SZAFIR
KRAJOWA IZBA ROZLICZENIOWA S.A.

Podręcznik użytkownika

SZAFIR 1.2.7 – bezpieczne urządzenie do składania i weryfikacji podpisów elektronicznych

http://www.kir.com.pl

Informacje prawne

Niniejszy podręcznik użytkownika został opublikowany przez Krajową Izbę Rozliczeniową S.A. bez żadnych gwarancji kompletności zawartych w nim informacji.

W dowolnym momencie Krajowa Izba Rozliczeniowa S.A. może wprowadzić ulepszenia i zmiany wynikające z błędów typograficznych, niedokładności aktualnych informacji czy ulepszeń oprogramowania bądź sprzętu. Takie zmiany będą uwzględniane w następnych wydaniach tego podręcznika.

Spis treści

1. Wprowadzenie

1.1. Co to jest i do czego służy aplikacja SZAFIR?

Aplikacja SZAFIR służy do składania i weryfikowania zwykłych oraz bezpiecznych podpisów elektronicznych oraz znakowania czasem. Aplikacja umożliwia składanie i weryfikację podpisu elektronicznego w formatach XAdES (w wariantach XAdES-BES, XAdES-T, XAdES-C) oraz PKCS#7 (z możliwością znakowania czasem); możliwe jest także składanie podpisu wielokrotnego PKCS#7 oraz kontrasygnaty XAdES.

Aplikacja dostępna jest w dwóch wersjach:

- pełnej,
- weryfikująco-demonstracyjnej.

Wersja pełna umożliwia składanie i weryfikację zwykłego i bezpiecznego podpisu elektronicznego oraz znakowanie czasem.

Wersja weryfikująco-demonstracyjna umożliwia weryfikację zwykłego oraz bezpiecznego podpisu elektronicznego. W tej wersji składanie podpisu składanie podpisu elektronicznego jest możliwe tylko przy wykorzystaniu dostarczonego z aplikacją, testowego certyfikatu zapisanego w pliku.

> PIN testowego certyfikatu „CN=SZAFIR – Demo, O=SZAFIR, C=PL", który dystrybuowany jest razem z aplikacją to **„Szafir123."** (z kropką na końcu, bez cudzysłowów).

Obie wersje aplikacji – zarówno pełna, jak i weryfikująco-demonstracyjna – spełniają wymagania nałożone na oprogramowanie podpisujące i weryfikujące w Rozporządzeniu z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dziennik Ustaw Nr 128, poz. 1094) co oznacza, że wraz ze współpracującym z nimi komponentami technicznymi stanowią one, odpowiednio, bezpieczne urządzenie do składania i weryfikacji oraz bezpieczne urządzenie do weryfikacji podpisów elektronicznych.

Aplikacja do składania i weryfikacji podpisów elektronicznych SZAFIR nie jest oprogramowaniem publicznym w rozumieniu rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków tech-

nicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu.

1.2. Podstawowe informacje o podpisie elektronicznym

1.2.1. Definicja

„Podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.” – art. 3 Ustawy o podpisie elektronicznym.

Podstawowe własności podpisu elektronicznego:

- unikalność – każdy elektroniczny dokument posiada unikalny podpis cyfrowy ściśle z nim związany,
- integralność – jakakolwiek zmiana dokumentu podpisanego cyfrowo zostanie natychmiast wykryta w momencie weryfikacji podpisu,
- niezaprzeczalność – tylko osoba posiadająca klucz prywatny korespondujący z kluczem publicznym wykorzystanym do weryfikacji podpisu mogła wygenerować podpis pod dokumentem.

Podpis elektroniczny, często traktowany jako odpowiednik odręcznego podpisu złożonego pod dokumentem papierowym, tak naprawdę zapewnia znacznie więcej. W przypadku dokumentu papierowego nawet po złożeniu pod nim podpisu możliwe jest dokonanie zmian, dla których niemożliwe będzie wskazanie czy zostały naniesione przed czy po złożeniu podpisu. Podpis cyfrowy całkowicie wyklucza tego typu manipulacje dokonywane na dokumentach elektronicznych. Dodatkowo unikalność podpisu cyfrowego gwarantuje, iż nie zostanie on dołączony do innej wiadomości, co może mieć miejsce w przypadku podpisu złożonego „na papierze”.

1.2.2. Działanie

Konstrukcja podpisu elektronicznego wykorzystuje technikę szyfrowania z kluczem publicznym. Podstawą działania szyfrów z kluczem publicznym są dwa klucze: klucz prywatny oraz klucz publiczny. Tak jak wskazują przyjęte zwyczajowo nazwy kluczy, klucz publiczny

jest udostępniany wszystkim osobom, z którymi kontaktuje się dana osoba, zaś klucz prywatny, dla zachowania bezpieczeństwa systemu, musi pozostać pod wyłączną kontrolą jego właściciela. Istotną własnością wymienionych kluczy jest to, iż praktycznie niemożliwe jest odgadnięcie klucza prywatnego na podstawie znajomości klucza publicznego. Własność ta gwarantuje, iż podpisany dokument, który został poprawnie zweryfikowany kluczem publicznym mógł być stworzony tylko przez posiadacza klucza prywatnego.

> Podpis elektroniczny jest wykorzystywany, między innymi, do zabezpieczania transakcji przesyłanych w ramach systemu elektronicznych rozliczeń międzybankowych ELIXIR prowadzonego od 1993 roku przez Krajową Izbę Rozliczeniową S.A.

1.2.3. Rola certyfikatów klucza publicznego

Niezwykle istotne dla zapewnienia wiarygodności podpisu cyfrowego jest wykorzystanie właściwego klucza publicznego nadawcy wiadomości. Nawet jeżeli klucz publiczny jest dołączony do wiadomości lub też był przesłany drogą elektroniczną, osoba wykorzystująca klucz publiczny do weryfikacji podpisu nie ma pewności czy rzeczywiście jego właścicielem jest nadawca wiadomości. Potwierdzenie przynależności klucza publicznego do danej osoby zapewniają certyfikaty klucza publicznego.

„Certyfikat – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.” – art. 3 Ustawy o podpisie elektronicznym.

Certyfikat jest to plik, podpisany cyfrowo przez podmiot świadczący usługi certyfikacyjne, który zawiera dane o właścicielu certyfikatu, jego klucz publiczny oraz informacje, kto wystawił ten certyfikat, a tym samym poświadcza prawdziwość zawartych w nim danych. Podmiot świadczący usługi certyfikacyjne przed wydaniem certyfikatu jest zobowiązany do rzetelnego zweryfikowania tożsamości osoby ubiegającej się o wydanie certyfikatu oraz do sprawdzenia czy posiada ona klucz prywatny komplementarny do przedstawionego do certyfikacji klucza publicznego. Tylko wówczas certyfikat klucza publicznego, wydany przez zaufany podmiot, może pełnić rolę elektronicznego dowodu tożsamości. Zastosowanie takich certyfikatów klucza publicznego w znaczący sposób wpływa na podniesienie poziomu bezpieczeństwa komunikacji w sieciach teleinformatycznych.

> Certyfikaty klucza publicznego są wykorzystywane, między innymi, do weryfikacji podpisów elektronicznych pod transakcjami przesyłanymi w ramach systemu ELIXIR. Na potrzeby systemu ELIXIR generowaniem i zarządzaniem certyfikatami klucza publicznego zajmuje się stworzony przez KIR S.A. system SZAFIR.

Wykorzystanie do weryfikowania podpisu cyfrowego klucza zawartego w certyfikacie danej osoby daje odbiorcy pewność w przypadku pozytywnej weryfikacji podpisu, że za otrzyma-

ną wiadomością kryje się konkretna, wskazana w certyfikacie osoba. To pozwala na zrównanie, przy spełnieniu wymienionych w Ustawie o podpisie elektronicznym warunków, podpisu odręcznego z elektronicznym.

„Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej." – art. 5 Ustawy o podpisie elektronicznym.

1.3. Słownik podstawowych pojęć z dziedziny podpisu elektronicznego

Bezpieczne urządzenie do składania i weryfikacji podpisu elektronicznego – sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający złożenie podpisu lub poświadczenia elektronicznego przy wykorzystaniu danych służących do składania podpisu lub poświadczenia elektronicznego oraz w sposób umożliwiający identyfikację osoby fizycznej, która złożyła podpis elektroniczny, przy wykorzystaniu danych służących do weryfikacji podpisu elektronicznego lub w sposób umożliwiający identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne, przy wykorzystaniu danych służących do weryfikacji poświadczenia elektronicznego, spełniające określone wymagania Ustawy o podpisie elektronicznym.

Bezpieczny podpis elektroniczny – według Ustawy o podpisie elektronicznym jest to podpis elektroniczny, który:

- jest przyporządkowany wyłącznie do osoby fizycznej składającej podpis,
- jest sporządzany za pomocą podlegających wyłącznej kontroli osoby fizycznej składającej podpis elektronicznych bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Certyfikat – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby fizycznej składającej podpis elektroniczny.

CRL – lista unieważnionych i zawieszonych certyfikatów, wydawana przez podmiot świadczący usługi certyfikacyjne, zawierająca numer kolejny listy, datę jej publikacji, przewidywany czas publikacji kolejnej listy, określenie podmiotu wydającego listę, numery seryjne unieważnionych i zawieszonych certyfikatów.

Dane służące do składania podpisu elektronicznego – niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tę osobę do składania podpisu elektronicznego.

Dane służące do weryfikacji podpisu elektronicznego – niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane do identyfikacji osoby fizycznej składającej podpis elektroniczny.

Komponent techniczny – komponent techniczny w rozumieniu rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych

i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. Nr 128, poz 1094).

Oprogramowanie publiczne – oprogramowanie podpisujące, do którego w normalnych warunkach eksploatacji może mieć dostęp każdy; programowaniem publicznym nie jest w szczególności oprogramowanie używane w mieszkaniu prywatnym, lokalu biurowym lub telefonie komórkowym (Dz.U. Nr 128 Poz. 1094).

Podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, służą do identyfikacji osoby fizycznej składającej podpis elektroniczny.

PIN – Personal Identification Number. Kod zabezpieczający zawartość karty kryptograficznej przed niepowołanym użyciem.

PKCS – nazwa zestawu standardów z dziedziny kryptografii klucza publicznego.

PKCS#7 – format podpisu elektronicznego. Główne charakterystyki tego formatu podpisu to:

- Możliwość podpisywania plików tekstowych oraz binarnych.
- Zapisywanie podpisu w postaci pliku w formacie PKCS#7.
- Możliwość składania podpisu:
  - pojedynczego (jednemu obiektowi danych odpowiada jeden plik z jednym podpisem),
  - wielokrotnego (jednemu obiektowi danych odpowiada jeden plik, zawierający jednak wiele podpisów).

Podmiot świadczący usługi certyfikacyjne – według Ustawy o podpisie elektronicznym: przedsiębiorca, Narodowy Bank Polski albo organ władzy publicznej, świadczący co najmniej jedną z usług certyfikacyjnych.

Wielokrotny podpis elektroniczny – podpis dołączany do już istniejącego podpisu poprzez włączenie kolejnej struktury podpisu związanej z aktualnie wykonywanym podpisem do większej struktury, przy czym struktury podpisu są od siebie niezależne tzn. nie ma znaczenia ich kolejność, ważność oraz nie istnieją między nimi żadne powiązania w momencie tworzenia dowolnej z nich.

Rozporządzenie – rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. Nr 128, poz 1094).

Ścieżka certyfikacji – ścieżka certyfikacji w rozumieniu rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne (Dz.U. Nr 128 Poz. 1094).

Ustawa o podpisie elektronicznym – Ustawa o podpisie elektronicznym z dnia 18 września 2001 roku.

Weryfikacja podpisu elektronicznego – operacja sprawdzająca poprawność podpisu elektronicznego, w wyniku której następuje zidentyfikowanie tożsamości podpisującego oraz ustalenie, czy podpisany dokument nie został nielegalnie zmodyfikowany, a certyfikat służący do weryfikacji podpisu elektronicznego unieważniony lub zawieszony.

XAdES – XML Advanced Electronic Signature, format podpisu elektronicznego oparty o XML-DSIG z dodatkowymi funkcjami dla podpisu kwalifikowanego. Główne charakterystyki tego formatu podpisu to:

- Możliwość podpisywania obiektów, które mogą być zidentyfikowane poprzez URI (ang. Uniform Resource Identifier) – w szczególności obiektami takim mogą być:
  - zewnętrzne dokumenty XML,
  - zewnętrzne fragmenty dokumentów XML,
  - części dokumentu XML, w którym osadzony jest podpis.
  - pliki tekstowe,
  - pliki binarne.
- Zapisywanie podpisu elektronicznego w postaci elementu dokumentu XML, przy czym podpis ten może być:
  - opakowujący (zawierać w sobie podpisywany element),
  - opakowany (być zawartym w podpisywanym elemencie),
  - oddzielny (znajdować się obok elementu podpisywanego, w tym samym lub w innym dokumencie XML).
- Możliwość składania podpisu w formach:
  - XAdES-BES (podstawowa forma podpisu XAdES);
  - XAdES-T (podpis XAdES oznakowany czasem);
  - XAdES-C (podpis XAdES oznakowany czasem, z dołączonymi informacjami – certyfikatami oraz CRL – zapewniającymi długotrwałą ważność dowodową podpisu).
- Możliwość zapisywania wielu podpisów w jednym pliku XML oraz składania podpisu wbudowanego (kontrasygnaty).

XML-DSIG – XML-Signature, format podpisu elektronicznego dla XML. Jego rozszerzeniem jest format XAdES.

Znakowanie czasem – usługa polegająca na dołączeniu do dokumentu w postaci elektronicznej oznaczenia czasu w chwili wykonania tej usługi oraz elektronicznego poświadczenia tak powstałych danych przez podmiot świadczący tę usługę. Znakowanie czasem jest usługą płatną – skorzystanie z niej wymaga podpisania odpowiedniej umowy. Dostęp do usługi weryfikowany jest na podstawie certyfikatu używanego przez użytkownika do podpisania wniosku o wydanie znacznika czasu; certyfikat testowy dystrybuowany z wersją weryfikująco-demonstracyjną aplikacji nie umożliwia korzystania z usługi znakowania czasem.

2. Rozpoczynanie pracy z aplikacją

Aplikacja SZAFIR służy do składania i weryfikacji podpisów elektronicznych. Z założenia ma ona przy tym spełniać wymagania szerokiego grona użytkowników podpisu elektronicznego: zarówno tych zainteresowanych okazjonalnym podpisywaniem niewielkich ilości dokumentów, jak i użytkowników biznesowych podpisujących i weryfikujących jednorazowo duże ilości dokumentów.

Silnik kryptograficzny to niewidoczna dla użytkownika część aplikacji, która odpowiada za wykonywanie operacji kryptograficznych. W oparciu o wbudowane algorytmy kryptograficzne oraz informacje zapisane w konfiguracji aplikacji silnik realizuje **zadania** (takie jak np. składanie lub weryfikacja podpisów elektronicznych) zlecone mu za pośrednictwem graficznego **interfejsu użytkownika**.

Interfejs użytkownika to część aplikacji odpowiedzialna za interakcję z użytkownikiem, pozwalająca na wygodne konfigurowanie aplikacji oraz **zarządzanie zadaniami** zlecanymi silnikowi kryptograficznemu.

Zarządzanie zadaniami obejmuje ich dodawanie, zmianę lub usuwanie oraz nadzór nad ich wykonywaniem. Obecnie w ramach aplikacji istnieją dwa rodzaje zadań:

- zadania składania podpisu,
- zadania weryfikacji podpisu.

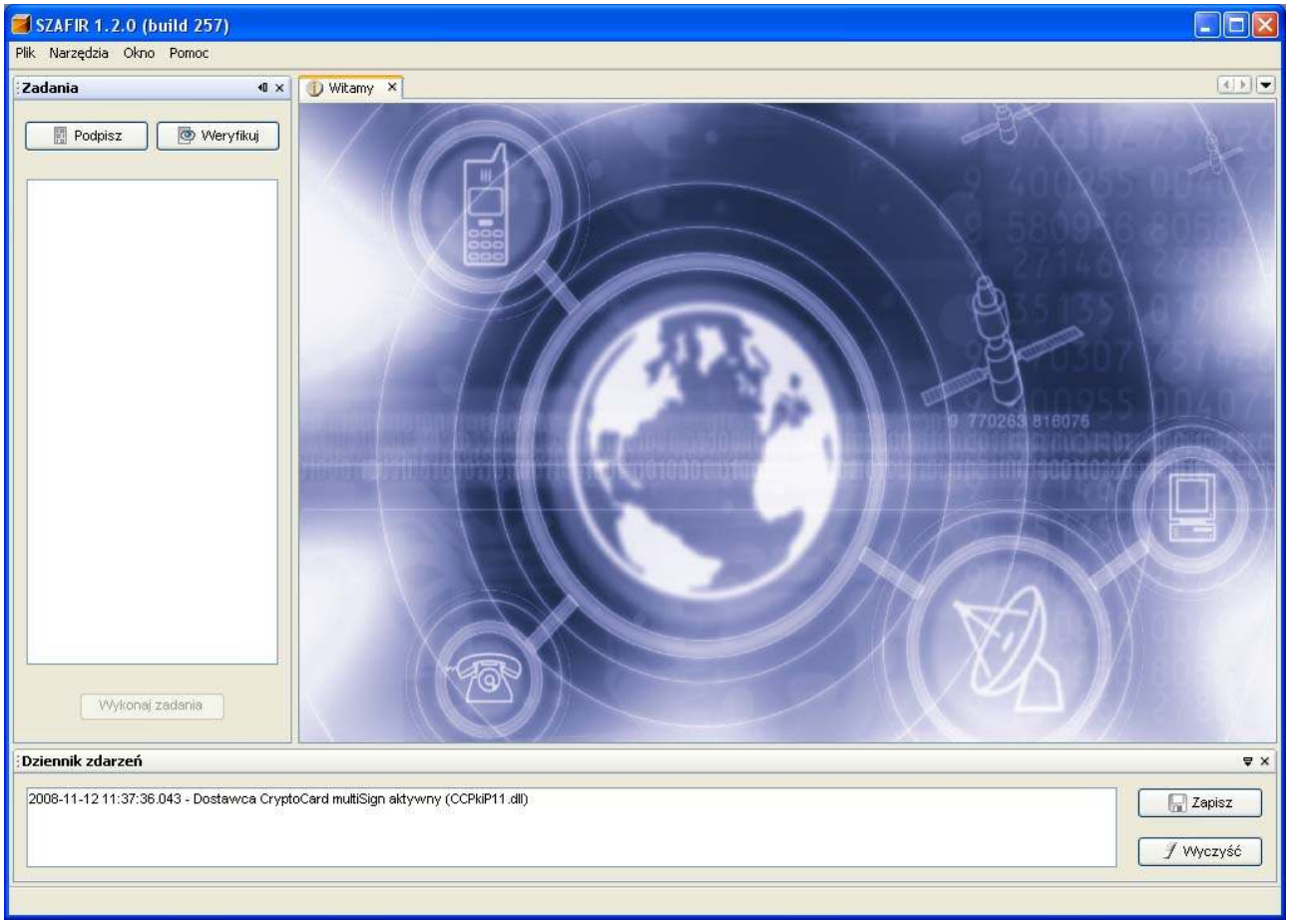
Zadanie składania podpisu to wskazanie:

- jakie informacje należy podpisać,
- w jakim formacie i gdzie należy zapisać podpis elektroniczny,
- jakich należy użyć opcji dodatkowych, takich jak: zakres informacji umieszczanych w podpisie, certyfikaty użyte do złożenia podpisu, konieczność oznakowania podpisu czasem itp..

Zadanie weryfikacji podpisu to wskazanie:

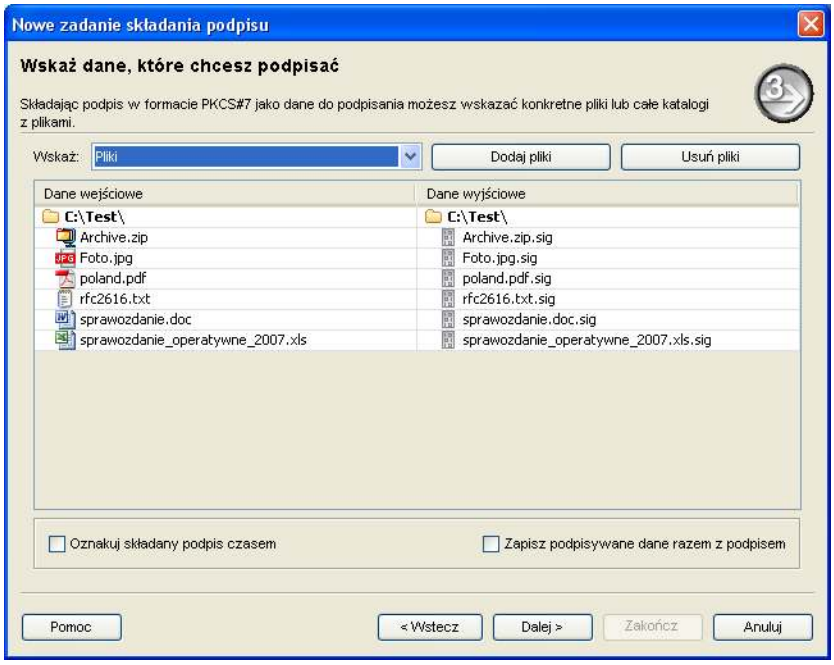
- które podpisy należy zweryfikować,
- jakich należy użyć opcji dodatkowych, takich jak: konieczność oznaczenia podpisu czasem, dodania do niego informacji koniecznych do zapewnienia tzw. długotrwałej ważności dowodowej podpisu (certyfikatów i list certyfikatów zawieszonych i unieważnionych) itp..

