Krajowa Izba Rozliczeniowa S.A.

SZAFIR

SZAFIR Weryfikująca

Podręcznik użytkownika

Informacje prawne

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

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

SPIS TREŚCI

1. Wprowadzenie

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

Aplikacja SZAFIR Weryfikująca służy do weryfikowania zwykłych oraz bezpiecznych podpisów elektronicznych. Umożliwia weryfikację podpisu elektronicznego w formatach XAdES (w wariantach XAdES-BES, XAdES-T, XAdES-C), PKCS#7 oraz S-MIME.

Aplikacja SZAFIR Weryfikująca spełnia wymagania nałożone na oprogramowanie 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 (Dz. U. Nr 128, poz. 1094) co oznacza, że wraz ze współpracującym z nią komponentem technicznym stanowi ona bezpieczne urządzenie do weryfikacji podpisów elektronicznych.

Aplikacja SZAFIR Weryfikująca 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.

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

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

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

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

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

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

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

PKCS – nazwa zestawu standardów z dziedziny kryptografii klucza publicznego.

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

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

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

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

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

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

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

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

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

- Możliwość podpisywania obiektów, które mogą być zidentyfikowane poprzez URI (ang. Uniform Resource Identifier) – w szczególności obiektami takim mogą być:
  - zewnętrzne dokumenty XML,
  - zewnętrzne fragmenty dokumentów XML,
  - części dokumentu XML, w którym osadzony jest podpis.
  - pliki tekstowe,
  - pliki binarne.

- Zapisywanie podpisu elektronicznego w postaci elementu dokumentu XML, przy czym podpis ten może być:
  - opakowujący (zawierać w sobie podpisywany element),
  - opakowany (być zawartym w podpisywanym elemencie),
  - oddzielny (znajdować się obok elementu podpisywanego, w tym samym lub w innym dokumencie XML).

- Możliwość składania podpisu w formach:
  - XAdES-BES (podstawowa forma podpisu XAdES);
  - XAdES-T (podpis XAdES oznakowany czasem);
  - XAdES-C (podpis XAdES oznakowany czasem, z dołączonymi informacjami – certyfikatami oraz CRL – zapewniającymi długotrwałą ważność dowodową podpisu).

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

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

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

2. Weryfikowanie podpisów

2.1. Przygotowanie aplikacji do pracy

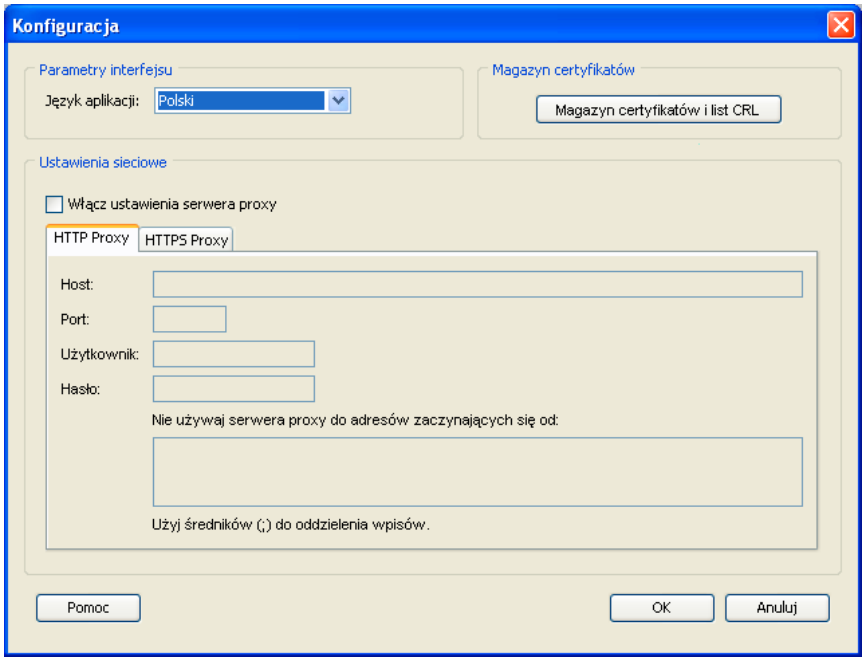
Główne okno aplikacji, które jest widoczne zaraz po uruchomieniu zostało przygotowane w ten sposób, aby nawet użytkownikom korzystającym z niej po raz pierwszy ułatwić obsługę. Trzy duże przyciski po lewej stronie umożliwiają dostęp do wszystkich funkcji programu. Dla wygody funkcje te posiadają również skróty klawiaturowe:

- Weryfikuj – F2
- Konfiguracja – F10
- Pomoc – F1

Rysunek 1. Główne okno aplikacji.

