BGŻ BNP PARIBAS

# Instrukcja instalacji urządzeń kryptograficznych

## dla użytkowników zmieniających metodę logowania i autoryzacji transakcji z kodów SMS na podpis elektroniczny

Aby możliwe było korzystanie w systemie Pl@net lub BiznesPl@net z urządzeń kryptograficznych (karty kryptograficznej lub nośnika USB) służących do generowania podpisów elektronicznych, wymagane jest wykonanie następujących czynności:

1. **Instalacja oprogramowania Comarch SmartCard do obsługi urządzeń kryptograficznych**
2. **Instalacja komponentu do generowania podpisów elektronicznych**
3. **Inicjalizacja karty lub nośnika USB**

Prosimy o wykonanie tych czynności w kolejności przedstawionej powyżej. Prosimy nie podłączać czytnika kart ani nośnika USB do komputera zanim nie zostanie zainstalowane oprogramowanie Comarch SmartCard do obsługi urządzeń kryptograficznych.

**Uwaga:** Urządzenia kryptograficzne są obsługiwane w systemach Pl@net i BiznesPl@net w systemie operacyjnym Microsoft Windows (Vista / XP / 2000), w przeglądarkach Microsoft Internet Explorer (w wersji 5.5 z SP2 lub nowszej), Mozilla Firefox (w wersji 1.5 lub nowszej) oraz Netscape Browser (wersja 7.1 lub nowsza).

Jeżeli:
**korzystasz z systemu Pl@net lub BiznesPl@net autoryzując zlecenia kodami SMS**,
i chcesz zmienić metodę logowania i autoryzacji na podpis elektroniczny, generowany przy pomocy kluczy zapisanych na bezpiecznym urządzeniu kryptograficznym, możesz to zrobić o ile posiadasz odpowiednie urządzenie - nośnik kryptograficzny USB lub kartę kryptograficzną (wraz z czytnikiem kart).

Jeżeli jeszcze nie posiadasz takiego urządzenia, możesz go zamówić składając "Zamówienie nośnika kryptograficznego USB lub karty kryptograficznej" (jest ono dostępne w Pl@net w zakładce "Wnioski", funkcja "Nowy wniosek lub dyspozycja", sekcja "Inne wnioski" oraz w BiznesPl@net w zakładce "Inne", funkcja "Wnioski" > "Nowy wniosek lub dyspozycja", sekcja "Wnioski systemowe").

## 1. Instalacja oprogramowania Comarch SmartCard do obsługi urządzeń kryptograficznych

Instalacja oprogramowania Comarch SmartCard umożliwiającego obsługę urządzeń kryptograficznych - kart kryptograficznych oraz nośników USB, odbywa się za pomocą łatwego w obsłudze kreatora. Plik instalacyjny ComarchSmartCard.exe jest udostępniony na stronach internetowych BNP Paribas Bank Polska SA, w dziale "Bankowość internetowa", w sekcji "Do pobrania" (z prawej strony ekranu), pod adresem: http://www.bgzbnpparibas.pl/files/comarchsc_bnpparibas.exe (rozmiar pliku: 20.5 MB).

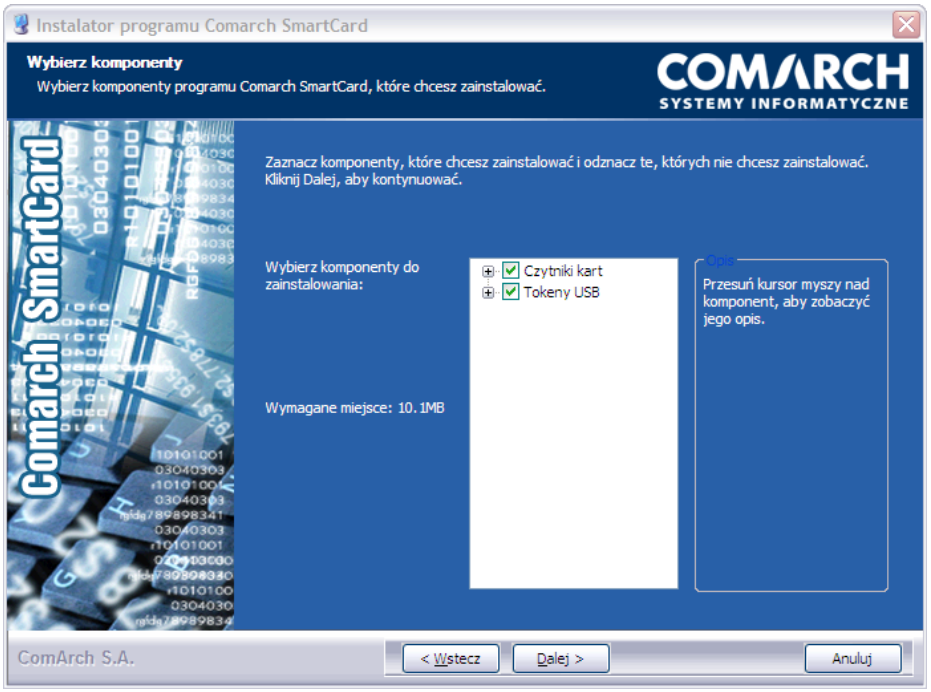
Pobierz plik ComarchSmartCard.exe, a następnie uruchom go.