Do zarządzania zadaniami służy **okno zadań**, z poziomu którego można uruchomić asystentów składania i weryfikacji podpisu oraz wykonać zdefiniowane przy pomocy asystentów zadania.



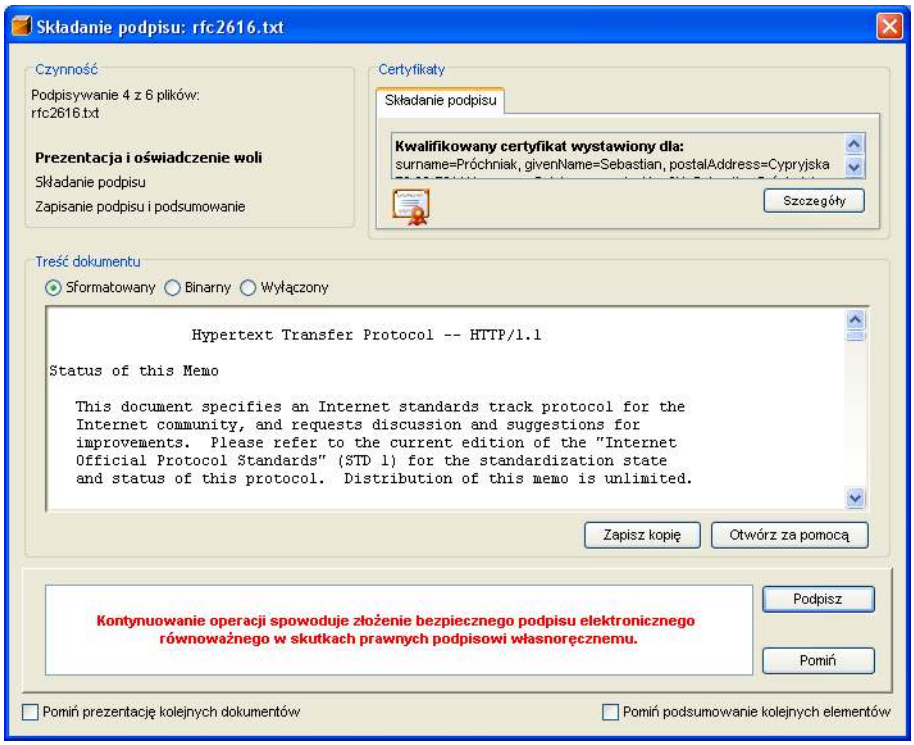
Rysunek 1. Główne okno aplikacji – po lewej stronie okno zadań.

Widoczne w oknie zadań przyciski „Podpisz” i „Weryfikuj” uruchamiają, odpowiednio, asystenta składania oraz asystenta weryfikacji podpisu, prowadzących użytkownika przez kolejne etapy definiowania zadań składania i weryfikacji podpisów.



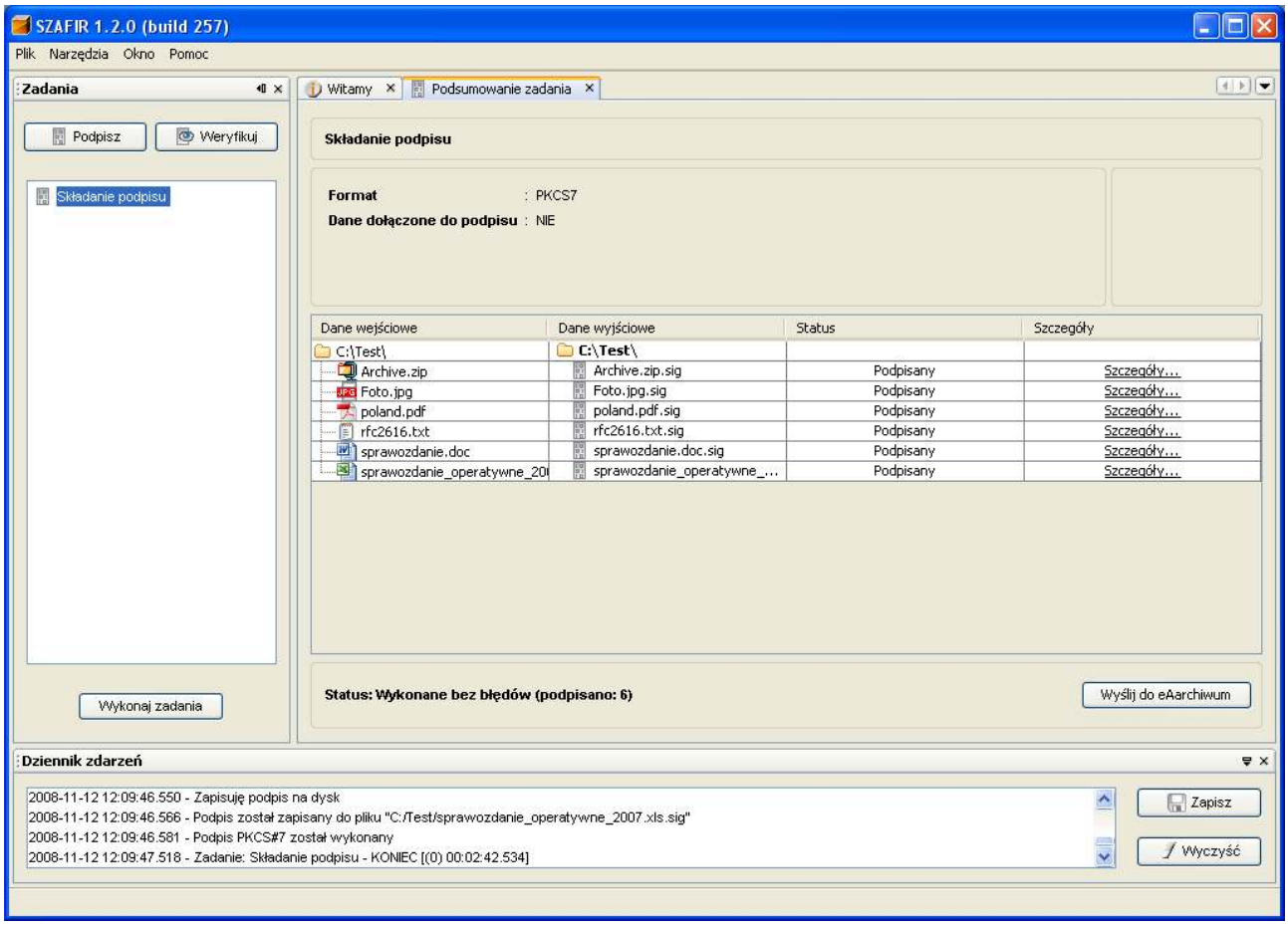
Rysunek 2. Przykładowy ekran asystenta składania podpisu – wskazywanie danych do podpisania.

Zdefiniowane zadania można uruchamiać bezpośrednio po ich zdefiniowaniu, bądź dodawać do listy zadań i wykonywać w późniejszym czasie, uruchamiając ich wykonywanie przy pomocy przycisku „Wykonaj”. W trakcie wykonywania zadań kolejne etapy składania lub weryfikacji podpisu widoczne są w oknach składania oraz weryfikacji podpisu.



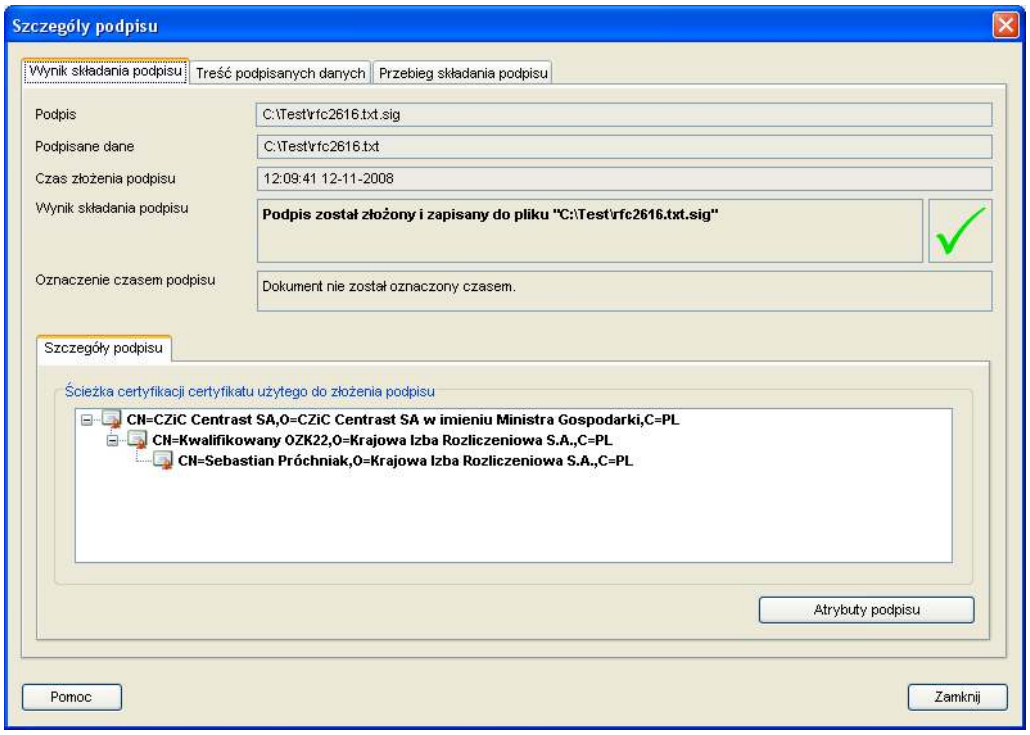
Rysunek 3. Okno składania podpisu – prezentacja treści i oświadczenie woli.

Po zakończeniu wykonywania zadania jest ono nadal widoczne na liście zadań. Zaznaczenie zadania na liście zadań spowoduje wyświetlenie okna podsumowania zadania.



Rysunek 4. Główne okno aplikacji – po prawej widoczne okno podsumowania zadania.

Korzystając z przycisku „Szczegóły” można przeglądać szczegóły złożonych i zweryfikowanych podpisów.



Rysunek 5. Okno szczegółów podpisu.

3. Składanie podpisu

Funkcjonalność aplikacji SZAFIR w dziedzinie składania podpisu obejmuje:

- Składanie zwykłego oraz bezpiecznego podpisu elektronicznego w formatach PKCS#7 oraz XAdES.

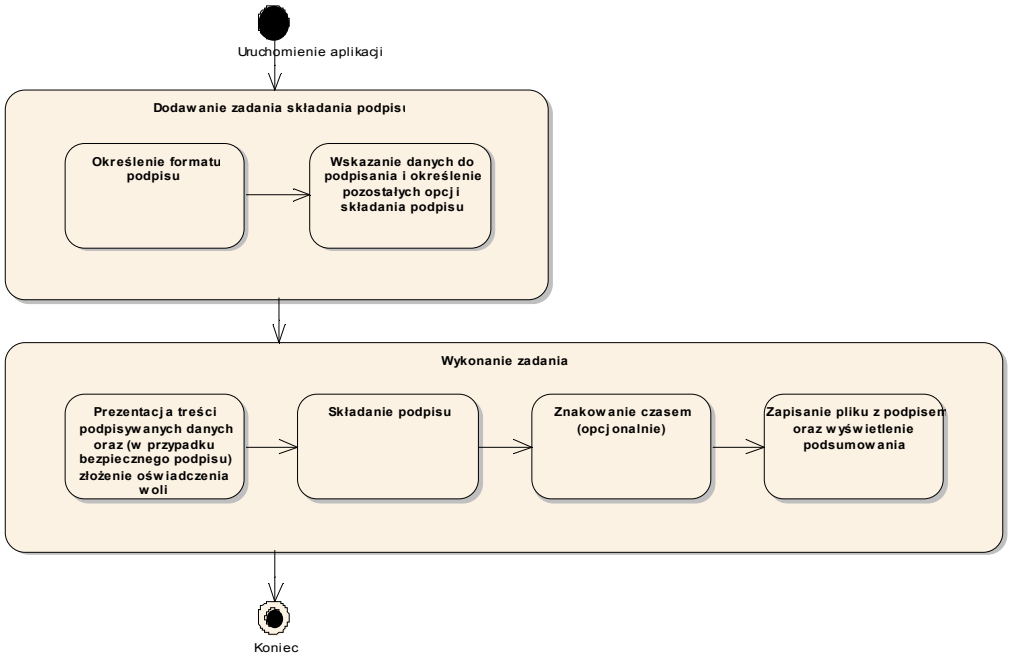
  > W wersji weryfikująco-demonstracyjnej aplikacji składanie podpisu elektronicznego jest możliwe tylko przy wykorzystaniu testowego certyfikatu zapisanego w pliku dostarczanym razem z aplikacją SZAFIR.

- Znakowania czasem podpisu zarówno w procesie jego składania, jak i weryfikacji, przy czym możliwe jest użycie różnych certyfikatów i par kluczy dla procesów składania podpisu i znakowania czasem.

  > Znakowanie czasem jest usługą płatną – korzystanie z niej możliwe jest po podpisaniu odpowiedniej umowy. Dostęp do usługi weryfikowany jest na podstawie certyfikatu używanego przez użytkownika do podpisania wniosku o wydanie znacznika czasu; certyfikat testowy dystrybuowany z wersją weryfikująco-demonstracyjną aplikacji nie umożliwia korzystania z usługi znakowania czasem.

- Możliwość dołączenia podpisywanych danych do pliku z podpisem.
- Możliwość strumieniowego składania podpisów poprzez:
  - możliwość definiowania zadań obejmujących składanie podpisów pod wieloma plikami jednocześnie,
  - możliwość określenia limitu czasu lub limitu ilości operacji kryptograficznych, do osiągnięcia których możliwe będzie wykorzystywanie komponentu technicznego po jednokrotnym podaniu kodu PIN.

Składanie podpisu elektronicznego przy wykorzystaniu aplikacji SZAFIR odbywa się dwu-etapowo: najpierw definiowane jest zadanie składania podpisu, wskazujące jakie dane, w jakim formacie i przy użyciu jakich opcji należy podpisać, a następnie zadanie to jest pod nadzorem użytkownika i przy jego udziale wykonywane.



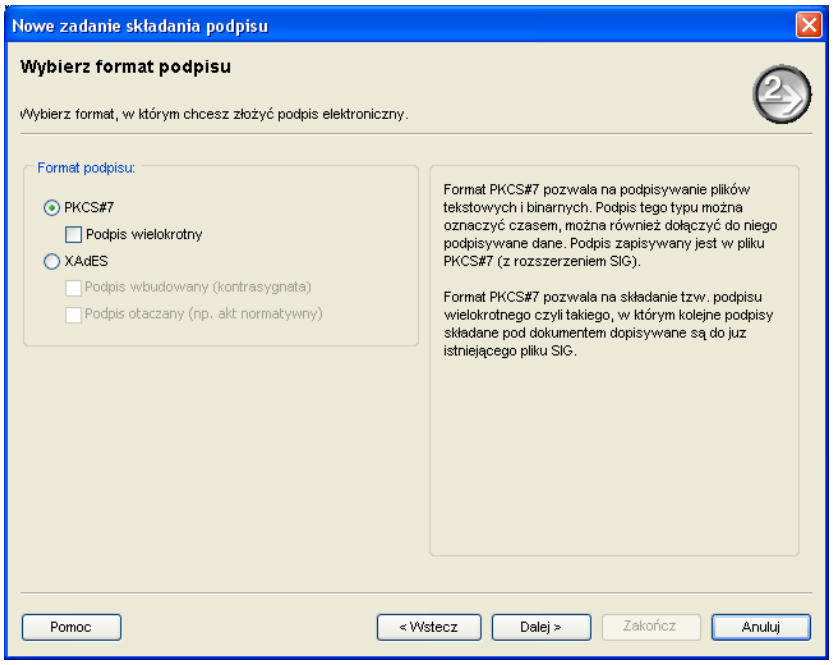
Rysunek 6. Składanie podpisu – kolejność zdarzeń.

3.1. Dodawanie zadania składania podpisu

1. Aby utworzyć nowe zadanie składania podpisu należy kliknąć na przycisku „Podpisz" w oknie listy zadań lub wybrać opcję „Nowe zadanie składania podpisu" z menu Plik. Pojawi się okno asystenta składania podpisu:

Rysunek 7. Asystent składania podpisu - ekran powitalny.

2. W celu kontynuowania dodawania zadania należy kliknąć na przycisku „Dalej”. Pojawi się okno wyboru formatu nowo tworzonego podpisu elektronicznego:



Rysunek 8. Asystent składania podpisu – wybór formatu podpisu.

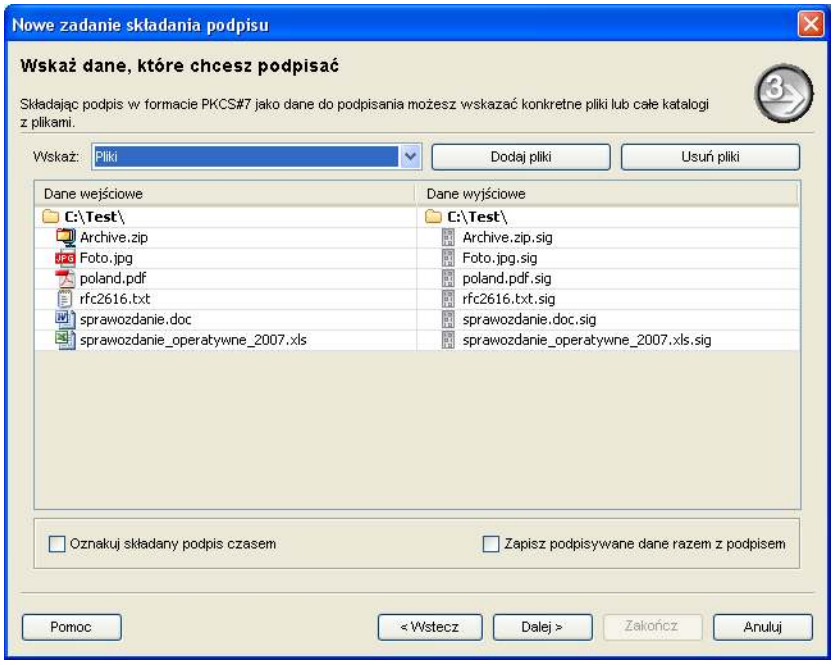
To okno umożliwia wybór formatu, w jakim złożony zostanie podpis elektroniczny:

- **PKCS#7.** Należy wybrać tę opcję aby złożyć podpis elektroniczny w formacie PKCS#7. Format ten pozwala na podpisywanie plików tekstowych i binarnych, oznaczyć go czasem oraz dołączyć do niego podpisywane dane. Podpis zapisywany jest w pliku PKCS#7 (z rozszerzeniem SIG).
  - **Podpis wielokrotny.** Należy zaznaczyć tę opcję aby złożyć podpis PKCS#7 w trybie składania podpisu wielokrotnego – kolejny podpis składany pod dokumentem dopisany zostanie do już istniejącego pliku SIG.
- **XAdES.** Należy wybrać tę opcję aby złożyć podpis elektroniczny w formacie XAdES. Format ten pozwala na podpisywanie plików tekstowych i binarnych oraz dokumentów i elementów (fragmentów dokumentów) XML. Podpis tego typu można oznaczyć czasem, można również dołączyć do niego podpisywane dane oraz, opcjonalnie, certyfikaty i listy CRL przydatne w procesie jego weryfikacji, zapewniając tym samym długotrwałą ważność dowodową podpisu. Format XAdES pozwala na składanie podpisu wielokrotnego oraz, dodatkowo, podpisu wbudowanego, czyli podpisu pod podpisem (kontrasygnaty), albo podpisu otaczanego, czyli podpisu umieszczonego „w danych” podpisywanych.

- **Podpis wbudowany (kontrasygnata).** Należy zaznaczyć tę opcję aby złożyć podpis XAdES w trybie składania podpisu wbudowanego (kontrasygnaty) – kolejny podpis zostanie złożony pod już istniejącym podpisem XAdES.
- **Podpis otaczany.** Należy zaznaczyć tę opcję aby złożyć podpis XAdES w trybie składania podpisu otaczanego. Podpis otaczany umożliwia podpisanie dokumentu XML i osadzenie wykonanego podpisu wewnątrz tego dokumentu. Ten wariant podpisu w formacie XAdES ponadto umożliwia podpisanie razem ze wskazanym dokumentem dowolnych załączników (plików w dowolnym formacie).

3. W celu kontynuowania dodawania zadania należy kliknąć na przycisku „Dalej".

   Jeżeli nie został wybrany wariant podpisu otaczanego formatu XAdES użytkownik powinien zobaczyć poniższe okno.



Rysunek 9a. Asystent składania podpisu – wskazywanie danych do podpisania.