Weryfikacja podpisów elektronicznych wymaga, by komputer na którym uruchamiana jest aplikacja był wyposażony w połączenie z siecią Internet. Dla komputerów, które łączą się z siecią Internet przez serwer proxy, przy pierwszym uruchomieniu aplikacji, należy ustawić parametry tego serwera. Szczegółowe parametry sieciowe powinien podać administrator sieci.

Konfiguracja aplikacji zawiera dwa podstawowe elementy: parametry interfejsu i ustawienia sieciowe oraz magazyn certyfikatów.



Rysunek 2. Okno konfiguracji

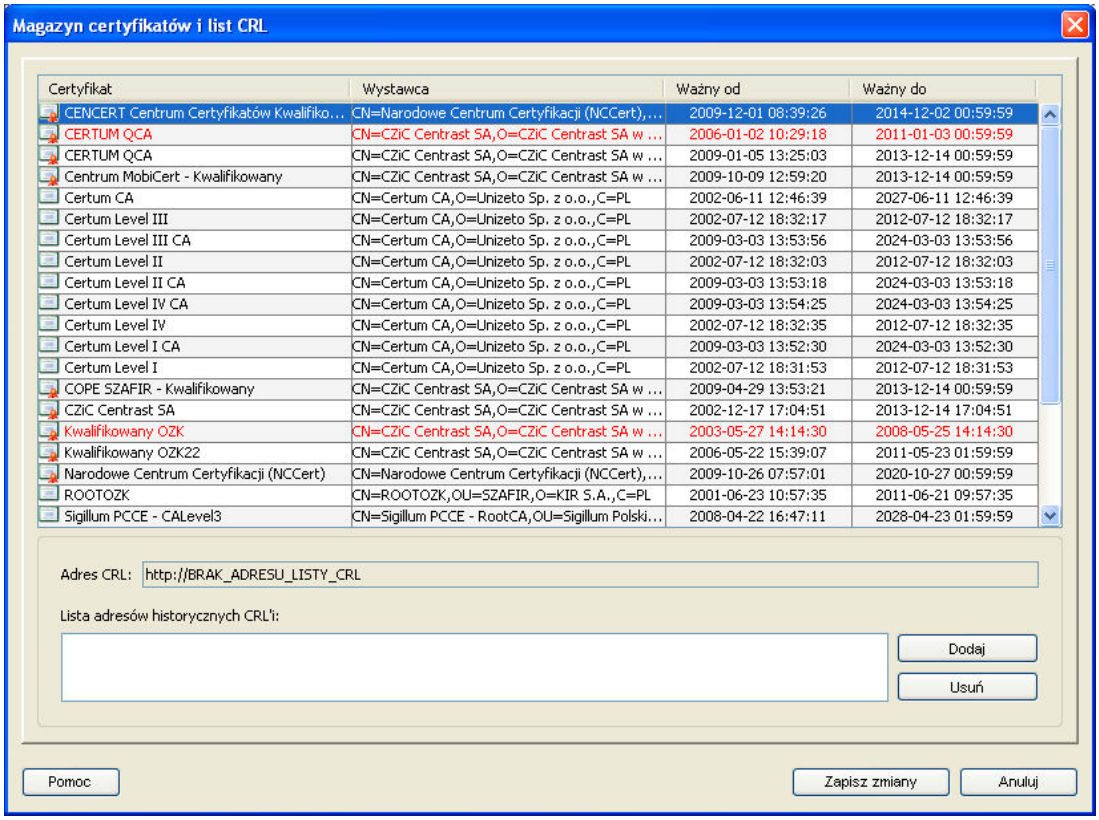
Języka aplikacji - pozwala na zmianę języka wszystkich komunikatów, przycisków i etykiet jakie występują w aplikacji. Ustawienia sieciowe - zawierają parametry serwera proxy dla protokołów HTTP oraz HTTPS. Jeżeli połączenie z siecią Internet nie odbywa się przez serwer proxy wszystkie pola powinny być puste. W przeciwnym razie:

- Host i Port - powinny zawierać właściwy adres serwera.
- Użytkownik i Hasło - wypełniamy tylko dla serwerów proxy, które wymagają autoryzacji.
- Ostatnie pole pozwala wpisać adresy lub maski adresów serwerów, z którymi połączenia odbywają się z ominięciem serwera proxy.

