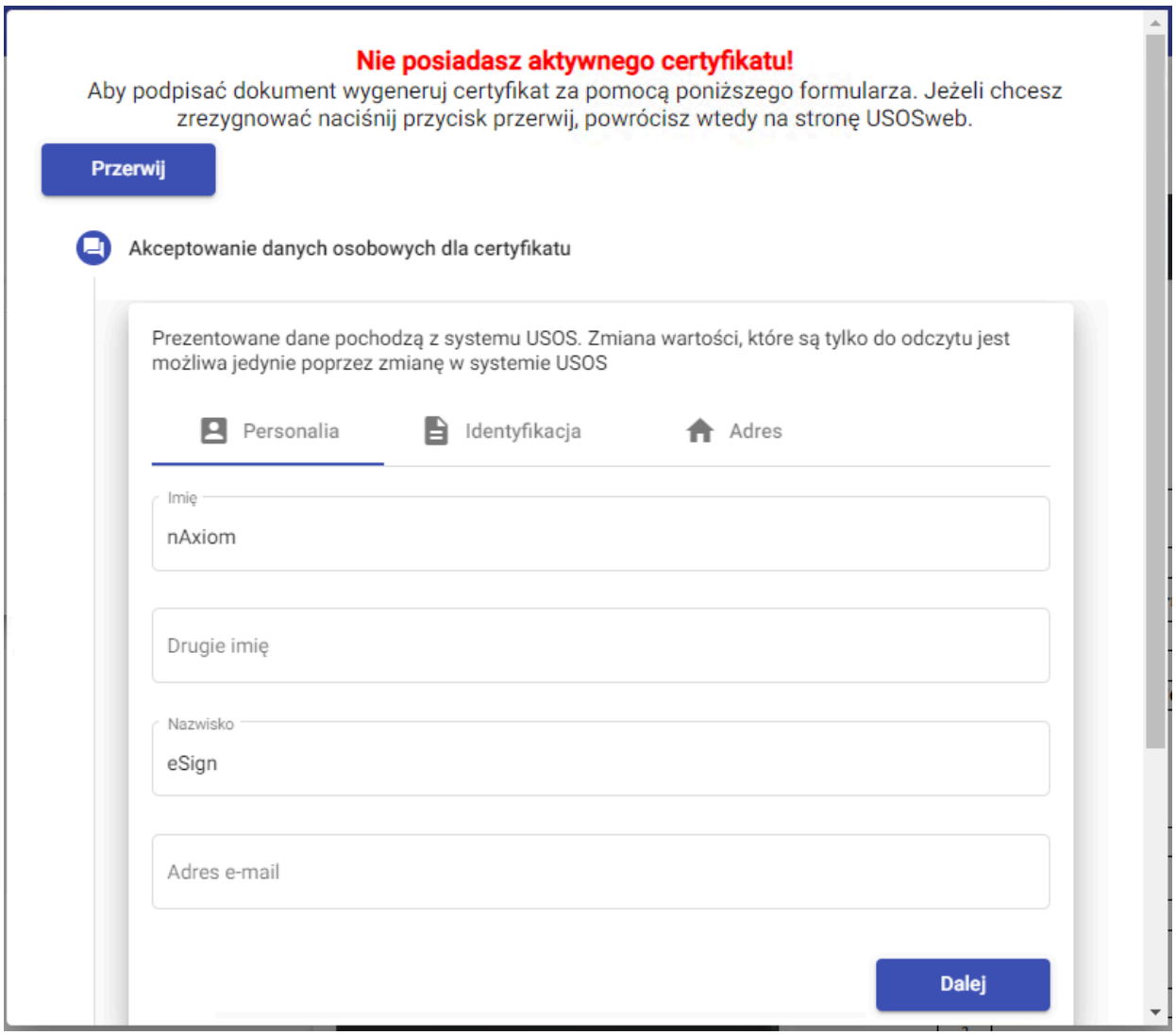
Z kolei jako parametr `Link` w tej akcji można wpisać zapytanie SQL, które zbuduje odpowiedni URL prowadzący do strony podpisu.

```
SELECT CONCAT('https://sign.tst.lcl/ui/signbox?order-id=',
              CAST({@OrderId} AS VARCHAR(40)),'&lang=',
              /*SELECT na język, obsługiwane pl lub en*/'pl')
```

