



SZAFIR 2.0

Urządzenie do składania i weryfikacji podpisów

Informacje prawne

Krajowa Izba Rozliczeniowa S.A. oświadcza, że wszelkie prawa autorskie dotyczące tej dokumentacji są zastrzeżone, łącznie z tłumaczeniem na języki obce. Żaden fragment tej dokumentacji nie może być wykorzystany i rozpowszechniany w jakiegokolwiek formie bez zgody KIR S.A.

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.

This product includes software developed by IAIK of Graz University of Technology.

IAIK PKCS#11 Wrapper

Copyright (c) 2002 Graz University of Technology. All rights reserved.

Niniejsze oprogramowanie wykorzystuje bibliotekę do obsługi kart kryptograficznych CryptoCard multiSign autorstwa firmy CryptoTech.

Spis treści

1.	Wprowadzenie	4
1.1.	Co to jest i do czego służy aplikacja SZAFIR?	4
1.2.	Podstawowe informacje o podpisie elektronicznym	4
1.2.1.	Definicja	4
1.2.2.	Działanie	5
1.2.3.	Rola certyfikatów klucza publicznego	5
1.3.	Słownik podstawowych pojęć z dziedziny podpisu elektronicznego	7
2.	Rozpoczynanie pracy z aplikacją	11
2.1.	Główne okno aplikacji	11
2.2.	Menu aplikacji	12
2.3.	Pierwsze uruchomienie	13
3.	Składanie podpisu	15
3.1.	Składanie podpisu – przycisk „podpisz”	16
3.2.	Kreator podpisu	22
4.	Weryfikacja podpisu	27
4.1.	Weryfikacja podpisu – przycisk „weryfikuj”	28
4.2.	Kreator weryfikacji	34
5.	Znakowanie czasem	37
5.1.	Znakowanie czasem – przycisk „oznakuj czasem”	37
6.	Szyfrowanie i odszyfrowywanie	42
6.1.	Szyfrowanie	42
6.2.	Odszyfrowywanie	45
7.	Obsługa eArchiwum w ramach usługi EDDM	49
7.1.	Podstawowe informacje o usłudze EDDM	49
7.2.	Zastosowanie aplikacji SZAFIR w ramach usługi EDDM	50
7.3.	Wysyłanie plików do eArchiwum	51
7.3.1.	Konfiguracja aplikacji	51
7.3.2.	Wysyłanie plików do eArchiwum	51
8.	Instalacja i konfiguracja	56
8.1.	Minimalne wymagania	56
8.2.	Instalacja	57
8.3.	Uaktualnianie	61
8.4.	Konfiguracja	61
8.4.1.	Okno dostępnych konfiguracji	62
8.4.2.	Okno edycji konfiguracji	63
8.4.3.	Okno opcji zabezpieczeń	71
8.4.4.	Okno ustawiania hasła administratora	72
8.5.	Magazyn certyfikatów i list CRL	73
9.	Informacje dodatkowe	75
9.1.	Numeracja wersji aplikacji	75

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, XAdES-A) oraz PKCS#7 (z możliwością znakowania czasem). Możliwe jest także składanie podpisu wielokrotnego PKCS#7 oraz kontrasygnaty XAdES.

Program spełnia 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 współpracującymi z nim 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 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.

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 otrzymaną 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 i które umożliwiają identyfikację tej osoby.

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 wa-

runków 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).

PAdES - PDF Advanced Electronic Signatures, format podpisu elektronicznego, osadzony w strukturze plików PDF.

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.

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.

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.

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.

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 takimi 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).
 - XAdES-A (podpis XAdES oznakowany czasem, z dołączonymi informacjami – certyfikatami oraz CRL – zapewniającymi długotrwałą rozszerzoną ważność dowodową podpisu).

- Możliwość zapisywania wielu podpisów w jednym pliku XML oraz składania podpisu wbudowanego (kontrasygnaty).

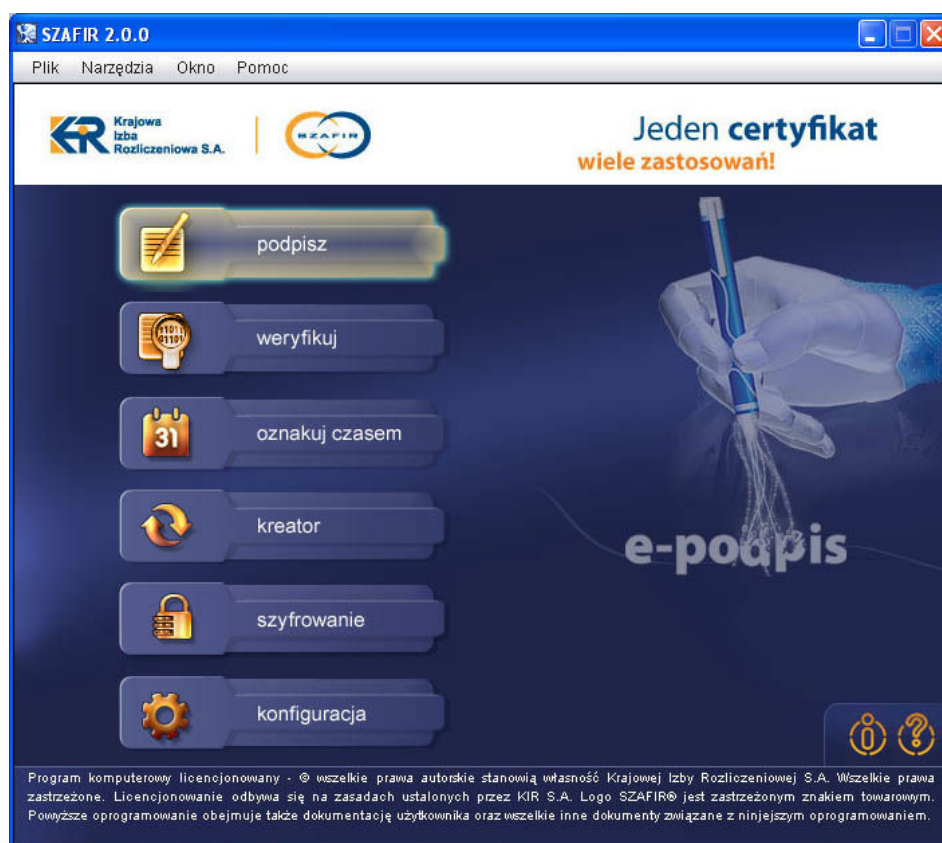
XML-DSIG – XML-Signature, format podpisu elektronicznego dla XML. Jego rozszerzeniem jest format XAdES.

Znakowanie czasem – usługa polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonych podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego 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 użytego przez użytkownika do podpisania wniosku o wydanie znacznika czasu.

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 większe ilości dokumentów.

2.1. Główne okno aplikacji



Rysunek 1. Główne okno aplikacji.

Widoczne na ekranie głównym przyciski **podpisz** i **weryfikuj** pozwalają na szybkie wykonanie wybranej czynności z maksymalnie ograniczoną do niezbędnych liczbą wskazywanych parametrów. W przypadku podpisywania użytkownik wskazuje tylko dane (pliki),

które chce podpisać, parametry (takie jak format podpisu) aplikacja pobiera z konfiguracji – użytkownik może je zmienić i zapisać jako domyślne.

W przypadku weryfikacji program prosi o wskazanie tylko pliku z podpisem i ewentualnie danych podpisanych, jeżeli sam nie będzie mógł ich zlokalizować.

Przycisk **oznakuj czasem** umożliwia użytkownikowi oznaczenie czasem dowolnego pliku.

Kolejny przycisk **kreator** uaktywnia dwa przyciski reprezentujące dwa kreatory podpisu lub weryfikacji. Obie funkcje pozwalają użytkownikowi określić szczegółowe parametry dotyczące wybranego procesu (podpisywania lub weryfikacji).

Przycisk **szyfrowanie**, kryje dwie funkcje: **szyfruj** i **odszyfruj**. W obu przypadkach użytkownikowi ukazać się okna pozwalające na wskazanie plików do zaszyfrowania lub odszyfrowania wraz z możliwością ustawienia szczegółowych parametrów (w przypadku szyfrowania).

Ostatni w tej części ekranu przycisk **konfiguracja** otwiera okno z listą dostępnych (zdefiniowanych) konfiguracji.

W prawej dolnej części ekranu znajdują się dwa przyciski graficzne, otwierające odpowiednio stronę internetową dotyczącą podpisu elektronicznego oraz okno pomocy.

2.2. Menu aplikacji

Główne menu aplikacji składa się z następujących elementów:

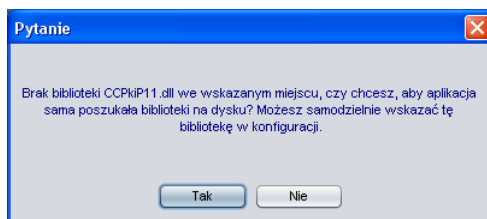
- Menu **Plik**
 - **Podpisz**
 - **Weryfikuj**
 - **Oznakuj czasem**
 - **Szyfruj**
 - **Odszyfruj**
 - **Zakończ**

Trzy pierwsze odpowiadają przyciskom o takich samych nazwach z ekranu głównego aplikacji. Opcje Szyfruj i Odszyfruj odpowiadają funkcjom ukrytym pod przyciskiem Szyfrowanie na ekranie głównym. Ostatnia opcja Zakończ zamyka okno główne i kończy pracę programu SZAFIR.

- **Menu Narzędzia**
 - **Kreator zadania** – menu rozwijające się na dwie opcje Podpisywania i Weryfikacji - odpowiada to przyciskowi kreator z głównego okna aplikacji;
 - **Język** – pozwala przełączać ustawienia językowe interfejsu aplikacji;
 - **Konfiguracja** – otwierająca okno dostępnych konfiguracji, podobnie jak przycisk o tej samej nazwie na ekranie głównym;
- **Menu Okno**
 - **Dziennik zdarzeń** – otwiera okno dziennika, w którym zapisywane są informacje dotyczące pracy aplikacji i wykonywanych przez nią czynności;
 - **Wysyłanie do eArchiwum** – otwiera okno dialogowe pozwalające wysłać dane do serwera eArchiwum; Funkcjonalność ta opisana jest w dalszej części tego podręcznika;
- **Menu Pomoc**
 - **Spis treści** – otwiera okno pomocy podręcznej zawierającej opis aplikacji oraz wskazówki dotyczące używania poszczególnych elementów w programie;
 - **Licencja** – wyświetla treść umowy licencyjnej aplikacji SZAFIR;
 - **Aktualizacja aplikacji** – uruchamia sprawdzenie, czy dostępna jest nowsza wersja programu od używanej przez użytkownika;
 - **O programie** – okno zawierające m.in. parametry systemowo-środowiskowe, używaną wersję Javy i ścieżki do katalogów wykorzystywanych przez aplikację;

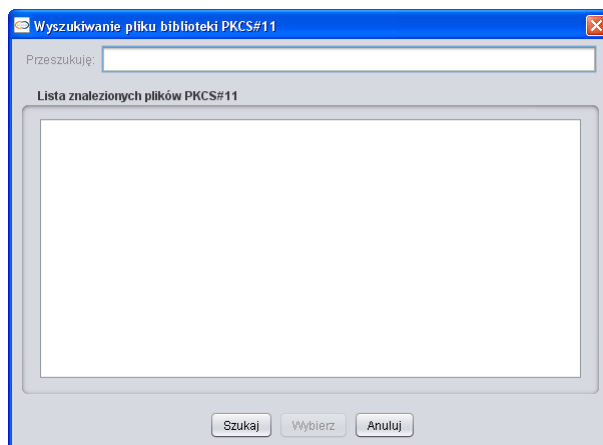
2.3. Pierwsze uruchomienie

Podczas pierwszego uruchomienia aplikacja sprawdza, czy w konfiguracji są zdefiniowane wszystkie niezbędne do pracy parametry. Jeżeli aplikacja nie znajdzie prawidłowej ścieżki do biblioteki CCPkIP11.dll wyświetla następujące okno z komunikatem.



Rysunek 2. Komunikat o braku wskazania biblioteki CCPkIP11.dll.

Biblioteka ta jest niezbędna, aby można było m.in. wykonać podpis elektroniczny przy użyciu certyfikatu przechowywanego na karcie mikroprocesorowej. Zaleca się wybieranie opcji Tak, która oznacza, że program sam poszuka na dysku twardym lokalizacji owej biblioteki. Biblioteka ta jest instalowana razem z pakietem CryptoCard Suite.



Rysunek 3. Wyszukiwanie brakującej biblioteki na dysku.

Uruchomienie procesu przeszukiwania dysku rozpoczynamy przyciskiem Szukaj. Znalezione na dysku biblioteki są automatycznie dodawane do listy znalezionych plików. W celu wskazania aplikacji, którą bibliotekę (lokalizację) ma zapamiętać w konfiguracji należy zaznaczyć ją na liście i wybrać przycisk Wybierz.

3. Składanie podpisu

Funkcjonalność aplikacji SZAFIR w dziedzinie składania podpisu obejmuje:

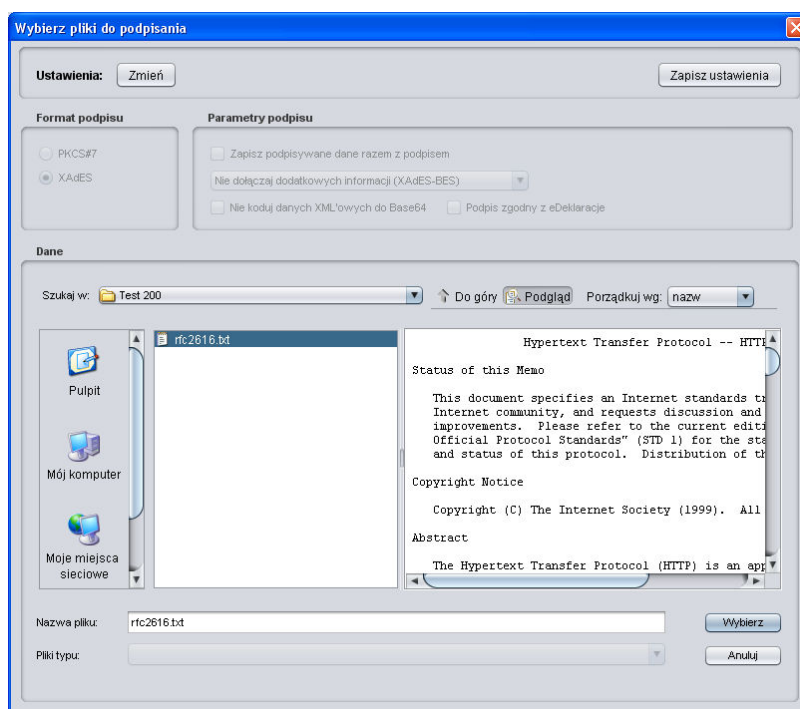
- Składanie zwykłego oraz bezpiecznego podpisu elektronicznego w formatach PKCS#7 oraz XAdES.
- Znakowania czasem podpisu zarówno w procesie jego składania, jak i weryfikacji, przy czym możliwe jest użycie różnych certyfikatów i par kluczy dla procesów składania podpisu i znakowania czasem.

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.

- Możliwość dołączenia podpisywanych danych do pliku z podpisem.
- Możliwość strumieniowego składania podpisów poprzez wskazanie grupy plików lub katalogu z plikami, które mają zostać podpisane.

3.1. Składanie podpisu – przycisk „podpisz”

Aby złożyć podpis z wykorzystaniem najczęściej używanych parametrów (format podpisu, etc.) należy kliknąć na przycisk podpisz (główny ekran) lub wybrać z menu Plik -> Podpisz. Pojawi się poniższe okno.

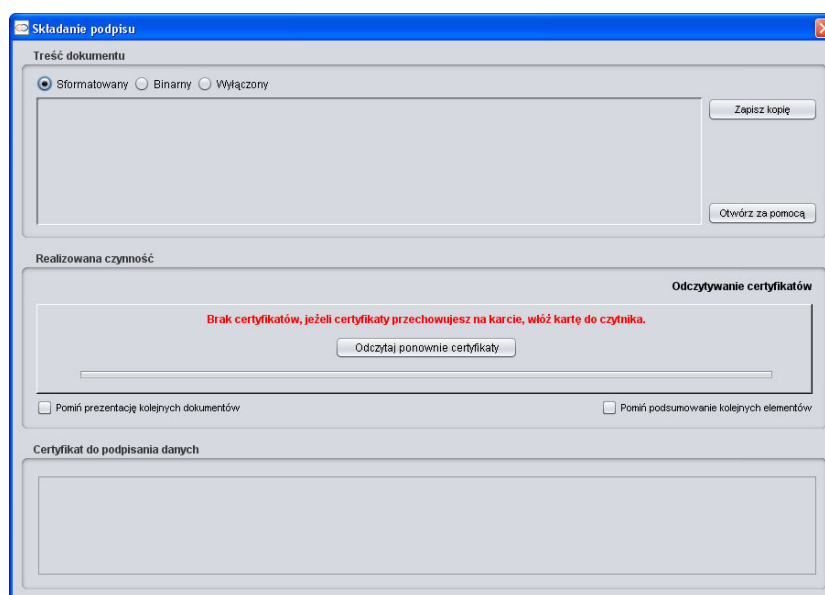


Rysunek 4. Składanie podpisu – przycisk „podpisz”.

W oknie tym, użytkownik wskazuje pliki, które zamierza podpisać. Format i parametry podpisu domyślnie są zablokowane do edycji, można je uaktywnić naciskając przycisk „Zmień” w części ustawienia. Opcje dotyczące formatu podpisu oraz pozostałe parametry są analogiczne jak przy podpisywaniu z wykorzystaniem kreatora i zostały opisane w części „Kreator podpisu”.

Przycisk „Zapisz ustawienia” zapamiętuje format i parametry podpisu w aktywnej konfiguracji, zostaną one użyte przy ponownym podpisywaniu dokumentów. Jeżeli w konfiguracji zostało ustawione hasło administratora i zaznaczona opcja: „Wymagaj podania hasła przed zapisaniem zmian w konfiguracji” to aplikacja przed zapisaniem poprosi o to hasło.

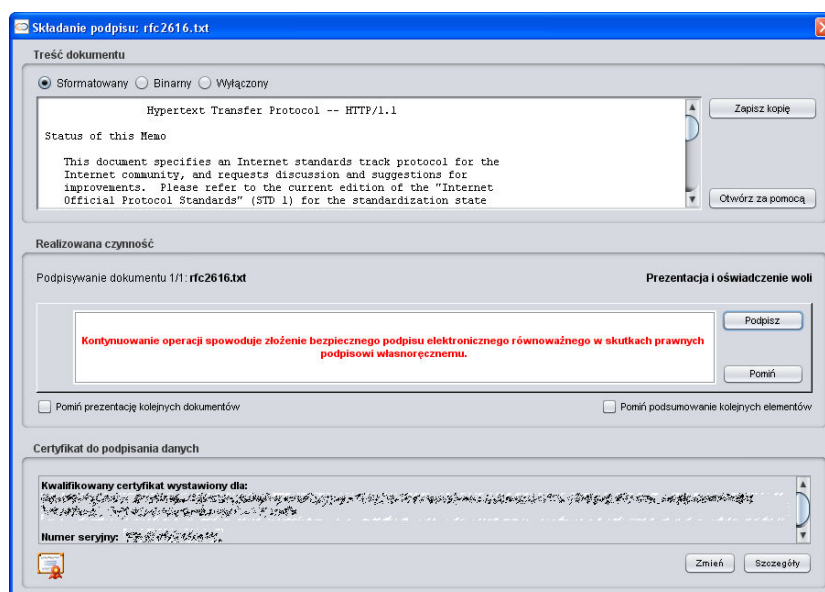
Do procesu podpisywania przechodzimy naciskając przycisk „Wybierz” w prawym dolnym rogu okna.



Rysunek 5. Składanie podpisu – brak certyfikatów.

Aplikacja automatycznie sprawdza, czy karta z certyfikatami jest umieszczona w czytniku, jeżeli znajdzie kartę wybiera certyfikat wg preferencji ustawionych w konfiguracji. W przypadku, kiedy aplikacja nie może znaleźć certyfikatów prosi użytkownika o umieszczenie karty w czytniku - obrazuje to powyższy ekran. Po umieszczeniu karty należy wcisnąć przycisk „Odczytaj ponownie certyfikaty”. Certyfikat, który zostanie użyty do podpisania danych jest prezentowany w dolej części tego ekranu.