2.1.1. Magazyn certyfikatów i list CRL

Magazyn certyfikatów i list CRL w aplikacji SZAFIR Weryfikująca to miejsce w którym użytkownik może zobaczyć listę certyfikatów CA (urzędów certyfikacji) znanych aplikacji. Podstawowe okno magazynu certyfikatów przedstawione poniżej prezentuje certyfikaty, ich wystawców oraz okresy ważności (kolorem czerwonym prezentowane są certyfikaty, których ważność już upłynęła). Okno to możemy wyświetlić wybierając przycisk „Magazyn certyfikatów i list CRL” z poziomu okna

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



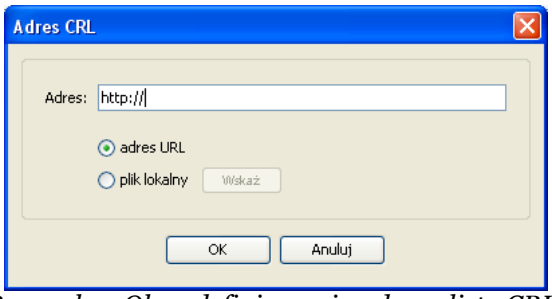
Rysunek 3. Okno magazynu certyfikatów.

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'i" 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 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.

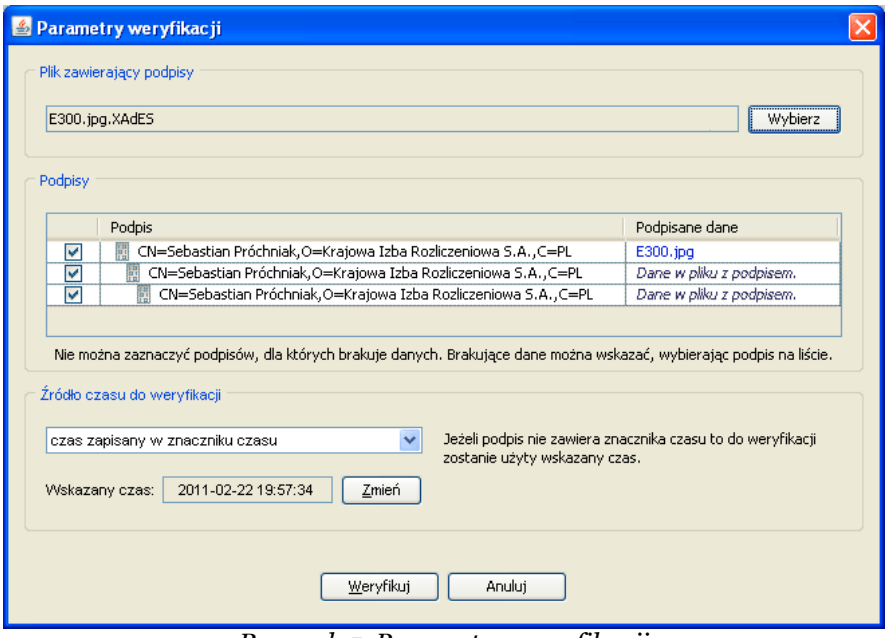


Rysunek 4. Okno definiowania adresu listy CRL.

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

2.2. Parametry weryfikacji

Okno parametry weryfikacji pozwala, na określenie wszystkich niezbędnych danych i parametrów do przeprowadzenia procesu weryfikacji.