**Uwaga:** Instalacja oprogramowania Comarch SmartCard wymaga posiadania uprawnień administratora na danym komputerze.

Po uruchomieniu instalatora, postępuj zgodnie ze wskazówkami wyświetlanymi na ekranie, posługując się przyciskiem "Dalej".

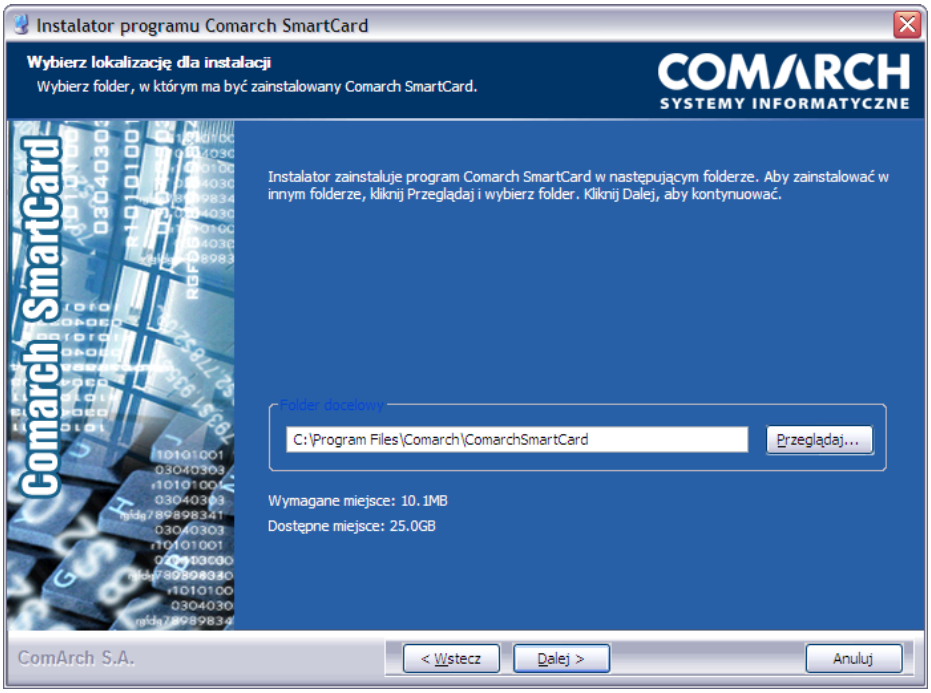

Zapoznaj się z warunkami umowy licencyjnej i zaakceptuj jej warunki zaznaczając pole wyboru "Akceptuję warunki umowy licencyjnej", a następnie kliknij przycisk "Dalej":

Instalator zaproponuje teraz instalację sterowników do czytnika kart oraz nośników kryptograficznych USB. Pozostaw zaznaczone pola wyboru przy obydwu komponentach (zarówno "Czytniki kart" jak i "Tokeny USB") i kliknij "Dalej".