Jeżeli dane będą równocześnie oznaczane czasem to zostanie zaprezentowany drugi certyfikat, który zostanie wykorzystany do tego celu. Certyfikaty do podpisywania i oznaczania czasem mogą być te same lub różne. Użytkownik naturalnie może zmienić certyfikaty, które wskazała aplikacja, do tego celu służą przyciski „Zmień” przy certyfikatach.



Rysunek 6. Składanie podpisu – prezentacja danych.

Okno „Składanie podpisu...” umożliwia użytkownikowi nadzór nad procesem składania podpisu elektronicznego.

- **Treść dokumentu.** 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.

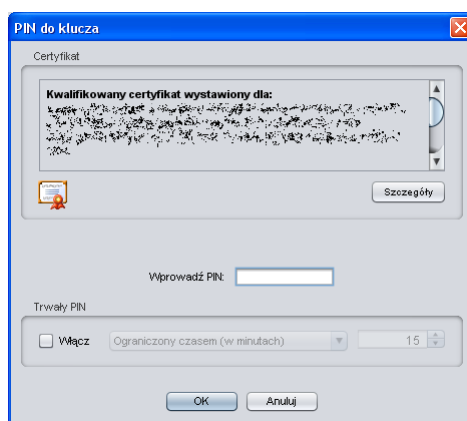
Korzystanie do podglądu podpisanej treści z aplikacji zewnętrznych stanowi pewne ryzyko w przypadku przeglądania plików w formatach umożliwiających wbudowywanie makr oraz wyświetlanie zawartości w sposób dynamiczny, zależny np. od bieżącej daty, lokalizacji bądź nazwy użytkownika. Istnieje bowiem niebezpieczeństwo, że te same dane wyglądać będą inaczej u osoby składającej podpis, a inaczej u osoby weryfikującej podpis.

- **Realizowana 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.** 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.

- **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.
- **Certyfikaty.** W tej ramce wyświetlane są informacje o certyfikatach używanych w trakcie składania podpisu elektronicznego oraz oznaczania czasem.

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:



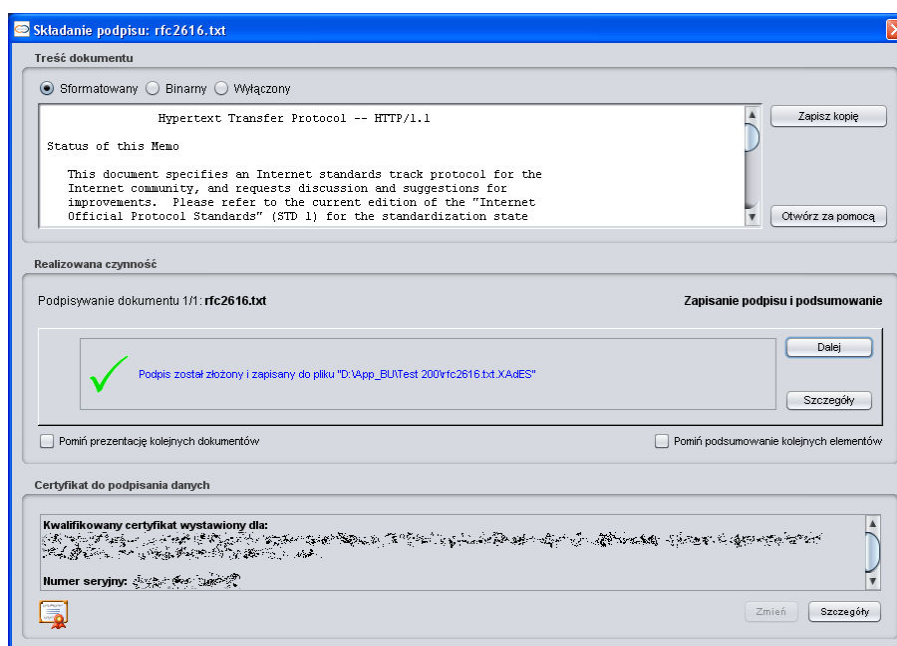
Rysunek 7. Okno wprowadzania kodu PIN.

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 ilością operacji** pozwala na określenie limitu możliwych do wykonania operacji kryptograficznych.

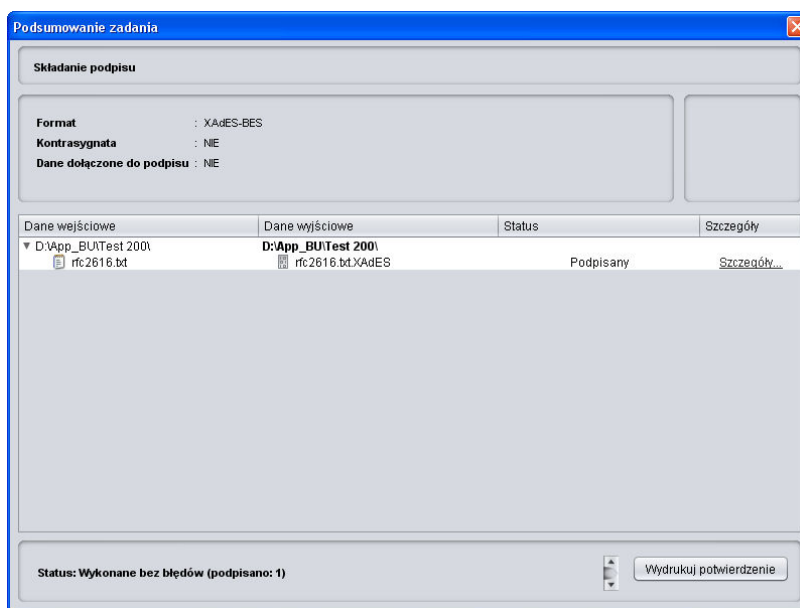
Użycie trwałego PIN zmniejsza bezpieczeństwo aplikacji oraz karty kryptograficznej z uwagi na to, że PIN – choć w formie zaszyfrowanej – przechowywany jest jednak w pamięci komputera.

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:



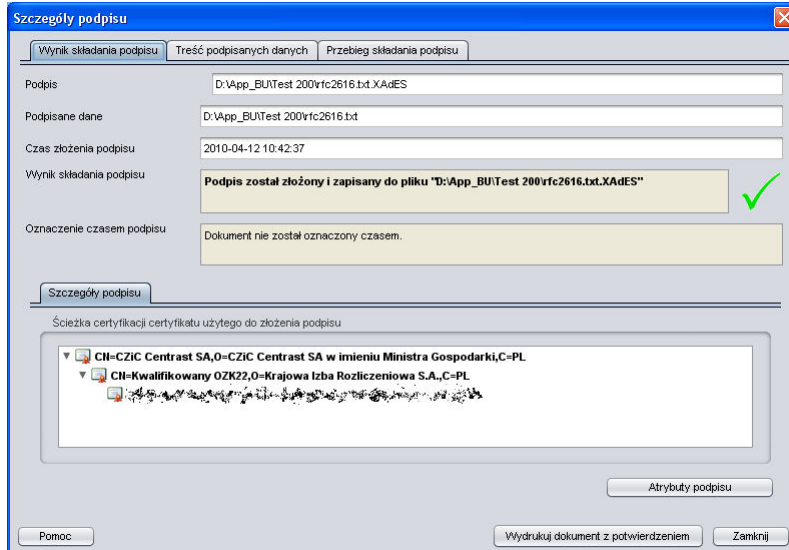
Rysunek 8. Okno składanie podpisu - podsumowanie.

Po wykonaniu ostatniego podpisu i zamknięciu okna podpisywania, aplikacja wyświetli nowe okno „Podsumowanie zadania”. W oknie tym użytkownik może zobaczyć status każdego pliku oraz szczegóły dotyczące jego podpisania. W dolnej części okna znajduje się przycisk „Wydrukuj potwierdzenie”, który pozwala użytkownikowi wydrukować raport z przeprowadzonego właśnie procesu podpisywania. Raport jest przygotowany jako dokument PDF, co pozwala użytkownikowi na podgląd lub wydruk (jeżeli na komputerze zainstalowany jest program Adobe Reader) oraz na zapisanie go w postaci pliku.



Rysunek 9. Podsumowanie zadania.

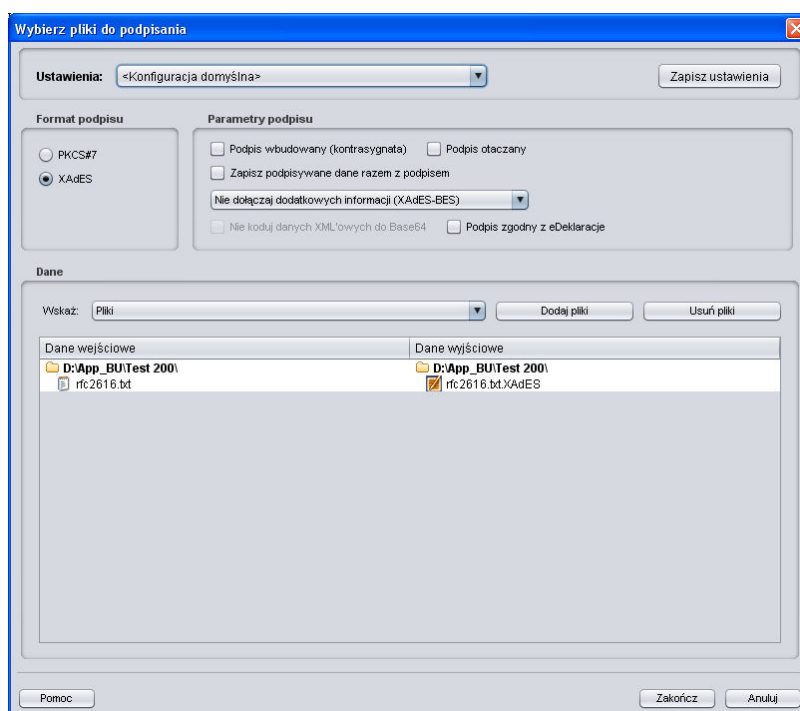
Korzystając z przycisku „Szczegóły” można przeglądać szczegóły złożonych podpisów oraz przebieg wykonanego procesu. Z okna tego można również wydrukować podpisany dokument (tylko wybrane formaty dokumentów) wraz z potwierdzeniem wykonanego podpisu.



Rysunek 10. Szczegóły podpisu.

3.2. Kreator podpisu

Okno kreatora podpisu dostępne jest z ekranu głównego pod przyciskiem „kreator -> podpis” lub z menu „Narzędzia -> Kreator zadania -> Podpisywania” pozwala użytkownikowi na określenie parametrów dotyczących podpisu oraz wskazanie wielu plików lub katalogów z plikami do podpisania.



Rysunek 11. Kreator podpisu.

Część ustawienia zawiera rozwijalną listę zdefiniowanych w aplikacji konfiguracji, format i parametry podpisu domyślnie ustawione są na podstawie aktywnej konfiguracji. Wybierając inną dostępną konfigurację z listy format i parametry zostaną zmienione zgodnie z ową konfiguracją.

Przycisk „Zapisz ustawienia” zapamiętuje format i parametry podpisu w konfiguracji wybranej na liście i ustawia tę konfigurację jako aktywną, co oznacza, że aplikacja będzie od tej pory używać właśnie tej konfiguracji. Jeżeli w konfiguracji zostało ustawione hasło administratora i zaznaczona któraś z opcji: „Wymagaj podania hasła przed zapisaniem zmian w konfiguracji” lub „Wymagaj podania hasła przed załadowaniem innej konfiguracji” to aplikacja przed zapisaniem poprosi o to hasło.

Format podpisu. Tutaj użytkownik wybiera w jakim formacie ma zostać złożony podpis. **Parametry podpisu** znajdujące się po prawej stronie i są ściśle powiązane z for-

matem, dlatego są inne dla każdego formatu. Dostępne formaty podpisu i powiązane z nimi parametry:

- **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.
 - **Zapisz podpisywane dane razem z podpisem.** Opcję tę zaznacza się, aby podpisywane dane zostały umieszczone w pliku podpisu. Aplikacja pozwala na dodawanie bardzo dużych danych do pliku z podpisem, jednak nie zaleca się stosowania tego rozwiązania dla dużych plików z danymi.
 - **Oznakuj składany podpis czasem.** Należy zaznaczyć tę opcję, aby do składanego podpisu w formacie PKCS#7 dołączyć oznaczenie czasem 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.

- **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 (kontrasygната).** 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).
 - **Zapisz podpisywane dane razem z podpisem.** Analogicznie jak dla PKCS#7, opcję tę zaznacza się, aby podpisywane dane zostały umieszczone w pliku podpisu. Nie zaleca się stosowania tego rozwiązania dla dużych plików z danymi.

- **Forma 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.
 - **Dołącz znacznik czasu, certyfikaty i listy CRL (XAdES-A)** – zostanie złożony podpis w formacie XAdES-A, zawierający znacznik czasu oraz informacje zapewniające tzw. długotrwałą rozszerzoną ważność dowodową podpisu.
- **Nie koduj danych XML'owych do Base64.** Opcja ta dotyczy sytuacji, w której wybrano, aby podpisane dane zostały zapisane razem z podpisem („Zapisz podpisywane dane razem z podpisem”) i podpisywane dane stanowią dokument XML lub jego fragment. Domyślnie podpisywane dane są kodowane do formatu Base64 ponieważ sam format XAdES jest dokumentem XML. W przypadku danych binarnych dane muszą zostać zakodowane, natomiast w przypadku danych XML dane mogą, ale nie muszą być zapisywane jako Base64. W ten sposób użytkownik może zdecydować o kodowaniu danych podpisanych w pliku podpisu XAdES.
- **Podpis zgodny z eDeklaracje.** Należy zaznaczyć tę opcję, jeżeli podpisany dokument jest elektroniczną deklaracją podatkową i będzie składany drogą elektroniczną w systemie e-Deklaracje. Na chwilę obecną, system e-Deklaracje przyjmuje podpisy wykonane z zaznaczonymi dodatkowo opcjami „Zapisz podpisywane dane razem z podpisem” oraz „Nie koduj danych XML'owych do Base64”.

Część **Dane** pozwala określić użytkownikowi dane, które mają zostać podpisane.

- **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.
- **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 niezbędny do zbudowania ścieżki dostępu do podpiswanego elementu, tzw. URI. Wskazanie elementu XML nieposiadającego 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.

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) lub w miejscu zdefiniowanym w konfiguracji aplikacji.
- 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 lub w miejscu zdefiniowanym w konfiguracji aplikacji.

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.

Jeżeli został wybrany wariant podpisu otaczanego formatu XAdES okno zmieni swoją postać na przedstawioną poniżej.

- **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.

Rysunek 12. Kreator podpisu – podpis otaczany.

Po wybraniu przycisku „Zakończ” rozpocznie się proces podpisywania, który został opisany w poprzedniej części.

4. Weryfikacja podpisu

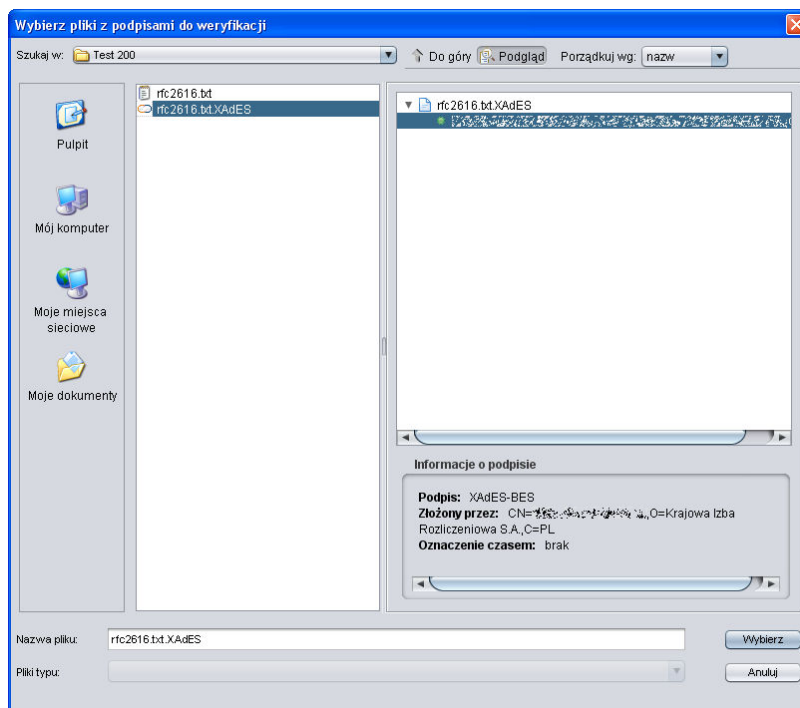
Funkcjonalność aplikacji SZAFIR w zakresie weryfikacji podpisu obejmuje:

- Weryfikowanie zwykłych oraz bezpiecznych podpisów elektronicznych w formatach:
 - PKCS#7 (podpis pojedynczy i wielokrotny)
 - XAdES-BES, XAdES-T, XAdES-C, XAdES-A (podpis pojedynczy, wiele podpisów w plikach oraz podpis wbudowany i otaczany).
 - PAdES, PAdES-T
- Znakowanie czasem podpisu 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.
- Możliwości strumieniowego weryfikowania podpisów, poprzez wskazanie grupy plików lub katalogów z plikami zawierającymi podpisy.

4.1. Weryfikacja podpisu – przycisk „weryfikuj”

W celu szybkiej weryfikacji plików z podpisem, bez określania parametrów weryfikacji (zostaną przyjęte domyślne) należy kliknąć na przycisk weryfikuj (ekran główny) lub wybrać z menu Plik -> Weryfikuj. Pojawi się okno przedstawione na poniższym rysunku.



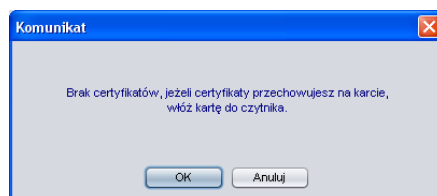
Rysunek 13. Weryfikacja podpisu – przycisk „weryfikuj”.

W oknie tym, użytkownik wskazuje tylko pliki, zawierające podpisy, które zamierza zweryfikować. Część „Informacje o podpisie” zawiera podstawowe informacje dotyczące wskazanego podpisu na liście podpisów umieszczonej powyżej. Do procesu weryfikowania przechodzimy naciskając przycisk Wybierz w prawym dolnym rogu okna.

W przypadku kiedy aplikacja nie będzie mogła znaleźć plików z danymi dla wskazanych przez użytkownika podpisów, użytkownik zostanie automatycznie przeniesiony do kreatora weryfikacji. W kreatorze istnieje możliwość wskazania brakujących danych lub pominięcia wybranych podpisów w procesie weryfikacji.

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. Aplikacja automatycznie sprawdza, czy karta z certyfika-

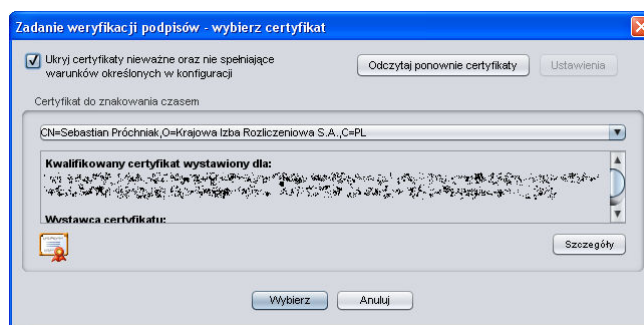
tami jest umieszczona w czytniku, jeżeli znajdzie kartę wybiera certyfikat wg preferencji ustawionych w konfiguracji. W przypadku, kiedy aplikacja nie może znaleźć certyfikatów prosi użytkownika o umieszczenie karty w czytniku - obrazuje to poniższy ekran. Po umieszczeniu karty należy wcisnąć przycisk „OK”.



Rysunek 14. Komunikat – brak certyfikatów.

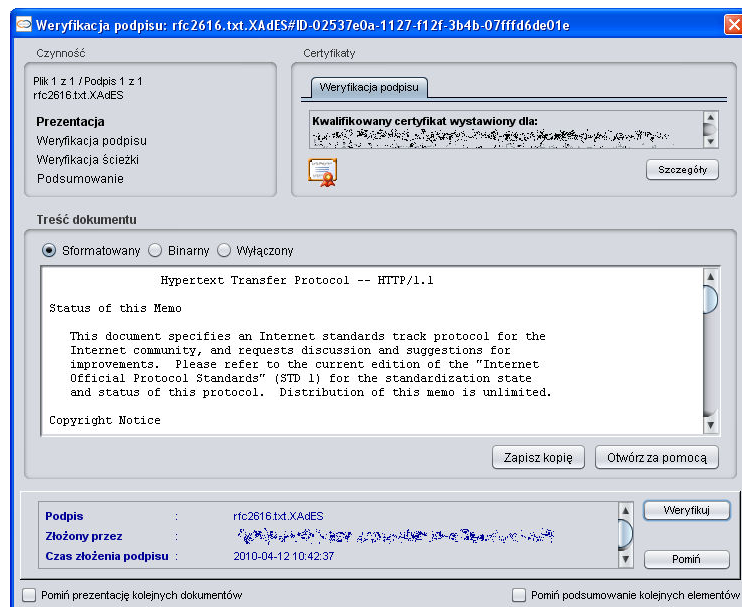
Wybrany certyfikat prezentowany jest w oknie przedstawionym na poniższym rysunku. Użytkownik może wybrać inny korzystając z listy rozwijalnej.