To okno umożliwia wskazanie danych, które mają zostać opatrzone podpisem elektronicznym oraz określenie szczegółowych opcji składania podpisu:

- **Wskaż:**
  - **Pliki.** Należy wybrać tę opcję, aby podpisać jeden lub kilka wskazanych przez siebie plików dowolnego typu.
  - **Katalogi.** Należy wybrać tę opcję, aby podpisać zawartość jednego lub kilku wskazanych przez siebie katalogów.

> Tym, co odróżnia podpisywanie plików od podpisywania katalogu jest moment odczytania i „zamknięcia" listy plików do podpisania: w przypadku podpisywania plików aplikacja odczytuje wskazane pliki w momencie dodawania zadania składania podpisu, natomiast w przypadku podpisywania katalogu aplikacja odczytuje zawartość katalogu (biorąc pod uwagę wszystkie znajdujące się w nim pliki) dopiero w momencie wykonywania zadania.

- **Elementy XML (tylko dla podpisów XAdES).** Należy wybrać tę opcję aby podpisać zawartość jednego lub kilku wskazanych przez siebie elementów XML.

  > Aby można było podpisać element XML musi on posiadać atrybut o nazwie *Id* zawierający identyfikator zgodny z niezbędny w celu zbudowania ścieżki dostępu do podpisywanego elementu, tzw. URI. Wskazanie elementu XML nie posiadającego tego atrybutu powoduje, że przycisk „Wybierz" pozostaje nieaktywny.

- **Podpisy PKCS#7 (tylko dla wielokrotnych podpisów PKCS#7).** Ta opcja jest jedyną dostępną w przypadku składania wielokrotnego podpisu PKCS#7.
- **Podpisy XAdES (tylko dla wbudowanych podpisów XAdES).** Ta opcja jest jedyną dostępną w przypadku składania wbudowanego podpisu XAdES.

- **Lista obiektów do podpisania.** Korzystając z przycisku *Dodaj* należy dodać obiekty wybranego wyżej typu do listy obiektów do podpisania. Do listy tej można dodać dowolną ilość plików, katalogów lub elementów XML. Dla każdego dodanego obiektu aplikacja wstępnie określi miejsce zapisania podpisu:
  - Podpisy elektroniczne dla plików zapisywane będą w katalogach, z których pochodzą wybrane pliki, w plikach z rozszerzeniem SIG (dla podpisów PKCS#7) lub XAdES (dla podpisów XAdES).
  - Podpisy elektroniczne wskazanych elementów XML domyślnie zapisywane będą w plikach z rozszerzeniem XAdES, w katalogach w których znajdują się pliki z których pochodzą podpisywane elementy XML.

  Miejsce zapisania plików z podpisami oraz ich nazwy można zmienić klikając dwukrotnie na zaproponowanej przez aplikację ścieżce wyjściowej oraz nazwach plików z podpisami na liście obiektów do podpisania.

- **Opcje składania podpisu:**
  - **Forma XAdES (tylko dla podpisów XAdES).** Należy określić zakres informacji dodawanych do podpisu w formacie XAdES:
    - **Nie dołączaj dodatkowych informacji (XAdES-BES)** – zostanie złożona podstawowa forma podpisu XAdES.
    - **Dołącz znacznik czasu (XAdES-T)** – zostanie złożony podpis w formacie XAdES-T, zawierający oznaczenie czasem podpisu.

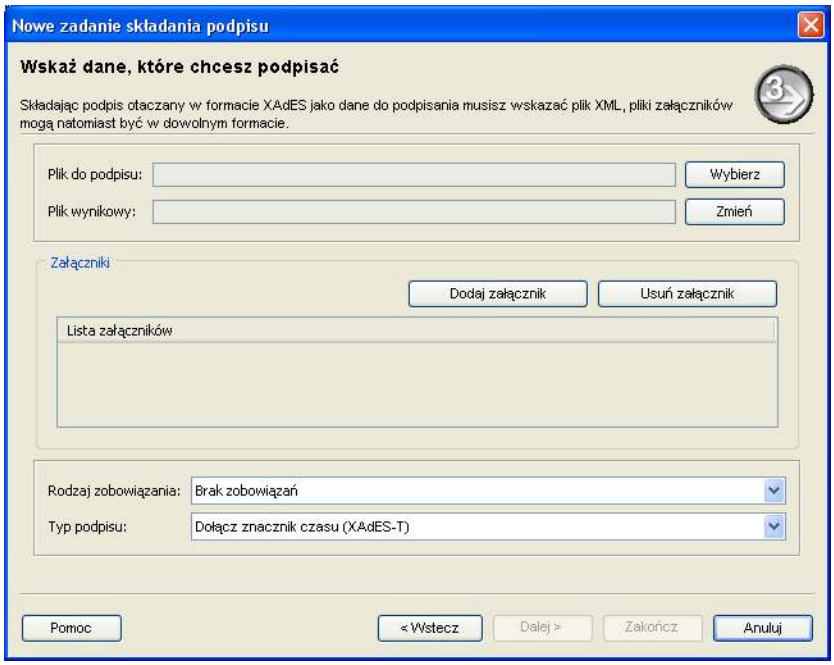
- **Dołącz znacznik czasu, certyfikaty i listy CRL (XAdES-C)** – zostanie złożony podpis w formacie XAdES-C, zawierający znacznik czasu oraz informacje zapewniające tzw. długotrwałą ważność dowodową podpisu.

- **Oznakuj składany podpis czasem (tylko dla podpisów PKCS#7)**. Należy zaznaczyć tę opcję aby do składanego podpisu w formacie PKCS#7 dołączyć oznaczenie czasem podpisu.

- **Zapisz podpisywane dane razem z podpisem.** Należy zaznaczyć tę opcję, aby do składanego podpisu dołączyć podpisywane dane.

> Znakowanie czasem jest usługą płatną – korzystanie z niej możliwe jest po podpisaniu odpowiedniej umowy. Dostęp do usługi weryfikowany jest na podstawie certyfikatu używanego przez użytkownika do podpisania wniosku o wydanie znacznika czasu; certyfikat testowy dystrybuowany z wersją weryfikująco-demonstracyjną aplikacji nie umożliwia korzystania z usługi znakowania czasem. Oznacza to, że w wersji weryfikująco-demonstracyjnej aplikacji próba skorzystania z opcji „Dołącz znacznik czasu (XAdES-T)", „Dołącz znacznik czasu, certyfikaty i listy CRL (XAdES-C)" lub „Oznakuj składany podpis czasem (tylko dla podpisów PKCS#7)" zakończy się niepowodzeniem.

Jeżeli został wybrany wariant podpisu otaczanego formatu XAdES użytkownikowi zostanie zaprezentowane następujące okno.

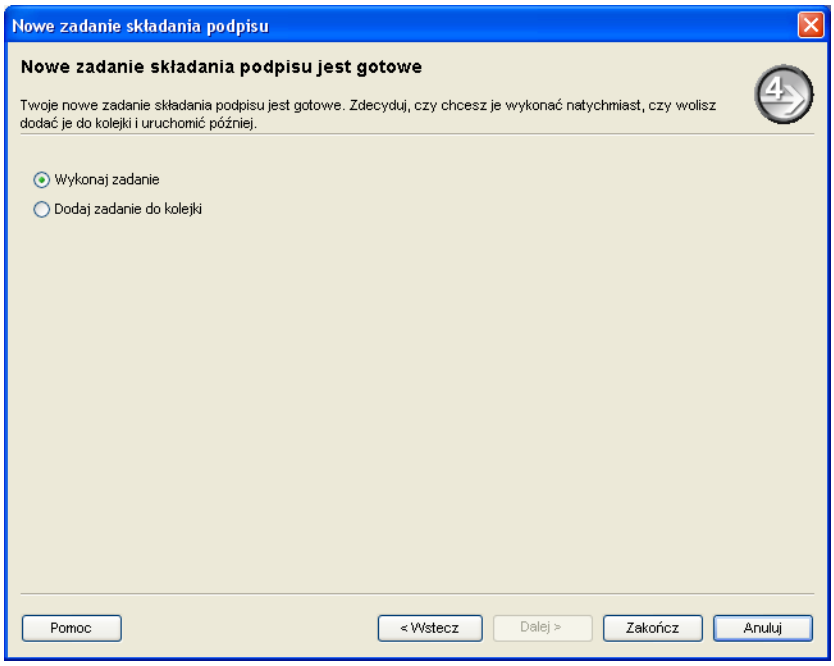


Rysunek 10b. Asystent składania podpisu – wskazywanie danych do podpisania.

To okno umożliwia wskazanie danych, które mają zostać opatrzone podpisem elektronicznym oraz określenie szczegółowych opcji składania podpisu:

- **Plik do podpisu.** Korzystając z przycisku *Wybierz* należy wskazać plik XML, który ma zostać podpisany.
- **Plik wynikowy.** Korzystając z przycisku *Zmień* użytkownik może zmienić zaproponowaną przez aplikację nazwę pliku wynikowego lub jego lokalizację. Plik wynikowy po zakończonym sukcesem procesie podpisywania, będzie zawierał podpisywany dokument XML z osadzonym wewnątrz podpisem.
- **Załączniki.** Korzystając z przycisku *Dodaj załącznik* można dodać pliki stanowiące załączniki do podpisywanego dokumentu. Pliki załączników nie są bezpośrednio dołączane do pliku wynikowego, ale ich zawartość jest uwzględniana w podpisywanej treści, a ich obecność jest zaznaczona w samym podpisie.
- **Rodzaj zobowiązania.** Z rozwijalnej listy opcji należy wybrać jeden rodzaj zobowiązania dla wykonywanego podpisu lub *brak zobowiązań*. Rodzaj zobowiązań można traktować jako cel złożenia podpisu elektronicznego.
- **Typ podpisu.** Należy określić zakres informacji dodawanych do podpisu w formacie XAdES:
  - **Nie dołączaj dodatkowych informacji (XAdES-BES)** – zostanie złożona podstawowa forma podpisu XAdES.
  - **Dołącz znacznik czasu (XAdES-T)** – zostanie złożony podpis w formacie XAdES-T, zawierający oznaczenie czasem podpisu.

4. W celu kontynuowania dodawania zadania należy kliknąć na przycisku „Dalej”. Pojawi się okno z podsumowaniem działania asystenta składania podpisu:



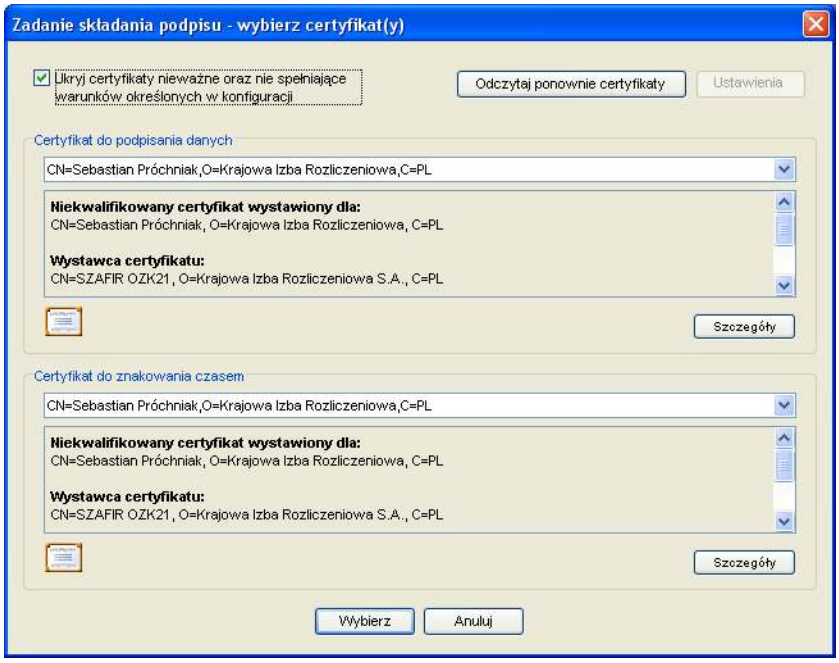
Rysunek 11. Asystent składania podpisu – podsumowanie.

To okno umożliwia określenie momentu wykonania nowo zdefiniowanego zadania:

- **Wykonaj zadanie.** Należy wybrać tę opcję aby bezpośrednio po zakończeniu działania asystenta i dodaniu zadania do kolejki uruchomić wykonywanie nowo zdefiniowanego zadania.
- **Dodaj do kolejki.** Należy wybrać tę opcję aby po zakończeniu działania asystenta tylko dodać zadanie do kolejki, nie uruchamiając jego wykonywania.

3.2. Wykonanie zadania składania podpisu

1. W zależności od tego, jaki moment uruchomienia zadania wybrano podczas definiowania zadania, wykonywanie nowo zdefiniowanego zadania składania podpisu rozpoczyna się bezpośrednio po utworzeniu nowego zadania lub w następstwie kliknięcia na przycisku „Wykonaj" w oknie listy zadań. Wykonywanie zadania rozpoczyna się od określenia, jakich certyfikatów należy użyć do złożenia podpisu i, opcjonalnie, złożenia wniosku o uzyskanie znacznika czasu. W tym celu wyświetlane jest okno „Wybierz certyfikaty" umożliwiające użytkownikowi wskazanie niezbędnych certyfikatów:



Rysunek 12. Okno wyboru certyfikatów.

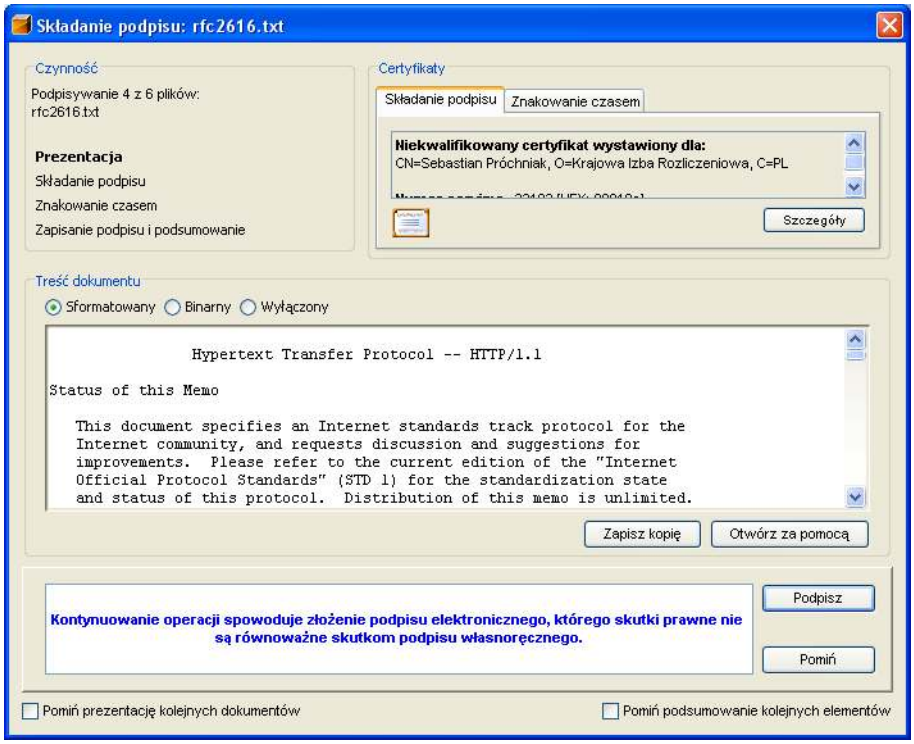
Wybór certyfikatów podlega następującym ograniczeniom:

a) Jeżeli w konfiguracji aplikacji zaznaczono, iż do składania podpisu lub podpisania wniosku o wydanie znacznika czasu używany ma być konkretny certyfikat wówczas krok ten jest, w odniesieniu do danej czynności, pomijany (aplikacja nie pozwala na wybranie innego certyfikatu niż określony w konfiguracji aplikacji).

b) W wersji weryfikująco-demonstracyjnej aplikacji składanie podpisu elektronicznego jest możliwe tylko przy wykorzystaniu testowego certyfikatu zapisanego w pliku dostarczanym razem z aplikacją SZAFIR. Certyfikat ten nie umożliwia podpisania wniosku o wydanie znacznika czasu, dlatego próba składania podpisu z jednoczesnym uzyskaniem znacznika czasu przy użyciu tej wersji oprogramowania zakończy się niepowodzeniem.

c) Nie można wybrać certyfikatu, którego okres ważności jeszcze się nie rozpoczął bądź już upłynął.

2. W celu kontynuowania składania podpisu należy wybrać stosowne certyfikaty i kliknąć na przycisku „Wybierz”. Zostanie wyświetlone okno składania podpisu:



Rysunek 13. Okno składania podpisu – prezentacja treści i oświadczenie woli.

To okno umożliwia użytkownikowi nadzór nad procesem składania podpisu elektronicznego.

- **Czynność.** W tej ramce wyświetlane są informacje o aktualnie wykonywanej czynności (takiej jak podpisywanie pliku o określonej nazwie) i jej kolejnych krokach:
  - **Prezentacja treści i oświadczenie woli.**
  - **Składanie podpisu.**
  - **Znakowanie czasem.**
  - **Podsumowanie.**
- **Certyfikaty.** W tej ramce wyświetlane są informacje o certyfikatach używanych w trakcie składania podpisu elektronicznego.
  - **Składanie podpisu.** Na tej zakładce wyświetlane są podstawowe parametry certyfikatu używanego do składania podpisu elektronicznego.
  - **Znakowanie czasem.** Na tej zakładce wyświetlane są podstawowe parametry certyfikatu używanego do podpisania wniosku o wydanie znacznika czasu.

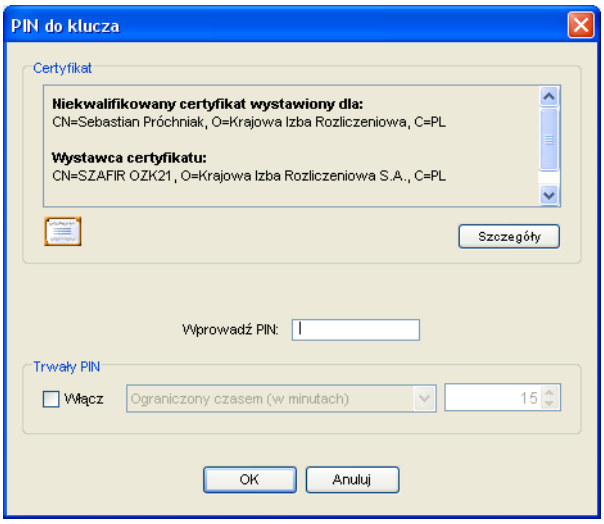
- **Podpisywane dane.** W tym polu prezentowana jest treść podpisywanych danych. Aplikacja potrafi samodzielnie zaprezentować treść plików następujących typów:
  - .TXT
  - .XML
  - .RTF
  - .JPG, .BMP, .GIF i szereg innych plików graficznych

  Pliki innych typów mogą być wyświetlane przy pomocy zewnętrznych aplikacji. Użytkownik może wybrać aplikację z listy programów zarejestrowanych w systemie operacyjnym lub wskazać dowolną inną aplikację, przy pomocy której chce obejrzeć zawartość pliku.
- **Informacje o kolejno wykonywanych krokach** wyświetlane są w panelu na dole okna składania podpisu:
  - **Prezentacja treści i oświadczenie woli.** Przed rozpoczęciem składania podpisu aplikacja prezentuje treść podpisywanego dokumentu oraz wyświetla informację o prawnych skutkach składania podpisu elektronicznego przy użyciu aktualnie wybranego certyfikatu. Użytkownik może zdecydować o rozpoczęciu podpisywania danych lub ich pominięciu.
    - **Podpisz** rozpoczyna składanie podpisu elektronicznego.
    - **Pomiń** pomija składanie podpisu elektronicznego.
    - **Pomiń prezentację kolejnych dokumentów** – jeżeli ta opcja zostanie zaznaczona, wówczas podpisywanie kolejnych dokumentów odbywać się będzie z pominięciem ich prezentacji oraz żądania złożenia oświadczenia woli przez użytkownika.
  - **Składanie podpisu.** Po uzyskaniu oświadczenia woli użytkownika aplikacja rozpoczyna składanie podpisu elektronicznego.
  - **Znakowanie czasem.** Po złożeniu podpisu elektronicznego aplikacja zwraca się z wnioskiem o wydanie znacznika czasu dla nowo utworzonego podpisu.

    > Znakowanie czasem jest usługą płatną – korzystanie z niej możliwe jest po podpisaniu odpowiedniej umowy. Dostęp do usługi weryfikowany jest na podstawie certyfikatu używanego przez użytkownika do podpisania wniosku o wydanie znacznika czasu; certyfikat testowy dystrybuowany z wersją weryfikująco-demonstracyjną aplikacji nie umożliwia korzystania z usługi znakowania czasem.
  - **Podsumowanie.** Po zakończeniu składania podpisu i znakowania czasem aplikacja zapisuje plik z podpisem i wyświetla podsumowanie wykonanych operacji.