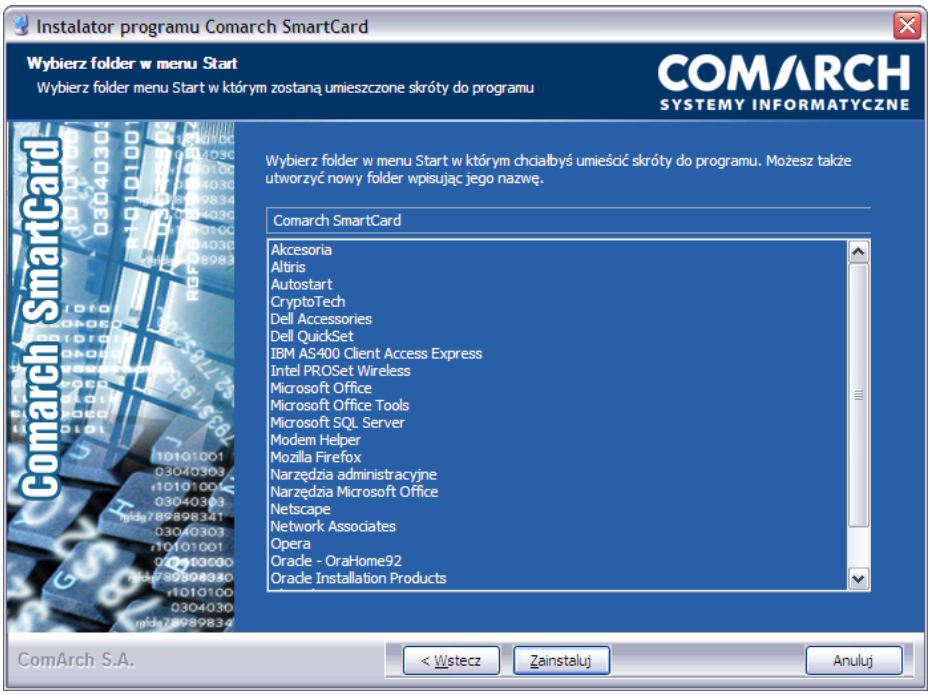



*Jeżeli nie chcesz instalować nadmiarowych sterowników, możesz odznaczyć pole wyboru przy urządzeniach, z których nie będziesz korzystał - jeśli zamierzasz używać tylko nośnika kryptograficznego USB, wystarczy że zainstalujesz sterowniki Gem e-Seal z grupy "Tokeny USB". Z kolei, jeśli będziesz korzystać z kart kryptograficznych i czytnika dystrybuowanego przez BNP Paribas Bank Polska SA, wystarczy że zainstalujesz sterowniki do czytnika GemPCTwin USB. Natomiast jeśli posiadasz inny (własny) czytnik, możesz odznaczyć wszystkie pola wyboru, aby nie instalować żadnych sterowników.*

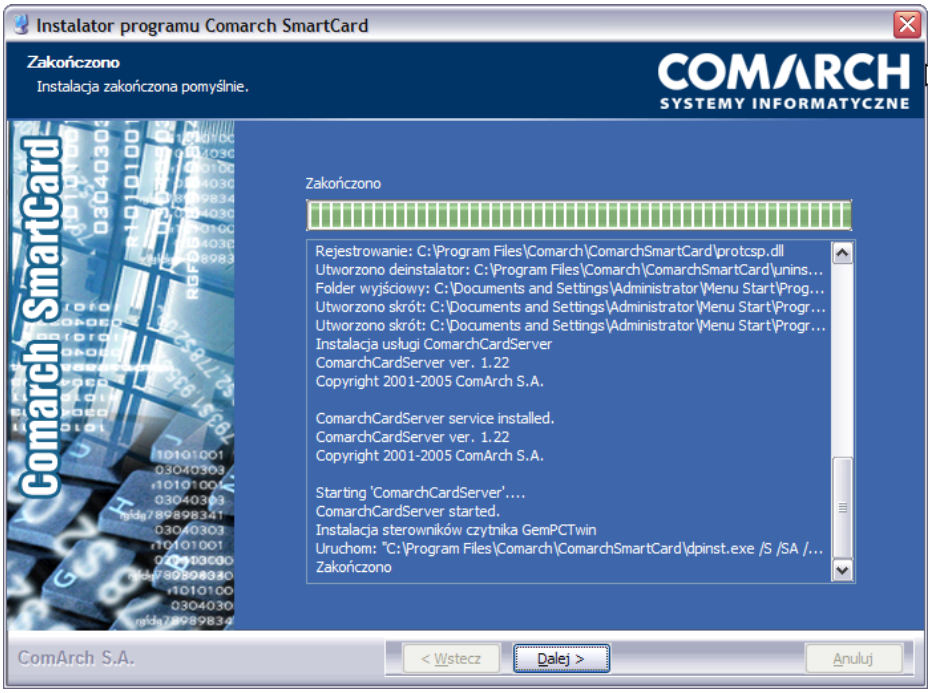
Następnie, określ miejsce instalacji aplikacji - zaakceptuj domyślnie proponowany folder lub zmień go korzystając z przycisku "Przeglądaj...":