W konfiguracji można ustawić ograniczenia dotyczące używanych certyfikatów. Jeżeli takie ograniczenia zostały ustawione, aplikacja w tym miejscu nie pozwoli wybrać certyfikatu niezgodnego z tymi ustawieniami.



Rysunek 15. Weryfikacja podpisów – wybierz certyfikat.

Po wybraniu certyfikatu i naciśnięciu przycisku „Wybierz” użytkownikowi zostanie zaprezentowane okno weryfikacji.



Rysunek 16. Weryfikacja podpisu.

Okno weryfikacji umożliwia użytkownikowi nadzór nad procesem weryfikacji podpisów elektronicznych.

- **Czynność.** W tej ramce wyświetlane są informacje o aktualnie wykonywanej czynności (takiej jak weryfikacja określonego podpisu elektronicznego) i jej kolejnych krokach:
 - **Prezentacja.** Przed rozpoczęciem weryfikacji podpisu aplikacja prezentuje najważniejsze informacje o weryfikowanym podpisie oraz treści podpisanego dokumentu.
 - **Weryfikuj** rozpoczyna weryfikację podpisu elektronicznego.
 - **Pomiń** pomija weryfikację podpisu elektronicznego.
 - **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.

- **Weryfikacja ścieżki certyfikacji.** Po zweryfikowaniu poprawności weryfikowanego podpisu na poziomie algorytmów szyfrowych oraz ewentualnym oznacze-

niu podpisu czasem aplikacja weryfikuje ścieżkę certyfikacji certyfikatu używanego do zweryfikowania podpisu elektronicznego.

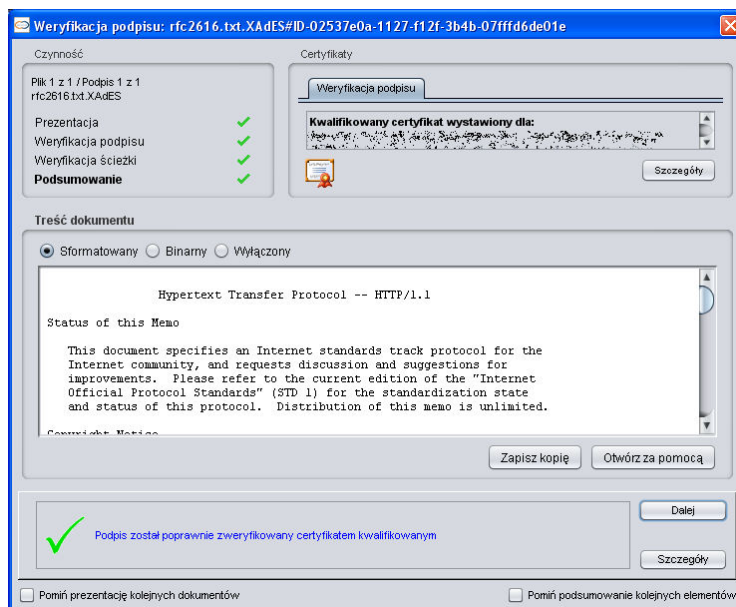
- **Podsumowanie.** Po zakończeniu procesu weryfikacji podpisu aplikacja wyświetla informację o wyniku weryfikacji.
- **Szczegóły** wyświetla szczegóły zakończonego właśnie procesu weryfikacji podpisu.
- **Dalej** rozpoczyna weryfikację kolejnego podpisu (jeżeli w ramach aktualnie wykonywanego zadania pozostały jeszcze jakieś podpisy do weryfikacji).
- **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.
- **Treść dokumentu.** 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.

Korzystanie do podglądu podpisanej treści z aplikacji zewnętrznych stanowi pewne ryzyko w przypadku przeglądania plików w formatach umożliwiających wbudowywanie makr oraz wyświetlanie zawartości w sposób dynamiczny, zależny np. od bieżącej daty, lokalizacji bądź nazwy użytkownika. Istnieje bowiem niebezpieczeństwo, że te same dane wyglądać będą inaczej u osoby składającej podpis, a inaczej u osoby weryfikującej podpis.

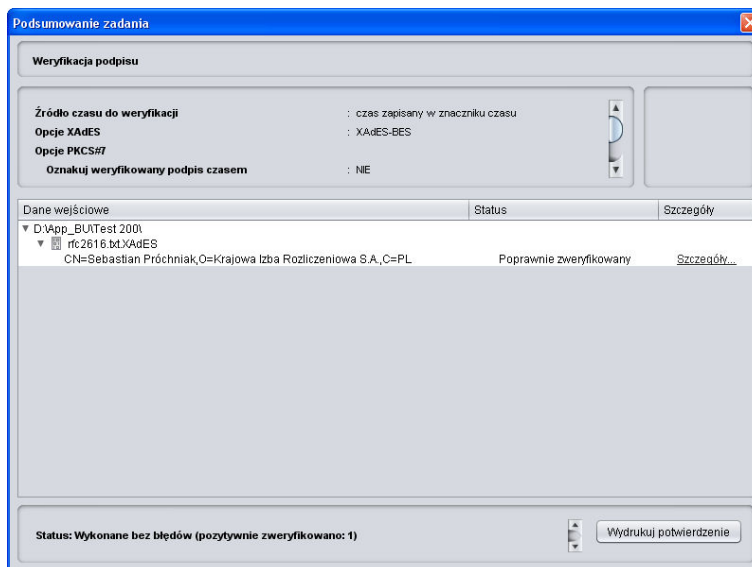
Pomiń prezentację kolejnych dokumentów – jeżeli ta opcja zostanie zaznaczona, wówczas weryfikowanie kolejnych podpisów odbywać się będzie z pominięciem ich prezentacji.

Pomiń podsumowanie kolejnych elementów – jeżeli ta opcja zostanie zaznaczona, wówczas weryfikacja kolejnych podpisów odbywać się będzie z pominięciem wyświetlania podsumowania.



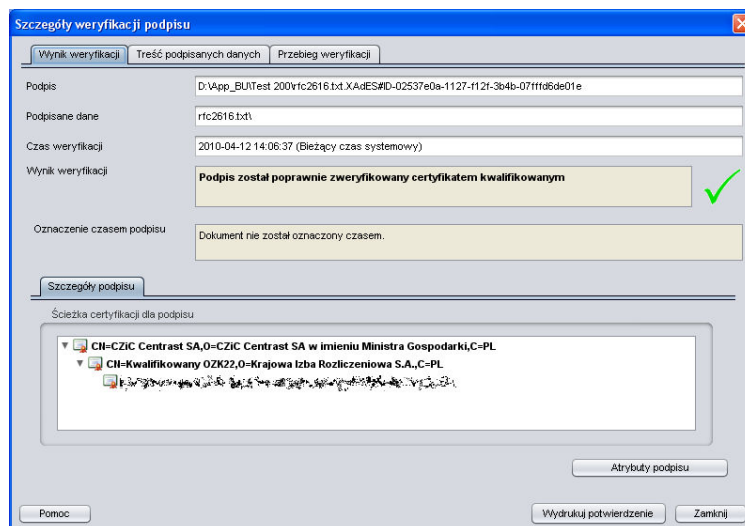
Rysunek 17. Weryfikacja podpisu - podsumowanie.

Po wykonaniu weryfikacji ostatniego podpisu i zamknięciu okna weryfikacji, aplikacja wyświetli nowe okno „Podsumowanie zadania”. W oknie tym użytkownik może zobaczyć status każdego podpisu oraz szczegóły dotyczące jego weryfikacji. W dolnej części okna znajduje się przycisk „Wydrukuj potwierdzenie”, który pozwala użytkownikowi wydrukować raport z przeprowadzonego właśnie procesu weryfikacji. Raport jest przygotowany jako dokument PDF, co pozwala użytkownikowi na podgląd lub wydruk (jeżeli na komputerze zainstalowany jest program Adobe Reader) oraz na zapisanie go w postaci pliku.



Rysunek 18. Podsumowanie zadania.

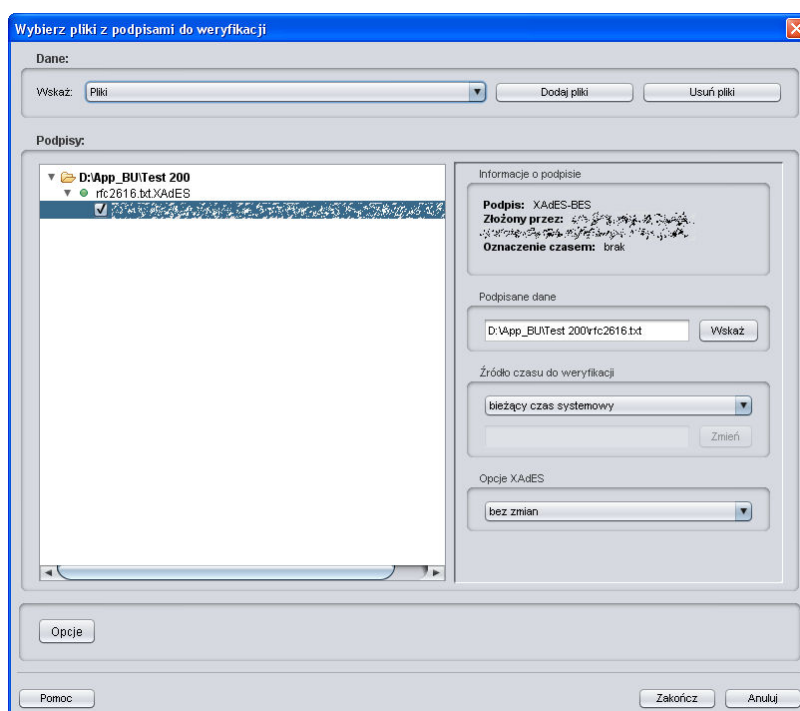
Korzystając z przycisku „Szczegóły” można przeglądać szczegóły weryfikowanych podpisów oraz przebieg wykonanego procesu. Z okna tego można również wydrukować podpisany dokument (tylko wybrane formaty dokumentów) wraz z potwierdzeniem wykonanego podpisu.



Rysunek 19. Szczegóły weryfikacji podpisu.

4.2. Kreator weryfikacji

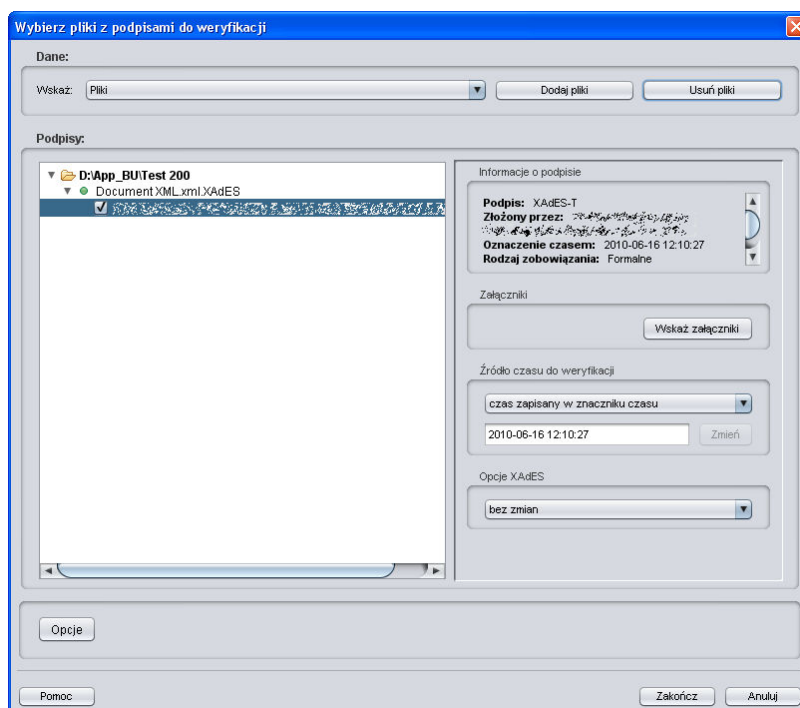
Okno kreatora weryfikacji dostępne z ekranu głównego pod przyciskiem „kreator -> weryfikacji” lub z menu „Narzędzia -> Kreator zadania -> Weryfikacji” pozwala użytkownikowi na określenie parametrów dotyczących weryfikacji podpisów oraz wskazanie wielu plików lub katalogów z plikami zawierającymi podpisy.



Rysunek 20. Kreator weryfikacji podpisów.

- **Dane.** Ta część pozwala użytkownikowi wskazać pliki lub katalogi zawierające pliki z podpisami, które mają zostać zweryfikowane.
 - **Pliki.** Należy wskazać tę opcję aby zweryfikować podpisy znajdujące się w jednym lub wielu wskazanych plikach.
 - **Katalogi.** Należy wskazać tę opcję aby zweryfikować podpisy znajdujące się we wszystkich plikach znajdujących się w jednym lub kilku wskazanych katalogach.
- **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 wariantcie 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. Kreator weryfikacji podpisów – podpis otaczany.

- **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).
 - **XAdES-A.** 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 rozszerzoną ważność dowodową (opcja dostępna tylko jeżeli weryfikowany podpis jest w formie niższej niż XAdES-A).

Po wybraniu przycisku „Zakończ” rozpocznie się proces weryfikacji, który został opisany w poprzedniej części.

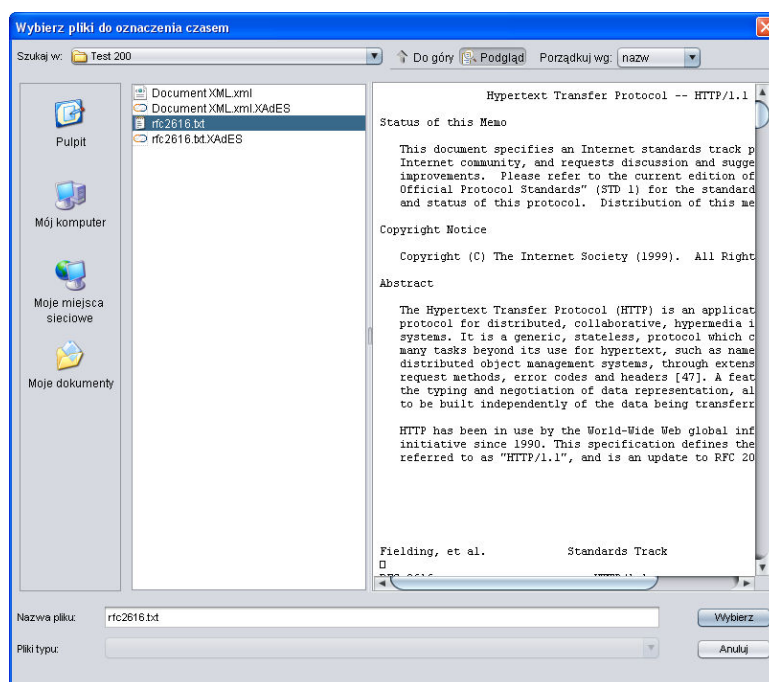
5. Znakowanie czasem

Aplikacja SZAFIR umożliwia użytkownikowi oznakowanie czasem dowolnego dokumentu (pliku) bez wykonania podpisu elektronicznego pod tym dokumentem. Posiada możliwość strumieniowego znakowania czasem poprzez wskazanie grupy plików lub katalogu z plikami, które mają zostać oznakowane.

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.

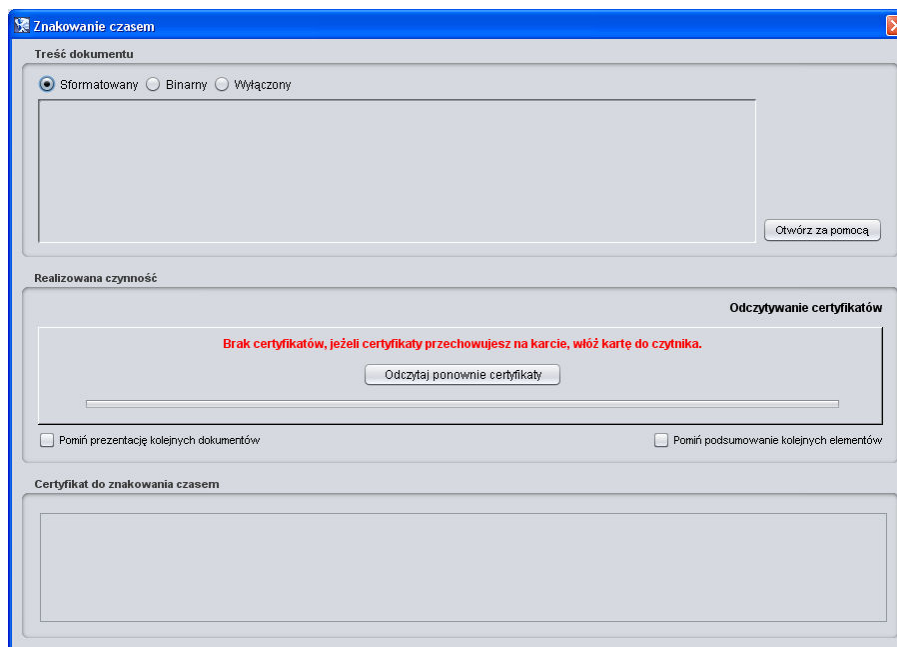
5.1. Znakowanie czasem – przycisk „oznakuj czasem”

Aby oznakować czasem dowolny dokument (plik) bez składania podpisu elektronicznego należy kliknąć na przycisk oznakuj czasem (główny ekran) lub wybrać z menu Plik -> Oznakuj czasem. Pojawi się poniższe okno.



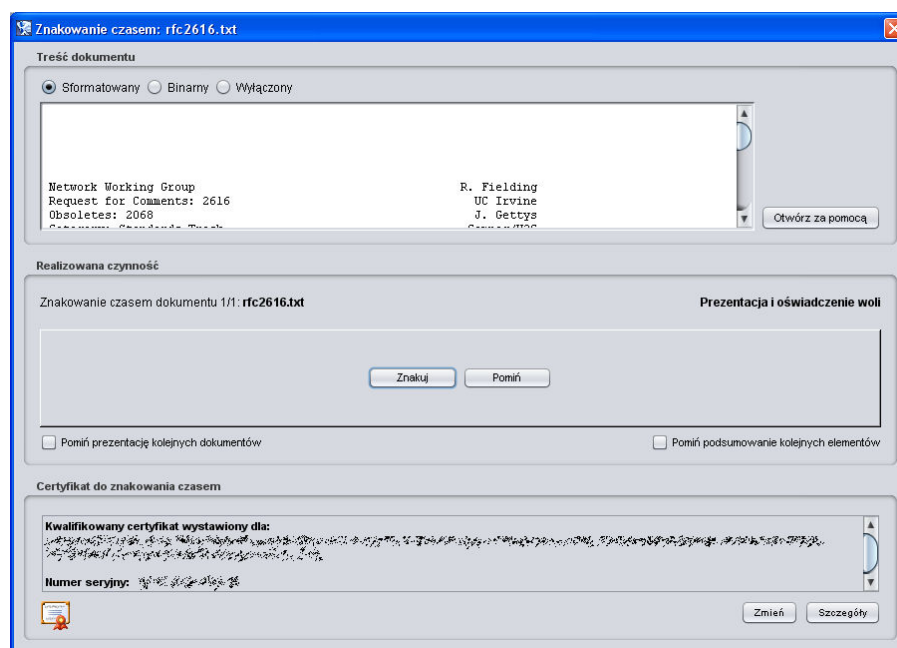
Rysunek 22. Oznakowanie czasem dokumentu.

W oknie tym, użytkownik wskazuje pliki, które zamierza oznakować czasem. Do procesu znakowania przechodzimy naciskając przycisk „Wybierz” w prawym dolnym rogu okna.



Rysunek 23. Znakowanie czasem – brak certyfikatów.

Podobnie jak przy podpisywaniu aplikacja automatycznie sprawdza, czy karta z certyfikatami jest umieszczona w czytniku. Pomimo tego, że sam dokument nie jest podpisywany, to użytkownik musi podpisać żądanie wysyłane do serwera znakowania czasem, dlatego niezbędne jest wskazanie certyfikatu.