- **Szczegóły** wyświetla szczegóły zakończonego właśnie procesu składania podpisu.
- **Dalej** rozpoczyna składanie kolejnego podpisu (jeżeli w ramach aktualnie wykonywanego zadania pozostały jeszcze jakieś podpisy do złożenia).
- **Anuluj** anuluje wykonywanie bieżącego zadania.
- **Pomiń podsumowanie kolejnych dokumentów** – jeżeli ta opcja zostanie zaznaczona, wówczas podpisywanie kolejnych dokumentów odbywać się będzie z pominięciem wyświetlania podsumowania.

3. W celu kontynuowania składania podpisu należy kliknąć na przycisku „Podpisz". Aplikacja rozpocznie składanie podpisu oraz znakowanie czasem. Za każdym razem gdy do przeprowadzenia operacji kryptograficznej niezbędne będzie uzyskanie dostępu do karty kryptograficznej lub zabezpieczonego pliku z certyfikatem, pojawi się okno wprowadzania PIN:



Rysunek 14. Okno wprowadzania PIN.

To okno pozwala na wprowadzenie kodu PIN, który jest niezbędny w celu odblokowania dostępu do karty kryptograficznej lub zabezpieczonego pliku z certyfikatem; możliwe jest również wprowadzenie za jego pomocą tzw. trwałego PIN, pozwalającego, poprzez przechowanie przez określony czas kodu PIN w pamięci aplikacji, na składanie podpisów i znakowanie czasem bez udziału użytkownika:

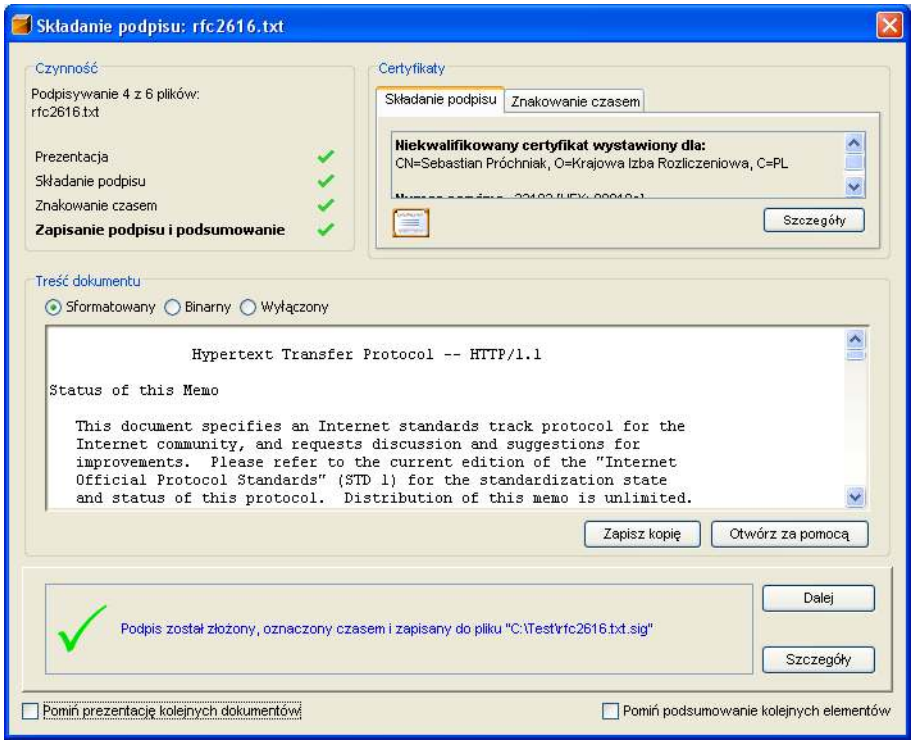
- **Wprowadź PIN do klucza.** Należy podać kod PIN do karty kryptograficznej lub zabezpieczonego pliku, w którym przechowywany jest certyfikat oraz para kluczy kryptograficznych.

> PIN testowego certyfikatu „CN=SZAFIR – Demo, O=SZAFIR, C=PL", który dystrybuowany jest razem z aplikacją to **„Szafir123."** (z kropką na końcu, bez cudzysłowów).

- **Trwały PIN.**
  - **Włącz** udostępnia możliwość użycia trwałego PIN.
  - **Ograniczony czasem (w minutach)** pozwala na określenie limitu czasu.
  - **Ograniczony ilości operacji** pozwala na określenie limitu możliwych do wykonania operacji kryptograficznych.

> Użycie trwałego PIN zmniejsza bezpieczeństwo aplikacji oraz karty kryptograficznej z uwagi na to, że PIN – choć w formie zaszyfrowanej – przechowywany jest jednak w pamięci komputera.

4. Po wprowadzeniu kodu PIN i jego zatwierdzeniu przyciskiem „OK” aplikacja złoży podpis elektroniczny oraz oznakuje złożony podpis czasem. W oknie składania podpisu pojawi się podsumowanie wykonanych operacji:



Rysunek 15. Okno składania podpisu – podsumowanie.

4. Weryfikacja podpisu

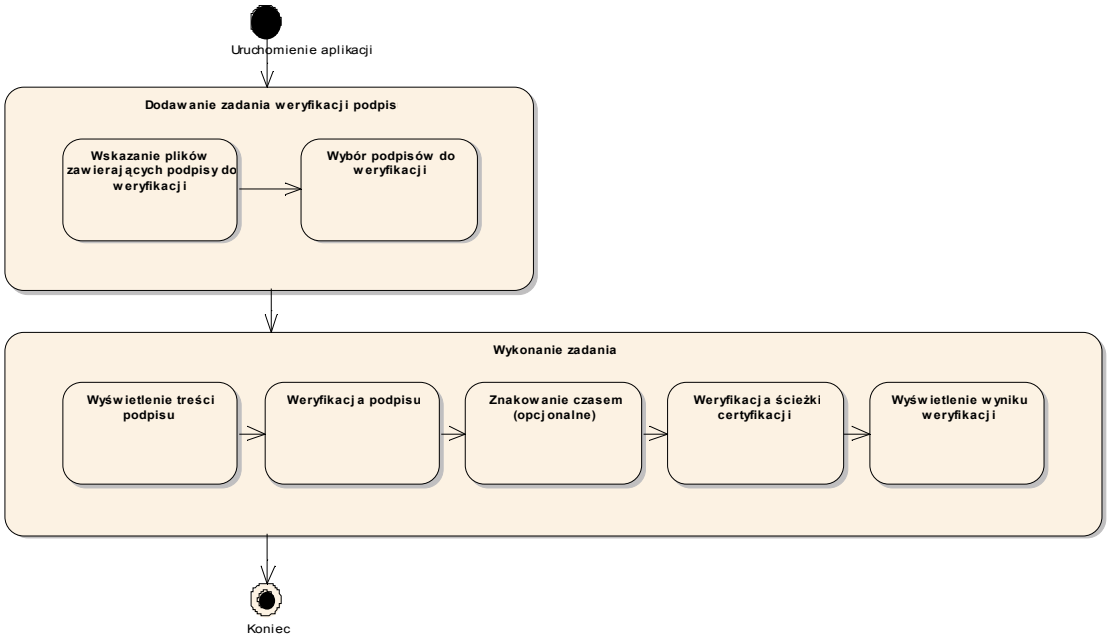
Funkcjonalność aplikacji SZAFIR w zakresie weryfikacji podpisu obejmuje:

- Weryfikowanie zwykłych oraz bezpiecznych podpisów elektronicznych w formatach:
  - PKCS#7 (podpis pojedynczy i wielokrotny)
  - XAdES-BES, XAdES-T, XAdES-C (podpis pojedynczy, wiele podpisów w plików oraz podpis wbudowany).
- Znakowanie czasem podpisu zarówno w procesie jego weryfikacji.

> Znakowanie czasem jest usługą płatną – korzystanie z niej możliwe jest po podpisaniu odpowiedniej umowy. Dostęp do usługi weryfikowany jest na podstawie certyfikatu używanego przez użytkownika do podpisania wniosku o wydanie znacznika czasu; certyfikat testowy dystrybuowany z wersją weryfikująco-demonstracyjną aplikacji nie umożliwia korzystania z usługi znakowania czasem.

- Możliwości strumieniowego weryfikowania podpisów, poprzez:
  - możliwość definiowania zadań obejmujących weryfikację wielu podpisów jednocześnie,
  - możliwość określenia limitu czasu lub limitu ilości operacji kryptograficznych, do osiągnięcia których możliwe będzie wykorzystywanie komponentu technicznego (np. w celu oznakowania czasem podpisu w procesie jego weryfikacji) po jednokrotnym podaniu kodu PIN.

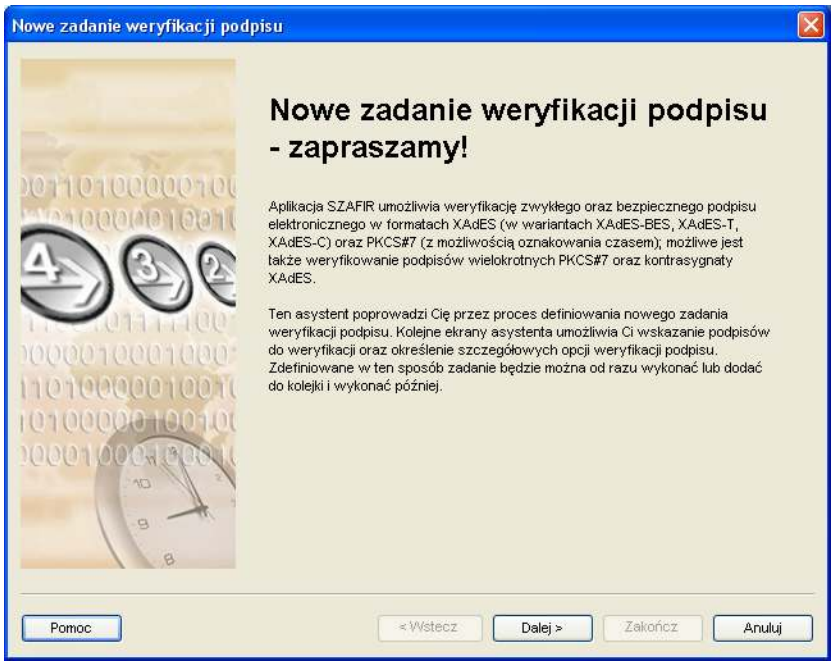
Weryfikacja podpisu elektronicznego przy wykorzystaniu aplikacji SZAFIR odbywa się dwuetapowo: najpierw definiowane jest zadanie weryfikacji podpisu, wskazujące które podpisy i przy użyciu jakich opcji należy zweryfikować, a następnie zadanie to jest pod nadzorem użytkownika i przy jego udziale wykonywane.



Rysunek 16. Weryfikacja podpisu – kolejność zdarzeń.

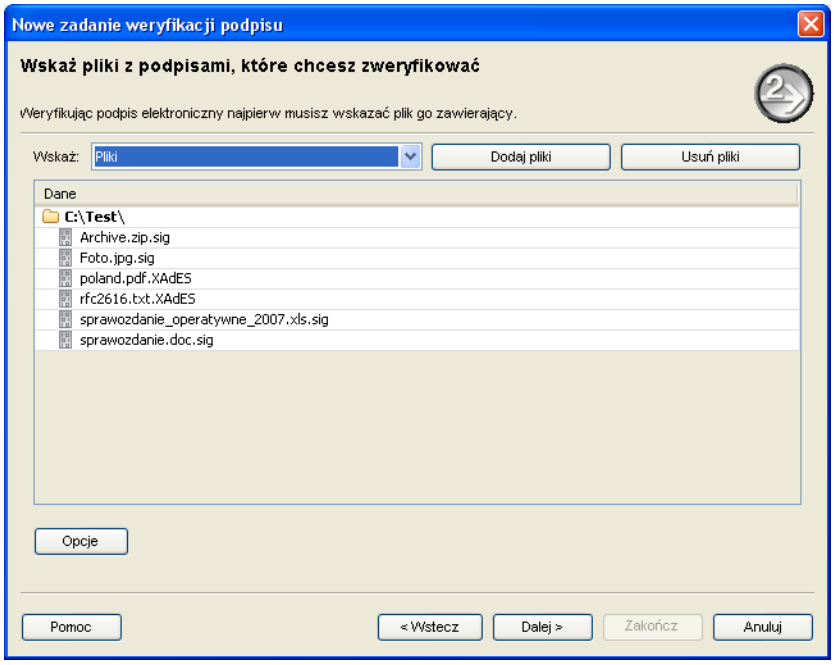
4.1. Dodawanie zadania weryfikacji podpisu

1. Aby utworzyć nowe zadanie weryfikacji podpisu należy kliknąć na przycisku „Weryfikuj” w oknie listy zadań lub wybrać opcję „Nowe zadanie weryfikacji podpisu” z menu Plik. Pojawi się okno asystenta weryfikacji podpisu:



Rysunek 17. Asystent weryfikacji podpisu – ekran powitalny.

2. W celu kontynuowania dodawania zadania należy kliknąć na przycisku „Dalej”. Pojawi się okno wyboru plików z podpisami do weryfikacji:

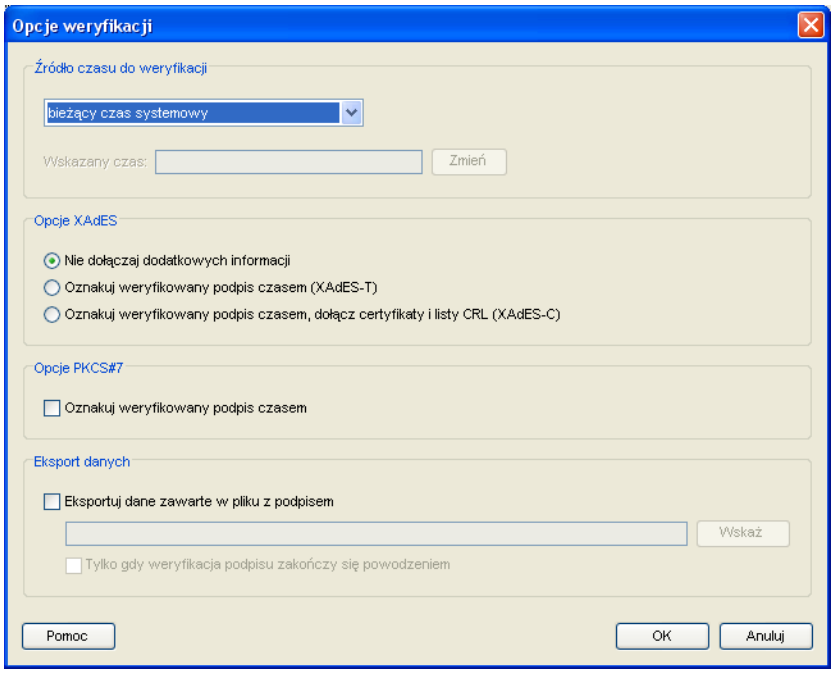


Rysunek 18. Asystent weryfikacji podpisu – wskazywanie plików z podpisami do weryfikacji.

To okno umożliwia wskazanie plików zawierających podpisy elektroniczne, które mają zostać poddane weryfikacji oraz określenie szczegółowych opcji składania podpisu.

- **Wskaż:**
  - **Pliki.** Należy wskazać tę opcję aby zweryfikować podpisy znajdujące się w jednym lub kilku wskazanych plikach.
  - **Katalogi.** Należy wskazać tę opcję aby zweryfikować podpisy znajdujące się we wszystkich plikach znajdujących się w jednym lub kilku wskazanych katalogach.
    - Tym, co odróżnia weryfikowanie podpisów znajdujących się we wskazanych plikach od weryfikacji podpisów znajdujących się we wszystkich plikach znajdujących się we wskazanych katalogach jest moment odczytania i „zamknięcia” listy plików z podpisami do weryfikacji: w pierwszym przypadku aplikacja odczytuje wskazane pliki w momencie dodawania zadania weryfikacji podpisu, natomiast w przypadku weryfikacji zawartości katalogu aplikacja odczytuje zawartość katalogu (biorąc pod uwagę wszystkie znajdujące się w nim pliki i znajdujące się w plikach podpisy) dopiero w momencie wykonywania zadania.
- **Lista obiektów zawierających podpisy do weryfikacji.** Korzystając z przycisku *Dodaj* należy dodać obiekty pliki lub katalogi do listy obiektów zawierających podpisy do weryfikacji. Do listy tej można dodać dowolną ilość plików, katalogów lub elementów XML.

- **Opcje.** Należy użyć tego przycisku aby otworzyć okno domyślnych opcji weryfikacji:



Rysunek 19. Okno domyślnych opcji weryfikacji.

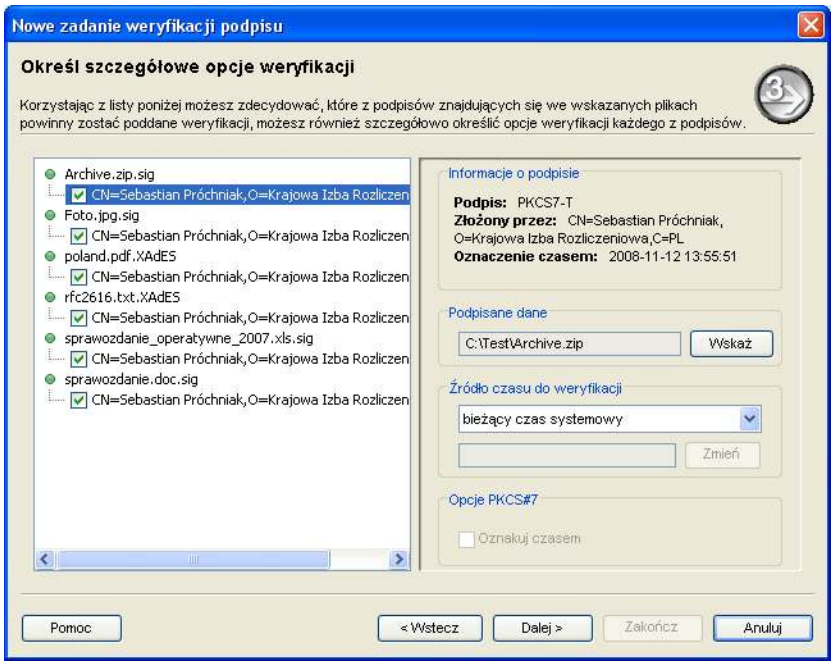
Domyślne opcje weryfikacji podpisu obejmują:

- ustawienie **Źródła czasu do weryfikacji:**
  - **Czas zapisany w znaczniku czasu.** Należy wybrać tę opcję, aby do weryfikacji podpisów domyślnie używać czasu zapisanego w znaczniku czasu pod podpisem. W przypadku podpisów nie zawierających znaczników czasu do weryfikacji podpisu zostanie użyty czas wskazany przez użytkownika.
  - **Bieżący czas systemowy.** Należy wybrać tę opcję, aby do weryfikacji podpisów domyślnie używać bieżącego czasu systemowego.
  - **Czas wskazany przez użytkownika.** Należy wybrać tę opcję, aby do weryfikacji podpisu używać czasu wskazanego przez użytkownika.
  - **Czas zapisany w atrybucie SigningTime.** Należy wybrać tę opcję, aby do weryfikacji podpisu używać czasu zapisanego w atrybucie SigningTime.
- określenie **Opcji XAdES:**
  - **Nie dołączaj dodatkowych informacji.** Należy wybrać tę opcję, aby domyślnie nie zmieniać formy XAdES weryfikowanych podpisów podpisu.
  - **Oznakuj weryfikowany podpis czasem (XAdES-T).** Należy wybrać tę opcję, aby domyślnie oznaczać weryfikowane podpisy czasem i tym samym podnosić je do formy XAdES-T.

- **Oznakuj weryfikowany podpis czasem, dołącz certyfikaty i listy CRL (XAdES-C).** Należy wybrać tę opcję, aby domyślnie oznaczać weryfikowane podpisy czasem (jeżeli nie zostały jeszcze oznaczony czasem) oraz dołączać do nich certyfikaty i listy CRL, zapewniając im tym samym tzw. długotrwałą ważność dowodową.

- określenie **Opcje PKCS#7:**
  - **Oznakuj weryfikowany podpis czasem.** Należy zaznaczyć tę opcję, aby domyślnie znakować weryfikowane podpisy czasem.
- określenie opcji **Eksportu danych:**
  - **Eksportuj dane zawarte w pliku z podpisem.** Należy zaznaczyć tę opcję, aby dane zawarte w plikach z podpisami zapisywać we wskazanym katalogu.
    - **Tylko gdy weryfikacja podpisu zakończy się powodzeniem.** Domyślnie aplikacja zapisuje podpisane dane we wskazanym katalogu tylko wtedy, gdy weryfikacja podpisu elektronicznego zakończy się pozytywnie. Należy zaznaczyć tę opcję, aby podpisane dane zawarte w plikach z podpisami zapisywać we wskazanym katalogu niezależnie od wyniku weryfikacji podpisu.