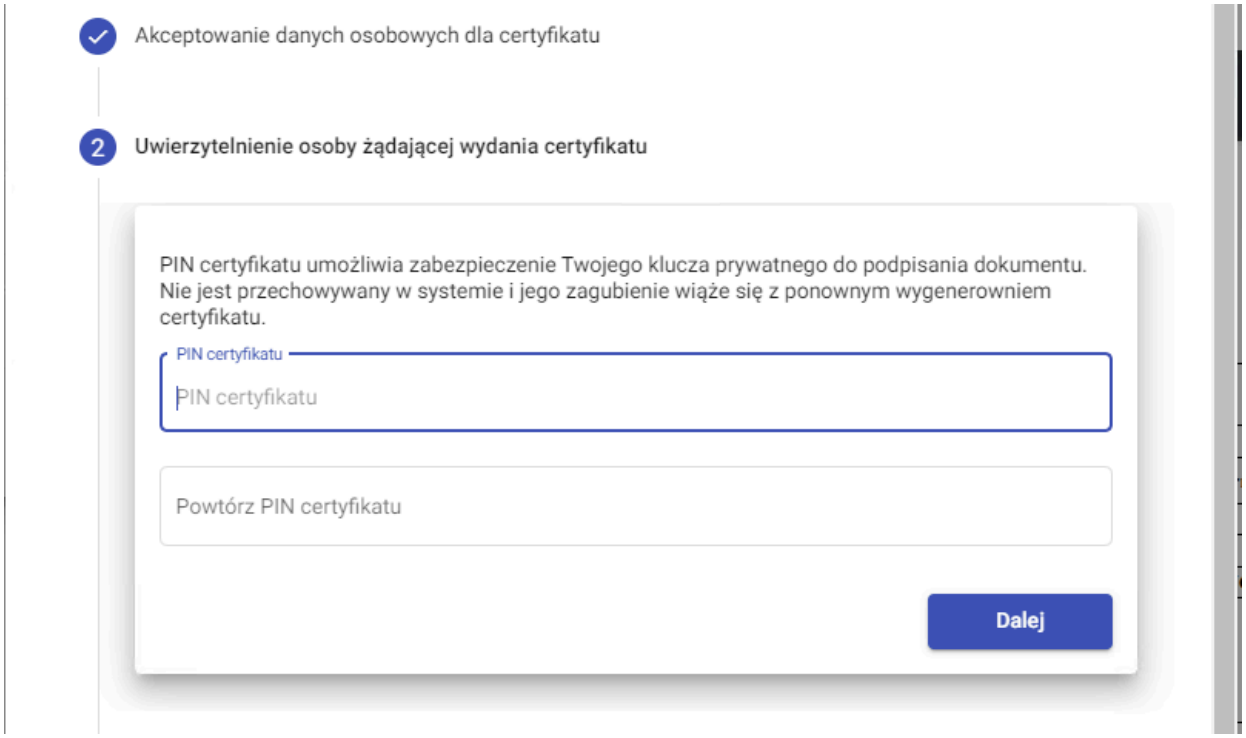
4. Składanie pierwszego podpisu typu INNER

W przypadku podpisu typu *INNER* po wysłaniu dokumentów do podpisu użytkownik musi przejść na stronę usługi podpisu w celu potwierdzenia tożsamości poprzez podanie kodu PIN do certyfikatu. Jeśli certyfikat nie został jeszcze wygenerowany, trzeba to zrobić przed podpisaniem dokumentu. Ta czynność jest wykonywana tylko jeden raz i przebiega w następujących krokach:

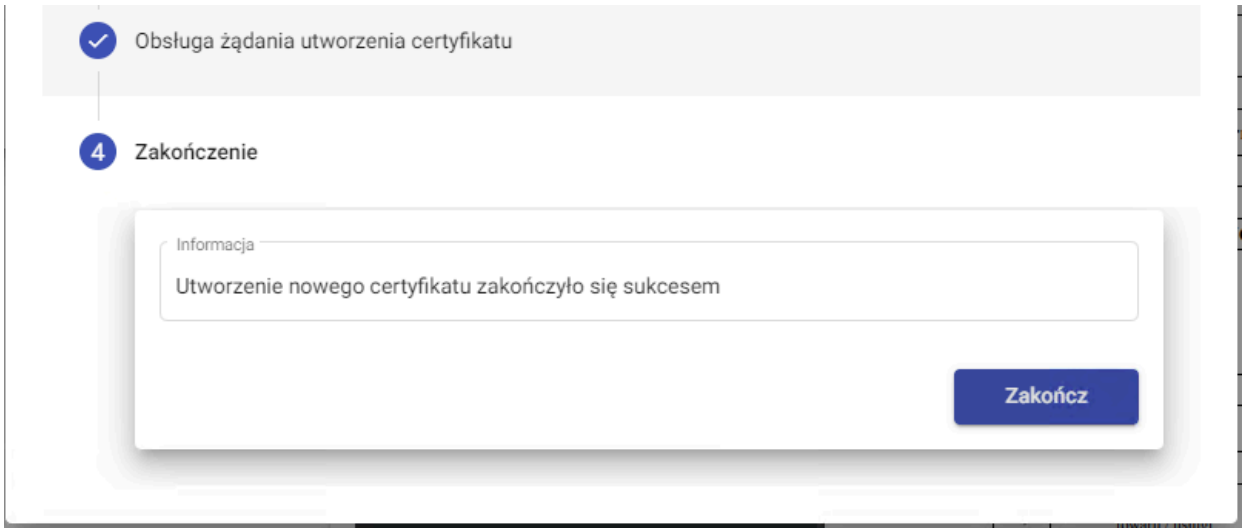
1. Zostaje wyświetlone okno z danymi pobranymi z ActiveDirectory. Kliknij przycisk `Dalej`.