Rysunek 24. Znakowanie czasem – prezentacja danych.

Okno „Znakowanie czasem...” umożliwia użytkownikowi nadzór nad procesem znakowania czasem dokumentu.

- **Treść dokumentu.** W tym polu prezentowana jest treść danych, które mają zostać oznakowane czasem. 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.

Korzystanie do podglądu podpisanej treści z aplikacji zewnętrznych stanowi pewne ryzyko w przypadku przeglądania plików w formatach umożliwiających wbudowywanie makr oraz wyświetlanie zawartości w sposób dynamiczny, zależny np. od bieżącej daty, lokalizacji bądź nazwy użytkownika. Istnieje bowiem niebezpieczeństwo, że te same dane wyglądać będą inaczej u osoby składającej podpis, a inaczej u osoby weryfikującej podpis.

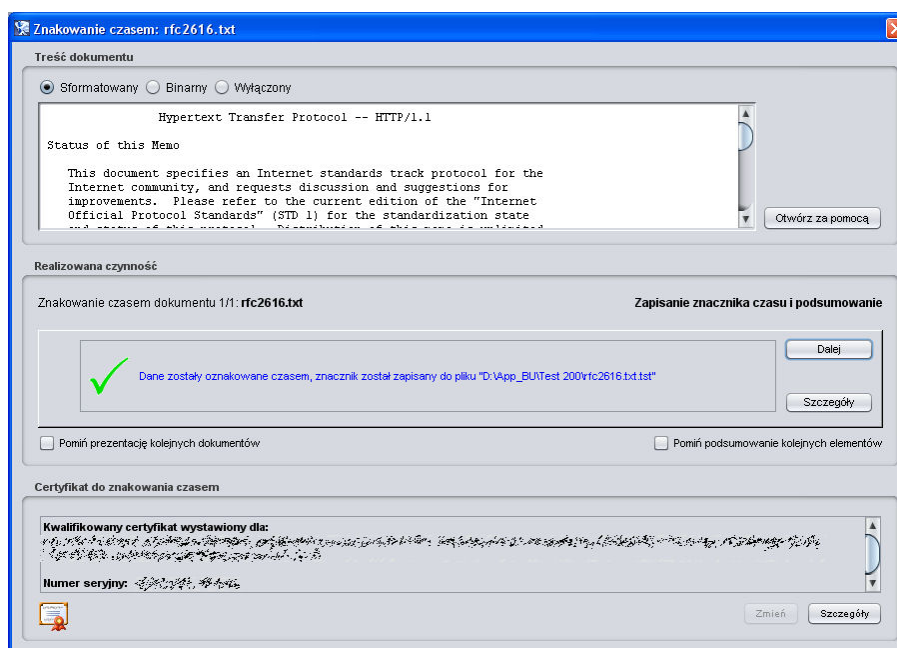
- **Realizowana czynność.** W tej ramce wyświetlane są informacje o aktualnie wykonywanej czynności (takiej jak znakowanie pliku o określonej nazwie) i jej kolejnych krokach:
 - **Prezentacja treści.** Przed rozpoczęciem oznaczania czasem aplikacja prezentuje treść podpisywanego dokumentu oraz wyświetla informację o skutkach prawnych oznaczenia czasem dokumentu. Użytkownik może zdecydować o rozpoczęciu znakowania danych lub ich pominięciu.
 - **Znakuj** rozpoczyna znakowanie czasem dokumentu.
 - **Pomiń** pomija znakowanie dokumentu.
 - **Pomiń prezentację kolejnych dokumentów** – jeżeli ta opcja zostanie zaznaczona, wówczas oznaczanie kolejnych dokumentów odbywać się będzie z pominięciem ich prezentacji.
 - **Znakowanie czasem.** Aplikacja zwraca się z wnioskiem o wydanie znacznika czasu dla przetwarzanego dokumentu.

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.

- **Podsumowanie.** Po zakończeniu znakowania czasem aplikacja zapisuje plik ze znacznikiem czasu (z rozszerzeniem TST) i wyświetla podsumowanie wykonanych operacji.
 - **Szczegóły** wyświetla szczegóły zakończonego właśnie procesu znakowania czasem.
 - **Dalej** rozpoczyna znakowanie kolejnego dokumentu (jeżeli w ramach aktualnie wykonywanego zadania pozostały jeszcze jakieś dokumenty do oznaczenia).
 - **Pomiń podsumowanie kolejnych dokumentów** – jeżeli ta opcja zostanie zaznaczona, wówczas podpisywanie kolejnych dokumentów odbywać się będzie z pominięciem wyświetlania podsumowania.
- **Certyfikat.** W tej ramce wyświetlane są informacje o certyfikacie używanym w trakcie oznaczania czasem dokumentu.

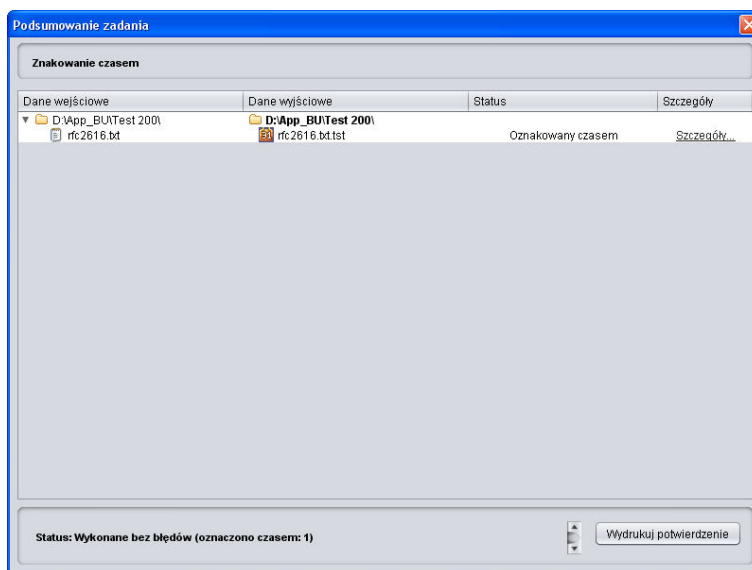
W celu kontynuowania znakowania czasem kliknąć na przycisku „Znakuj”. Aplikacja rozpocznie oznaczanie czasem. Za każdym razem gdy do przeprowadzenia operacji kryptograficznej niezbędne będzie uzyskanie dostępu do karty kryptograficznej lub zabezpieczonego pliku z certyfikatem, pojawi się okno wprowadzania PIN.

Po wprowadzeniu kodu PIN i jego zatwierdzeniu przyciskiem „OK” aplikacja wyśle żądanie wydania znacznika czasu do serwera znakowania czasem, a następnie zapisze otrzymany znacznik w pliku. W oknie znakowania pojawi się podsumowanie wykonanych operacji.



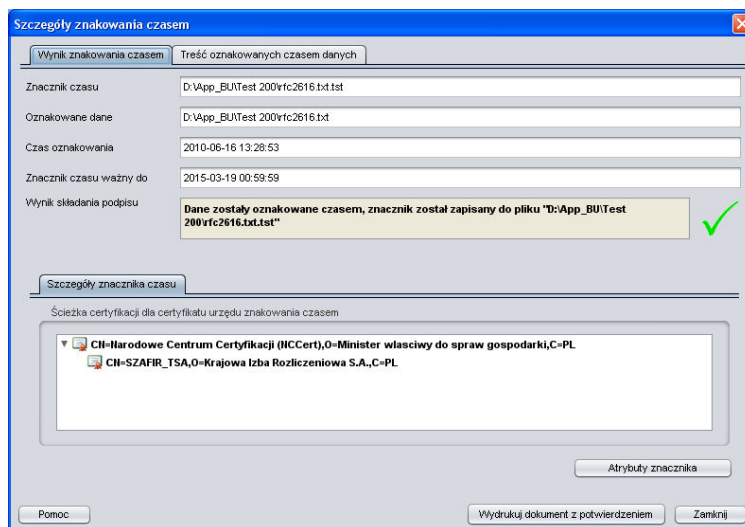
Rysunek 25. Okno znakowanie czasem - podsumowanie.

Po wykonaniu ostatniego oznaczania czasem i zamknięciu powyższego okna, aplikacja wyświetli nowe okno „Podsumowanie zadania”. W oknie tym użytkownik może zobaczyć status każdego pliku oraz szczegóły dotyczące jego oznakowania. W dolnej części okna znajduje się przycisk „Wydrukuj potwierdzenie”, który pozwala użytkownikowi wydrukować raport z przeprowadzonego właśnie procesu znakowania czasem. Raport jest przygotowany jako dokument PDF, co pozwala użytkownikowi na podgląd lub wydruk (jeżeli na komputerze zainstalowany jest program Adobe Reader) oraz na zapisanie go w postaci pliku.



Rysunek 26. Podsumowanie zadania.

Korzystając z przycisku „Szczegóły” można przeglądać szczegóły dotyczące oznaczonych dokumentów oraz przebieg wykonanego procesu. Z okna tego można również wydrukować podpisany dokument (tylko wybrane formaty dokumentów) wraz z potwierdzeniem wykonanego podpisu.



Rysunek 27. Szczegóły znakowania czasem.

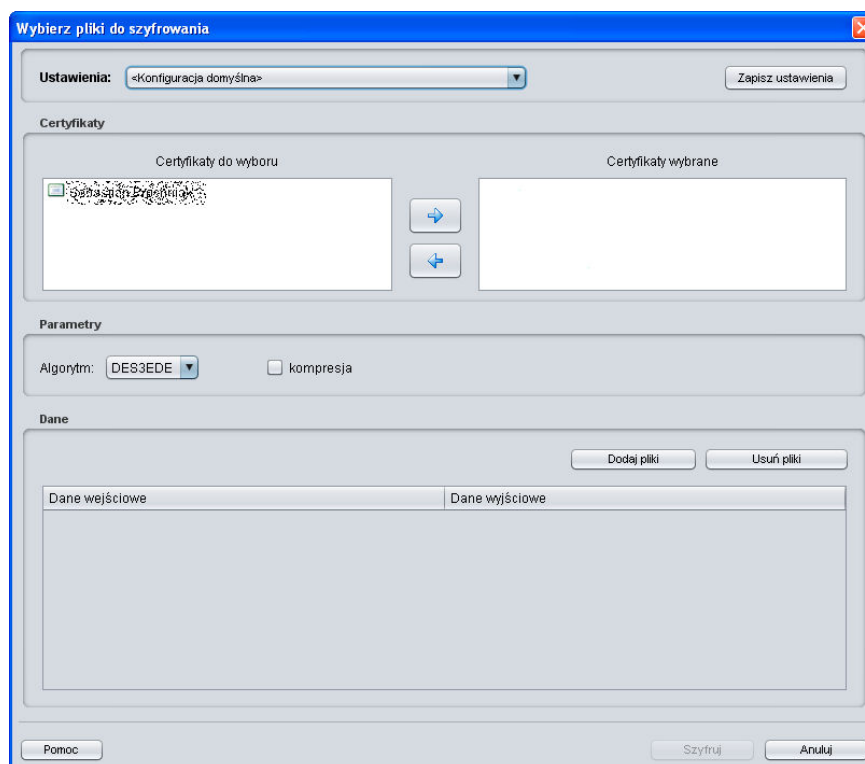
6. Szyfrowanie i odszyfrowywanie

Funkcjonalność aplikacji SZAFIR w zakresie szyfrowania obejmuje:

- Szyfrowanie dokumentów (plików) przy użyciu algorytmów DES3EDE lub AES.
- Możliwość kompresji danych szyfrowanych.
- Możliwość szyfrowania jednego dokumentu wieloma certyfikatami, co pozwala zwiększyć listę odbiorców zaszyfrowanego dokumentu.
- Możliwość strumieniowego szyfrowania plików poprzez wskazanie grupy plików, które mają zostać zaszyfrowane.

6.1. Szyfrowanie

Do szyfrowania plików służy przycisk Szyfrowanie -> Szyfruj na ekranie głównym aplikacji lub opcja w menu: Plik -> Szyfruj.



Rysunek 28. Szyfrowanie – dane i parametry.

Część ustawienia zawiera rozwijalną listę zdefiniowanych w aplikacji konfiguracji, wybrane certyfikaty, algorytm oraz kompresja domyślnie ustawione są na podstawie aktywnej konfiguracji. Wybierając inną dostępną konfigurację wspomniane parametry zostaną zmienione zgodnie z ową konfiguracją.

Przycisk „Zapisz ustawienia” zapamiętuje algorytm oraz kompresję w konfiguracji wybranej na liście i ustawia tę konfigurację jako aktywną, co oznacza, że aplikacja będzie od tej pory używać właśnie tej konfiguracji. Jeżeli w konfiguracji zostało ustawione hasło administratora i zaznaczona któraś z opcji: „Wymagaj podania hasła przed zapisaniem zmian w konfiguracji” lub „Wymagaj podania hasła przed załadowaniem innej konfiguracji” to aplikacja przed zapisaniem poprosi o to hasło.

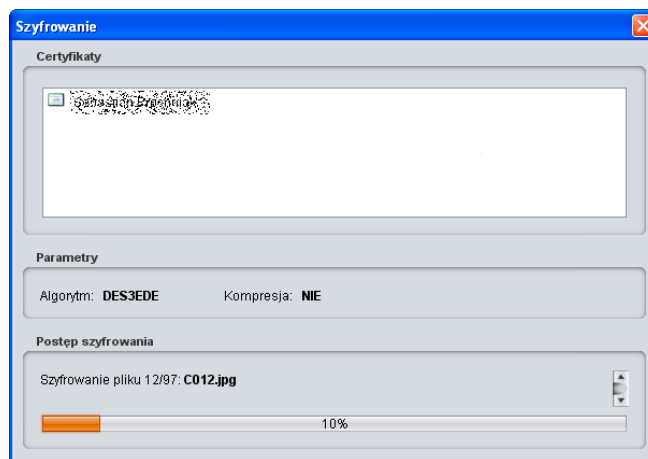
Część **Certyfikaty** pozwala użytkownikowi wybrać certyfikaty, które zostaną użyte w procesie szyfrowania. Certyfikaty wybiera się wskazując je na liście po lewej stronie i naciskając na przycisk ze strzałką „->”. Użytkownik może wskazać kilka certyfikatów. Do usuwania certyfikatów z listy wybranych służy przycisk ze strzałką „<-”.

Lista certyfikatów do wyboru zawiera tylko certyfikaty, które zostały dodane do magazynu certyfikatów do grupy certyfikaty do szyfrowania. Magazyn certyfikatów dostępny jest z menu Narzędzia -> Magazyn certyfikatów i list CRL, został opisany w dalszej części podręcznika.

Część **Parametry** pozwala użytkownikowi określić jaki algorytm zostanie użyty w procesie szyfrowania oraz czy dane szyfrowane mają zostać skompresowane.

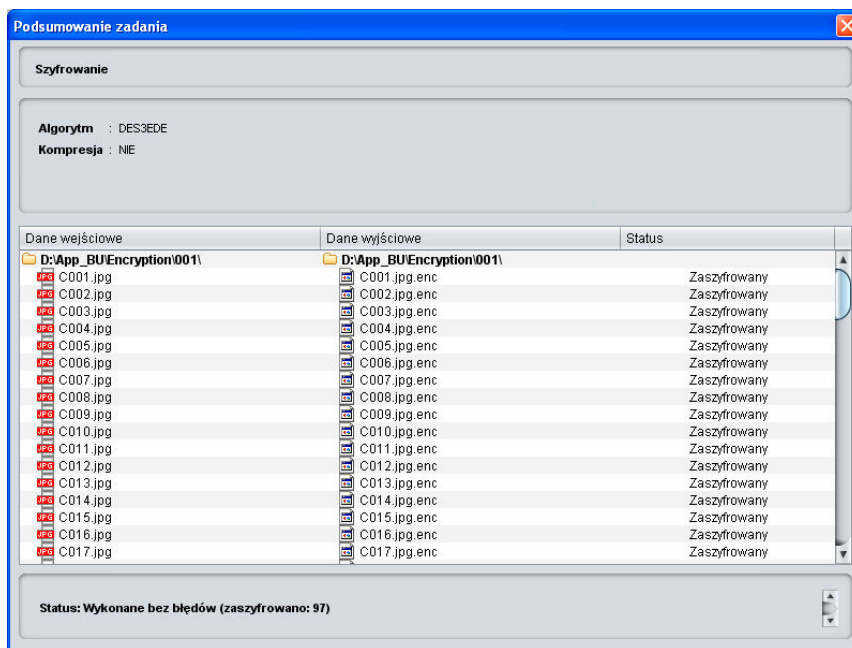
Część **Dane** pozwala określić użytkownikowi dane, które mają zostać zaszyfrowane. Użytkownik może wskazać wiele plików do zaszyfrowania.

Po wybraniu przycisku „Szyfruj” rozpocznie się proces szyfrowania. Jeżeli użytkownik wskazał wiele plików to podczas procesu szyfrowania będzie mógł zobaczyć postęp całego procesu.



Rysunek 29. Szyfrowanie.

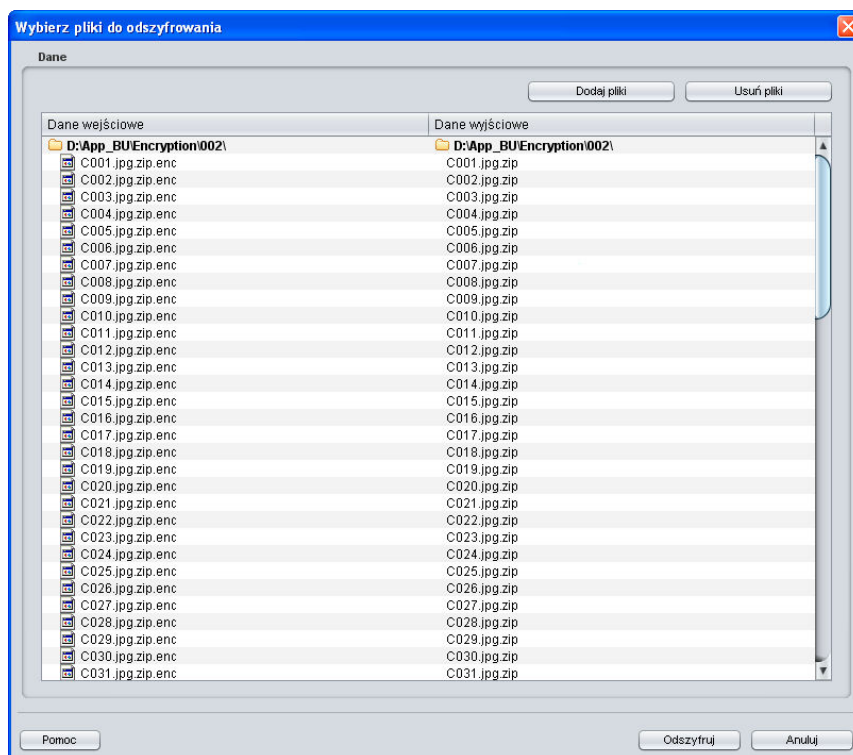
Po zaszyfrowaniu ostatniego pliku i zamknięciu okna szyfrowania, aplikacja wyświetli nowe okno „Podsumowanie zadania”. W oknie tym użytkownik może zobaczyć status każdego pliku.



Rysunek 30. Szyfrowanie - podsumowanie zadania.

6.2. Odszyfrowywanie

Do odszyfrowywania plików służy przycisk Szyfrowanie -> Odszyfruj na ekranie głównym aplikacji lub opcja w menu: Plik -> Odszyfruj.



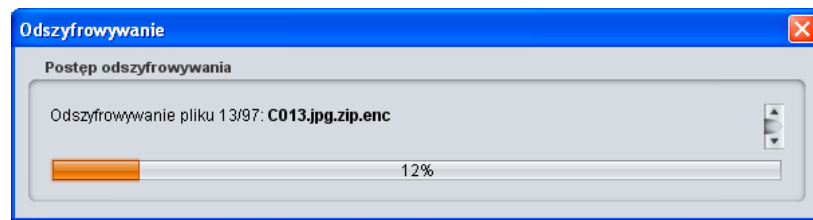
Rysunek 31. Odszyfrowywanie – dane.

Część **Dane** pozwala określić użytkownikowi pliki, które mają zostać odszyfrowane. Użytkownik może wskazać wiele plików do odszyfrowania.