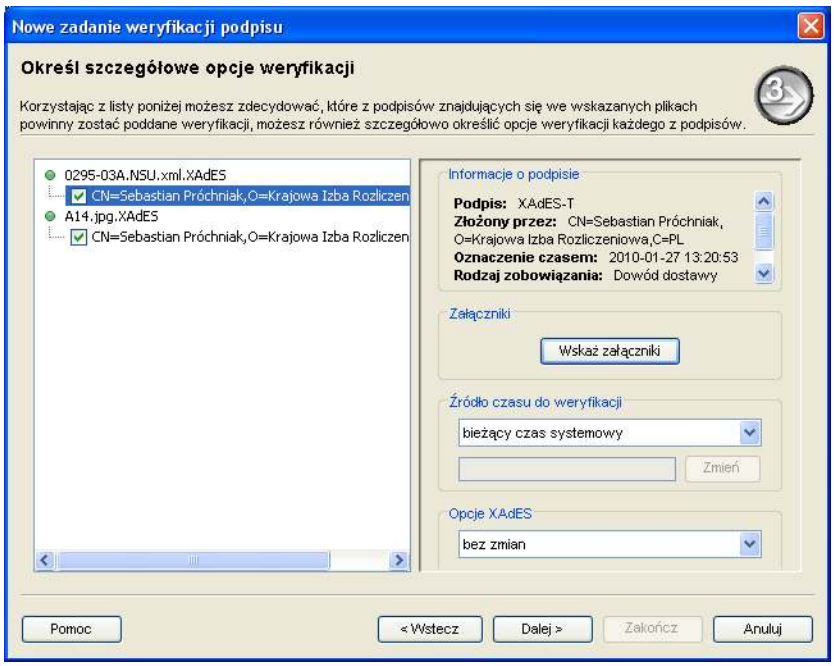
3. Po wskazaniu listy plików zawierających podpisy do weryfikacji oraz zatwierdzeniu domyślnych opcji weryfikacji należy kliknąć na przycisku „Dalej”. Pojawi się okno szczegółowych opcji weryfikacji:



Rysunek 20. Asystent weryfikacji podpisu – określenie szczegółowych opcji weryfikacji.

To okno umożliwia zatwierdzenie listy podpisów do weryfikacji i określenie szczegółowych opcji weryfikacji dla każdego z podpisów:

- **Lista podpisów.** W tym polu znajduje się lista wszystkich podpisów odczytanych ze wskazanych plików. Zmieniając zaznaczenie poszczególnych podpisów można decydować o tym, które z nich poddane zostaną weryfikacji (domyślnie weryfikowane są wszystkie podpisy).
- **Informacje o podpisie.** W tym polu wyświetlone są podstawowe informacje o aktualnie zaznaczonym na liście podpisie.
- **Podpisane dane.** W tym polu wyświetlana jest informacja o danych, które użyte zostaną w procesie weryfikacji podpisu elektronicznego. Mogą to być:
  - **Dane zawarte w weryfikowanym podpisie.** Jeżeli weryfikowany podpis zawiera podpisane dane, zostaną one użyte w procesie weryfikacji podpisu.
  - **Dane zapisane w zewnętrznym pliku lub elemencie XML.** Jeżeli weryfikowany podpis nie zawiera podpisanych danych, a jedynie wskazanie na nie (nazwę pliku lub wskazanie na element XML) wówczas aplikacja próbuje zlokalizować podpisane dane na podstawie informacji zawartych w weryfikowanym podpisie.
- **Załączniki (tylko podpis w formacie XAdES w wariancie podpisu otaczanego).** Przycisk *Wskaż załączniki* umożliwia wskazanie lokalizacji dla plików załączników, które brały udział w procesie podpisywania dokumentu. Jeżeli pliki załączników znajdują się w tym samym miejscu co podpisany dokument i nazwy plików załączników nie zostały zmienione aplikacja sama zauważy ich obecność. W przeciwnym razie tekst na przycisku *Wskaż załączniki* zostanie wyświetlony w kolorze czerwonym, aby zasygnalizować brak lokalizacji dla wszystkich lub tylko niektórych plików.

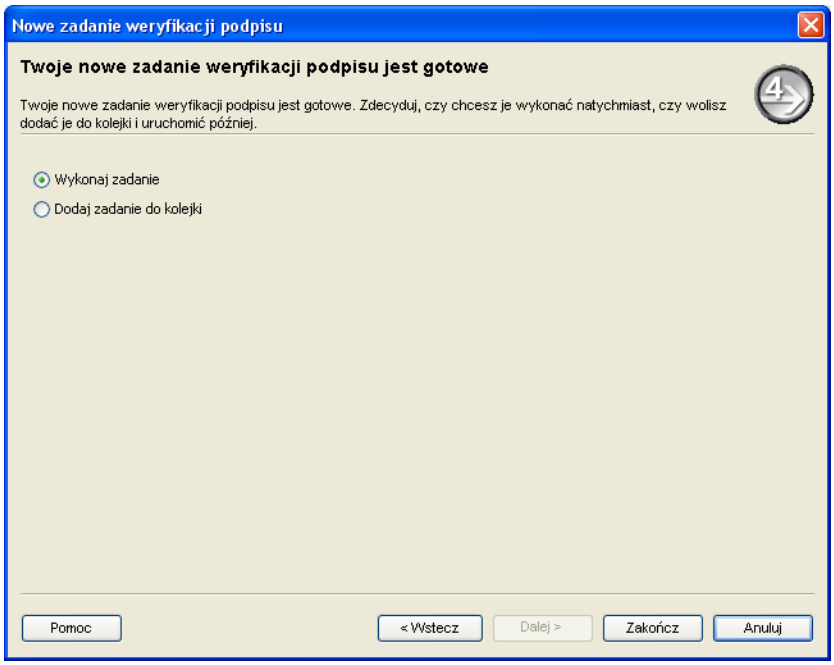


Rysunek 21. Asystent weryfikacji podpisu – określenie szczegółowych opcji weryfikacji.

- **Źródło czasu do weryfikacji.** W tej sekcji można zdecydować, które źródło czasu zostanie użyte podczas weryfikacji podpisu elektronicznego.
  - **Czas zapisany w znaczniku czasu.** Należy wybrać tę opcję, aby do weryfikacji podpisu użyć czasu zapisanego w znaczniku czasu pod podpisem (opcja dostępna tylko jeżeli podpis został wcześniej oznaczony czasem).
  - **Bieżący czas systemowy.** Należy wybrać tę opcję, aby do weryfikacji podpisu użyć bieżącego czasu systemowego.
  - **Czas wskazany przez użytkownika.** Należy wybrać tę opcję, aby do weryfikacji podpisu użyć czasu wskazanego przez użytkownika.
  - **Czas zapisany w atrybucie SigningTime.** Należy wybrać tę opcję, aby do weryfikacji podpisu użyć czasu zapisanego w atrybucie SigningTime.
- **Opcje PKCS#7:**
  - **Znakowanie czasem.** Należy zaznaczyć tę opcję, aby oznakować weryfikowany podpis czasem (opcja dostępna tylko jeżeli weryfikowany podpis nie został jeszcze oznaczony czasem).
- **Opcje XAdES:**
  - **Bez zmian.** Należy wybrać tę opcję, aby nie zmieniać formy XAdES weryfikowanego podpisu.
  - **XAdES-T.** Należy wybrać tę opcję, aby oznaczyć weryfikowany podpis czasem i tym samym podnieść go do formy XAdES-T (opcja dostępna tylko jeżeli weryfikowany podpis nie został jeszcze oznaczony czasem).
  - **XAdES-C.** Należy wybrać tę opcję, aby oznaczyć weryfikowany podpis czasem (jeżeli nie został jeszcze oznaczony czasem) oraz dołączyć do niego certyfikaty i listy CRL, zapewniając mu tym samym tzw. długotrwałą ważność dowodową (opcja dostępna tylko jeżeli certyfikaty i listy CRL nie zostały jeszcze dołączone do weryfikowanego podpisu).

> Znakowanie czasem jest usługą płatną – korzystanie z niej możliwe jest po podpisaniu odpowiedniej umowy. Dostęp do usługi weryfikowany jest na podstawie certyfikatu używanego przez użytkownika do podpisania wniosku o wydanie znacznika czasu; certyfikat testowy dystrybuowany z wersją weryfikująco-demonstracyjną aplikacji nie umożliwia korzystania z usługi znakowania czasem. Oznacza to, że w wersji weryfikująco-demonstracyjnej aplikacji próba skorzystania z opcji „XAdES-T" lub „XAdES-C" (opcje XAdES) lub „Znakowanie czasem" (opcje PKCS#7) zakończy się niepowodzeniem.

4. W celu kontynuowania dodawania zadania należy kliknąć na przycisku „Dalej”. Pojawi się okno z podsumowaniem działania asystenta weryfikacji podpisu:



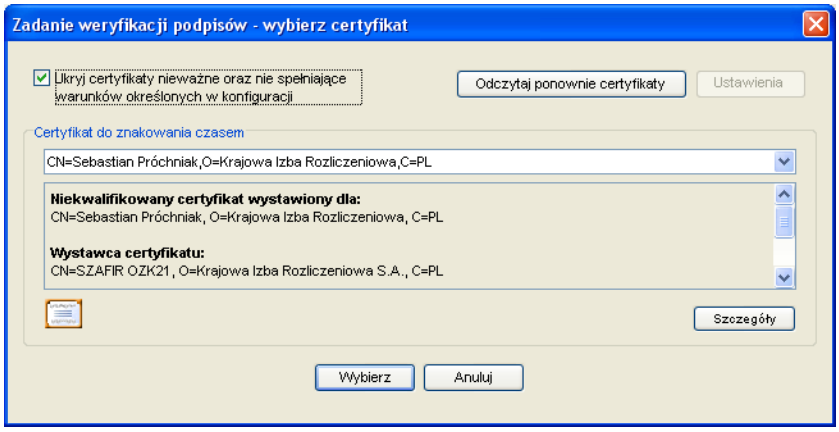
Rysunek 22. Asystent weryfikacji podpisu – podsumowanie.

To okno umożliwia określenie momentu wykonania nowo zdefiniowanego zadania:

- **Wykonaj zadanie.** Należy wybrać tę opcję aby bezpośrednio po zakończeniu działania asystenta i dodaniu zadania do kolejki uruchomić wykonywanie nowo zdefiniowanego zadania.
- **Dodaj do kolejki.** Należy wybrać tę opcję aby po zakończeniu działania asystenta tylko dodać zadanie do kolejki, nie uruchamiając jego wykonywania.

4.2. Wykonanie zadania weryfikacji podpisu

1. W zależności od tego, jaki moment uruchomienia zadania wybrano podczas definiowania zadania, wykonywanie nowo zdefiniowanego zadania weryfikacji podpisu rozpoczyna się bezpośrednio po utworzeniu nowego zadania lub w następstwie kliknięcia na przycisku „Wykonaj” w oknie listy zadań. Jeżeli w ramach zadania ma zostać dokonane znakowanie czasem, wówczas wykonywanie zadania rozpoczyna się od określenia, jakiego certyfikatu należy użyć do podpisania wniosku o uzyskanie znacznika czasu. W tym celu wyświetlane jest okno „Wybierz certyfikaty” umożliwiające użytkownikowi wskazanie niezbędnego certyfikatu:



Rysunek 23. Okno wyboru certyfikatów.

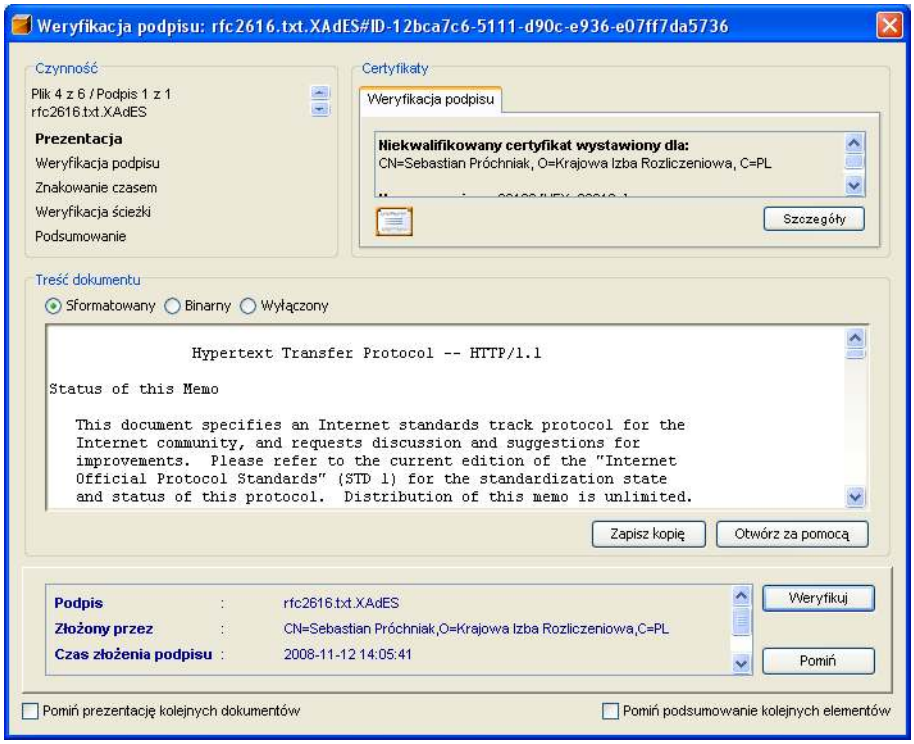
Wybór certyfikatów podlega następującym ograniczeniom:

a) Jeżeli w konfiguracji aplikacji zaznaczono, iż do składania podpisu lub znakowania czasem używany ma być konkretny certyfikat wówczas krok ten jest, w odniesieniu do danej czynności, pomijany (aplikacja nie pozwala na wybranie innego certyfikatu niż określony w konfiguracji aplikacji).

b) W wersji weryfikująco-demonstracyjnej aplikacji składanie podpisu elektronicznego jest możliwe tylko przy wykorzystaniu testowego certyfikatu zapisanego w pliku dostarczanym razem z aplikacją SZAFIR. Certyfikat ten nie umożliwia podpisania wniosku o wydanie znacznika czasu, dlatego próba weryfikowania podpisu z jednoczesnym uzyskaniem znacznika czasu przy użyciu tej wersji oprogramowania zakończy się niepowodzeniem.

c) Nie można wybrać certyfikatu, którego okres ważności jeszcze się nie rozpoczął bądź już upłynął.

2. W celu kontynuowania składania podpisu należy wybrać stosowny certyfikaty i kliknąć na przycisku „Wybierz”. Zostanie wyświetlone okno weryfikacji podpisu:



Rysunek 24. Okno weryfikacji podpisu.

To okno umożliwia użytkownikowi nadzór nad procesem weryfikacji podpisu elektronicznego.

- **Czynność.** W tej ramce wyświetlane są informacje o aktualnie wykonywanej czynności (takiej jak weryfikacja określonego podpisu elektronicznego) i jej kolejnych krokach:
  - **Prezentacja podpisu.**
  - **Weryfikacja podpisu.**
  - **Znakowanie czasem.**
  - **Weryfikacja ścieżki certyfikacji.**
  - **Podsumowanie.**
- **Certyfikaty.** W tej ramce wyświetlane są informacje o certyfikatach używanych w trakcie weryfikacji podpisu elektronicznego.
  - **Weryfikacja podpisu.** Na tej zakładce wyświetlane są podstawowe parametry certyfikatu używanego do weryfikacji podpisu elektronicznego.
  - **Weryfikacja znacznika czasu.** Na tej zakładce wyświetlane są podstawowe parametry certyfikatu używanego do weryfikacji znacznika czasu.

- **Znakowanie czasem.** Na tej zakładce wyświetlane są podstawowe parametry certyfikatu używanego do podpisania wniosku o wydanie znacznika czasu.

- **Podpisane dane.** W tym polu prezentowana jest treść podpisanych danych. Aplikacja potrafi samodzielnie zaprezentować treść plików następujących typów:
  - .TXT
  - .XML
  - .RTF
  - .JPG, .BMP, .GIF i szereg innych plików graficznych

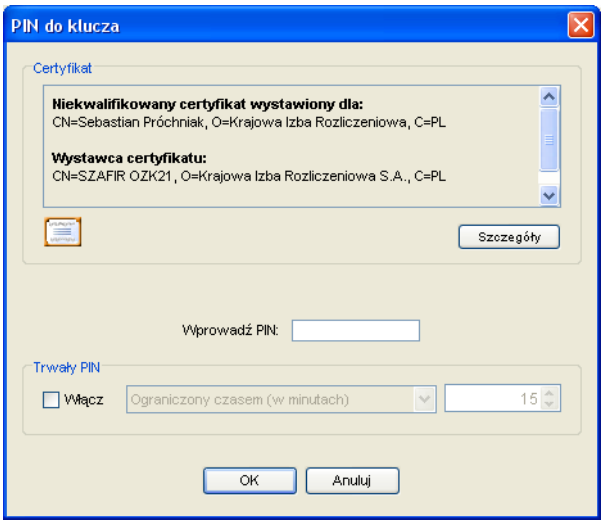
  Pliki innych typów mogą być wyświetlane przy pomocy zewnętrznych aplikacji. Użytkownik może wybrać aplikację z listy programów zarejestrowanych w systemie operacyjnym lub wskazać dowolną inną aplikację, przy pomocy której chce obejrzeć zawartość pliku.

- **Informacje związane z kolejno wykonywanymi krokami** wyświetlane są w panelu na dole okna weryfikacji podpisu:
  - **Prezentacja podpisu.** Przed rozpoczęciem weryfikacji podpisu aplikacja prezentuje najważniejsze informacje o weryfikowanym podpisie wraz z treści podpisanego dokumentu.
    - **Weryfikuj** rozpoczyna weryfikację podpisu elektronicznego.
    - **Pomiń** pomija weryfikację podpisu elektronicznego.
    - **Pomiń prezentację kolejnych podpisów** – jeżeli ta opcja zostanie zaznaczona, wówczas weryfikowanie kolejnych podpisów odbywać się będzie z pominięciem ich prezentacji.
  - **Weryfikacja podpisu.** Po podjęciu przez użytkownika decyzji o weryfikowaniu danego podpisu aplikacja rozpoczyna weryfikację podpisu elektronicznego na poziomie algorytmów szyfrowych.
  - **Znakowanie czasem.** Po zweryfikowaniu poprawności weryfikowanego podpisu na poziomie algorytmów szyfrowych aplikacja opcjonalnie oznacza weryfikowany podpis czasem (tylko jeżeli taka opcja została zaakceptowana przez użytkownika i tylko jeżeli weryfikowany podpis nie zawiera jeszcze znacznika czasu).

    > Znakowanie czasem jest usługą płatną – korzystanie z niej możliwe jest po podpisaniu odpowiedniej umowy. Dostęp do usługi weryfikowany jest na podstawie certyfikatu używanego przez użytkownika do podpisania wniosku o wydanie znacznika czasu; certyfikat testowy dystrybuowany z wersją weryfikująco-demonstracyjną aplikacji nie umożliwia korzystania z usługi znakowania czasem.

- **Weryfikacja ścieżki certyfikacji.** Po zweryfikowaniu poprawności weryfikowanego podpisu na poziomie algorytmów szyfrowych oraz ewentualnym oznaczeniu podpisu czasem aplikacja weryfikuje ścieżkę certyfikacji certyfikatu używanego do zweryfikowania podpisu elektronicznego.
- **Podsumowanie.** Po zakończeniu procesu weryfikacji podpisu aplikacja wyświetla informację o wyniku weryfikacji.
  - **Szczegóły** wyświetla szczegóły zakończonego właśnie procesu weryfikacji podpisu.
  - **Dalej** rozpoczyna weryfikację kolejnego podpisu (jeżeli w ramach aktualnie wykonywanego zadania pozostały jeszcze jakieś podpisy do weryfikacji).
  - **Anuluj** anuluje wykonywanie bieżącego zadania.
  - **Pomiń podsumowanie kolejnych podpisów** – jeżeli ta opcja zostanie zaznaczona, wówczas weryfikacja kolejnych podpisów odbywać się będzie z pominięciem wyświetlania podsumowania.

3. W celu kontynuowania weryfikacji podpisu należy kliknąć na przycisku „Weryfikuj". Aplikacja rozpocznie weryfikację podpisu oraz, opcjonalnie, znakowanie czasem. Za każdym razem gdy do przeprowadzenia operacji kryptograficznej niezbędne będzie uzyskanie dostępu do karty kryptograficznej lub zabezpieczonego pliku z certyfikatem, pojawi się okno wprowadzania PIN:



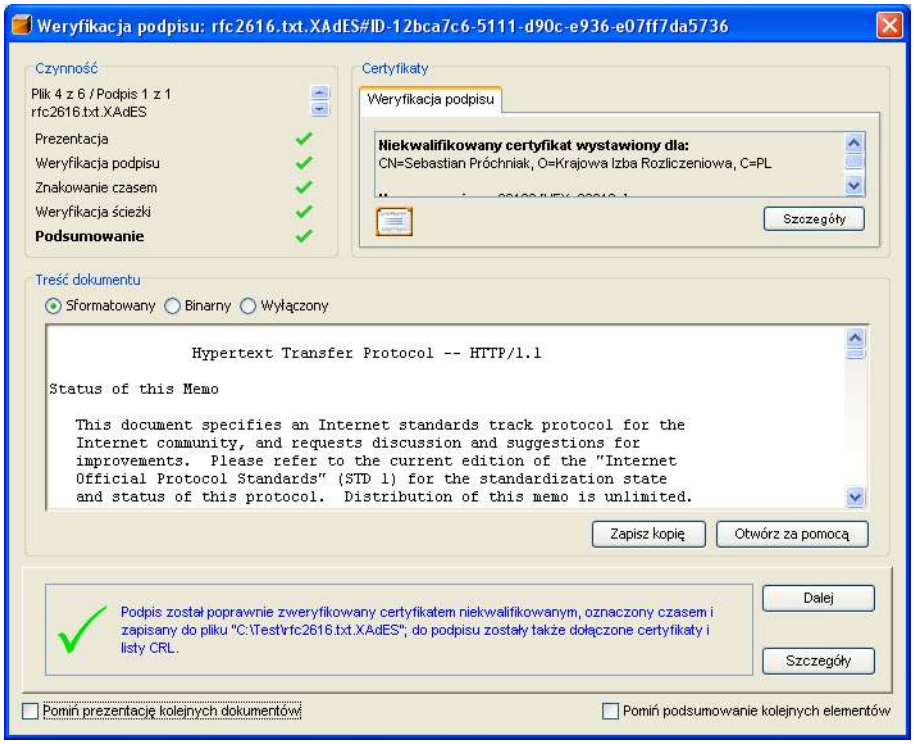
Rysunek 25. Okno wprowadzania PIN.