Rysunek 5. Parametry weryfikacji

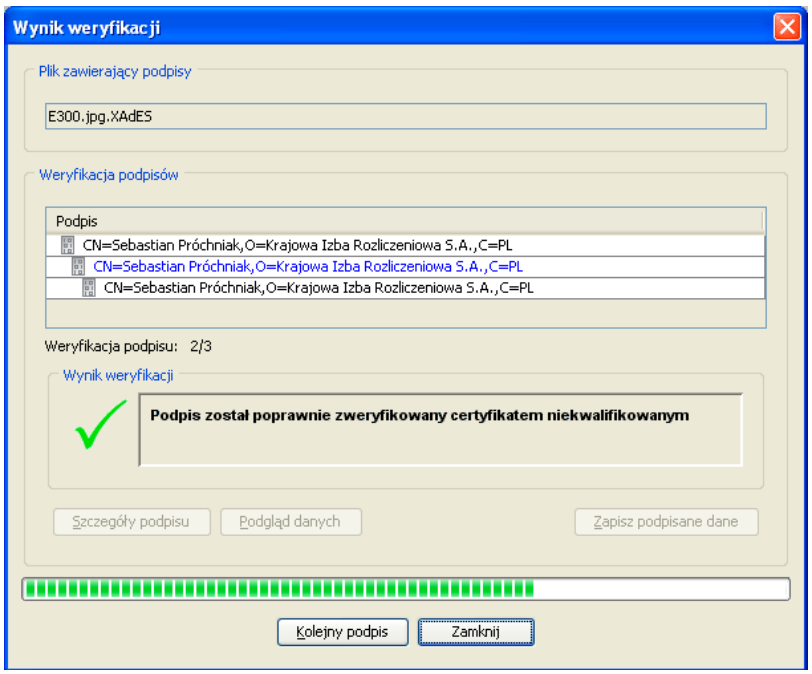
- **Plik zawierający podpisy** - to pierwszy element, jaki należy wskazać. Możemy to zrobić naciskają przycisk 'Wskaż'. Jeżeli wskazany plik zawiera podpisy, zostaną one wyświetlone w tabeli poniżej z zachowaniem hierarchii.

- **Podpisy** - tabela z podpisami pozwala zaznaczyć lub odznaczyć podpisy, które mają zostać zweryfikowane. Aplikacja nie pozwala na zaznaczanie podpisów, dla których nie może znaleźć podpisanych danych. Taka sytuacja jest sygnalizowana komunikatem w tabeli: 'Brak podpisanych danych'. Dla takich podpisów, można wskazać plik zawierający podpisane dane klikając dwukrotnie na podpisie w tabeli lub wybierając ten podpis z klawiatury i wciskając klawisz Enter.

- **Źródło czasu do weryfikacji** - użytkownik może wybrać źródło związane bezpośrednio z podpisem, czy znacznikiem czasu lub wskazać konkretny czas na jaki mają być weryfikowane wskazane podpisy.

2.3. Wynik weryfikacji

Proces weryfikacji podzielony jest na tyle etapów, ile podpisów zaznaczył wcześniej użytkownik. Pierwszy podpis weryfikowany jest automatycznie, natomiast każdy kolejny po wciśnięciu przycisku 'Kolejny podpis'. Dzięki temu użytkownik od razu widzi wynik weryfikacji danego podpisu.



Rysunek 6. Wynik weryfikacji

Weryfikacja dowolnego podpisu może mieć wynik: pozytywnie zweryfikowany, niekompletnie lub negatywnie zweryfikowany.

- **Pozytywnie zweryfikowany** - taki wynik oznacza, że te konkretne dane zostały faktycznie podpisane tym konkretnym certyfikatem (kluczem). Wszystko się zgadza pod względem kryptograficznym, a ponadto certyfikat użyty do podpisu został pozytywnie zweryfikowany (sprawdzony, czy nie jest unieważniony).

- **Niekompletnie zweryfikowany** - wynik ten mówi nam, że kryptograficznie dane te zostały podpisane tym konkretnym certyfikatem (kluczem), jednak aplikacja nie mogła zweryfikować certyfikatu i/lub jego ścieżki certyfikacji. Najczęściej przyczyną takiego wyniku jest to, że aplikacja nie może pobrać aktualnej listy CRL z powodu problemu z połączeniem z siecią Internet (przez nie ustawione lub błędnie ustawione parametry serwera proxy w konfiguracji).