Po wybraniu przycisku „Odszyfruj” rozpocznie się proces odszyfrowywania. Aplikacja automatycznie sprawdza, czy posiada certyfikat, który umożliwia odszyfrowanie danego pliku. Certyfikatów aplikacja szuka na karcie kryptograficznej włożonej do czytnika oraz w plikach PKCS#12 zdefiniowanych w konfiguracji w zakładce „Komponent techniczny”. Jeżeli żaden ze znalezionych certyfikatów nie pozwala na odszyfrowanie to aplikacja prosi użytkownika o wskazanie właściwego certyfikatu.

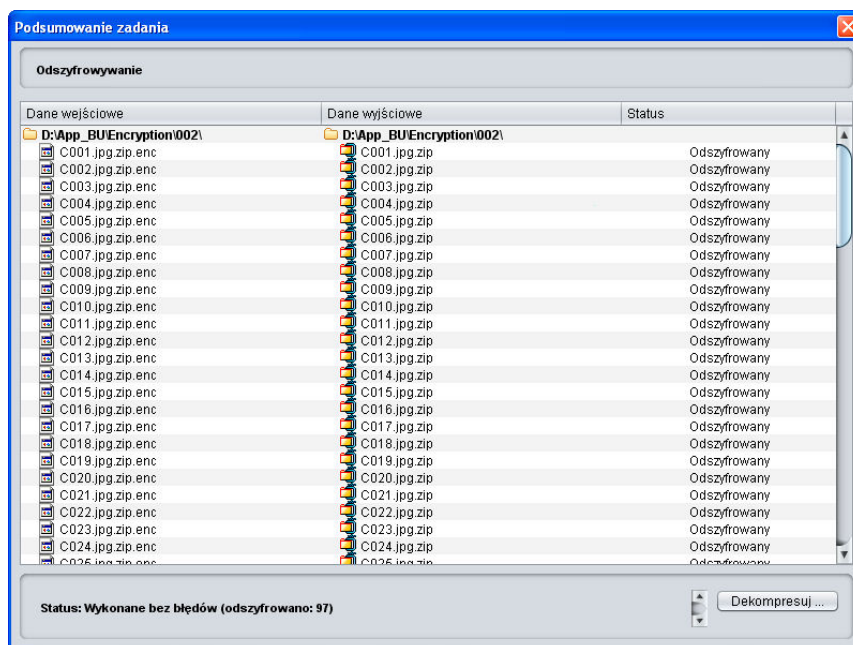
Za każdym razem gdy do przeprowadzenia operacji kryptograficznej niezbędne będzie uzyskanie dostępu do karty kryptograficznej lub zabezpieczonego pliku z certyfikatem, pojawi się okno z prośbą wprowadzenia PIN’u. Okno to zostało opisane w części dotyczącej składania podpisu.

Jeżeli użytkownik wskazał wiele plików to podczas procesu odszyfrowywania będzie mógł zobaczyć postęp całego procesu.



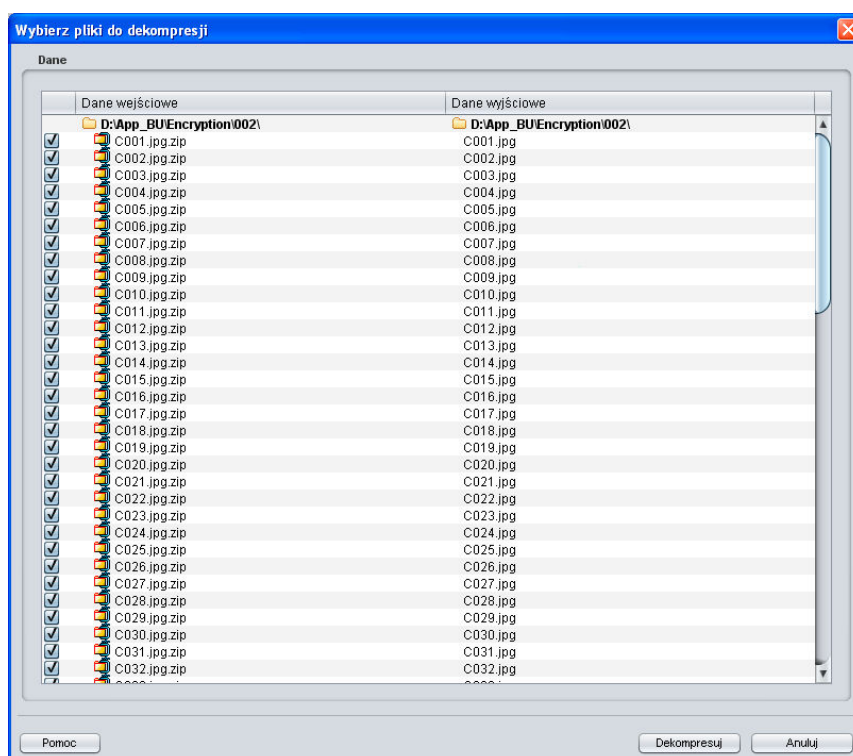
Rysunek 32. Odszyfrowywanie.

Po odszyfrowaniu ostatniego pliku i zamknięciu okna odszyfrowywania, aplikacja wyświetli nowe okno „Podsumowanie zadania”. W oknie tym użytkownik może zobaczyć status każdego pliku.



Rysunek 33. Odszyfrowywanie - podsumowanie zadania.

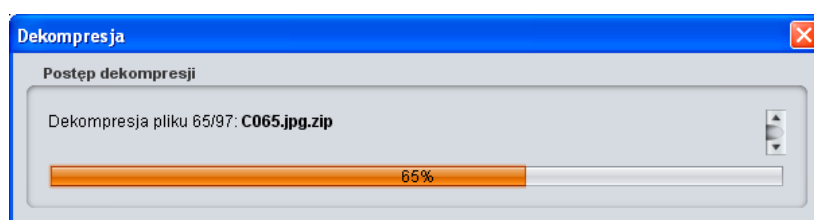
Jeżeli wśród odszyfrowanych plików znajdują się takie, które były kompresowane podczas szyfrowania aplikacją SZAFIR, na ekranie podsumowania pojawi się przycisk „Dekompresuj”, który umożliwia dekompresję odszyfrowanych plików. Okno dekompresji przedstawiono poniżej.



Rysunek 34. Dekompresja – wybór plików.

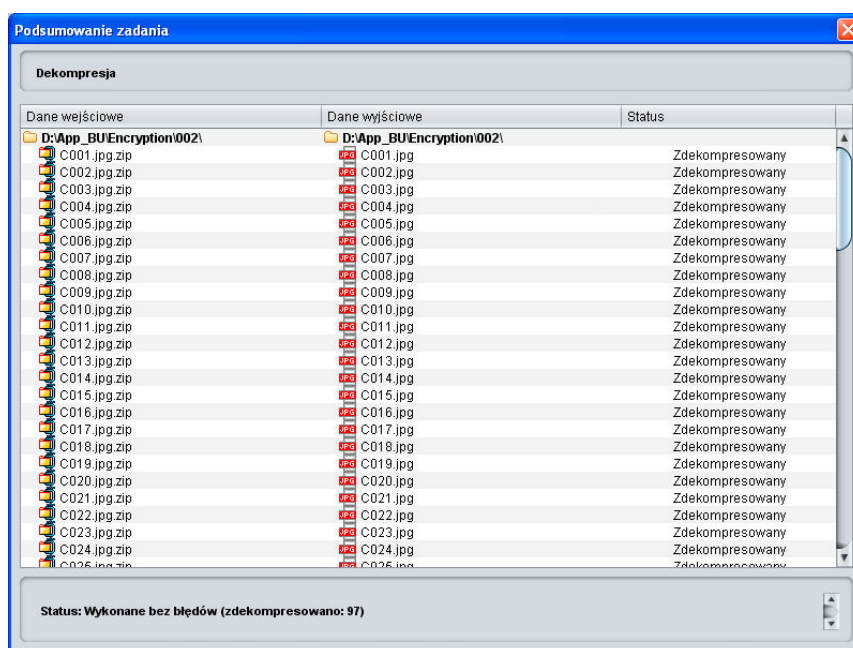
W oknie tym użytkownik może zdecydować, które z plików mają zostać poddane dekompresji. Sam proces dekompresji zostanie rozpoczęty po naciśnięciu przycisku „Dekompresuj” w dolnej części okna.

Jeżeli użytkownik wskazał wiele plików to podczas procesu dekompresji będzie mógł zobaczyć postęp całego procesu.



Rysunek 35. Dekompresja.

Po dekompresji ostatniego pliku i zamknięciu okna dekompresji, aplikacja wyświetli nowe okno „Podsumowanie zadania”. W oknie tym użytkownik może zobaczyć status każdego pliku.



Rysunek 36. Dekompresja - podsumowanie zadania

7. Obsługa eArchiwum w ramach usługi EDDM

7.1. Podstawowe informacje o usłudze EDDM

EDDM (ang. *Electronic Document Delivery and Management*) to usługa umożliwiająca bezpieczne przechowywanie 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.

7.2. Zastosowanie aplikacji SZAFIR w ramach usługi EDDM

Większość funkcjonalności usługi EDDM (zapisywanie pojedynczych 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 multimedialne 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, 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 powi-

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.

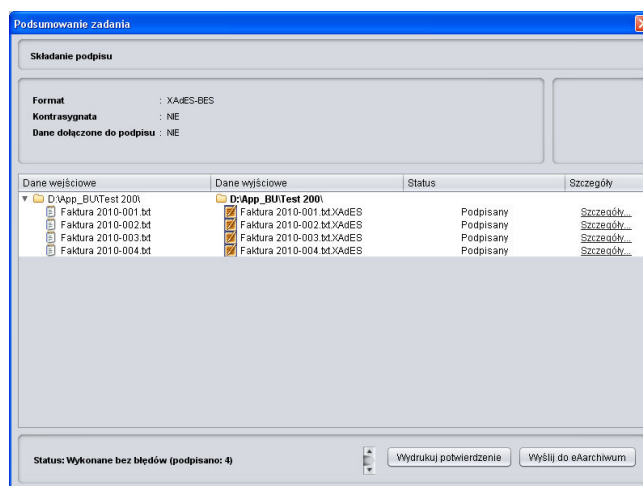
7.3. Wysyłanie plików do eArchiwum

7.3.1. 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.

7.3.2. Wysyłanie plików do eArchiwum

1. Aby wysłać dokumenty do eArchiwum należy wykonać podpis elektroniczny pod dokumentem lub zweryfikować podpis. Po wykonaniu zadania pojawi się okno podsumowania zadania:

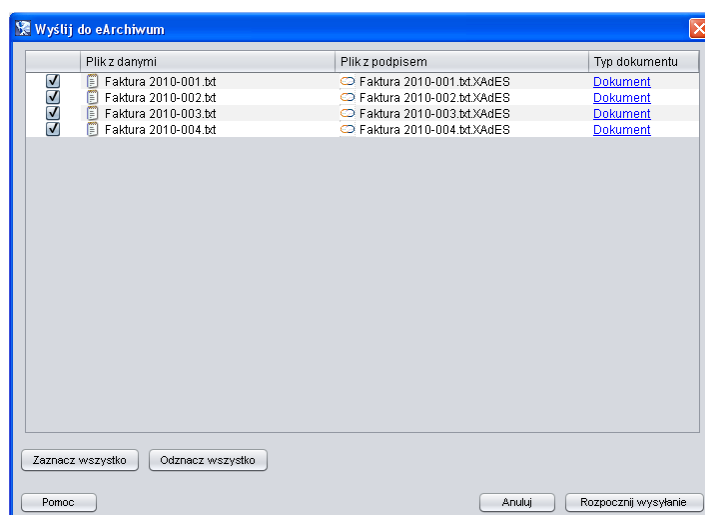


Rysunek 37. Okno podsumowanie zadania z widocznym przyciskiem „Wyślij do eArchiwum”.

² W 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.

Przycisk „Wyślij do eArchiwum” jest widoczny tylko wtedy, kiedy w aktywnej konfiguracji aplikacji zaznaczona została opcja „Włącz obsługę eArchiwum”.

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

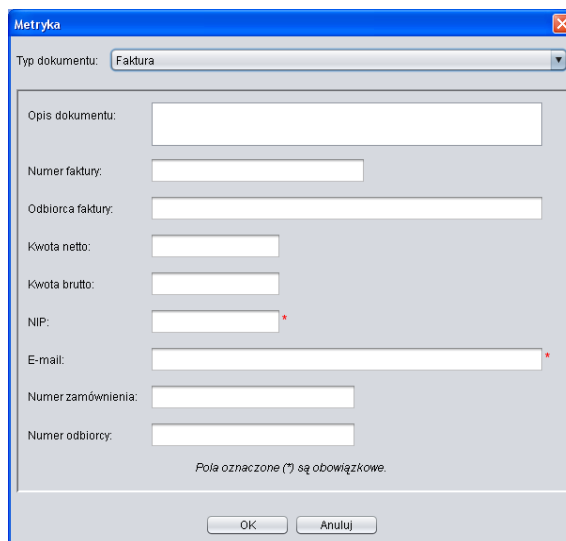


Rysunek 38. Okno „Wyślij do eArchiwum”.

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

- W pierwszej kolumnie 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 podstawowy typ „Dokument”.

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

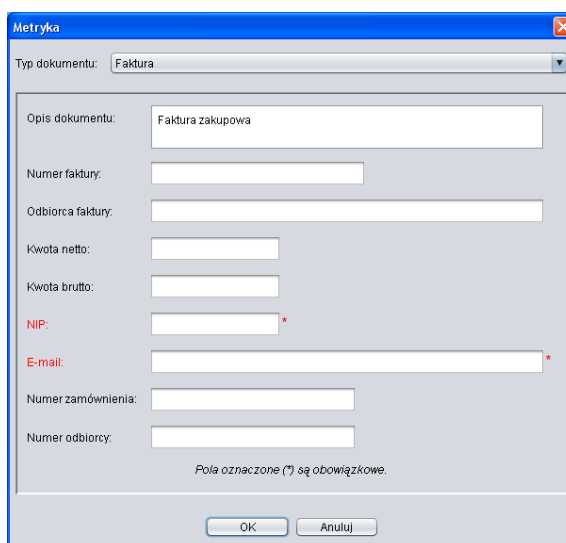


Rysunek 39. Okno edycji metadanych.

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

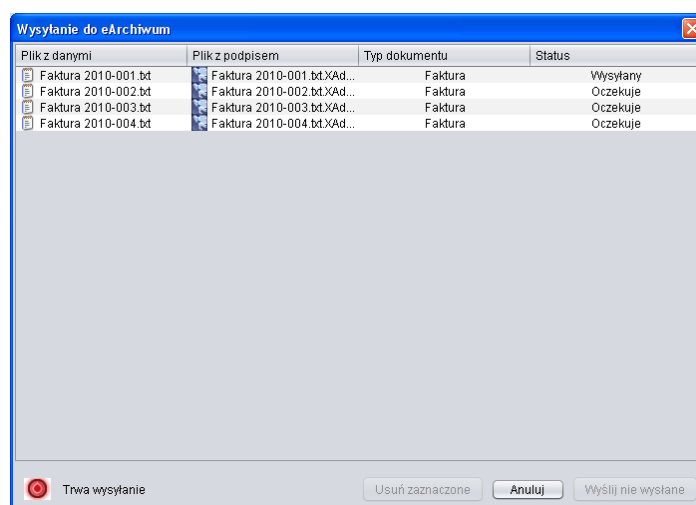
- **Typ dokumentu.** Należy wybrać z rozwijanej listy typ dokumentu.
- **Treść metryki.** Należy wprowadzić w poszczególne pola informacje opisujące dokument.

Po wypełnieniu formularza należy kliknąć na przycisku „OK”. Wprowadzone dane zostaną sprawdzone pod kątem ich zgodności z wymaganiami dla danego typu dokumentu. Pola obowiązkowe, które nie zostały wypełnione lub pola wypełnione błędnie zostaną oznaczone kolorem czerwonym na formularzu.



Rysunek 40. Okno edycji metadanych z niewypełnionymi polami obowiązkowymi.

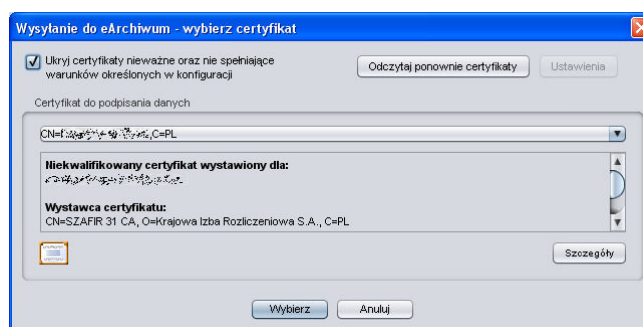
- b) Aby rozpocząć wysyłanie plików do eArchiwum należy kliknąć na przycisku „Rozpocznij wysyłanie”.
3. Po rozpoczęciu wysyłania plików do eArchiwum pojawi się okno „Wysyłanie do eArchiwum”, wysyłanie odbywa się w tle, więc okno można zamknąć i pracować dalej z aplikacją. W każdej chwili okno dostępne jest poprzez menu aplikacji: Okno -> Wysyłanie do eArchiwum.



Rysunek 41. Okno „Wysyłanie do eArchiwum”.

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

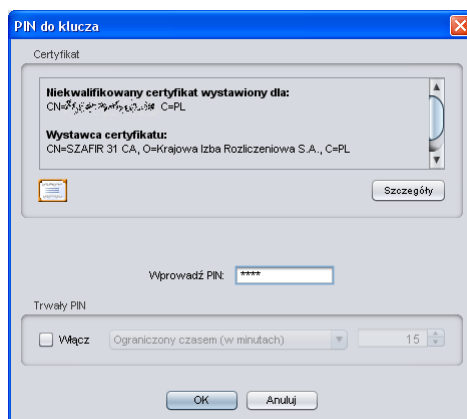
- a) Bezpośrednio po wyświetleniu okna aplikacja rozpoczyna proces wysyłanie dokumentów, zaczynając od uwierzytelnienia w eArchiwum przy użyciu certyfikatu niekwalifikowanego. Pojawi się okno wyboru certyfikatu³:



Rysunek 42. Okno wyboru certyfikatu.

³ Certyfikat, który ma być używany podczas uwierzytelnienia można wskazać w konfiguracji aplikacji.

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



Rysunek 43. Okno wyboru certyfikatu.

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

8. Instalacja i konfiguracja

8.1. Minimalne wymagania

Do poprawnej pracy aplikacja SZAFIR wymaga komputera klasy IBM PC pracującego pod kontrolą systemu operacyjnego Microsoft Windows 2000 SP4 lub nowszego, na którym zainstalowane jest środowisko Java w wersji 1.6 update 10 lub nowsze, przy czym:

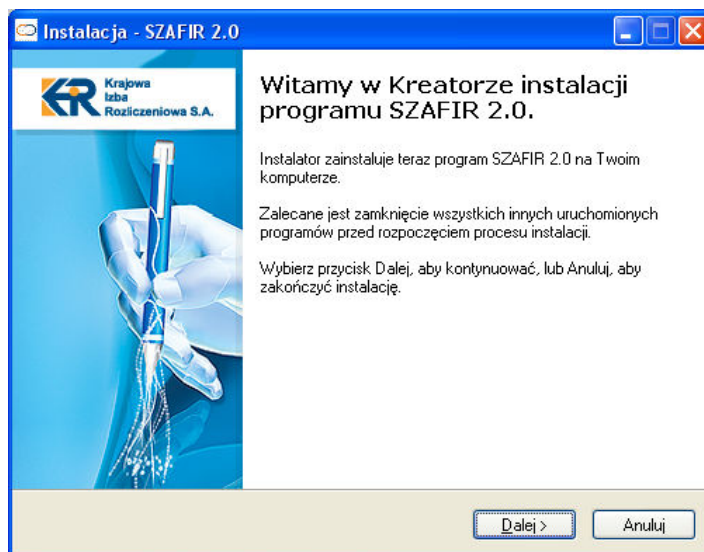
- Wykorzystanie funkcji weryfikacji podpisu wymaga, by komputer wyposażony był w połączenie z siecią Internet, w celu pobrania list certyfikatów unieważnionych i zawieszonych,
- Wykorzystanie funkcji składania podpisu oraz znakowania czasem przy użyciu certyfikatów przechowywanych na kartach kryptograficznych 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.⁴ W wersji 2.0 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
cryptoCertum3PKCS11.dll	Unizeto	Unizeto, część kwalifikowana	Microsoft Windows

⁴ 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.