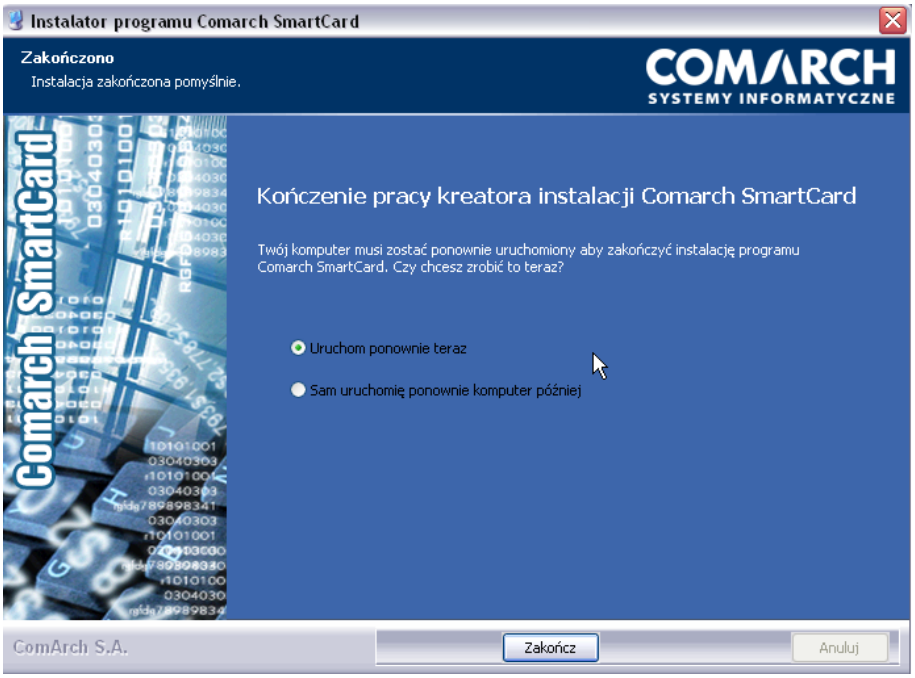
W kolejnym kroku instalator poprosi o wybranie foldera w menu Start, w którym umieszczony zostanie skrót uruchamiający aplikację. Wskaż folder i kliknij "Zainstaluj":




Gdy kreator poinformuje o zakończeniu instalacji, kliknij "Dalej":



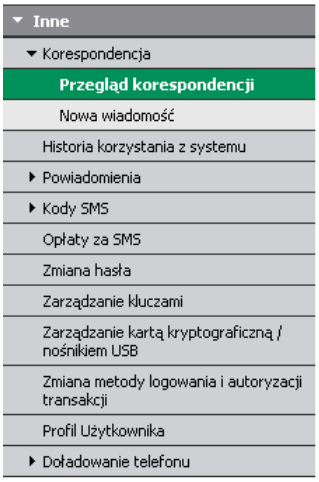
Instalacja dobiegła końca. Jeśli korzystasz z systemu Windows 98 lub Windows ME konieczne będzie jeszcze zrestartowanie komputera - zaznacz opcję "Uruchom ponownie teraz" i kliknij "Zakończ". W przypadku nowszych wersji systemu Windows (Vista, XP lub Windows 2000) restart nie jest konieczny - zaznacz opcję "Sam uruchomię komputer później" i kliknij "Zakończ"

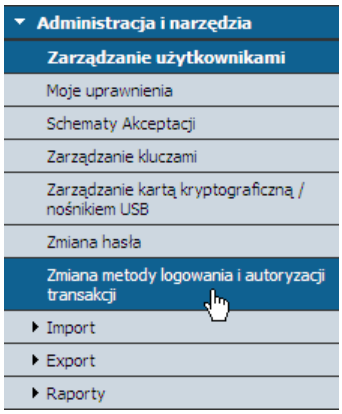



## 2. Instalacja komponentu do generowania podpisów elektronicznych

Podłącz teraz nośnik USB do komputera lub podłącz czytnik kart i włóż kartę do czytnika.