1. Wpisz kod PIN do generowanego certyfikatu; co najmniej 6 znaków.

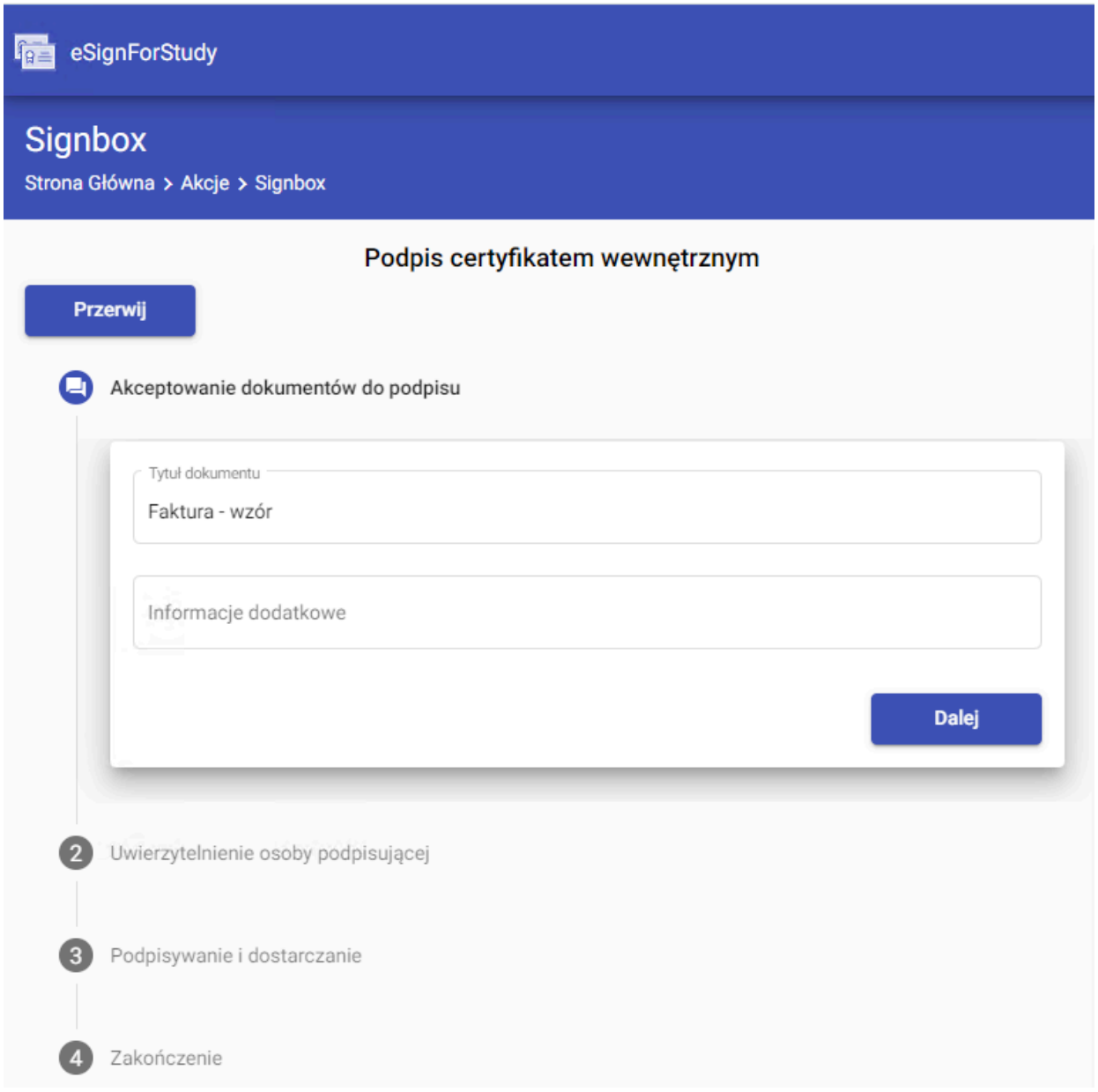


2. Zostanie wyświetlony komunikat o pomyślnym