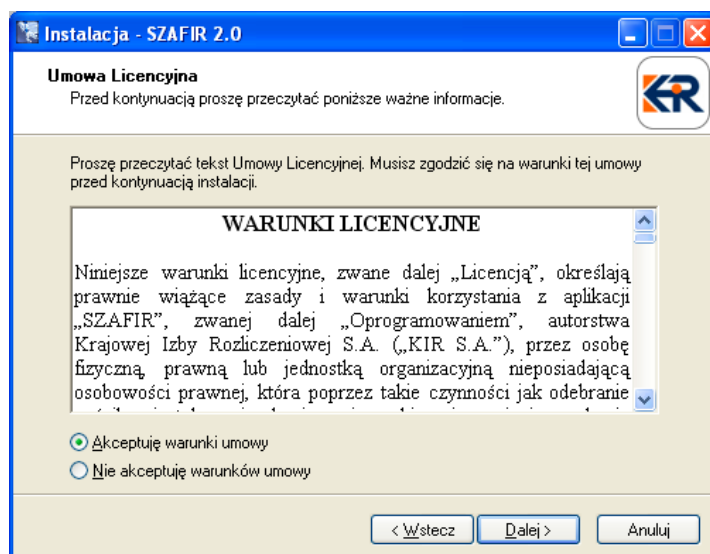
8.2. Instalacja

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



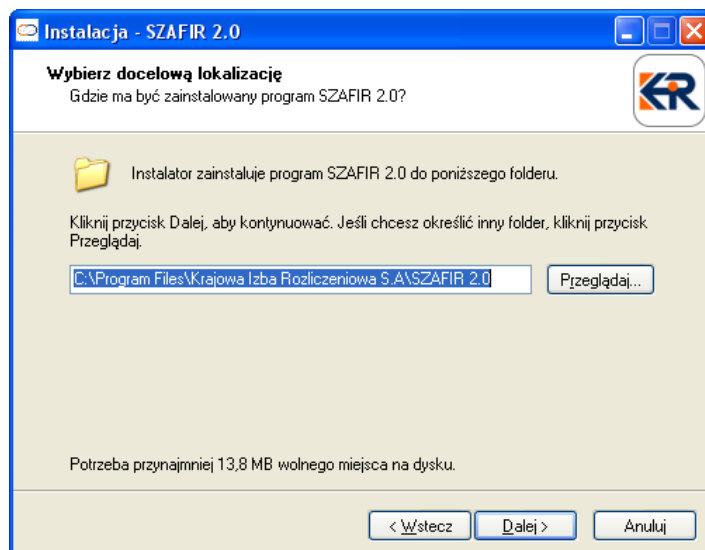
Rysunek 44. Kreator instalacji aplikacji – ekran powitalny.

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



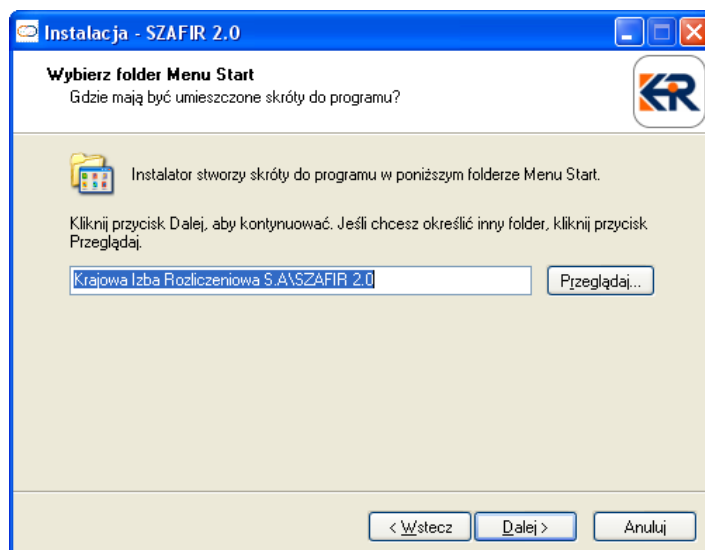
Rysunek 45. Kreator instalacji aplikacji – umowa licencyjna.

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 46. Kreator instalacji aplikacji – wybór docelowej lokalizacji.

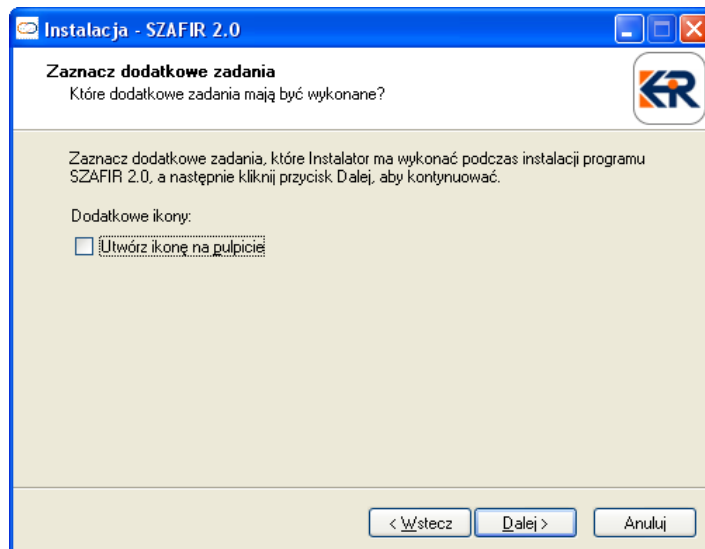
4. W celu kontynuowania instalacji należy kliknąć w przycisk „Dalej”. Pojawi się okno „Wybierz folder Menu Start”:



Rysunek 47. Kreator instalacji aplikacji – wybór folderu Menu Start.

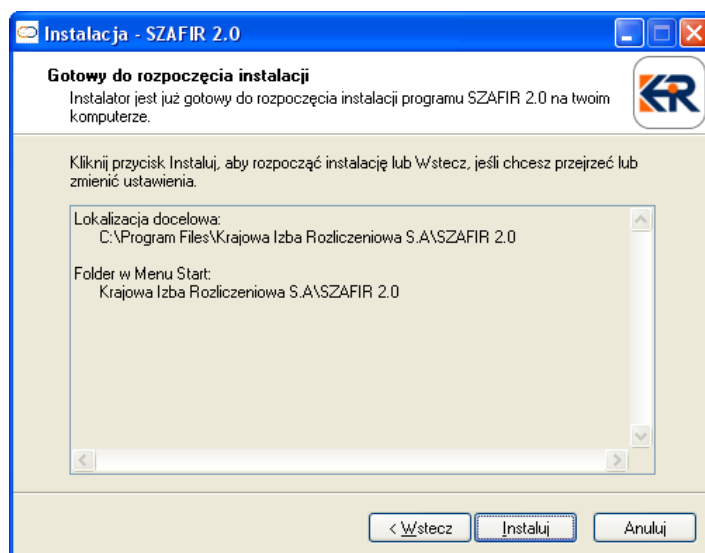
Zaleca się skorzystanie z opcji domyślnie zaproponowanych przez program instalacyjny.

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



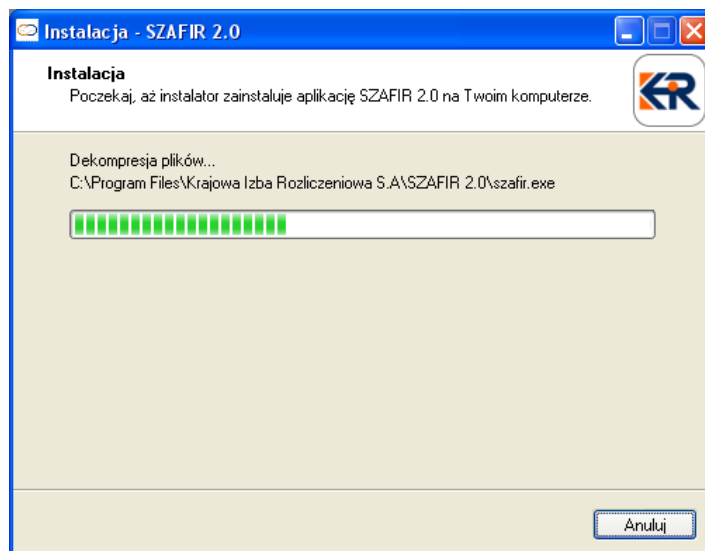
Rysunek 48. Kreator instalacji aplikacji – dodatkowe opcje instalacji.

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



Rysunek 49. Kreator instalacji aplikacji – podsumowanie.

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



Rysunek 50. Kreator instalacji aplikacji – kopiowanie plików.

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



Rysunek 51. Kreator instalacji aplikacji – koniec instalacji.

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

8.3. Uaktualnianie

Domyślnie aplikacja instalowana jest do katalogu zawierającego w nazwie wersję *major* i *minor* aplikacji (np. SZAFIR 2.0)⁵. 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.

8.4. 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).

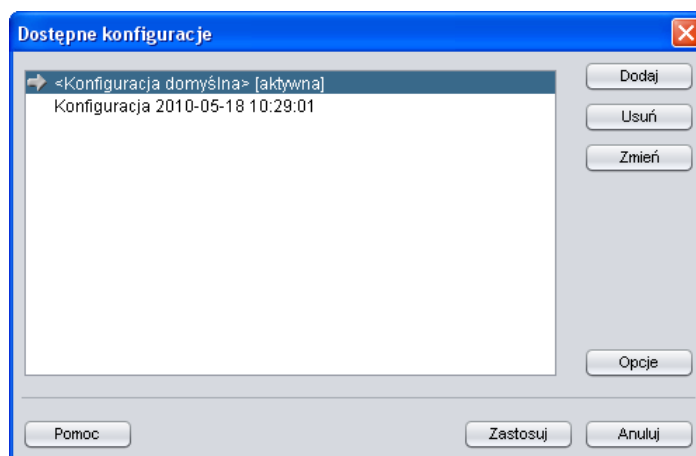
Użytkownik może zmieniać oba rodzaje konfiguracji z tym, że w przypadku konfiguracji dodatkowej nie jest konieczne definiowanie zawartości wszystkich opcji: na poszczególnych zakładkach okna edycji konfiguracji można zaznaczyć opcję „Użyj konfiguracji domyślnej” i wówczas ustawienia, których ta opcja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

⁵ Więcej o numerowaniu wersji aplikacji można przeczytać w rozdziale 9.1. „Numeracja wersji aplikacji”.

Użytkownik naciskając przycisk „konfiguracja” na ekranie głównym lub wybierając z menu opcję Narzędzia -> Konfiguracja 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 konfiguracje, oraz – przy pomocy przycisku "Zastosuj" – decydować która konfiguracja będzie aktywna, czyli używana w czasie pracy aplikacji.

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

8.4.1. Okno dostępnych konfiguracji



Rysunek 52. 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, która konfiguracja będzie aktywna. Aktywna konfiguracja oznaczona jest ikoną strzałki z lewej strony nazwy oraz etykietą [aktywna] z prawej.

- **Lista dostępnych konfiguracji.** Lista zdefiniowanych przez użytkownika możliwych 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. Zarządzanie konfiguracją można ograniczyć poprzez określenie hasła administratora aplikacji oraz, opcjonalnie poprzez ustawienie ograniczeń w zapisywaniu i dokonywaniu zmian w aktywnej konfiguracji.
- **Zastosuj.** Należy użyć tego przycisku, aby ustawić daną konfigurację jako aktywną.
- **Anuluj.** Należy użyć tego przycisku aby zamknąć okno dostępnych konfiguracji nie dokonując zmian.

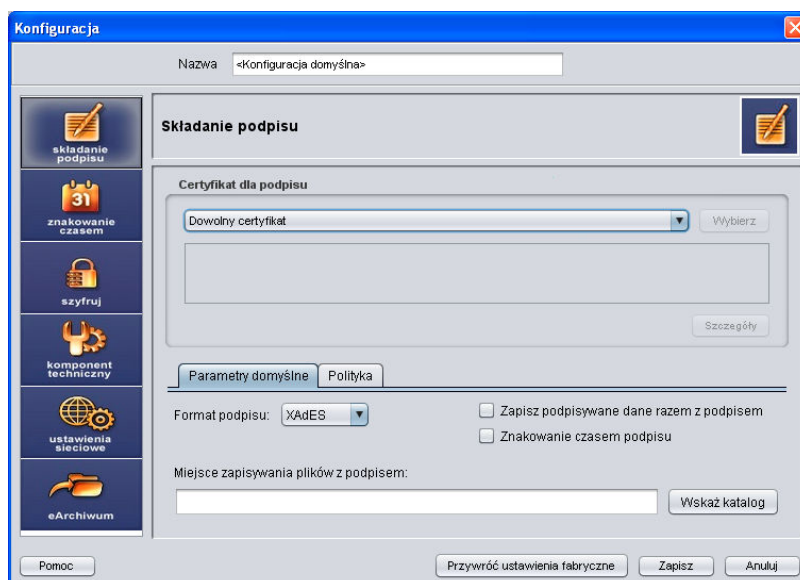
8.4.2. Okno edycji konfiguracji

To okno pozwala na zmianę wybranej konfiguracji aplikacji.

- **Nazwa konfiguracji.** Należy wprowadzić przyjazną nazwę, która będzie używana w odniesieniu do tej konfiguracji (konfiguracja domyślna ma stałą nazwę).

8.4.2.1. Składanie podpisu

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



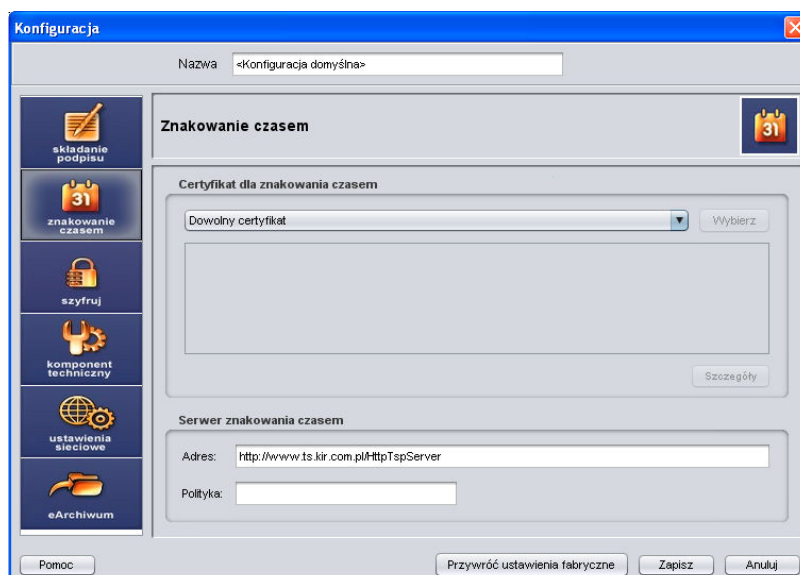
Rysunek 53. Okno edycyjne konfiguracji – zakładka: składanie podpisu.

- **Certyfikat dla 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 kwalifikowany certyfikat.** Należy wybrać tę opcję aby zezwolić na składanie podpisu przy użyciu dowolnego certyfikatu kwalifikowanego.
- **Dowolny niekwalifikowany certyfikat.** 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.
- **Parametry domyślne.** Korzystając z tej grupy parametrów użytkownik może ustawić domyślne parametry dla procesu podpisywania.
- **Polityka.** W tym miejscu można określić politykę zgodnie z którą składany jest podpis elektroniczny w formacie XAdES.
 - **Identyfikator polityki.** Należy wpisać identyfikator polityki składania podpisu.
 - **Plik polityki (skrót).** Należy wskazać plik zawierający politykę składania podpisu elektronicznego, aplikacja policzy z niego skrót, który wraz z identyfikatorem będzie dołączany do każdego wykonanego podpisu elektronicznego (XAdES).

8.4.2.2. Znakowanie czasem

W tej sekcji znajdują się ustawienia związane ze znakowaniem czasem.



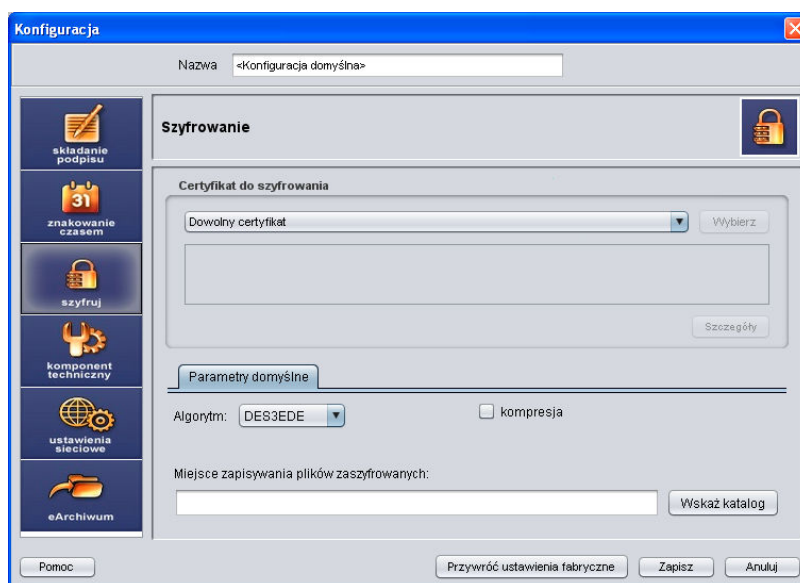
Rysunek 54. Okno edycyjne konfiguracji – zakładka: znakowanie czasem.

- **Certyfikat dla 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 kwalifikowany certyfikat.** Należy wybrać tę opcję aby zezwolić na znakowanie czasem przy użyciu dowolnego certyfikatu kwalifikowanego.
 - **Dowolny niekwalifikowany certyfikat.** 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.

8.4.2.3. Szyfrowanie

Ta sekcja zawiera domyślne parametry dla procesu szyfrowania.

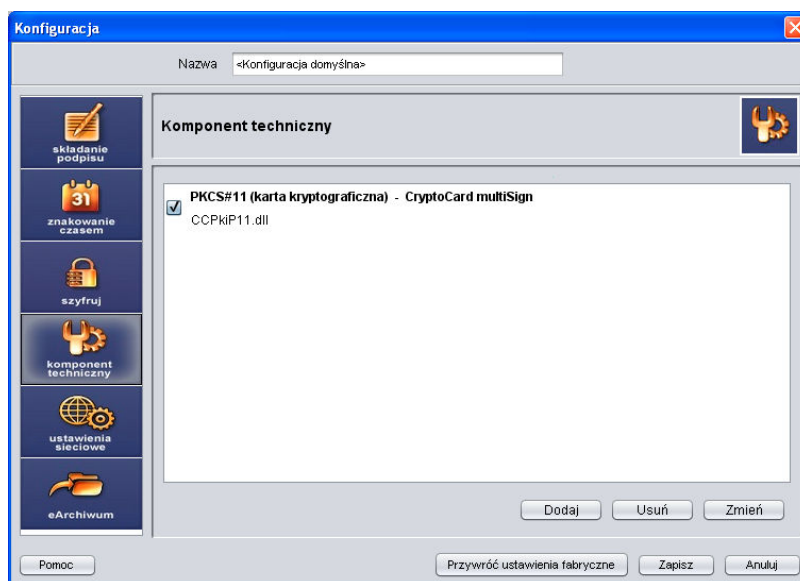


Rysunek 55. Okno edycyjne konfiguracji – zakładka: szyfruj.

- **Certyfikat do szyfrowania.** Korzystając z tego pola można określić konkretny certyfikat, który przy szyfrowaniu automatycznie zostanie dodany do listy certyfikatów wybranych. Przyciskiem Wybierz można wskazać jeden certyfikat z listy certyfikatów dostępnych w magazynie certyfikatów.
- **Parametry domyślne.** W tej części użytkownik może ustawić domyślne parametry dla procesu szyfrowania.

8.4.2.4. 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.



Rysunek 56. Okno edycyjne konfiguracji – zakładka: komponent techniczny.

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.

Dodawanie lub zmiana definicji dostawcy kryptograficznego

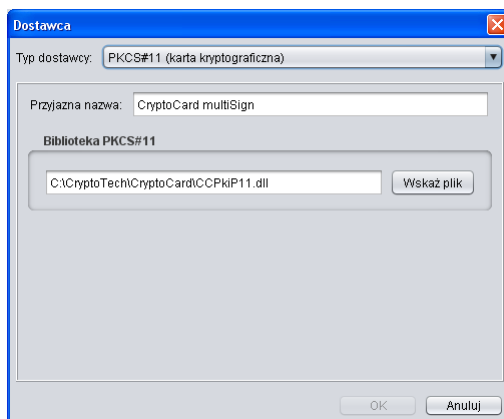
Dodawanie lub zmiana definicji dostawcy kryptograficznego odbywa się w oknie wyświetlanym po przyciśnięciu, odpowiednio, przycisków „Dodaj” oraz „Zmień” w zakładce „Komponent techniczny” okna edycji konfiguracji.