To okno pozwala na wprowadzenie kodu PIN, który jest niezbędny w celu odblokowania dostępu do karty kryptograficznej lub zabezpieczonego pliku z certyfikatem; możliwe jest również wprowadzenie za jego pomocą tzw. trwałego PIN, pozwalającego, poprzez przechowanie przez określony czas kodu PIN w pamięci aplikacji, na składanie podpisów i znakowanie czasem bez udziału użytkownika:

- **Wprowadź PIN do klucza.** Należy podać kod PIN do karty kryptograficznej lub zabezpieczonego pliku, w którym przechowywany jest certyfikat oraz para kluczy kryptograficznych.
- **Trwały PIN:**
  - **Włącz** udostępnia możliwość użycia trwałego PIN.
  - **Ograniczony czasem (w minutach)** pozwala na określenie limitu czasu.
  - **Ograniczony ilości operacji** pozwala na określenie limitu możliwych do wykonania operacji kryptograficznych.

> Użycie trwałego PIN zmniejsza bezpieczeństwo aplikacji oraz karty kryptograficznej z uwagi na to, że PIN – choć w formie zaszyfrowanej – przechowywany jest jednak w pamięci komputera.

4. Po wprowadzeniu kodu PIN i jego zatwierdzeniu przyciskiem „OK" aplikacja oznakuje weryfikowany podpis czasem, a następnie przystąpi do weryfikacji ścieżki certyfikacji certyfikatu użytego do zweryfikowania podpisu. Po zakończeniu weryfikacji podpisu w oknie weryfikacji podpisu pojawi się podsumowanie wykonanych operacji:



Rysunek 26. Okno weryfikacji podpisu – podsumowanie.

5. Obsługa eArchiwum w ramach usługi EDDM

5.1. Podstawowe informacje o usłudze EDDM

EDDM (ang. *Electronic Document Delivery and Management*) to usługa umożliwiająca bezpieczne przechowywania dokumentów w formie elektronicznej. Krajowa Izba Rozliczeniowa S.A. kieruje ją do wszystkich osób i firm, które chcą tanio i bezpiecznie przechowywać elektroniczne dokumenty, a także mieć do nich szybki i łatwy dostęp.

Funkcjonalność usługi EDDM obejmuje:

- Podpisywanie dokumentów bezpiecznym lub zwykłym podpisem elektronicznym.

  > Zestaw z aplikacją SZAFIR dostarczany w ramach świadczenia usług EDDM pozwala na podpisywanie wielu dokumentów elektronicznych po jednokrotnym podaniu kodu PIN do karty, co umożliwia podpisanie i zapisanie w eArchiwum wielu dokumentów (np. e-faktur) w krótkim czasie.

- Archiwizowanie podpisanych elektronicznie dokumentów.

  > Dzięki funkcjonalności usług EDDM w prosty i bezpieczny sposób można zarchiwizować podpisane elektronicznie dokumenty wszelkiego typu.

- Opisywanie archiwizowanych dokumentów przy pomocy metryk (tzw. metadanych) opisujących daną grupę dokumentów.
- Dostęp do wszystkich zarchiwizowanych dokumentów za pośrednictwem sieci Internet, 24 godziny na dobę.

  > Usługa EDDM pozwala na łatwe wyszukiwanie przechowywanych dokumentów elektronicznych i weryfikację podpisów pod tymi dokumentami.

- Przeglądanie i wyszukiwanie dokumentów według zadanych kryteriów lub przy pomocy wyszukiwania kontekstowego.

  > Funkcjonalność usług EDDM pozwala na łatwe i szybkie wyszukanie właściwych dokumentów zawierających określony tekst, słowo lub frazę. Funkcjonalność dotyczy różnego typu dokumentów, w tym formatów *.DOC, *.XLS, *.PPT. *.DJVU, *.PDF.

- Integracja z zewnętrznymi systemami obiegu dokumentów lub systemami księgowymi.

W ramach usługi EDDM możliwe jest przechowywanie wszystkich typów dokumentów elektronicznych, w tym: faktur elektronicznych, deklaracji podatkowych, deklaracji ZUS

i innych. Bezpieczeństwo przechowywania gwarantowane przez KIR S.A. – wszystkie przechowywane pliki są zdublowane na serwerach Izby umieszczonych w siedzibie zapasowej.

5.2. Zastosowanie aplikacji SZAFIR w ramach usługi EDDM

Większość funkcjonalności usługi EDDM (zapisywanie pojedyńczych dokumentów w eArchiwum, ich przeglądanie, wyświetlanie, drukowanie itp.) dostępne jest dla użytkowników za pośrednictwem interfejsu WWW i przeglądarki internetowej. Z uwagi jednak na to, że ręczne zapisywanie w ramach eArchiwum większej ilości dokumentów przy użyciu przeglądarki internetowej byłoby uciążliwe, w aplikację SZAFIR wbudowana została obsługa wysyłania dokumentów do eArchiwum: przy pomocy aplikacji SZAFIR możliwe jest wysyłanie do eArchiwum dokumentów, które zostały podpisane lub których podpisy zostały zweryfikowane w aplikacji SZAFIR.[1]

Dla każdego dokumentu do eArchiwum wysyłane są trzy informacje:

1. Plik zawierający podpisany dokument. Mogą to być dowolne pliki o wielkości nie przekraczającej pewnego określonego rozmiaru: e-faktury, dokumenty księgowe, pliki multimediów itp.
2. Plik zawierający właśnie złożony lub zweryfikowany podpis. Podpis może być w dowolnym wspieranym przez aplikację SZAFIR formacie, pod warunkiem, że będzie się znajdował w osobnym pliku.
3. Metadane opisujące dokument umieszczany w eArchiwum. Metadane (dane opisujące dane), są niezbędne do tego, by w eArchiwum można było dokumenty sortować, przeszukiwać i przeglądać według pewnych, charakterystycznych dla danych typów dokumentów, wartości, takich jak np. numer faktury czy numer NIP odbiorcy (w przypadku e-faktury) lub tytuł i wykonawca piosenki (w przypadku pliku MP3).

   Metadane mogą pochodzić z dwóch źródeł:

   a) Mogą być odczytywane z plików metryk, znajdujących się obok podpisanych lub zweryfikowanych dokumentów. Plik metryki powinien mieć nazwę taką, jak dokument, do którego się odnosi, z dodatkowym rozszerzeniem *.metadata. Plik metryki powin-

1 W obecnej wersji eArchiwum można przechowywać dokumenty lub dokumenty z podpisami - podpisy muszą się jednak znajdować w osobnych plikach, po jednym podpisie na plik. Oznacza to, że niemożliwe jest zapisanie w eArchiwum dokumentu, którego treść została dołączona do podpisanych danych lub któremu towarzyszy plik z podpisami zawierający większą ilość podpisów.

nien zawierać strukturę XML zgodną ze schematem opracowanym i publikowanym przez KIR S.A.[2]

b) Mogą być ręcznie wprowadzane przez użytkowników. Jeżeli dla danego dokumentu plik metryki nie został utworzony, wówczas użytkownik ma możliwość ręcznego wprowadzenia metadanych przed rozpoczęciem wysyłania plików do eArchiwum.

Pliki są wysyłane do eArchiwum po zakończeniu wykonywania zadania składania lub weryfikacji podpisu. Proces zapisywania plików do eArchiwum przebiega w tle, jego przebieg użytkownik może śledzić w osobnym oknie w ramach głównego okna aplikacji.

5.3. Wysyłanie plików do eArchiwum

5.3.1. Konfiguracja aplikacji

Aby umożliwić wysyłanie plików do eArchiwum, w konfiguracji aplikacji należy włączyć opcję „Włącz obsługę eArchiwum". Odblokuje to dostęp do opcji, za pomocą których należy zdefiniować adres eArchiwum oraz domyślny certyfikat, przy pomocy którego odbywać się będzie uwierzytelnienie aplikacji w eArchiwum.

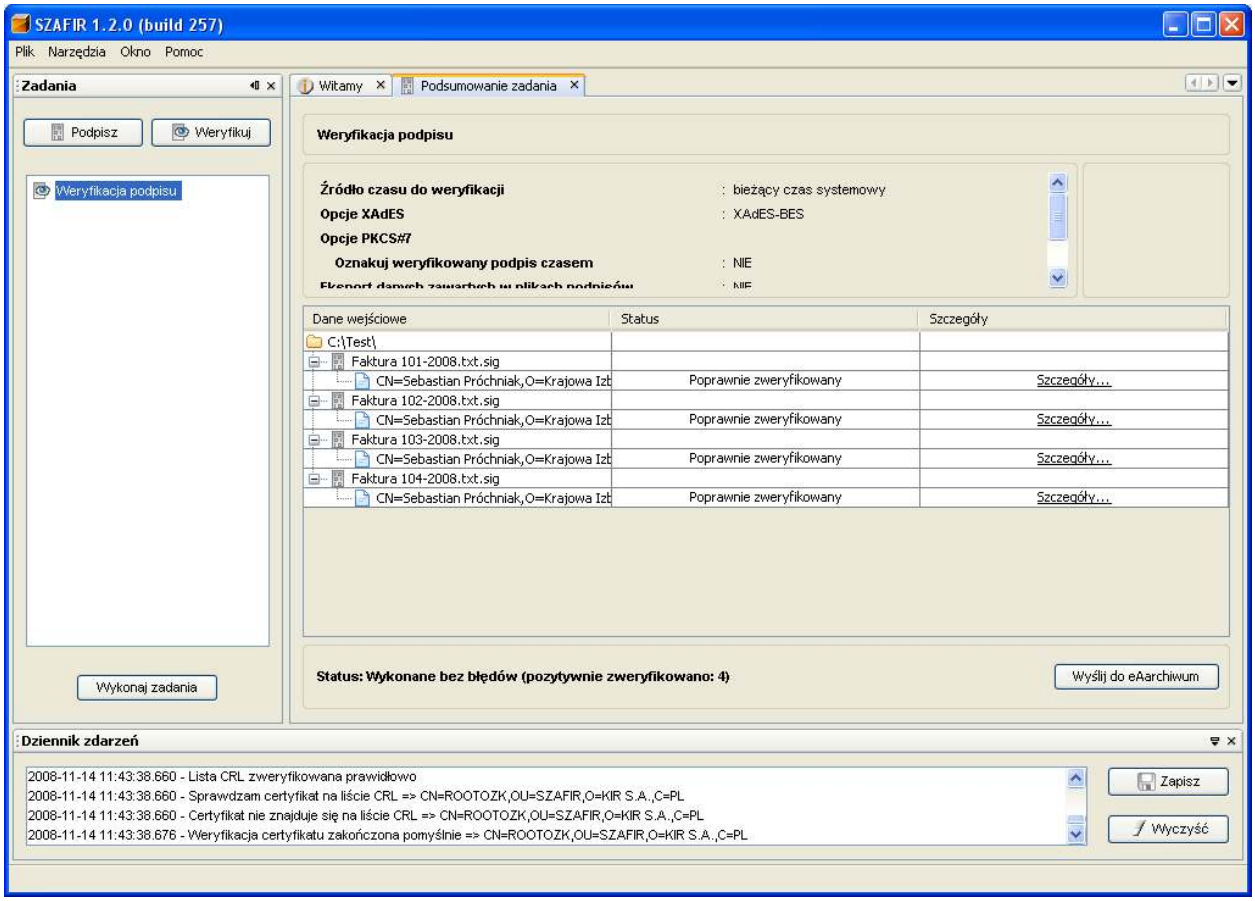
5.3.2. Definiowanie zadania składania lub weryfikacji podpisu

W przypadku, gdy użytkownik ma zaznaczoną opcję „Chcę korzystać z eArchiwum" i podczas definiowania zadania składania podpisu zaznaczy opcje, których użycie uniemożliwiłoby wysłanie podpisanych dokumentów do eArchiwum, wyświetlone zostanie ostrzeżenie mówiące o tym, że plików podpisanych w ten sposób nie będzie można zapisać w eArchiwum.

2 W najbliższej przyszłości Izba opracuje docelową listę wspieranych typów plików oraz pól je opisujących i przewidujemy, że osoby/firmy chcące korzystać z EDDM wyposażą swoje systemy generujące dokumenty w funkcjonalność tworzenia metryk zgodnych ze schematem opracowanym i opublikowanym przez KIR S.A.

5.3.3. Wysyłanie plików do eArchiwum

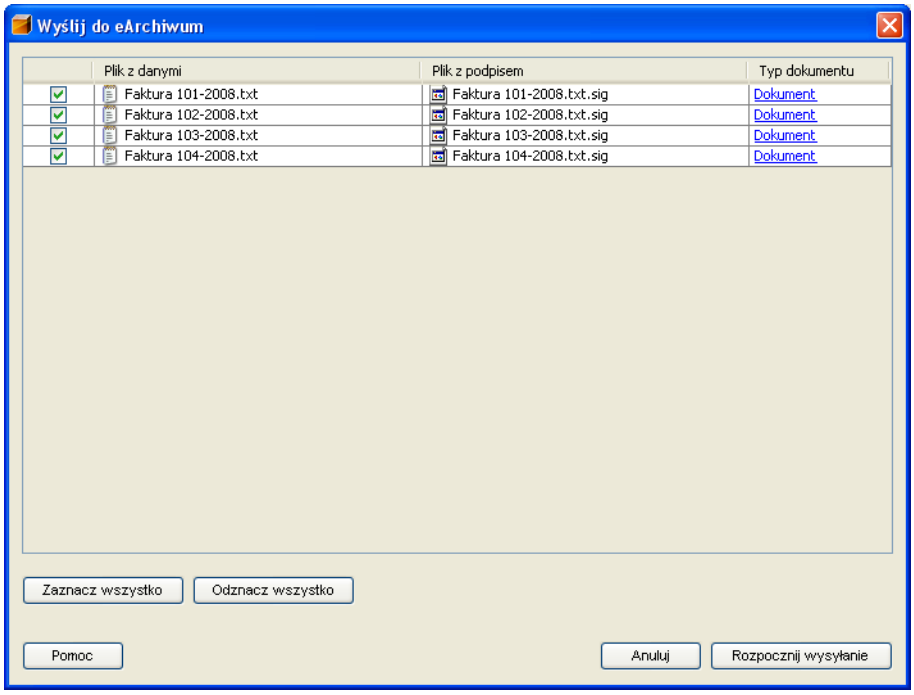
1. Aby wysłać dokumenty do eArchiwum należy zdefiniować i wykonać zadanie składania lub weryfikacji podpisu. Po wykonaniu zadania pojawi się okno podsumowania zadania:



Rysunek 27. Okno podsumowania zadania z widocznym przyciskiem „Wyślij do eArchiwum”.

Jeżeli w konfiguracji aplikacji zaznaczona została opcja „Włącz obsługę eArchiwum”, wówczas w oknie podsumowania zadania widoczny jest przycisk „Wyślij do eArchiwum”.

2. Aby wysłać pliki do eArchiwum należy kliknąć na przycisku „Wyślij do eArchiwum”. Pojawi się okno „Wyślij do eArchiwum”.

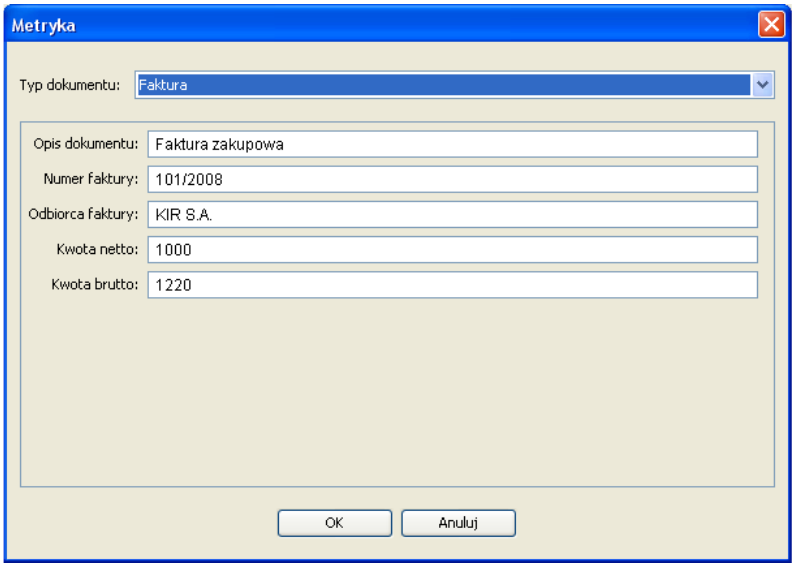


Rysunek 28. Okno „Wyślij do eArchiwum”.

To okno umożliwia wybranie plików, które mają być wysłane do eArchiwum::

- **Wyślij**. Należy zaznaczyć dokumenty, które mają zostać wysłane do eArchiwum (domyślnie zaznaczone są wszystkie dokumenty).
- **Plik z danymi/plik z podpisem**. W tych kolumnach widoczne są nazwy plików zawierających podpisane dane oraz pliki z podpisami.
- **Typ dokumentu**. W tej kolumnie widoczny jest typ dokumentu przypisany na podstawie odczytanej z pliku *.metadata metryki podpisanych danych. W razie braku metryki wszystkim dokumentom automatycznie przypisywany jest typ „Dokument”.

a) Aby utworzyć lub zmienić metadane opisujące podpisany dokument należy kliknąć na łączu w kolumnie „Typ dokumentu”. Pojawi się okno edycji metadanych:

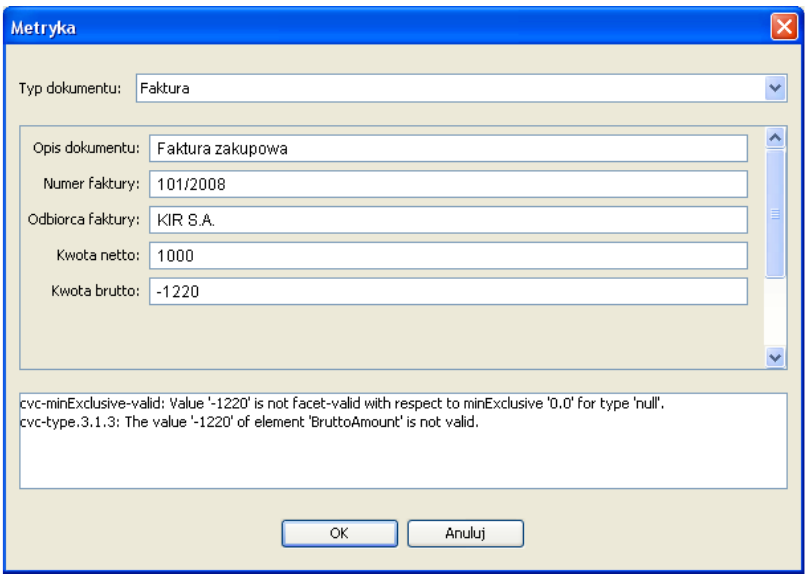


Rysunek 29. Okno edycji metadanych.

Z poziomu okna możliwe jest określenie typu dokumentu oraz wypełnienie pól opisujących wybrany typ:[3]

- **Typ dokumentu**. Należy wybrać z rozwijanej listy typ dokumentu.
- **Treść metryki**. Należy wprowadzić w poszczególne pola informacje opisujące dokument.