utworzeniu certyfikatu.

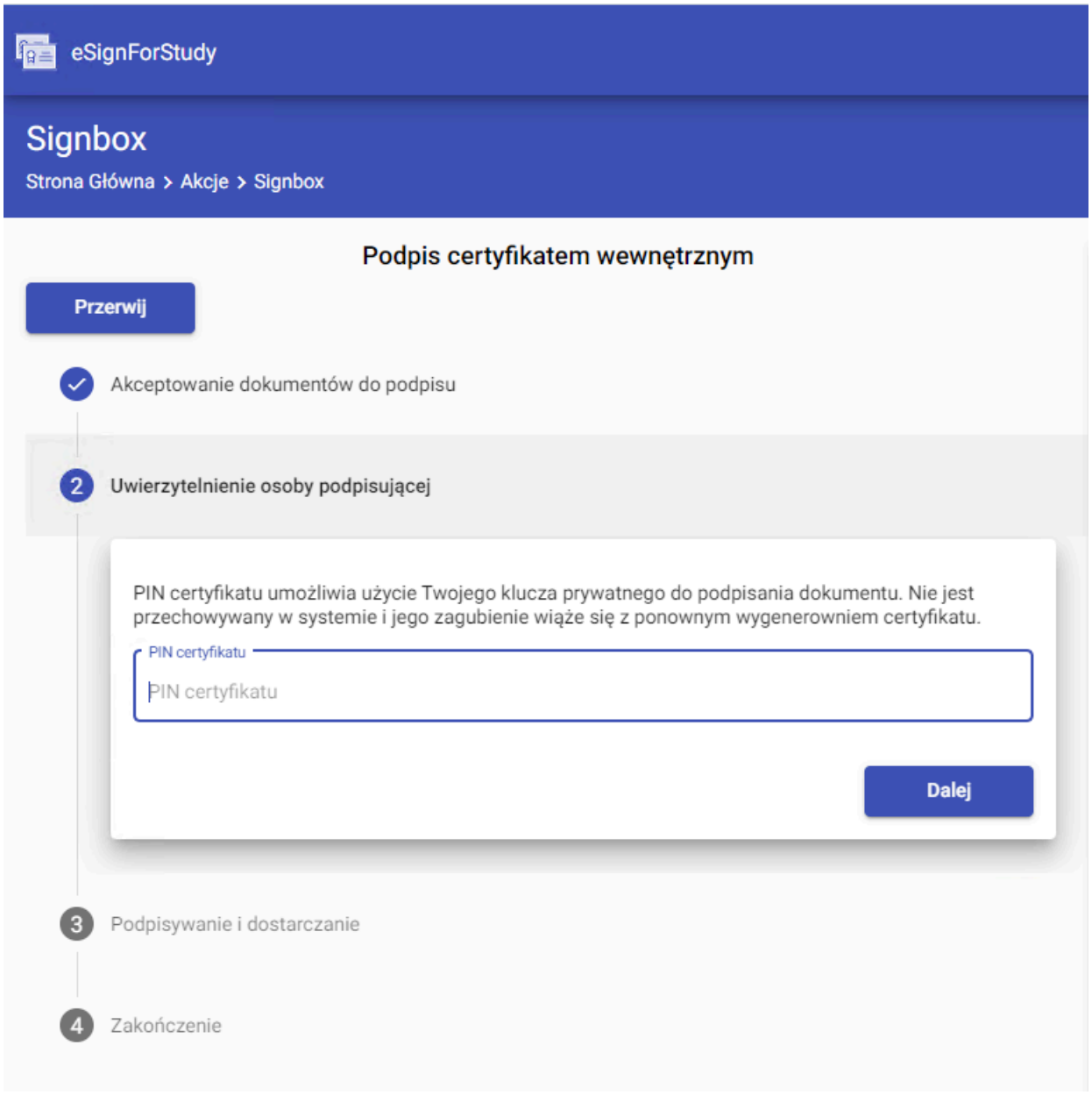


Następnie wykonywany jest proces podpisania przesłanych dokumentów, który obejmuje:

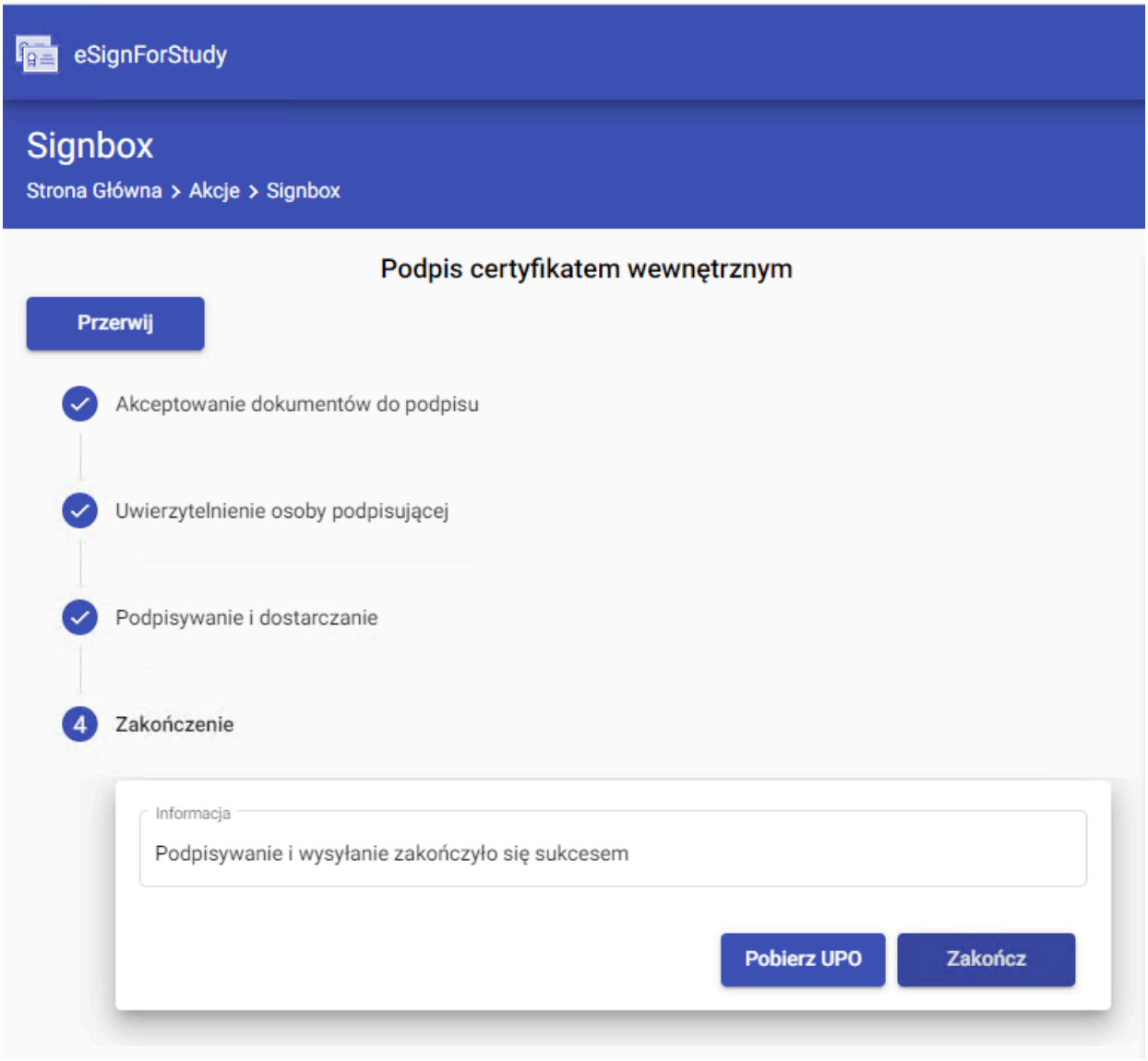
1. Akceptowanie dokumentów do podpisu.



2. Uwierzytelnienie osoby podpisującej



3. Podpisywanie i dostarczanie oraz zakończenie.

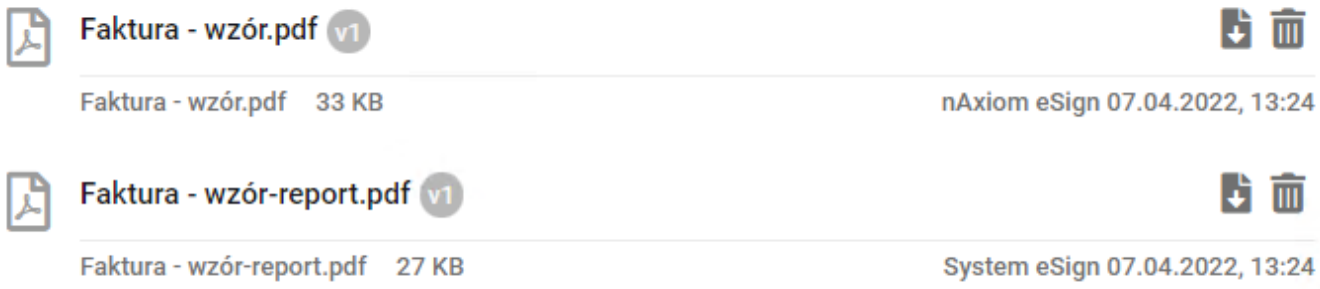


W końcowym kroku użytkownik może pobrać potwierdzenie UPO, a po kliknięciu przycisku `Zakończ` nastąpi powrót na stronę formularza, z którego podpis został zainicjowany.