**Jeżeli korzystasz z systemu Pl@net lub BiznesPl@net autoryzując zlecenia kodami SMS** i chcesz zmienić metodę logowania i autoryzacji na podpis elektroniczny, zaloguj się do Pl@net lub BiznesPl@net (dotychczasową metodą, czyli hasłem maskowanym), przejdź do zakładki "Inne" (w przypadku Pl@net) lub "Administracja i narzędzia" (w przypadku BiznesPl@net) i wybierz opcję "Zmiana metody logowania i autoryzacji transakcji".

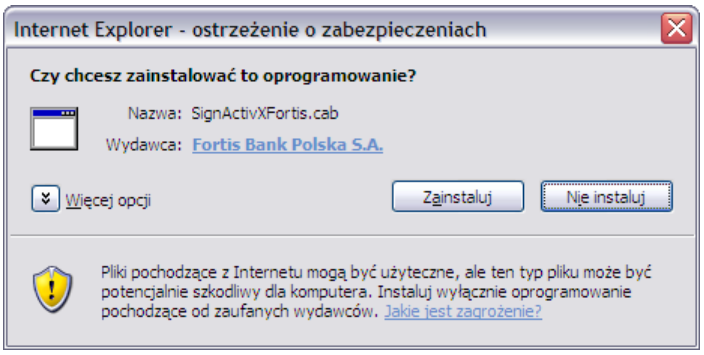



Zapoznaj się z informacjami zawartymi na formatce zmiany metody logowania i autoryzacji transakcji, a następnie kliknij "Wygeneruj klucz". Przeglądarka zaproponuje instalację komponentu do generowania podpisów elektronicznych.

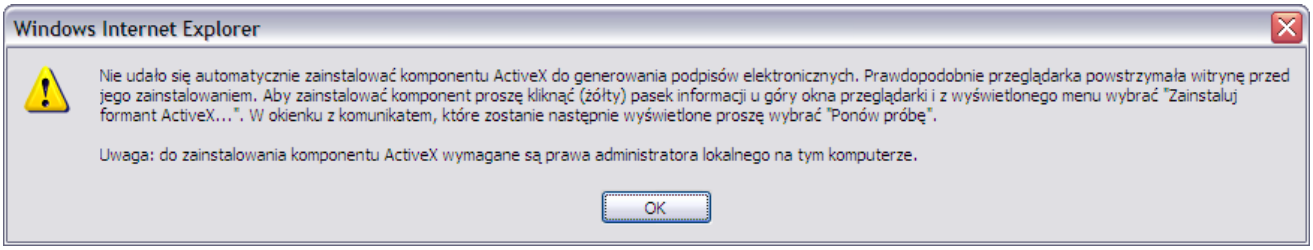
## Instalacja komponentu dla przeglądarki Microsoft Internet Explorer

Po kliknięciu przycisku "Wygeneruj klucz" na formatce "Zmiana metody logowania i autoryzacja transakcji", przeglądarka - o ile została uruchomiona z uprawnieniami administratora - zaproponuje instalację komponentu do generowania podpisów elektronicznych (chyba że jego najnowsza wersja jest już zainstalowana na komputerze, z którego korzystasz).




Kliknij "Zainstaluj", co spowoduje zainstalowanie komponentu.