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#12 (plik)

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

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



Rysunek 57. Okno „Dostawca” dla typu dostawcy: PKCS#11 (karta kryptograficzna).

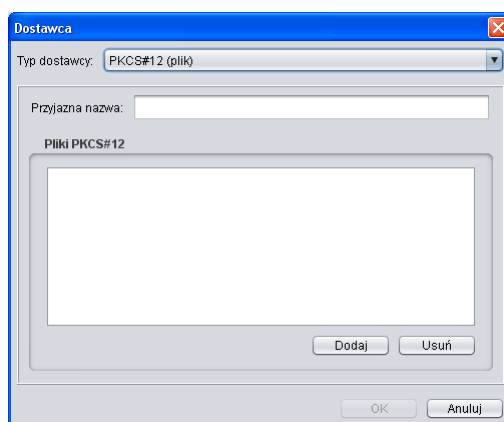
Dla typu dostawcy „PKCS#11 (karta kryptograficzna)” dostępne są następujące opcje:

- **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 kryptogra-

ficznych. Informacja o bibliotekach PKCS#11, których użycie zostało przetestowane z aplikacją, znajdują się w rozdziale „Minimalne wymagania”..

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.



Rysunek 58. Okno „Dostawca” dla typu dostawcy: PKCS#12 (plik).

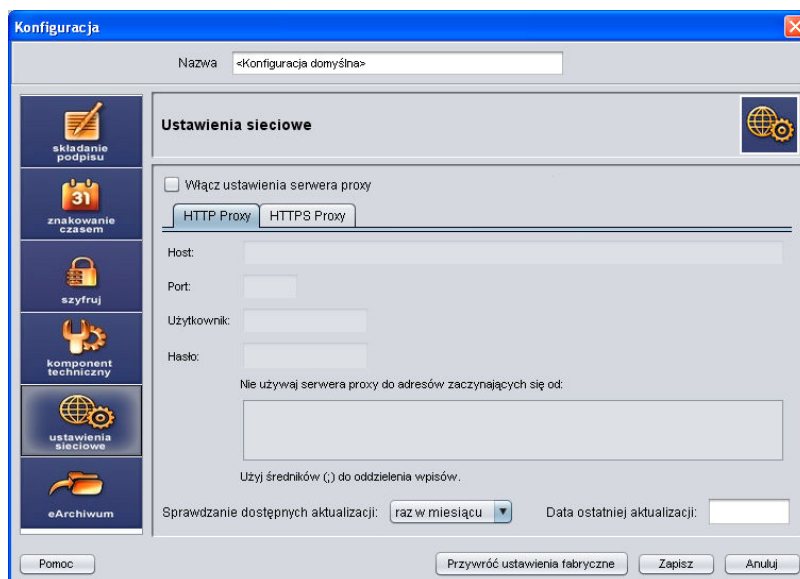
Dla typu dostawcy „PKCS#12 (plik)” dostępne są następujące opcje:

- **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.

8.4.2.5. 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.

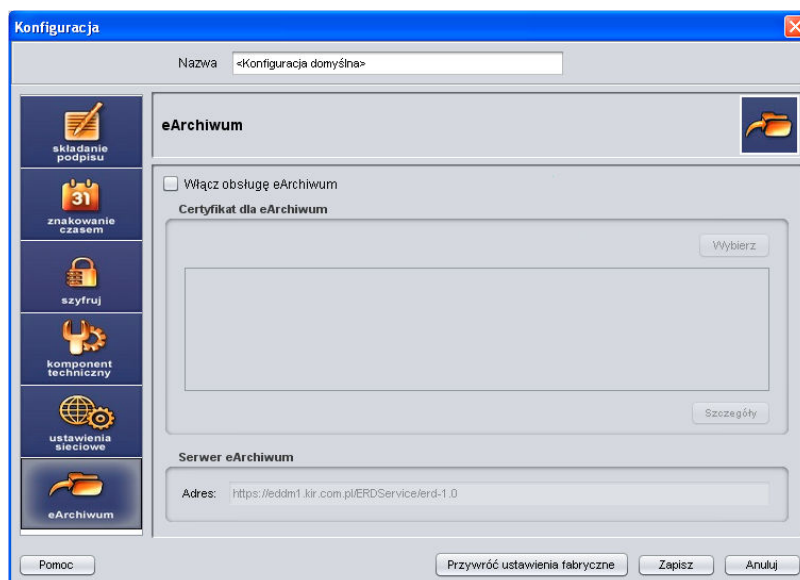


Rysunek 59. Okno edycyjne konfiguracji – zakładka: ustawienia sieciowe.

- **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 opcję „Włącz ustawienia serwera proxy” odznaczoną.
 - **Host.** Należy wpisać nazwę lub adres IP serwera proxy.
 - **Port.** Należy wpisać numer portu, pod którym dostępny jest serwer proxy.
 - **Użytkownik.** Jeżeli wymaga tego serwer proxy, należy wpisać nazwę użytkownika, wymaganego podczas nawiązywania połączenia z serwerem proxy.
 - **Hasło.** Jeżeli wymaga tego serwer proxy, należy wpisać hasło, wymagane 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.
- **Sprawdzanie dostępnych aktualizacji.** Aplikacja SZAFIR jest wyposażona w możliwość automatycznego wyszukiwania, pobierania i instalowania nowych wersji aplikacji. Opcja ta pozwala określić czy i jak często aplikacja ma sprawdzać dostępność nowej wersji.

8.4.2.6. eArchiwum

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

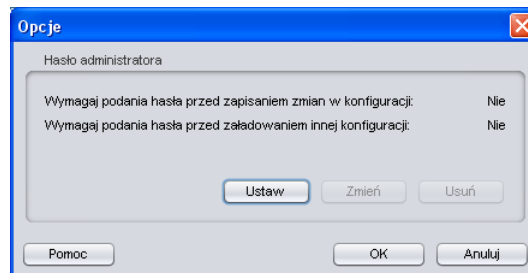


Rysunek 60. Okno edycyjne konfiguracji – zakładka: eArchiwum.

- **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. Po zainstalowaniu aplikacji adres serwera eArchiwum domyślnie wskazuje na serwer eArchiwum w KIR S.A. Dopuszcza się podanie w polu „adres” ścieżki lokalnego katalogu, ale należy zachować następujący format: `file:/C:\Katalog\Podkatalog\` (ścieżka do katalogu poprzedzona musi być wpisem „file:/”). W przypadku podania ścieżki do lokalnego katalogu, zostaną w nim zapisane paczki danych (w postaci plików ZIP) dokładnie takie, jakie zostałyby wysłane do serwera eArchiwum.

8.4.3. Okno opcji zabezpieczeń

To okno wyświetla aktualnie wybrane opcje zabezpieczeń aplikacji.



Rysunek 61. Okno opcji zabezpieczeń.

- **Opcje zabezpieczeń.**

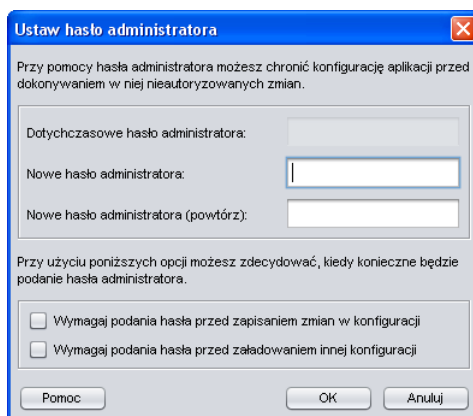
- **Wymagaj podania hasła przed zapisaniem zmian w konfiguracji.** Jeżeli ta opcja została uaktywniona, wówczas przed zapisaniem zmian w konfiguracji aplikacji wymagane jest podanie hasła administratora aplikacji.
- **Wymagaj podania hasła przed zastosowaniem innej konfiguracji.** Jeżeli ta opcja została 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.

8.4.4. Okno ustawiania hasła administratora

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



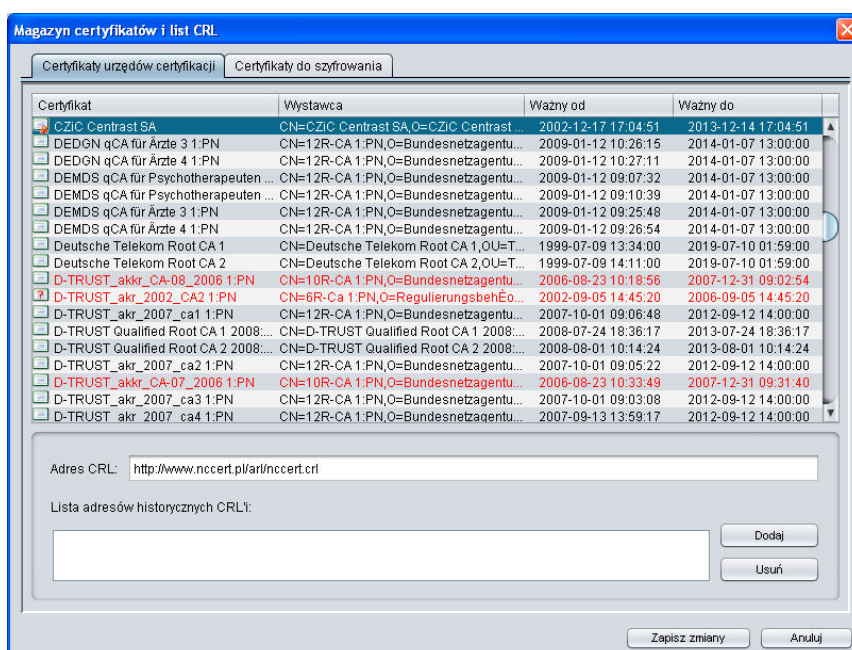
Rysunek 62. Okno ustawiania hasła administratora.

- **Hasło administratora.** Korzystając z pól w tej sekcji można zmienić hasło administratora.
 - **Dotychczasowe hasło administratora.** Jeżeli hasło administratora było ustawione wcześniej, 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 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 przez zastosowaniem innej konfiguracji.** Należy zaznaczyć tę opcję aby zapobiec używaniu konfiguracji innych niż aktualna przez użytkowników nie znających hasła administratora.

8.5. Magazyn certyfikatów i list CRL

Magazyn certyfikatów i list CRL w aplikacji SZAFIR to miejsce, w którym użytkownik może zobaczyć listę certyfikatów CA (urzędów certyfikacji) znanych aplikacji oraz dodać certyfikaty, które będą używane w procesie szyfrowania. Podstawowe okno magazynu certyfikatów posiada dwie zakładki. Pierwsza prezentuje certyfikaty CA, ich wystawców oraz okresy ważności (kolorem czerwonym prezentowane są certyfikaty, których ważność już upłynęła).

Okno to możemy wyświetlić wybierając z menu opcję „Narzędzia -> Magazyn certyfikatów i list CRL”.



Rysunek 63. Okno magazynu certyfikatów – zakładka „Certyfikaty urzędów certyfikacji”.

Szczegółowe informacje dotyczące konkretnego certyfikatu użytkownik może zobaczyć klikając dwa razy na liście w wybrany certyfikat.

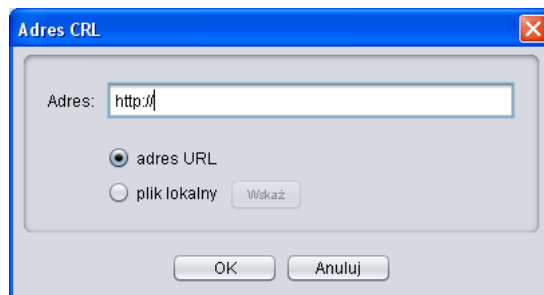
Pod listą certyfikatów znajdują się informacje o listach CRL dla wybranego certyfikatu CA. Pole „Adres CRL” zawiera informacje pod jakim adresem publikowana jest bieżąca lista CRL, natomiast „Lista adresów historycznych CRL” zawiera zbiór adresów sieciowych lub lokalizacji na dysku lokalnym do historycznych list CRL.

Historyczne listy CRL potrzebne są do poprawnej weryfikacji podpisów, złożonych przy użyciu certyfikatów, które w czasie weryfikacji nie są już ważne i bieżąca publikowana lista CRL dla danego urzędu certyfikacji nie zawiera już informacji o tych certyfikatach.

Aplikacja nie pozwala użytkownikowi modyfikować listy certyfikatów CA, a jedynie dodawać adresy dla historycznych list CRL. Dodawanie lub usuwanie pozycji z listy adresów hi-

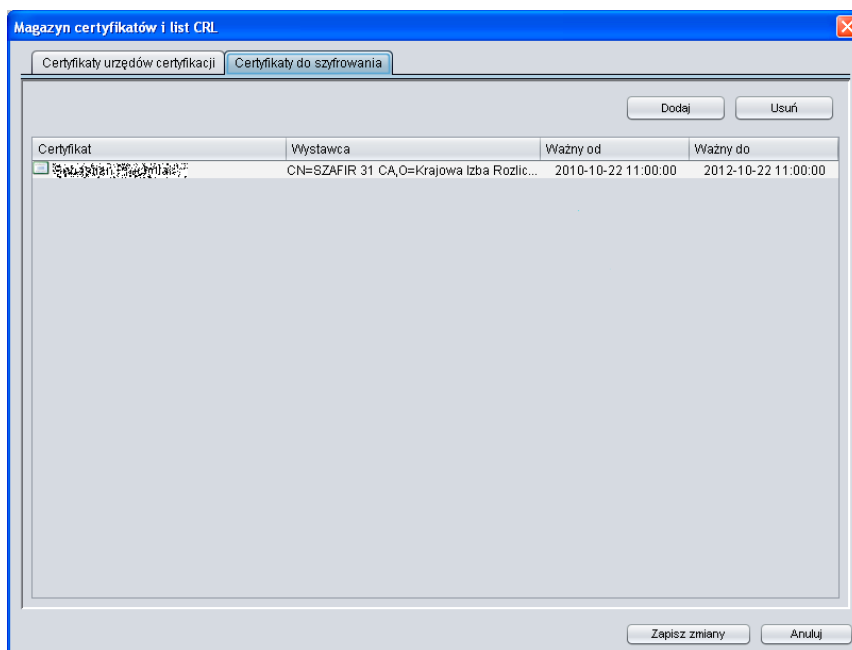
historycznych CRL'i użytkownik może wykonać przy użyciu przycisków „Dodaj” lub „Usuń” umieszczonych z boku listy.

Po wybraniu opcji „Dodaj” ukaże się okno w którym użytkownik może wprowadzić adres URL lub wskazać plik na dysku zawierający historyczną listę CRL.



Rysunek 64. Okno definiowania adresu listy CRL.

Druga zakładka „Certyfikaty do szyfrowania” zawiera certyfikaty dodane przez użytkownika dla procesu szyfrowania. Przy szyfrowaniu lista certyfikatów do wyboru zawiera tylko certyfikaty umieszczone w tej zakładce.



Rysunek 65. Okno magazynu certyfikatów – zakładka „Certyfikaty do szyfrowania”.

Wszystkie wprowadzone zmiany w magazynie certyfikatów użytkownik zatwierdza przyciskiem „Zapisz zmiany” lub odrzuca przyciskiem „Anuluj”.

9. Informacje dodatkowe

9.1. Numeracja wersji aplikacji

W miarę rozwijania programu oraz poprawiania ewentualnych błędów i usterek występujących w programie Krajowa Izba Rozliczeniowa S.A. publikuje 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 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 <i>release</i>	
		numer <i>minor</i>		
	numer <i>major</i>			
nazwa aplikacji				

Uchwała Nr XXXV/270/2014
Rady Powiatu Ropczycko-Sędziszowskiego
z dnia 14 listopada 2014 r.

w sprawie: zmian w budżecie powiatu na 2014 rok.

Na podstawie art. 211, art. 212 ust.1 i 2, art. 214, 215, 219 ust.3, art.222 ust. 1 i 2, art. 235 ust.1, art.236, ust.1, 2 i 4, art. 237, art.264 ust.3 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (j.t. Dz.U. z 2013 Nr 885 z późn. zm.) oraz *art. 12 pkt 5, pkt 9 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym* (j.t. Dz.U. z 2013 Nr 595 z późn. zm.) – Rada Powiatu uchwala, co następuje:

§ 1.1. Zwiększa się dochody budżetu powiatu na 2014 rok o kwotę 1.017.826.80 zł ,w tym:

1) dochody bieżące: 872.826,80 zł;

2) dochody majątkowe: 145.000,00 zł.

2. Zwiększenia planu dochodów budżetu powiatu przedstawia się następująco:

Dział	Nazwa działu	Źródła dochodów	Kwota
600	Transport i łączność, w tym : -dochody bieżące, w tym: -dochody majątkowe, w tym:	-środki na dofinansowanie zadań bieżących pozyskane z innych źródeł -dotacje z budżetów innych jednostek samorządu terytorialnego uzyskane na podstawie porozumień -dotacje celowe przekazane z budżetu państwa na realizację inwestycji i zakupów inwestycyjnych własnych powiatu	95.000,00,- 15.000,00,- 15.000,00,- 80.000,00,- 16.000,00,- 64.000,00,-
700	Gospodarka mieszkaniowa, w tym : -dochody bieżące, w tym:	-wpływy z dzierżawy	18.500,00,- 18.500,00,- 18.500,00,-
710	Działalność usługowa w tym: -dochody bieżące, w tym:	-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	4.963,00,- 4.963,00,- 4.963,00,-
754	Bezpieczeństwo publiczne i ochrona przeciwpożarowa, w tym :		75.039,00,-

Dział	Nazwa działu	Źródła dochodów	Kwota
	-dochody bieżące, w tym:	-dochody uzyskiwane przez powiatowe jednostki budżetowe powiatu	10.039,00,- 5.500,00,-
		-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	4.539,00,-
	-dochody majątkowe, w tym:	-dotacje celowe z budżetu państwa na inwestycje i zakupy inwestycyjne z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	65.000,00,- 65.000,00,-
758	Różne rozliczenia, w tym: -dochody bieżące, w tym:	-część oświatowa subwencji ogólnej dla jednostek samorządu terytorialnego	310.000,00,- 310.000,00,- 10.000,00,-
		-dochody uzyskiwane przez powiatowe jednostki budżetowe powiatu	300.000,00,-
801	Oświata i wychowanie, w tym: -dochody bieżące, w tym:	-dochody uzyskiwane przez powiatowe jednostki budżetowe powiatu	126.434,80,- 126.434,80,- 26.700,00,-
		- dotacje celowe w ramach programów finansowanych z udziałem środków europejskich, w tym:	99.734,80,-
		-środki pochodzące z budżetu Unii Europejskiej	99.734,80,-
852	Pomoc społeczna , w tym : -dochody bieżące, w tym:	-dotacje celowe z budżetu państwa na finansowanie lub dofinansowanie zadań własnych	312.890,00,- 312.890,00,- 176.570,00,-
		-dochody uzyskiwane przez powiatowe jednostki budżetowe powiatu	104.500,00,-

Dział	Nazwa działu	Źródła dochodów	Kwota
		-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	31.820,00,-
853	Pozostałe zadania w zakresie polityki społecznej, w tym: -dochody bieżące, w tym:	-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami -dochody uzyskiwane przez powiatowe jednostki budżetowe powiatu	75.000,00,- 75.000,00,- 10.000,00,- 65.000,00,-
Ogółem zwiększenie planu dochodów			1.017.826,80,-

§ 2. Zwiększa się wydatki budżetu powiatu na 2014 rok o kwotę 1.017.826,80 zł, w tym:

1. Zwiększenie planu wydatków bieżących na łączną kwotę 772.826,80 zł, w tym:

1) wydatki bieżące jednostek budżetowych w kwocie łącznej – 690.606,80 zł, z czego:

a) wydatki na wynagrodzenia i składki od nich naliczane – 332.390,00 zł;

b) wydatki związane z realizacją zadań statutowych jednostek budżetowych – 358.216,80 zł;

2) dotacje – 82.220,00 zł.

2. Wydatki majątkowe 245.000,00 zł, w tym:

a) wydatki na inwestycje i zakupy inwestycyjne w kwocie 245.000,00 zł.