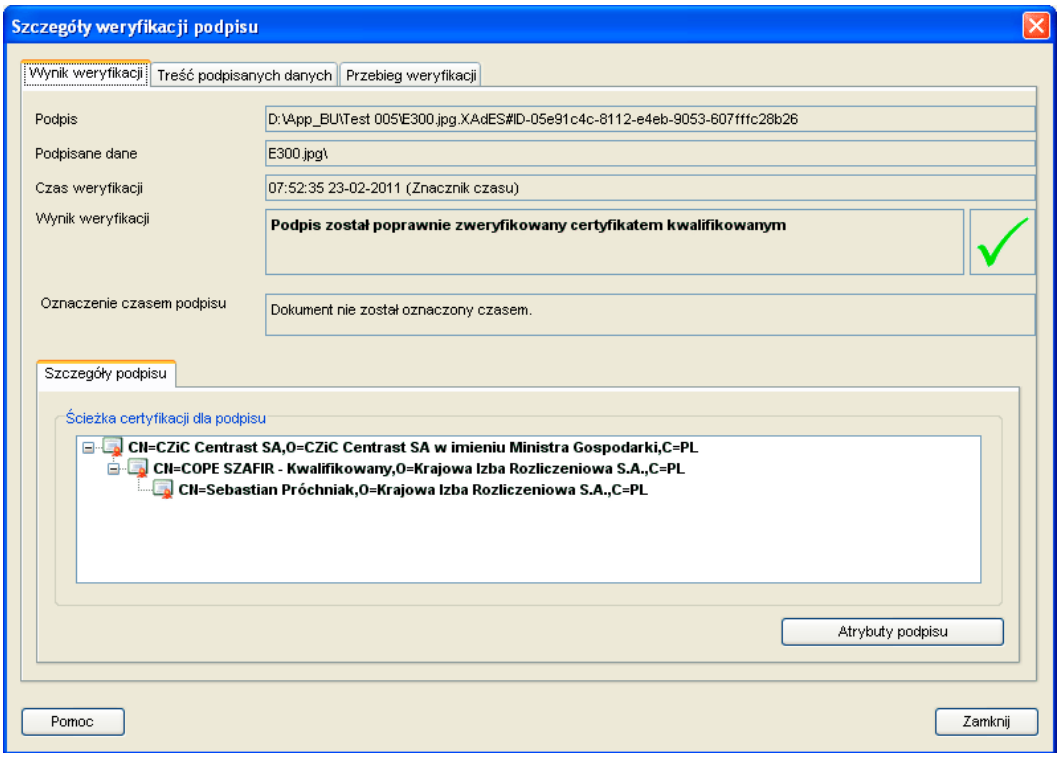
- **Negatywnie zweryfikowany** - wynik oznaczający, że te konkretne dane nie zostały podpisane tym konkretnym certyfikatem (kluczem). Najprawdopodobniej dla podpisu rozłącznego podpis dotyczy innych danych (innego pliku) lub dane od czasu wykonania podpisu zostały zmienione.

Po wykonaniu weryfikacji danego podpisu użytkownik poza wynikiem może zobaczyć dane użyte do weryfikacji podpisu, obejrzeć szczegóły lub dla podpisów z danymi wewnątrz pliku z podpisem zapisać owe dane na dysk do zewnętrznego pliku.

Dokładne informacje o weryfikacji podpisów zawiera okno 'Szczegóły weryfikacji podpisu', do którego można przejść naciskając przycisk 'Szczegóły podpisu' lub klikając dwukrotnie podpisie w tabeli z wynikami.

2.4. Szczegółowe informacje dotyczące weryfikacji

Okno ‘Szczegóły weryfikacji podpisu’ umożliwia zapoznanie się z wynikiem oraz szczegółami i przebiegiem weryfikacji podpisu elektronicznego.



Rysunek 7. Szczegóły weryfikacji podpisu

Wynik weryfikacji

- **Podpis.** W tym polu wyświetlana jest lokalizacja weryfikowanego podpisu. W zależności od typu podpisu, znajdować się on może w pliku PKCS#7 lub XML.

- **Podpisane dane**. W tym polu wyświetlana jest lokalizacja danych podpisanych weryfikowanym podpisem. Dane te znajdować się mogą:

  - w dowolnym pliku zapisanym na dysku
  - w pliku z podpisem
  - w samym podpisie (w przypadku podpisów XAdES).

- **Czas weryfikacji**. W tym polu wyświetlany jest czas, w oparciu o który została przeprowadzona weryfikacja podpisu elektronicznego - a ściślej rzecz ujmując, weryfikacja certyfikatu użytego do weryfikacji podpisu.

- **Wynik weryfikacji.** W tym polu wyświetlany jest wynik weryfikacji podpisu elektronicznego.

- **Oznaczenie czasem podpisu**. W tym polu wyświetlana jest informacja o oznaczeniu podpisu czasem:

    - Jeżeli podpis jest oznaczony czasem, wówczas w polu tym wyświetlany jest czas zapisany w znaczniku czasu.
    - Jeżeli podpis nie jest oznaczony czasem, wówczas w polu tym wyświetlana jest informacja o braku znacznika czasu.

- **Szczegóły podpisu.** Na tej zakładce wyświetlane są dodatkowe informacje istotne z punktu widzenia weryfikacji podpisu.