W zależności od konfiguracji przeglądarki (a także w przypadku braku wystarczających uprawnień, jako że instalacja komponentu wymaga uprawnień administratora lokalnego na danym komputerze), może pojawić się następujący komunikat:

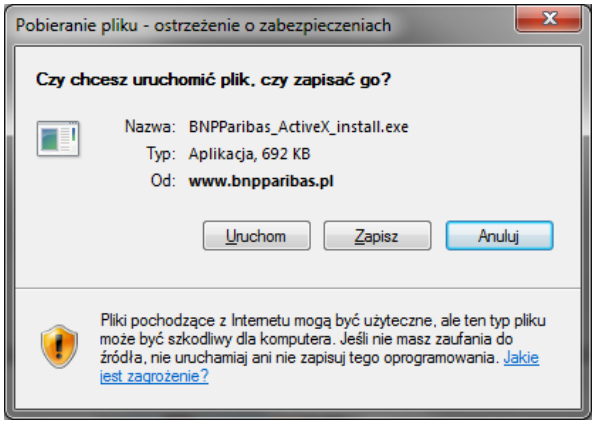



*Ten sam komunikat pojawi się również, jeżeli użytkownik ma uprawnienia administratora, ale kliknie "Nie instaluj".*

**Istnieje również <u>inna możliwość</u> zainstalowania komponentu, jaką jest użycie instalatora dostępnego na stronach internetowych BNP Paribas Bank Polska SA**, w dziale "Bankowość internetowa", w sekcji "Do pobrania" (z prawej strony ekranu), pod adresem:

http://www.bgzbnpparibas.pl/files/BNPParibas_ActiveX_install_x64.exe oraz
http://www.bgzbnpparibas.pl/files/BNPParibas_ActiveX_install.exe

W tym przypadku komponent należy pobrać na dysk komputera:

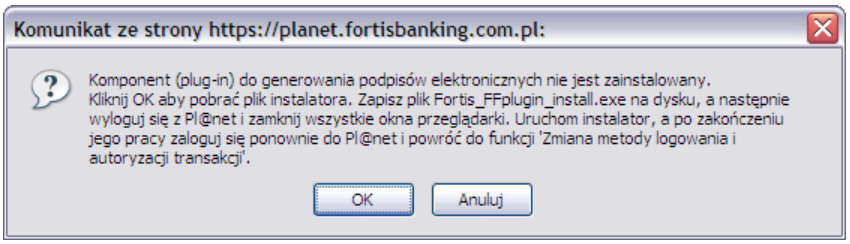


Następnie instalator należy uruchomić (wymagane są do tego uprawnienia administratora lokalnego na danym komputerze):

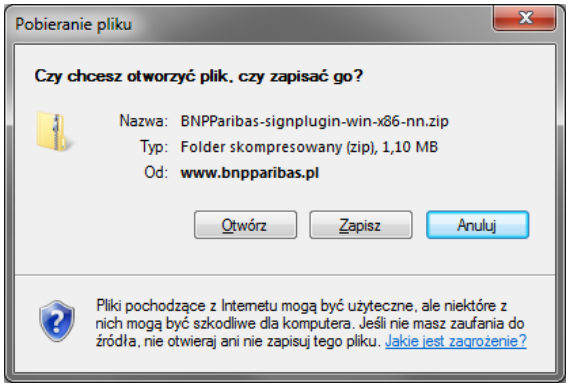

W kolejnych krokach należy wybrać przyciski "Zainstaluj" , "Dalej" , a następnie "Zakończ".

## Instalacja komponentu dla przeglądarek Mozilla Firefox i Netscape Browser

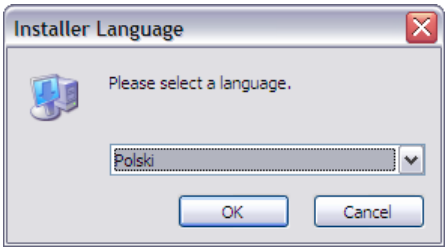
Po kliknięciu przycisku "Wygeneruj klucz" na formatce "Zmiana metody logowania i autoryzacja transakcji", przeglądarka zaproponuje pobranie komponentu do generowania podpisów elektronicznych (chyba że jego najnowsza wersja jest już zainstalowana na komputerze, z którego korzystasz).