3. Zwiększenie planu wydatków budżetu powiatu przedstawia się następująco:

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
600		Transport i łączność	195.000,00,-
	60014	Drogi publiczne powiatowe, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: - wydatki związane z realizacją ich statutowych zadań b) wydatki majątkowe, w tym: - inwestycje i zakupy inwestycyjne	195.000,00,- 15.000,00,- 15.000,00,- 15.000,00,- 180.000,00,- 180.000,00,-
710		Działalność usługowa	4.963,00,-
	71015	Nadzór budowlany, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: - wynagrodzenia i składki od nich naliczane	4.963,00,- 4.963,00,- 4.963,00,- 4.963,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
754		Bezpieczeństwo publiczne i ochrona przeciwpożarowa	75.039,00,-
	75411	Komendy powiatowe Państwowej Straży Pożarnej, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane b)wydatki majątkowe, w tym: 1)inwestycje i zakupy inwestycyjne	70.500,00,- 5.500,00,- 5.500,00,- 5.500,00,- 65.000,00,- 65.000,00,-
	75478	Usuwanie skutków klęsk żywiołowych, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	4.539,00,- 4.539,00,- 4.539,00,- 4.539,00,-
801		Oświata i wychowanie	291.934,80,-
	80120	Licea ogólnokształcące, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	21.000,00,- 21.000,00,- 21.000,00,- 21.000,00,-
	80130	Szkoły zawodowe, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań	165.200,00,- 165.200,00,- 165.200,00,- 53.000,00,- 112.200,00,-
	80195	Pozostała działalność, z tego : a)wydatki bieżące, w tym: 1)wydatki na programy finansowane ze środków pochodzących z budżetu Unii Europejskiej, w tym: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań,	105.734,80,- 105.734,80,- 105.734,80,- 6.688,00,- 99.046,80,-
851		Ochrona zdrowia	50.000,00,-
	85121	Lecznictwo ambulatoryjne, z tego : a) wydatki bieżące, w tym: 1) dotacje na zadania bieżące (dotacja celowa na dofinansowanie wydatków bieżących dla ZOZ Ropczyce - dotacja podmiotowa dla jednostek sektora finansów publicznych)	50.000,00,- 50.000,00,- 50.000,00,-
852		Pomoc społeczna	315.890,00,-
	85202	Domy pomocy społecznej, z tego : a)wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	276.770,00,- 276.770,00,- 276.770,00,- 163.300,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
		-wydatki związane z realizacją ich statutowych zadań	113.470,00,-
	85203	Ośrodki wsparcia, z tego : a) wydatki bieżące, w tym: 1) dotacje na zadania bieżące (dofinansowanie zadań zleconych do realizacji organizacjom pozarządowym – dotacja celowa dla Polskiego Stowarzyszenia Na Rzecz Osób z Upośledzeniem Umysłowym w Sędziszowie Młp.)	31.820,00,- 31.820,00,- 31.820,00,-
	85204	Rodziny zastępcze, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: - wydatki związane z realizacją ich statutowych zadań 2) dotacje na zadania bieżące dotacja celowa jednostek sektora finansów publicznych, w ramach porozumień między jednostkami samorządu terytorialnego na utrzymanie dzieci z terenu powiatu w rodzinach zastępczych	4.900,00,- 4.900,00,- 4.500,00,- 4.500,00,- 400,00,-
	85218	Powiatowe centra pomocy rodzinie, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: - wynagrodzenia i składki od nich naliczane	2.400,00,- 2.400,00,- 2.400,00,- 2.400,00,-
853		Pozostałe zadania w zakresie polityki społecznej	75.000,00,-
	85321	Zespoły ds. orzekania o niepełnosprawności, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: - wynagrodzenia i składki od nich naliczane - wydatki związane z realizacją ich statutowych zadań	10.000,00,- 10.000,00,- 10.000,00,- 6.000,00,- 4.000,00,-
	85333	Powiatowe urzędy pracy, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: - wynagrodzenia i składki od nich naliczane	65.000,00,- 65.000,00,- 65.000,00,- 65.000,00,-
854		Edukacyjna opieka wychowawcza	10.000,00,-
	85406	Poradnie psychologiczno-pedagogiczne oraz inne poradnie specjalistyczne, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: - wydatki związane z realizacją ich statutowych zadań	10.000,00,- 10.000,00,- 10.000,00,- 10.000,00,-
Ogółem zwiększony plan wydatków			1.017.826,80,-

§ 3.1. Zmniejsza się dochody budżetu powiatu na 2014 rok o kwotę 85.809,00 zł ,w tym:

1) dochody bieżące: 85.039,00 zł;

2) dochody majątkowe: 770,00 zł.

2. Zmniejszenia planu dochodów budżetu powiatu przedstawia się następująco:

Dział	Nazwa działu	Źródła dochodów	Kwota
600	Transport i łączność, w tym : -dochody majątkowe, w tym:	-dotacje celowe przekazane z budżetu państwa na realizację inwestycji i zakupów inwestycyjnych własnych powiatu	770,00,- 770,00,- 770,00,-
754	Bezpieczeństwo publiczne i ochrona przeciwpożarowa, w tym : -dochody bieżące, w tym:	-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	65.000,00,- 65.000,00,- 65.000,00,-
852	Pomoc społeczna , w tym : -dochody bieżące, w tym:	-dotacje celowe z budżetu państwa na finansowanie lub dofinansowanie zadań własnych	20.039,00,- 20.039,00,- 20.039,00,-
Ogółem zmniejszenie planu dochodów			85.809,00,-

§ 4.1. Zmniejsza się wydatki budżetu powiatu na 2014 rok o kwotę 85.809,00 zł ,w tym:

1. Zmniejszenie planu wydatków bieżących na łączną kwotę 85.039,00 zł, w tym:

1) wydatki bieżące jednostek budżetowych w kwocie łącznej – 85.039,00 zł, z czego:

a) wynagrodzenia i składki od nich naliczane – 85.039,00 zł,

2. Wydatki budżetu obejmują plan wydatków majątkowych na łączną kwotę 770,00 zł, w tym:

1) wydatki na inwestycje i zakupy inwestycyjne w kwocie – 770,00 zł.

2. Zmniejszenie planu wydatków budżetu powiatu przedstawia się następująco:

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
600		Transport i łączność	770,00,-
	60014	Drogi publiczne powiatowe, z tego : a) wydatki majątkowe, w tym: - inwestycje i zakupy inwestycyjne	770,00,- 770,00,- 770,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
754		Bezpieczeństwo publiczne i ochrona przeciwpożarowa	65.000,00,-
	75411	Komendy powiatowe Państwowej Straży Pożarnej z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym: -wynagrodzenia i składki od nich naliczane	65.000,00,- 65.000,00,- 65.000,00,-
852		Pomoc społeczna	20.039,00,-
	85202	Domy pomocy społecznej, z tego : a)wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	20.039,00,- 20.039,00,- 20.039,00,- 20.039,00,-
Ogółem zmniejszony plan wydatków			85.809,00,-

§ 5. Dokonuje się przeniesienia planowanych wydatków budżetowych według poniższego zestawienia:

Wydatki zmniejszenia

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
600		Transport i łączność	538.000,00,-
	60014	Drogi publiczne powiatowe, z tego : a)wydatki majątkowe, w tym: - inwestycje i zakupy inwestycyjne	500.000,00,- 500.000,00,- 500.000,00,-
	60078	Usuwanie skutków klęsk żywiołowych, z tego : a)wydatki majątkowe, w tym: - inwestycje i zakupy inwestycyjne	38.000,00,- 38.000,00,- 38.000,00,-
700		Gospodarka mieszkaniowa	15.235,00,-
	70005	Gospodarka gruntami i nieruchomościami, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	15.235,00,- 15.235,00,- 15.235,00,- 15.235,00,-
710		Działalność usługowa	110.000,00,-
	71012	Ośrodki dokumentacji geodezyjnej i kartograficznej, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	40.000,00,- 40.000,00,- 40.000,00,- 40.000,00,-
	71013	Prace geodezyjne i kartograficzne (nieinwestycyjne), z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	70.000,00,- 70.000,00,- 70.000,00,- 70.000,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
754		Bezpieczeństwo publiczne i ochrona przeciwpożarowa	54.061,75,-
	75411	Komendy powiatowe Państwowej Straży Pożarnej z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane 2)świadczenia na rzecz osób fizycznych	54.061,75,- 54.061,75,- 25.000,00,- 25.000,00,- 29.061,75,-
801		Oświata i wychowanie	452.937,09,-
	80120	Licea ogólnokształcące, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań 2)dotacje na zadania bieżące 3)świadczenia na rzecz osób fizycznych	132.434,10,- 132.434,10,- 120.150,00,- 120.150,00,- 10.803,00,- 1.481,10,-
	80111	Gimnazja specjalne, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	36.000,00,- 36.000,00,- 36.000,00,- 36.000,00,-
	80130	Szkoły zawodowe, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań 2)dotacje na zadania bieżące 3)świadczenia na rzecz osób fizycznych	209.347,00,- 209.347,00,- 128.000,00,- 30.000,00,- 98.000,00,- 78.347,00,- 3.000,00,-
	80146	Dokształcanie i doskonalenie nauczycieli, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	15.500,00,- 15.500,00,- 15.500,00,- 15.500,00,-
	80195	Pozostała działalność, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań 2)świadczenia na rzecz osób fizycznych 3)wydatki na programy finansowane ze środków pochodzących z budżetu Unii Europejskiej, w tym: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań, -świadczenia na rzecz osób fizycznych	59.655,99,- 59.655,99,- 1.875,70,- 875,70,- 1.000,00,- 3.137,87,- 54.642,42,- 39.048,83,- 301,20,- 15.292,39,-
851		Ochrona zdrowia	100.000,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
	85141	Ratownictwo medyczne, z tego: a)wydatki majątkowe, w tym: 1)inwestycje i zakupy inwestycyjne	100.000,00,- 100.000,00,- 100.000,00,-
852		Pomoc społeczna	22.400,12,-
	85201	Placówki opiekuńczo-wychowawcze, z tego : a)wydatki bieżące, w tym: 1)świadczenia na rzecz osób fizycznych	5.988,20,- 5.988,20,- 5.988,20,-
	85202	Domy pomocy społecznej, z tego : a)wydatki bieżące, w tym: 1)świadczenia na rzecz osób fizycznych	12.000,00,- 12.000,00,- 12.000,00,-
	85204	Rodziny zastępcze, z tego : a)wydatki bieżące, w tym: 1)świadczenia na rzecz osób fizycznych	811,92,- 811,92,- 811,92,-
	85218	Powiatowe centra pomocy rodzinie, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań 2)wydatki na programy finansowane ze środków pochodzących z budżetu Unii Europejskiej, w tym: -wydatki związane z realizacją ich statutowych zadań	3.600,00,- 3.600,00,- 181,08,- 181,08,- 3.418,92,- 3.418,92,-
853		Pozostałe zadania w zakresie polityki społecznej	20.000,00,-
	85333	Powiatowe urzędy pracy, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	20.000,00,- 20.000,00,- 20.000,00,- 20.000,00,-
854		Edukacyjna opieka wychowawcza	78.000,00,-
	85403	Specjalne ośrodki szkolno-wychowawcze, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań	78.000,00,- 78.000,00,- 78.000,00,- 48.000,00,- 30.000,00,-
900		Gospodarka komunalna i ochrona środowiska	2.000,00,-
	90005	Ochrona powietrza atmosferycznego i klimatu, z tego: a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	2.000,00,- 2.000,00,- 2.000,00,- 2.000,00,-
Ogółem zmniejszony plan wydatków			1.392.633,96,-

Wydatki zwiększenia

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
600		Transport i łączność	538.000,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
	60014	Drogi publiczne powiatowe, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	500.000,00,- 500.000,00,- 500.000,00,- 500.000,00,-
	60078	Usuwanie skutków klęsk żywiołowych, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	38.000,00,- 38.000,00,- 38.000,00,- 38.000,00,-
700		Gospodarka mieszkaniowa	23.235,00,-
	70005	Gospodarka gruntami i nieruchomościami, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	23.235,00,- 23.235,00,- 23.235,00,- 23.235,00,-
710		Działalność usługowa	110.000,00,-
	71012	Ośrodki dokumentacji geodezyjnej i kartograficznej, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane b)wydatki majątkowe, w tym: 1)inwestycje i zakupy inwestycyjne	110.000,00,- 40.000,00,- 40.000,00,- 40.000,00,- 70.000,00,- 70.000,00,-
754		Bezpieczeństwo publiczne i ochrona przeciwpożarowa	54.061,75,-
	75411	Komendy powiatowe Państwowej Straży Pożarnej z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	54.061,75,- 54.061,75,- 54.061,75,- 54.061,75,-
801		Oświata i wychowanie	376.737,09,-
	80102	Szkoły podstawowe specjalne, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	50.000,00,- 50.000,00,- 50.000,00,- 50.000,00,-
	80120	Licea ogólnokształcące, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań	71.481,10,- 71.481,10,- 71.481,10,- 70.000,00,- 1.481,10,-
	80130	Szkoły zawodowe, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na:	118.500,00,- 118.500,00,- 113.500,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
		-wynagrodzenia i składki od nich naliczane 2) świadczenia na rzecz osób fizycznych	113.500,00,- 5.000,00,-
	80134	Szkoły zawodowe specjalne, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	34.000,00,- 34.000,00,- 34.000,00,- 34.000,00,-
	80140	Centra kształcenia ustawicznego i praktycznego oraz ośrodki dokształcania zawodowego, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	42.000,00,- 42.000,00,- 42.000,00,- 42.000,00,-
	80195	Pozostała działalność, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań 2) świadczenia na rzecz osób fizycznych 3) wydatki na programy finansowane ze środków pochodzących z budżetu Unii Europejskiej, w tym: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań,	60.755,99,- 60.755,99,- 5.484,70,- 1.707,04,- 3.777,66,- 1.000,00,- 54.271,29,- 550,34,- 53.720,95,-
851		Ochrona zdrowia	130.000,00,-
	85111	Szpitala ogólne, w tym: a) wydatki majątkowe, w tym: 1) dotacje (dotacja celowa na dofinansowanie inwestycji i zakupów inwestycyjnych dla ZOZ Ropczyce - dotacja podmiotowa dla jednostek sektora finansów publicznych) 2) inwestycje i zakupy inwestycyjne	130.000,00,- 130.000,00,- 100.000,00,- 30.000,00,-
852		Pomoc społeczna	32.400,12,-
	85201	Placówki opiekuńczo-wychowawcze, z tego : a) wydatki bieżące, w tym: 1) świadczenia na rzecz osób fizycznych	988,20,- 988,20,- 988,20,-
	85202	Domy pomocy społecznej, z tego : a) wydatki bieżące, w tym: 1) wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań	22.000,00,- 22.000,00,- 22.000,00,- 10.000,00,- 12.000,00,-
	85204	Rodziny zastępcze, z tego : a) wydatki bieżące, w tym: 1) świadczenia na rzecz osób fizycznych	5.811,92,- 5.811,92,- 5.811,92,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
	85218	Powiatowe centra pomocy rodzinie, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane 2)świadczenia na rzecz osób fizycznych 3)wydatki na programy finansowane ze środków pochodzących z budżetu Unii Europejskiej, w tym: -wynagrodzenia i składki od nich naliczane - świadczenia na rzecz osób fizycznych	3.600,00,- 3.600,00,- 30,18,- 30,18,- 150,90,- 3.418,92,- 569,82,- 2.849,10,-
853		Pozostałe zadania w zakresie polityki społecznej	56.000,00,-
	85333	Powiatowe urzędy pracy, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	56.000,00,- 56.000,00,- 56.000,00,- 56.000,00,-
854		Edukacyjna opieka wychowawcza	67.000,00,-
	85406	Poradnie psychologiczno-pedagogiczne oraz inne poradnie specjalistyczne, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	35.000,00,- 35.000,00,- 35.000,00,- 35.000,00,-
	85410	Internaty i bursy szkolne, z tego: a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań	32.000,00,- 32.000,00,- 32.000,00,- 9.000,00,- 23.000,00,-
900		Gospodarka komunalna i ochrona środowiska	2.000,00,-
	90008	Ochrona różnorodności biologicznej i krajobrazu, z tego: a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	2.000,00,- 2.000,00,- 2.000,00,- 2.000,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
921		Kultura i ochrona dziedzictwa narodowego	1.800,00,-
	92195	Pozostała działalność, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	1.800,00,- 1.800,00,- 1.800,00,- 1.800,00,-
926		Kultura fizyczna	1.400,00,-
	92695	Pozostała działalność, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	1.400,00,- 1.400,00,- 1.400,00,- 1.400,00,-
Ogółem zwiększony plan wydatków			1.392.633,96,-

§ 6. W zmianach planu dochodów i wydatków budżetu powiatu wyodrębnia się:

- 1) dochody i wydatki związane z realizacją zadań zleconych z zakresu administracji rządowej i innych zadań zleconych ustawami:

Zwiększenia planu dochodów

Dział	Nazwa działu	Źródła dochodów	Kwota
710	Działalność usługowa w tym: -dochody bieżące, w tym:	-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	4.963,00,- 4.963,00,- 4.963,00,-
754	Bezpieczeństwo publiczne i ochrona przeciwpożarowa, w tym : -dochody bieżące, w tym: -dochody majątkowe, w tym:	-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami -dotacje celowe z budżetu państwa na inwestycje i zakupy inwestycyjne z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	69.539,00,- 4.539,00,- 4.539,00,- 65.000,00,- 65.000,00,-

Dział	Nazwa działu	Źródła dochodów	Kwota
852	Pomoc społeczna , w tym : -dochody bieżące, w tym:	-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	31.820,00,- 31.820,00,- 31.820,00,-
853	Pozostałe zadania w zakresie polityki społecznej, w tym: -dochody bieżące, w tym:	-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	10.000,00,- 10.000,00,- 10.000,00,-
Ogółem zwiększenie planu dochodów			116.322,00,-

Zwiększenie planu wydatków

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
710		Działalność usługowa	4.963,00,-
	71015	Nadzór budowlany, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane	4.963,00,- 4.963,00,- 4.963,00,- 4.963,00,-
754		Bezpieczeństwo publiczne i ochrona przeciwpożarowa	69.539,00,-
	75411	Komendy powiatowe Państwowej Straży Pożarnej, z tego : a)wydatki majątkowe, w tym: 1)inwestycje i zakupy inwestycyjne	65.000,00,- 65.000,00,- 65.000,00,-
	75478	Usuwanie skutków klęsk żywiołowych, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wydatki związane z realizacją ich statutowych zadań	4.539,00,- 4.539,00,- 4.539,00,- 4.539,00,-
852		Pomoc społeczna	31.820,00,-
	85203	Ośrodki wsparcia, z tego : a) wydatki bieżące, w tym: 1) dotacje na zadania bieżące (dofinansowanie zadań zleconych do realizacji organizacjom pozarządowym – dotacja celowa dla Polskiego Stowarzyszenia Na Rzecz	31.820,00,- 31.820,00,- 31.820,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
		Osób z Upośledzeniem Umysłowym w Sędziszowie Młp.)	
853		Pozostałe zadania w zakresie polityki społecznej	10.000,00,-
	85321	Zespoły ds. orzekania o niepełnosprawności, z tego : a)wydatki bieżące, w tym: 1)wydatki jednostek budżetowych, w tym na: -wynagrodzenia i składki od nich naliczane -wydatki związane z realizacją ich statutowych zadań	10.000,00,- 10.000,00,- 10.000,00,- 6.000,00,- 4.000,00,-
Ogółem zwiększony plan wydatków			116.322,00,-

Zmniejszenia planu dochodów

Dział	Nazwa działu	Źródła dochodów	Kwota
754	Bezpieczeństwo publiczne i ochrona przeciwpożarowa, w tym : -dochody bieżące, w tym:		65.000,00,-
		-dotacje celowe z budżetu państwa na zadania z zakresu administracji rządowej oraz na inne zadania zlecone ustawami	65.000,00,- 65.000,00,-
Ogółem zmniejszenie planu dochodów			65.000,00,-

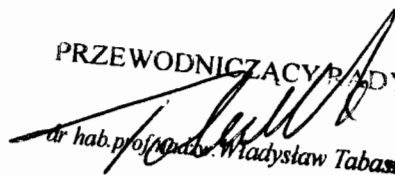
Zmniejszenie planu wydatków

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
754		Bezpieczeństwo publiczne i ochrona przeciwpożarowa	65.000,00,-
	75411	Komendy powiatowe Państwowej Straży Pożarnej z tego : a)wydatki bieżące, w tym:	65.000,00,- 65.000,00,-

Dział	Rozdział	Nazwa działu, rozdziału	Kwota
		1)wydatki jednostek budżetowych, w tym: -wynagrodzenia i składki od nich naliczane	65.000,00,- 65.000,00,-
Ogółem zmniejszony plan wydatków			65.000,00,-

§ 7. Wykonanie uchwały zleca się Zarządowi Powiatu Ropczycko-Sędziszowskiego.

§ 8. Uchwała wchodzi w życie z dniem podjęcia.

PRZEWODNICZĄCY RADY

 dr hab. prof. nadzw. Władysław Tabasz