Po wypełnieniu formularza należy kliknąć na przycisku „OK”. Wprowadzone dane zostaną sprawdzone pod kątem ich zgodności z wymaganiami dla danego typu dokumentu. W razie problemu zostanie wyświetlony komunikat o błędzie:

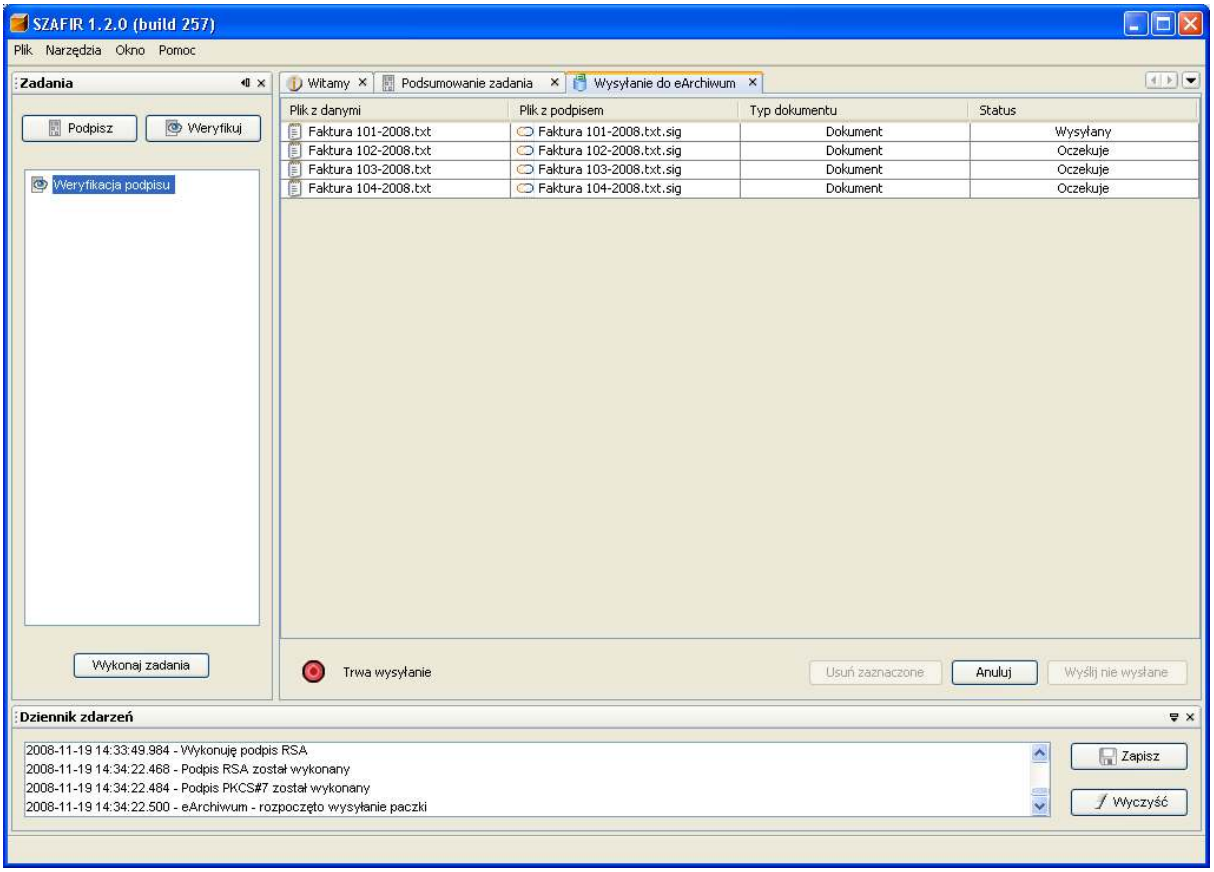


Rysunek 30. Okno edycji metadanych z widocznym komunikatem o błędzie.

3 Zarówno lista typów jak i opisujących je pól pochodzi ze schematu XML opracowanego przez KIR S.A.

b) Aby rozpocząć wysyłanie plików do eArchiwum należy kliknąć na przycisku „Rozpocznij wysyłanie”.

3. Po rozpoczęciu wysyłania plików do eArchiwum pojawi się okno „Wysyłanie do eArchiwum”:

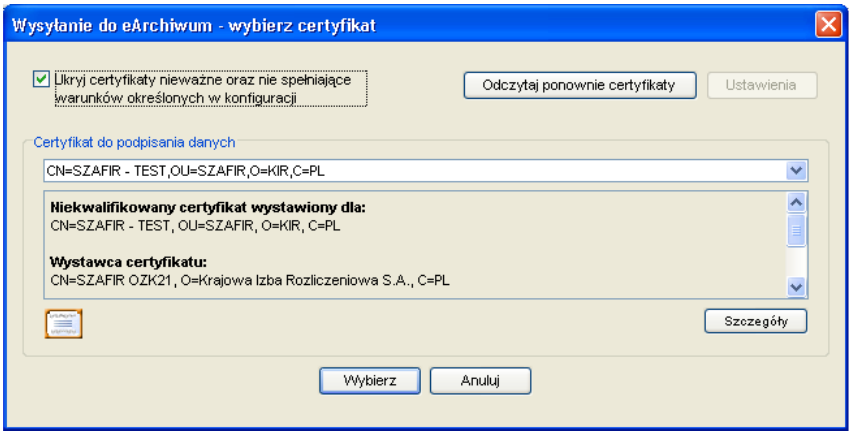


Rysunek 31. Okno „Wysyłanie do eArchiwum”.

W oknie „Wysyłanie do eArchiwum” można śledzić postęp w wysyłaniu plików:

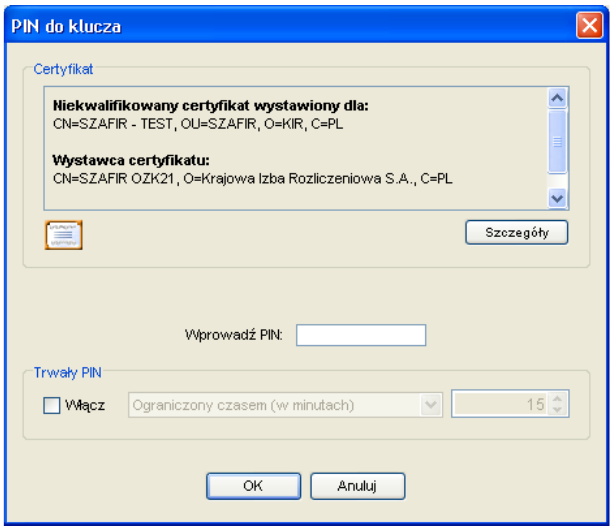
a) Bezpośrednio po wyświetleniu okna aplikacja rozpoczyna proces wysyłanie dokumentów, zaczynając od uwierzytelnienia w eArchiwum przy użyciu certyfikatu niekwalifikowanego. Pojawi się okno wyboru certyfikatu:[4]

4 Certyfikat, który ma być używany podczas uwierzytelnienia można wskazać w konfiguracji aplikacji.



Rysunek 32. Okno wyboru certyfikatu.

b) Po wybraniu certyfikatu aplikacja poprosi o podanie PIN do karty lub hasła do pliku, w którym przechowywany jest certyfikat.



Rysunek 33. Okno wprowadzania PIN.

c) Po uwierzytelnieniu w eArchiwum aplikacja rozpocznie wysyłanie kolejnych dokumentów – na liście plików, w kolumnie „Status”, widoczny będzie wynik wysyłania każdego z dokumentów.

6. Instalacja i konfiguracja

6.1. Minimalne wymagania

Do poprawnej pracy aplikacja SZAFIR wymaga komputera klasy IBM PC pracującego pod kontrolą systemu operacyjnego Mirosoft Windows 2000 SP4 lub nowszego (XP, 2003), na którym zainstalowane jest środowisko Java w wersji 1.5 lub nowsze, przy czym:

- Wykorzystanie funkcji weryfikacji podpisu wymaga, by komputer wyposażony był w połączenie z siecią Internet, w celu pobrania list certyfikatów unieważnionych i zawieszonych,
- Wykorzystanie funkcji składania podpisu oraz znakowania czasem przy użyciu certyfikatów przechowywanych na kartach kryptograficznych wymaga ponadto by na komputerze zainstalowane były:
  - czytnik kart kryptograficznych zgodny ze specyfikacją PC/SC,
  - oprogramowanie middleware pozwalające na komunikację komponentów programistycznych z kartą kryptograficzną przy wykorzystaniu interfejsu PKCS#11 w wersji 2.01 lub wyższej.[5] W wersji 1.2 działanie aplikacji zostało przetestowane z następującymi bibliotekami PKCS#11:

Nazwa biblioteki	Producent	Obsługiwane karty kryptograficzne	Platforma systemowa
CCPKIP11.dll	CryptoTech	CryptoCard multiSign	Microsoft Windows
aetpkss11.dll	Unizeto	Unizeto, część niekwalifikowana	Microsoft Windows
cryptoCertumPKCS11.dll	Unizeto	Unizeto, część kwalifikowana	Microsoft Windows

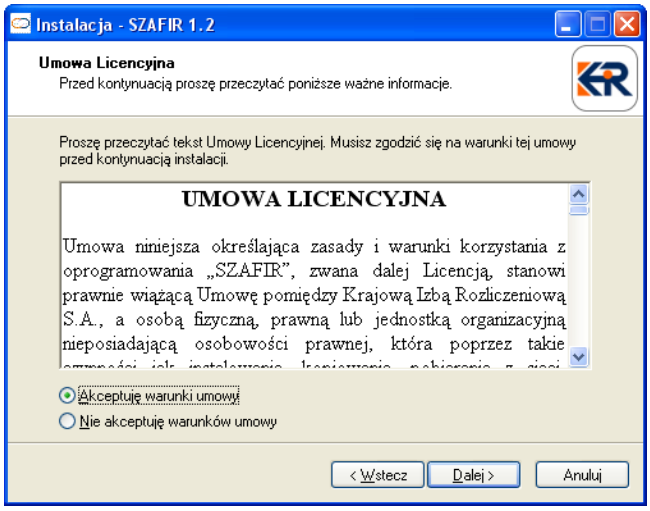
5 Obecnie w ofercie KIR S.A. znajduje się oprogramowanie middleware CryptoCard Suite firmy Cryptotech pozwalające na komunikację z kartą kryptograficzną CryptoCard multiSign pod kontrolą systemów operacyjnych MS Windows (od wersji 2000 wzwyż) oraz Linux.

6.2. Instalacja

1. W celu zainstalowania oprogramowania należy uruchomić plik zawierający pakiet instalacyjny programu. Pojawi się okno kreatora instalacji:

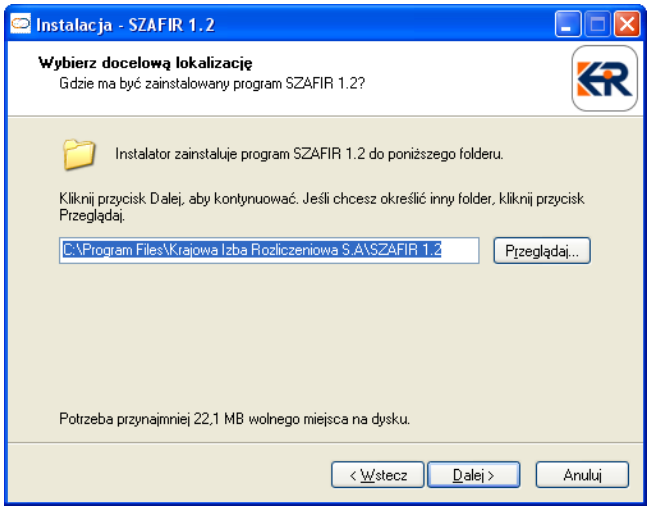
Rysunek 34. Kreator instalacji aplikacji – ekran powitalny.

2. W celu kontynuowania instalacji należy kliknąć w przycisk „Dalej”. Pojawi się okno zawierające tekst umowy licencyjnej aplikacji:



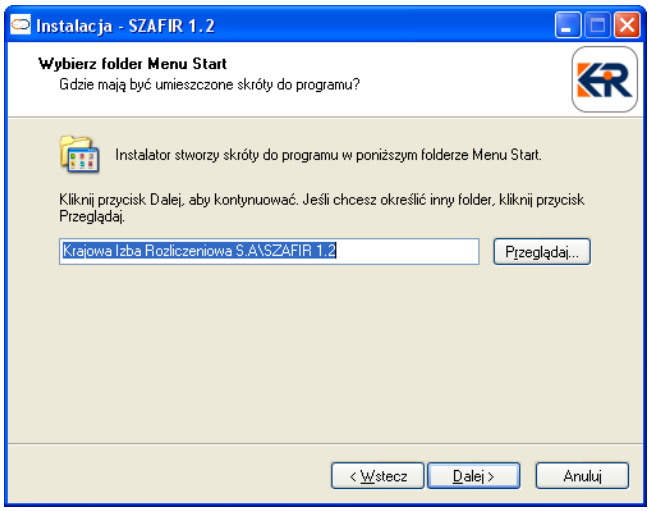
Rysunek 35. Kreator instalacji aplikacji – umowa licencyjna.

3. Należy zapoznać się z tekstem umowy i, w przypadku jego akceptacji, zaznaczyć opcję „Akceptuję warunki umowy”, a następnie kliknąć na przycisku „Dalej”. Pojawi się okno „Wybierz docelową lokalizację”:



Rysunek 36. Kreator instalacji aplikacji – wybór docelowej lokalizacji.

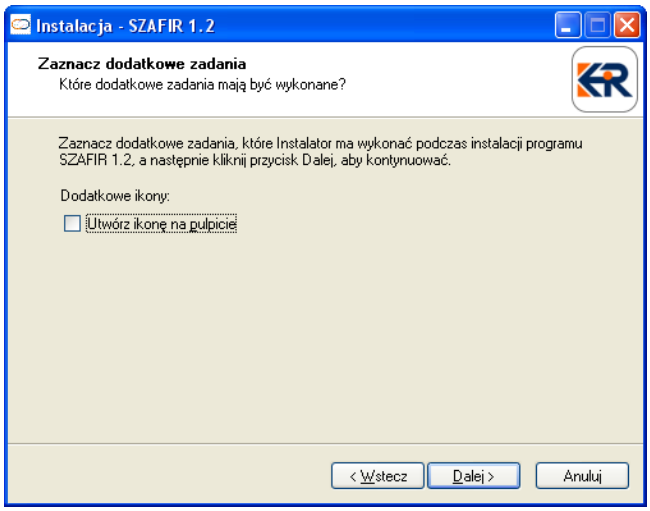
4. W celu kontynuowania instalacji należy kliknąć w przycisk „Dalej”. Pojawi się okno „Wybierz folder Menu Start”:



Rysunek 37. Kreator instalacji aplikacji – wybór folderu Menu Start.

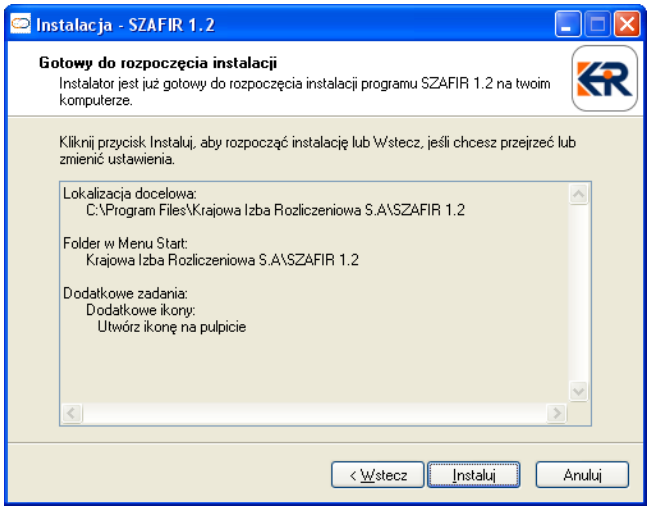
Zaleca się skorzystanie z opcji domyślnie zaproponowanych przez program instalacyjny.

5. W celu kontynuowania instalacji należy kliknąć w przycisk „Dalej”. Pojawi się okno z prośbą o wskazanie dodatkowych opcji instalacji:



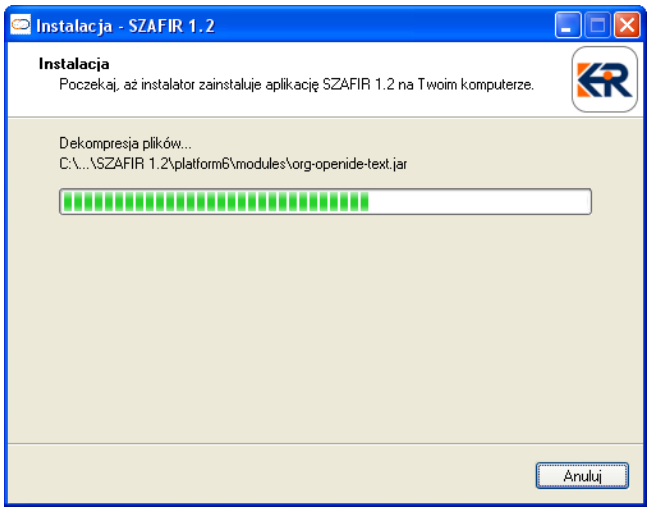
Rysunek 38. Kreator instalacji aplikacji – dodatkowe opcje instalacji.

6. W celu kontynuowania instalacji należy kliknąć w przycisk „Dalej”. Pojawi się okno z podsumowaniem wybranych opcji:



Rysunek 39. Kreator instalacji aplikacji – podsumowanie.

7. W celu kontynuowania instalacji należy kliknąć w przycisk „Dalej”. Program instalacyjny rozpocznie kopiowanie plików:



Rysunek 40. Kreator instalacji aplikacji – kopiowanie plików.

8. Po zakończeniu kopiowania plików program instalacyjny wyświetli okno z informacją o zakończeniu instalacji:

Rysunek 41. Kreator instalacji aplikacji – koniec instalacji.

9. W celu zakończenia instalacji należy kliknąć w przycisk „Zakończ”.

6.3. Uaktualnianie

Domyślnie aplikacja instalowana jest do katalogu zawierającego w nazwie wersję *major* i *minor* aplikacji (np. SZAFIR 1.0)[6]. Instalacja kolejnych wydań aplikacji w ramach tej samej wersji *minor* dokonywana będzie w trybie uaktualnienia: pliki aplikacji instalowane będą do tego samego katalogu, w którym zainstalowana została dana wersja funkcjonalna aplikacji; również w narzędziu „Dodaj lub usuń programy" systemu MS Windows kolejne wydania w ramach tej samej wersji funkcjonalnej zastępować będą wydania poprzednie.

Instalacja kolejnych wersji funkcjonalnych (np. SZAFIR 1.1, SZAFIR 1.2) dokonywana będzie w trybie nowej instalacji: pliki aplikacji instalowane będą w odpowiadających im nowych katalogach (odpowiednio: SZAFIR 1.1, SZAFIR 1.2); również w narzędziu „Dodaj lub usuń programy" systemu MS Windows kolejne wersje funkcjonalne będą dodawane obok wersji już istniejących. Poprzednie wersje funkcjonalne można, jeżeli nie są potrzebne, usunąć przy użyciu narzędzia „Dodaj lub usuń programy".

Instalacja testowych wersji aplikacji w ramach tej samej wersji testowej dokonywana jest w trybie uaktualnienia. Po zmianie numeru wersji testowej (np. z beta 1 na beta 2) instalacja dokonywana jest w trybie nowej instalacji.

6.4. Konfiguracja

Aplikacja SZAFIR ma możliwość wykorzystywania wielu zapisanych konfiguracji, co pozwala na dostosowanie sposobu jej działania do wymagań konkretnych użytkowników; dostęp do funkcji definiowania oraz zmiany aktywnej konfiguracji może być przy tym chroniony hasłem.

Bieżąca konfiguracja aplikacji jest sumą dwóch elementów: domyślnej konfiguracji aplikacji oraz, opcjonalnie, dodatkowej konfiguracji utworzonej i zapisanej przez użytkownika (takich zapisanych konfiguracji może być kilka).

Użytkownik może zmieniać oba rodzaje konfiguracji z tym, że w przypadku konfiguracji dodatkowej nie jest konieczne definiowanie zawartości wszystkich opcji: na poszczególnych zakładkach okna edycji konfiguracji można zaznaczyć opcję „Użyj konfiguracji domyślnej" i wówczas ustawienia, których ta opcja dotyczy, odczytane zostaną z konfiguracji domyślnej.

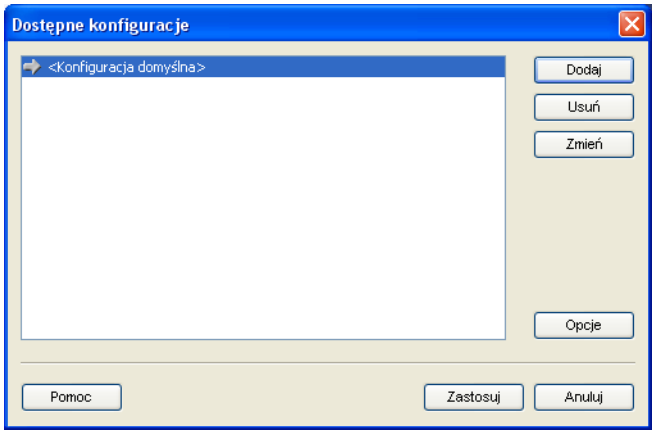
Użytkownik wybierając z menu opcję „Narzędzia\Ustawienia" otwiera okno „Dostępne konfiguracje", które wyświetla listę zdefiniowanych konfiguracji, wraz z konfiguracją domyślną. Korzystając z listy konfiguracji oraz dostępnych w oknie przycisków użytkownik może dodawać, usuwać (nie dotyczy konfiguracji domyślnej) lub zmieniać dostępne konfi-

6 Więcej o numerowaniu wersji aplikacji można przeczytać w rozdziale 7.1. „Numeracja wersji aplikacji".

guracje, oraz – przy pomocy przycisku "Zastosuj" – decydować o użyciu wybranej konfiguracji w czasie pracy aplikacji.