5. Weryfikacja podpisu na dokumencie

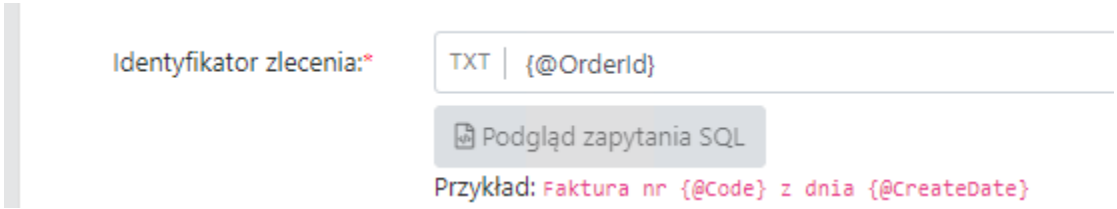
Akcja *Weryfikacja podpisu (eSign)* umożliwia przesłanie plików do usługi eSign w celu zweryfikowania podpisów. Wynikiem takiej akcji jest wygenerowanie raportu w formacie PDF. Plik z raportem dodany

zostanie do tej samej kategorii załączników co plik źródłowy i będzie mieć w nazwie dopisek *-report*. Jednym z parametrów akcji jest zapytanie SQL zwracające ID załączników do przesłania w celu weryfikacji podpisów, analogiczne jak w przypadku akcji wysyłki do podpisu. Drugi parametr to pole w modelu, w którym ma zostać zapisany zwrócony identyfikator zlecenia.