    - **Ścieżka certyfikacji certyfikatu użytego do weryfikacji podpisu.** W tym polu wyświetlana jest informacja o wszystkich certyfikatach zweryfikowanych w ramach weryfikacji podpisu. Certyfikaty przedstawione są w formie kaskady: od certyfikatu znajdującego się na samej górze hierarchii certyfikatów (tzw. roota) aż po certyfikat użyty do weryfikacji podpisu.

    > Należy zwrócić uwagę, że w istocie dopiero po prześledzeniu ścieżki certyfikacji certyfikatu użytego do weryfikacji podpisu możemy być pewni, że certyfikat ten istotnie należy do osoby, której dane widnieją pod podpisem elektronicznym. Dostępność technologii podpisu elektronicznego pozwala w zasadzie każdemu na wygenerowanie certyfikatu o dowolnych zapisanych w nim danych osobowych; dlatego weryfikując podpis elektroniczny należy zawsze sprawdzać, czy certyfikat użyty do weryfikacji podpisu został podpisany przez właściwy urząd certyfikujący.

    - **Atrybuty podpisu.** Po kliknięciu w ten przycisk zostanie wyświetlone okno zawierające szczegółowe informacje o weryfikowanym podpisie.

- **Szczegóły znacznika czasu**. Na tej zakładce wyświetlane są dodatkowe informacje istotne z punktu widzenia weryfikacji znacznika czasu.

- **Ścieżka certyfikacji certyfikatu użytego do weryfikacji znacznika czasu.** W tym polu wyświetlana jest informacja o wszystkich certyfikatach zweryfikowanych w ramach weryfikacji znacznika czasu pod podpisem. Certyfikaty przedstawione są w formie kaskady: od certyfikatu znajdującego się na samej górze hierarchii certyfikatów (tzw. roota) aż po certyfikat użyty do weryfikacji znacznika czasu.

- **Atrybuty znacznika czasu.** Po kliknięciu w ten przycisk zostanie wyświetlone okno zawierające szczegółowe informacje o weryfikowanym znaczniku czasu.

Przebieg weryfikacji

Na tej zakładce wyświetlany jest szczegółowy przebieg procesu weryfikacji podpisu elektronicznego.

Treść podpisanych danych

Na tej zakładce wyświetlana jest treść podpisanych danych. W przypadku gdy format danych uniemożliwia ich prezentację w ramach oprogramowania SZAFIR możliwe jest uruchomienie zewnętrznej aplikacji odpowiedzialnej za obsługę plików danego typu.

> 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 podpis weryfikującej.

3. Wymagania oraz instalacja

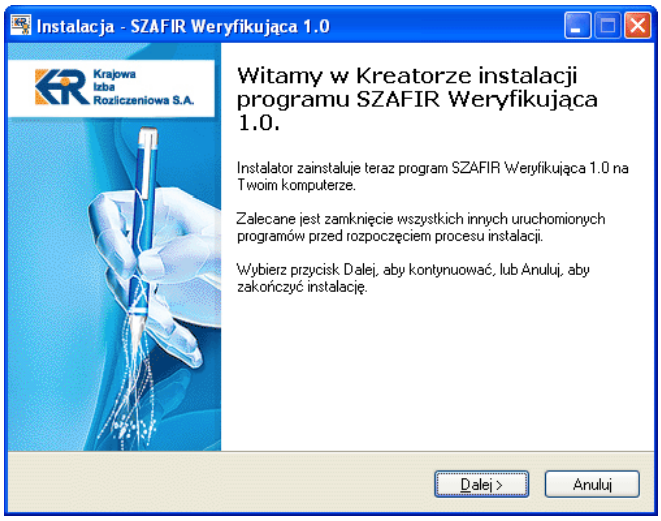
3.1. Minimalne wymagania

Do poprawnej pracy aplikacja SZAFIR Weryfikująca wymaga komputera klasy IBM PC pracującego pod kontrolą systemu operacyjnego Mirosoft Windows 2000 SP4 lub nowszego, na którym zainstalowane jest środowisko Java w wersji 1.5 lub nowsze.

Weryfikowanie podpisów elektronicznych wymaga, by komputer wyposażony był w połączenie z siecią Internet, w celu pobrania list certyfikatów unieważnionych i zawieszonych.