Użytkownik może ograniczyć możliwości zarządzania konfiguracją aplikacji poprzez określenie hasła administratora oraz, opcjonalnie, ograniczeń w zarządzaniu konfiguracją.

6.4.1. Okno dostępnych konfiguracji



Rysunek 42. Okno dostępnych konfiguracji.

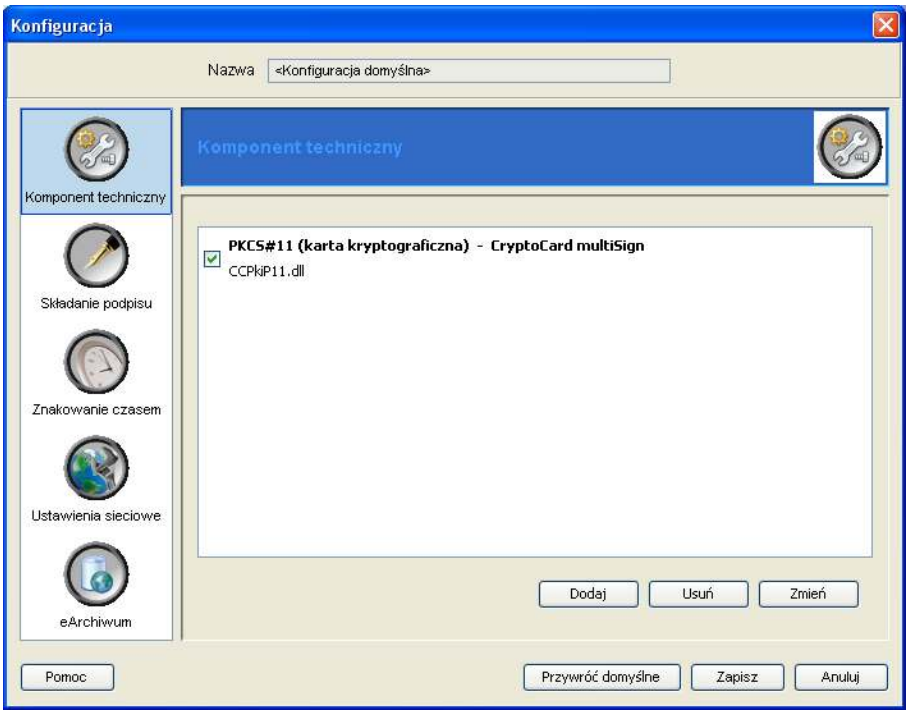
To okno umożliwia zarządzanie konfiguracjami aplikacji. Korzystając z listy dostępnych konfiguracji oraz dostępnych w oknie przycisków można dodawać, usuwać (nie dotyczy konfiguracji domyślnej) lub zmieniać dostępne konfiguracje, oraz - przy pomocy przycisku "Zastosuj" - decydować o użyciu w ramach aplikacji wybranej konfiguracji.

- **Lista dostępnych konfiguracji.** To pole wyświetla listę zdefiniowanych w aplikacji konfiguracji.
- **Dodaj.** Należy użyć tego przycisku aby dodać nową konfigurację.
- **Usuń.** Należy użyć tego przycisku, aby usunąć konfigurację zaznaczoną na liście dostępnych konfiguracji.
- **Zmień.** Należy użyć tego przycisku, aby zmienić konfigurację zaznaczoną na liście dostępnych konfiguracji.
- **Opcje.** Należy użyć tego przycisku, aby zmienić opcje zabezpieczeń konfiguracji. Zarządzania konfiguracją można ograniczyć poprzez określenie hasła administratora aplikacji oraz, opcjonalnie, ograniczeń w zapisywaniu i dokonywaniu zmiany aktywnej konfiguracji.
- **Zastosuj.** Należy użyć tego przycisku, aby użyć konfiguracji zaznaczonej na liście dostępnych konfiguracji.

- **Anuluj.** Należy użyć tego przycisku aby zamknąć okno dostępnych konfiguracji nie dokonując zmiany aktywnej konfiguracji.

6.4.2. Okno edycji konfiguracji

To okno pozwala na zmianę wybranej konfiguracji aplikacji.



Rysunek 43. Okno edycji konfiguracji.

- **Nazwa konfiguracji.** Należy wprowadzić nazwę, która będzie używana w odniesieniu do tej konfiguracji.

6.4.2.1. Komponent techniczny

Ta zakładka umożliwia wskazanie bibliotek PKCS#11, przy pomocy których aplikacja komunikować się będzie z (zawierającymi pary kluczy oraz certyfikaty) kartami kryptograficznymi oraz na wskazanie plików PKCS#12, zawierających pary kluczy oraz certyfikaty. Zakładka umożliwia:

- Wskazanie bibliotek PKCS#11, przy pomocy których aplikacja komunikować się będzie z (zawierającymi pary kluczy oraz certyfikaty) kartami kryptograficznymi.
- Wskazanie plików PKCS#12, zawierających pary kluczy oraz certyfikaty.

Zakładka zawiera następujące elementy:

Lista bibliotek PKCS#11 oraz plików PKCS#12. Na tej liście wyświetlane są wszystkie zdefiniowane biblioteki PKCS#11 oraz pliki PKCS#12, z których aplikacja korzystać będzie odczytując certyfikaty w procesie składania podpisu oraz podpisywania wniosku o oznaczenie dokumentu czasem.

Dodaj. Należy użyć tego przycisku, aby zdefiniować dodatkową bibliotekę PKCS#11 lub zestaw plików PKCS#12.

Usuń. Należy użyć tego przycisku, aby usunąć definicję biblioteki PKCS#11 lub zestawu plików PKCS#12.

Zmień. Należy użyć tego przycisku, aby zmienić definicję biblioteki PKCS#11 lub zestawu plików PKCS#12.

6.4.2.1.1. Dodawanie lub zmiana definicji dostawcy kryptograficznego

Dodawanie lub zmiana definicji dostawcy kryptograficznego odbywa się w oknie wyświetlanym po przyciśnięciu, odpowiednio, przycisków „Dodaj” oraz „Zmień” w zakładce „Komponent techniczny” okna edycji konfiguracji.

Przy pomocy tego okna możliwe jest zdefiniowanie ustawień dostawcy kryptograficznego - biblioteki PKCS#11 lub pliku PKCS#12. Obecnie obsługiwane przez aplikację typy dostawców kryptograficznych (nośników kluczy i certyfikatów) to:

- PKCS#11 (karta kryptograficzna)
- PKCS#11 (plik)

6.4.2.1.1.1. Dodawanie lub zmiana definicji dostawcy typu „PKCS#11 (karta kryptograficzna)”

Po wybraniu typu dostawcy „PKCS#11 (karta kryptograficzna)" okno konfiguracji dostawcy pozwala na wskazanie bibliotek PKCS#11, przy pomocy których aplikacja komunikować się będzie z (zawierającymi pary kluczy oraz certyfikaty) kartami kryptograficznymi.

Dla typu dostawcy „PKCS#11 (karta kryptograficzna)” dostępne są następujące opcje:

- **Przyjazna nazwa.** W tym polu należy określić łatwą do zapamiętania nazwę biblioteki PKCS#11 lub karty, którą przy jej pomocy należy obsłużyć.
- **Biblioteka PKCS#11.** W tym polu należy wskazać plik biblioteki PKCS#11, za pośrednictwem której aplikacja ma uzyskiwać dostęp do określonego typu kart kryptograficznych. Informacja o bibliotekach PKCS#11, których użycie zostało przetestowane z aplikacją, znajdują się w rozdziale ☐ „Minimalne wymagania” na stronie 54.

6.4.2.1.1.2. Dodawanie lub zmiana definicji dostawcy typu „PKCS#12 (plik)”

Po wybraniu typu dostawcy „PKCS#12 (plik)" okno konfiguracji dostawcy pozwala na wskazanie zestawu plików PKCS#12, zawierających pary kluczy oraz certyfikaty. Definiując kolejnych dostawców typu "PKCS#12 (plik)" można zdefiniować kilka zestawów takich plików.

Dla typu dostawcy „PKCS#11 (plik)” dostępne są następujące opcje:

- **Przyjazna nazwa.** W tym polu należy określić łatwą do zapamiętania nazwę zestawu plików PKCS#12.
- **Pliki PKCS#12.** Do znajdującej się w tym polu listy należy dodać pliki PKCS#12, zawierające pary kluczy oraz certyfikaty.

Generując we własnym zakresie pliki PKCS#12 należy zwrócić uwagę, by nie były one zaszyfrowane – w przeciwnym wypadku aplikacja nie będzie mogła odczytać z nich niezbędnych informacji.

6.4.2.2. Składanie podpisu

W tej sekcji znajdują się ustawienia związane ze składaniem podpisów elektronicznych.

- **Certyfikat do podpisu.** Korzystając z tego pola można określić, jakich certyfikatów można będzie używać w procesie składania podpisu elektronicznego.
  - **Dowolny certyfikat.** Należy wybrać tę opcję aby zezwolić na składanie podpisu przy użyciu dowolnego certyfikatu.
  - **Dowolny certyfikat kwalifikowany.** Należy wybrać tę opcję aby zezwolić na składanie podpisu przy użyciu dowolnego certyfikatu kwalifikowanego.
  - **Dowolny certyfikat niekwalifikowany.** Należy wybrać tę opcję aby zezwolić na składanie podpisu przy użyciu dowolnego certyfikatu niekwalifikowanego.
  - **Wskazany certyfikat.** Należy wybrać tę opcję aby zezwolić na składanie podpisu tylko przy użyciu konkretnego, wskazanego niżej certyfikatu.
    - **Wybierz.** Należy użyć tego przycisku aby wywołać okno wyboru certyfikatów.

6.4.2.3. Znakowanie czasem

W tej sekcji znajdują się ustawienia związane ze znakowaniem czasem.

- **Certyfikat do znakowania czasem.** Korzystając z tego pola można określić, jakich certyfikatów użytkownik będzie mógł użyć w procesie znakowania czasem do podpisywania żądań wystawienia znaczników czasu.
  - **Dowolny certyfikat.** Należy wybrać tę opcję aby zezwolić na znakowanie czasem przy użyciu dowolnego certyfikatu.
  - **Dowolny certyfikat kwalifikowany.** Należy wybrać tę opcję aby zezwolić na znakowanie czasem przy użyciu dowolnego certyfikatu kwalifikowanego.
  - **Dowolny certyfikat niekwalifikowany.** Należy wybrać tę opcję aby zezwolić na znakowanie czasem przy użyciu dowolnego certyfikatu niekwalifikowanego.
  - **Wskazany certyfikat.** Należy wybrać tę opcję aby zezwolić na znakowanie czasem tylko przy użyciu konkretnego, wskazanego niżej certyfikatu.
    - **Wybierz.** Należy użyć tego przycisku aby wywołać okno wyboru certyfikatów.
- **Serwer znakowania czasem.**
  - **Adres.** Należy wpisać adres usługi znakowania czasem.
  - **Polityka.** Należy wpisać identyfikator polityki znakowania czasem.

> Po zainstalowaniu aplikacji powyższe parametry domyślnie wskazują na serwer kwalifikowanej usługi znakowania czasem KIR S.A. oraz na stosowaną przez KIR S.A. politykę znakowania czasem.

6.4.2.4. Ustawienia sieciowe

W tej sekcji znajdują się ustawienia mające wpływ na sposób, w jaki aplikacja łączy się ze światem zewnętrznym. Połączenie takie jest niezbędne w procesie weryfikacji podpisów elektronicznych (aplikacja odwołuje się wówczas do serwerów, na których przechowywane są listy certyfikatów zawieszonych i unieważnionych) oraz w procesie znakowania czasem.

- **HTTP proxy/HTTPS proxy.** Dostawcy usług internetowych lub firmy mogą udostępniać lub wymagać łączenia się przez serwer proxy (zwany też serwerem pośredniczącym). Serwer proxy działa jako pośrednik między komputerem a siecią Internet, odfiltrowujący niepożądane próby połączeń z zewnątrz do wewnątrz sieci i chroniący, w celu zwiększenia bezpieczeństwa, komputery wewnątrz sieci przed dostępem z zewnątrz. Jeżeli nie zamierzasz używać serwera proxy (z Internetem łączysz się bezpośrednio) pozostaw to pola w tej sekcji puste.
  - **Host.** Należy wpisać nazwę lub adres IP serwera proxy.
  - **Port.** Należy wpisać numer portu, pod którym dostępny jest serwer proxy.

- **Użytkownik.** Jeżeli wymaga tego konfiguracja serwera proxy, należy wpisać nazwę użytkownika, której należy używać podczas nawiązywania połączenia z serwerem proxy.
- **Hasło.** Jeżeli wymaga tego konfiguracja serwera proxy, należy wpisać hasło, którego należy używać podczas nawiązywania połączenia z serwerem proxy.
- **Nie używaj serwera proxy do adresów zaczynających się od.** Należy wpisać nazwy lub adresy IP komputerów, do których nie trzeba będzie uzyskiwać połączenia za pośrednictwem serwera proxy. Przy określaniu nazw domen oraz hostów można używać symboli wieloznacznych, np. *.kir.com.pl.

- **Sprawdzaj automatycznie, czy jest dostępna nowa wersja**. Aplikacja SZAFIR jest wyposażona w możliwość automatycznego wyszukiwania, pobierania i instalowania nowych wersji aplikacji. Aby uaktywnić tę funkcjonalność należy zaznaczyć tę opcję.

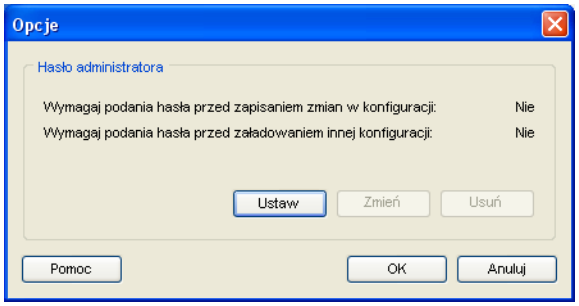
6.4.2.5. eArchiwum

W tej sekcji znajdują się ustawienia związane z wysyłaniem plików do eArchiwum w ramach usługi EDDM.

- **Włącz obsługę eArchiwum**. Aby umożliwić wysyłanie plików do eArchiwum, w konfiguracji aplikacji należy włączyć opcję „Włącz obsługę eArchiwum”. Odblokuje to dostęp do opcji, za pomocą których należy zdefiniować adres eArchiwum oraz domyślny certyfikat, przy pomocy którego odbywać się będzie uwierzytelnienie aplikacji w systemie eArchiwum.
- **Certyfikat dla eArchiwum**. Uwierzytelnienie w ramach eArchiwum dokonywane jest przy użyciu certyfikatu niekwalifikowanego. Korzystając z tej opcji można wskazać, który certyfikat ma być używany do tego celu.
- **Serwer eArchiwum**. Należy wpisać adres usługi sieciowej eArchiwum.

6.4.3. Okno opcji zabezpieczeń

To okno wyświetla aktualnie wybrane opcje zabezpieczeń aplikacji.

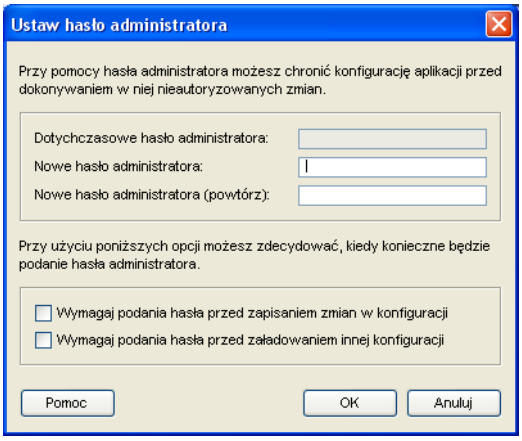


Rysunek 44. Okno opcji zabezpieczeń.

- **Opcje zabezpieczeń.**
  - **Wymagaj podania hasła administratora przed zapisaniem zmian w konfiguracji.** Jeżeli ta opcja została uaktywniona, wówczas przed zapisaniem zmian w konfiguracji aplikacji wymagane jest podanie hasła administratora aplikacji.
  - **Wymagaj podania hasła administratora przed zastosowaniem innej konfiguracji.** Jeżeli ta opcja została uaktywniona, wówczas przed użyciem innej konfiguracji wymagane jest podanie hasła administratora aplikacji.
- **Hasło administratora.**
  - **Ustaw.** Należy użyć tego przycisku, aby ustawić hasło administratora aplikacji.
  - **Zmień.** Należy użyć tego przycisku, aby zmienić hasło administratora aplikacji.
  - **Usuń.** Należy użyć tego przycisku, aby usunąć hasło administratora aplikacji.

6.4.4. Okno ustawiania hasła administratora

To okno umożliwia określenie hasła administratora oraz, opcjonalnie, ograniczeń w zarządzaniu konfiguracją aplikacji.



Rysunek 45. Okno ustawiania hasła administratora.

- **Hasło administratora.** Korzystając z pól w tej sekcji można zmienić hasło administratora.
  - **Dotychczasowe hasło administratora.** Jeżeli hasło administratora zostało już ustawione, aby je zmienić należy najpierw wprowadzić dotychczasowe hasło w tym polu.
  - **Nowe hasło administratora.** Należy wprowadzić nowe hasło administratora.
  - **Nowe hasło administratora (powtórz).** Należy wprowadzić nowe hasło administratora ponownie, w celu weryfikacji.
- **Opcje zabezpieczeń.** Jeżeli w aplikacji zostało ustawione hasło administratora wówczas możliwe jest ograniczenie możliwości zarządzania konfiguracją przez ustawienie opcji wymienionych poniżej.
  - **Wymagaj podania hasła administratora przez zapisaniem zmian w konfiguracji.** Należy zaznaczyć tę opcję aby zapobiec dokonywaniu zmian w konfiguracji aplikacji przez użytkowników nie znających hasła administratora.
  - **Wymagaj podania hasła administratora przez zastosowaniem innej konfiguracji.** Należy zaznaczyć tę opcję aby zapobiec używaniu konfiguracji innych niż aktualna przez użytkowników nie znających hasła administratora.

7. Informacje dodatkowe

7.1. Numeracja wersji aplikacji

W miarę rozwijania programu oraz poprawiania ewentualnych błędów i usterek występujących w programie Krajowa Izba Rozliczeniowa S.A. publikować będzie nowe, poprawione i uaktualnione wersje programu. Zasady publikacji nowych wersji aplikacji są następujące:

1. Wersje aplikacji odzwierciedlają kolejne zmiany aplikacji, w trakcie których odbywa się sukcesywne dodawanie nowych funkcji oraz usuwanie powstających w trakcie rozwoju błędów. Na wersję aplikacji składają się numery:

   a) *major*,

   b) *minor*,

   c) release.

   Poszczególne numery wersji *major/minor/release* zapisywane są kolejno po sobie i rozdzielone kropkami, a numer build dodawany jest w nawiasach, np. SZAFIR 1.0.0, SZAFIR 1.0.1, SZAFIR 1.1.2.

2. Wersja *major* (wersja podstawowa) to wspólne oznaczenie wszystkich wersji aplikacji bazujących na tych samych założeniach, mechanizmach itp. Przewiduje się, że wersja podstawowa zmieniać się będzie bardzo rzadko. Numeracja wersji rozpoczyna się od numeru 1.

3. Wersja *minor* (tzw. wersja funkcjonalna) oznacza kolejny etapy rozwoju programu w ramach tej samej wersji *major*. Wersja *minor* zmieniać się będzie w miarę implementowania znaczących nowych funkcjonalności lub istotnych zmian funkcjonalności istniejących. W ramach jednej wersji podstawowej może zostać opublikowanych wiele wersji funkcjonalnych. rozszerzających możliwości aplikacji poprzez dodanie do niej nowych funkcji i narzędzi. Numeracja wersji *minor* rozpoczyna się od 0 (wersja 1.0 to pierwsza wersja funkcjonalna w ramach pierwszej wersji podstawowej).

4. Wersja *release* (tzw. wydanie) oznacza numer wydania danej wersji *minor*. W ramach jednej wersji funkcjonalnej może zostać opublikowanych wiele kolejno numerowanych wydań zawierających poprawki ewentualnych błędów i usterek oraz drobne uzupełnienia i zmiany istniejącej funkcjonalności. Numeracja wersji *release* rozpoczyna się od 0

(wersja 1.0.0 to pierwsze wydanie pierwszej wersji funkcjonalnej w ramach pierwszej wersji podstawowej).

5. Przed opublikowaniem nowej wersji aplikacji KIR S.A. może udostępnić do testów tzw. wersję beta aplikacji. Wersja taka będzie nosić numer wersji docelowej (w notacji *major.minor.release*) z dodatkowym określeniem „beta" (np. SZAFIR 1.0.0 beta to numer testowej wersji 1.0.0 aplikacji; po zakończeniu testów i podjęciu decyzji o skierowaniu aplikacji do dystrybucji zostanie ona opublikowana jako SZAFIR 1.0.0).

Tabela 1. Schemat numeracji wersji aplikacji.

SZAFIR	1.	0.	0	beta
				|
				oznaczenie wersji beta (skierowanej do testów)
SZAFIR	1.	0.	0	
|	|	|	|	
|	|	|	|	
|	|	|	numer *release*
|	|	numer *minor*	
|	numer *major*		
nazwa aplikacji				