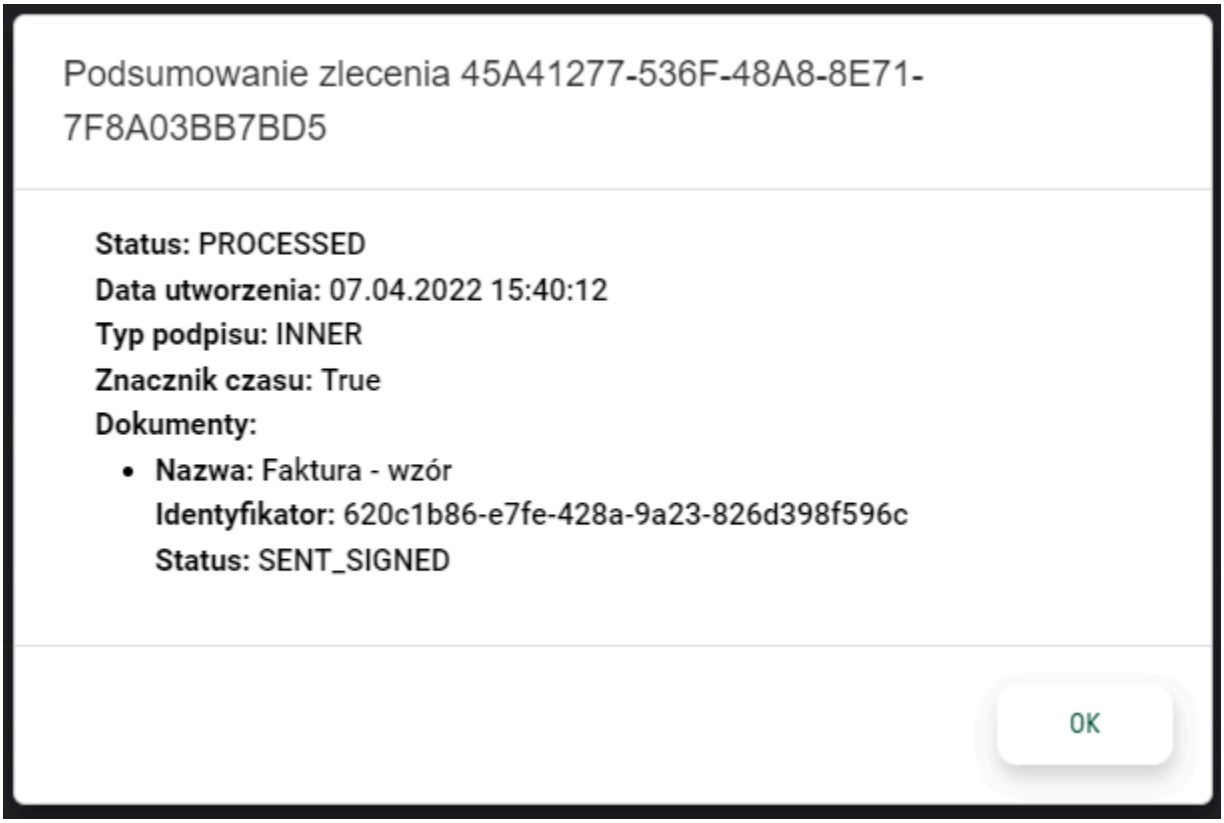


6. Akcja sprawdzenia statusu zlecenia

Akcja *Status zlecenia (eSign)* służy do odpytania usługi eSign o status zlecenia o identyfikatorze, który został zwrócony po wysłaniu dokumentu do podpisu. Jedynym parametrem konfiguracji jest identyfikator zlecenia.



W wyniku wykonania akcji jest wyświetlane okno z podsumowaniem podpisu, statusami dla zlecenia i plików.



7. Tabela *Attachments*

Tabela systemowa z załącznikami *core.Attachments* zawiera kolumnę *SignatureStatus*. W kolumnie są zapisywane statusy zwracane przez usługę eSign. Zasady ustawiania statusów są następujące:

- Jeśli dla kategorii załączników włączono wersjonowanie, plik otrzymany z eSign ma status 11 — *SENT_SIGNED*,
- Jeśli dla kategorii załączników włączono wersjonowanie, ale wystąpił błąd podczas podpisu, zostanie zaktualizowany status przesłanego dokumentu z nAxiom,
- Jeśli dla kategorii załączników nie włączono wersjonowania, status zostanie zaktualizowany dla przesłanego pliku.

Statusy zlecenia:

- 0 - PENDING,
- 1 - PREPARING,
- 2 - PROCESSING,
- 3 - PROCESSED,

- 4 - PROCESS_FAILED

Statusy dokumentów:

- 0 - NONE,
- 1 - CREATED,
- 2 - WITH_LOADED_FILE,
- 3 - LOADED_WITH_ERROR,
- 4 - IN_SENDING,
- 5 - IN_SIGNING,
- 6 - SIGNED,
- 7 - SIGN_FAULT,
- 8 - SIGNED_AND_EXTENDED_BY_TIMESTAMP,
- 9 - SIGNED_AND_ERROR_DURING_FAULT_EXTENDED_BY_TIMESTAMP,
- 10 - SIGN_CANCELED,
- 11 - SENT_SIGNED,
- 12 - SENT_FAULT,
- 13 - SEND_SIGNED_WITH_ERROR,
- 14 - SENT_FAULT_WITH_ERROR,
- 15 - IN_VERIFICATION,
- 16 - VERIFIED,
- 17 - VERIFICATION_FAULT,
- 18 - SENT_REPORT,
- 19 - SENT_REPORT_FAULT,
- 20 - SENT_REPORT_WITH_ERROR,
- 21 - SENT_REPORT_FAULT_WITH_ERROR,
- 22 - TO_DELETE,
- 23 - HISTORY_SAVE_FAULT,
- 24 - DOWNLOAD_SIGNED,
- 25 - DOWNLOAD_FAULT,
- 26 - VERIFICATION_DOCUMENT_ERROR