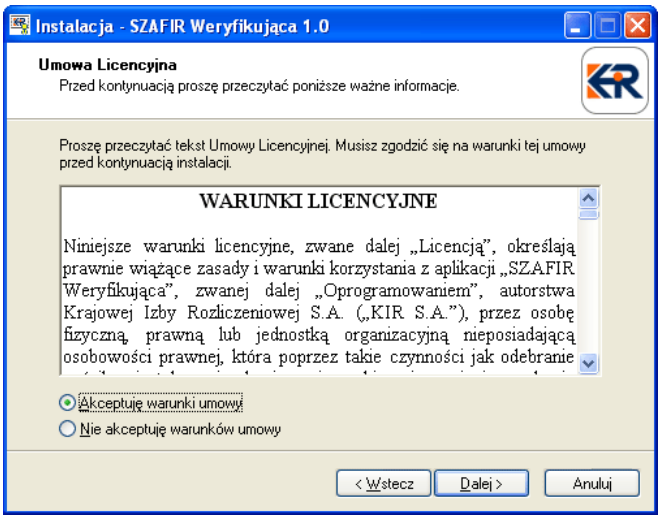
3.2. Instalacja

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



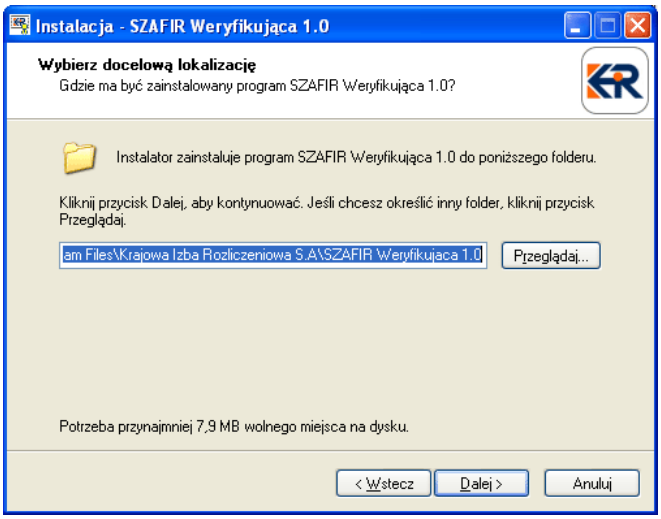
Rysunek 8. Kreator instalacji aplikacji – ekran powitalny.

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



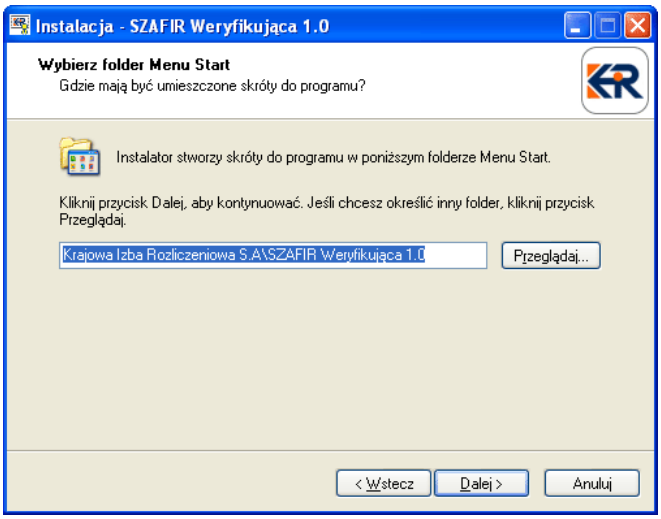
Rysunek 9. Kreator instalacji aplikacji – umowa licencyjna.

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 10. Kreator instalacji aplikacji – wybór docelowej lokalizacji.

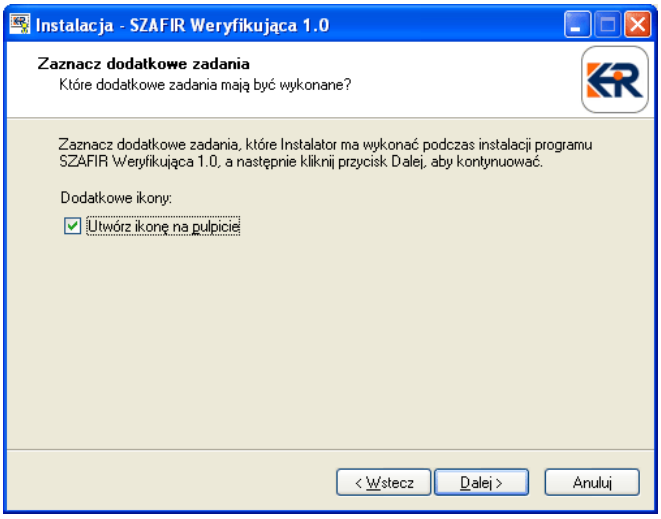
4. W celu kontynuowania instalacji należy kliknąć w przycisk „Dalej”. Pojawi się okno „Wybierz folder Menu Start”:



Rysunek 11. Kreator instalacji aplikacji – wybór folderu Menu Start.

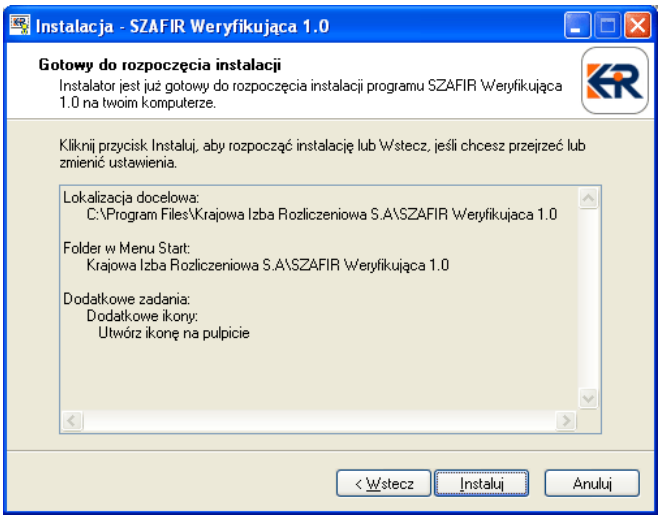
Zaleca się skorzystanie z opcji domyślnie zaproponowanych przez program instalacyjny.

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



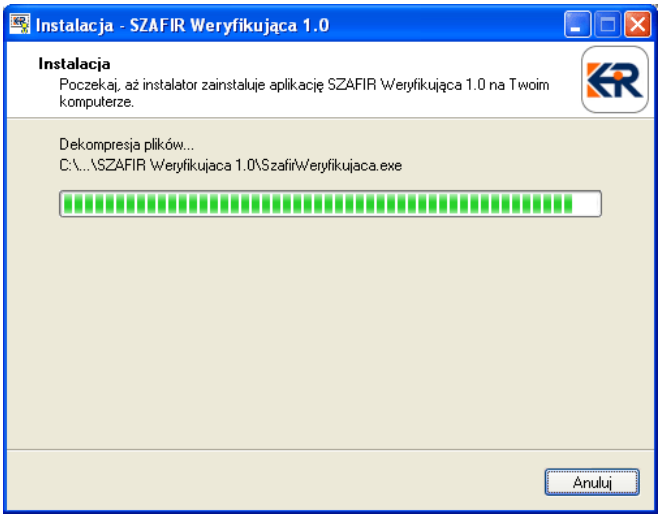
Rysunek 12. Kreator instalacji aplikacji – dodatkowe opcje instalacji.

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



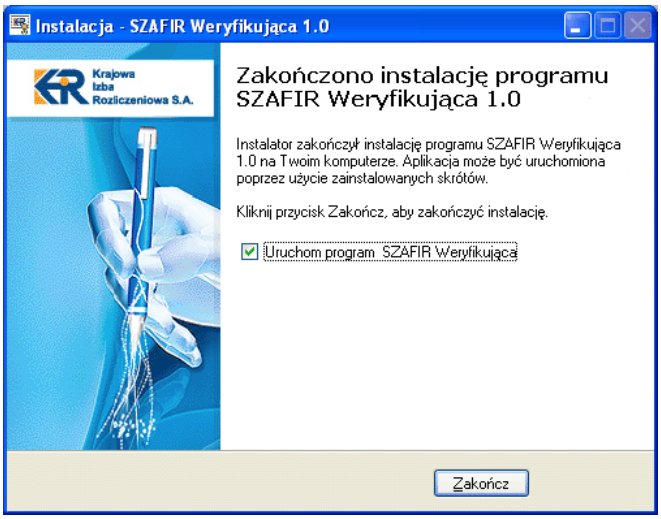
Rysunek 13. Kreator instalacji aplikacji – podsumowanie.

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



Rysunek 14. Kreator instalacji aplikacji – kopiowanie plików.

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



Rysunek 15. Kreator instalacji aplikacji – koniec instalacji.

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