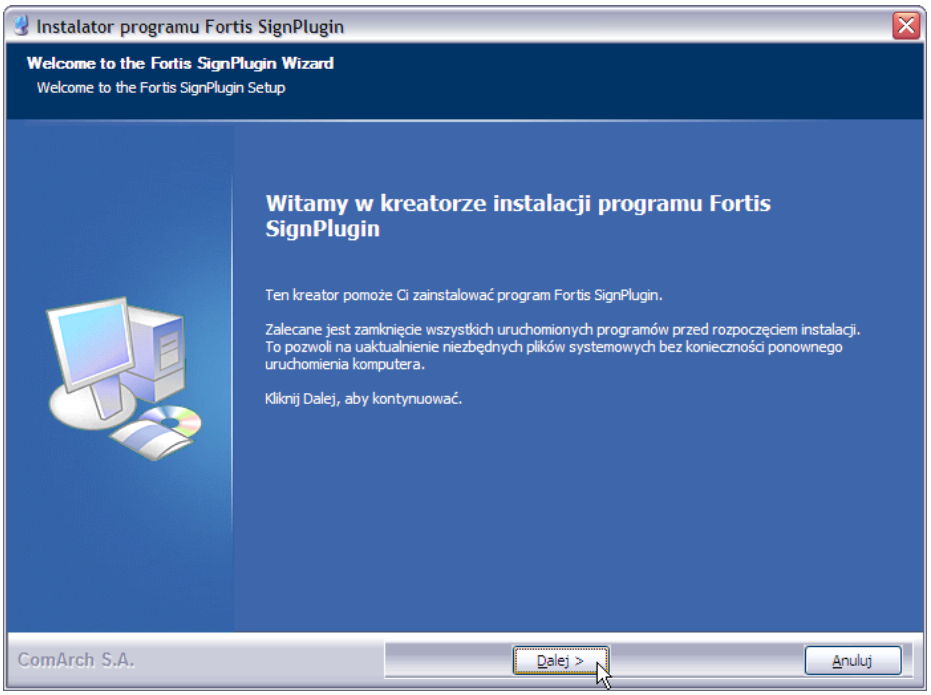

Kliknij "OK", a następnie zapisz plik instalatora na dysku.



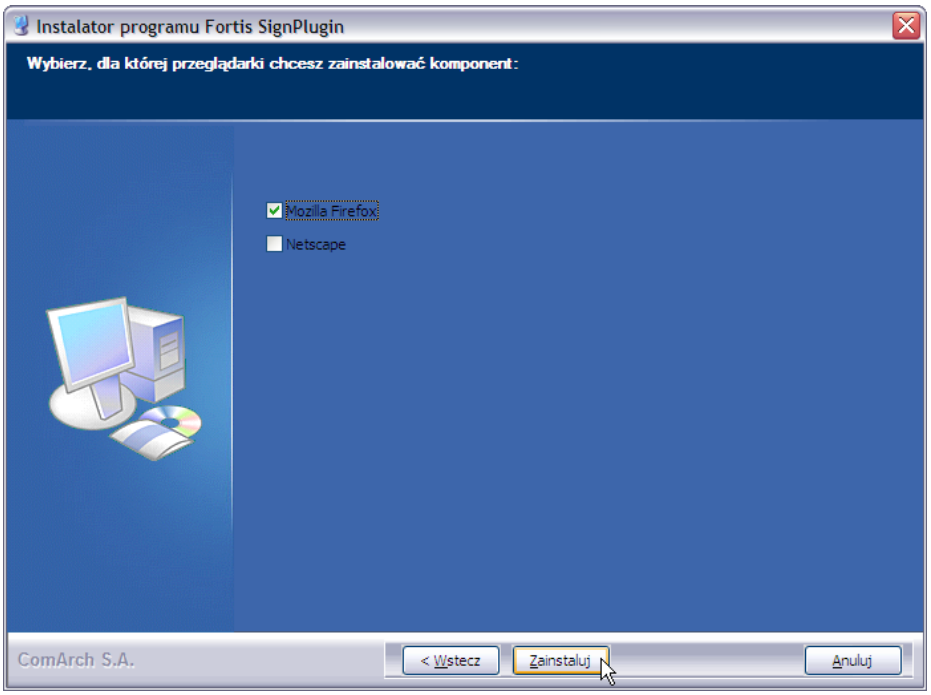
Uruchom plik instalatora (uprawnienia administratora nie są wymagane do instalacji):




Wybierz język instalatora (polski lub angielski) i kliknij "OK".

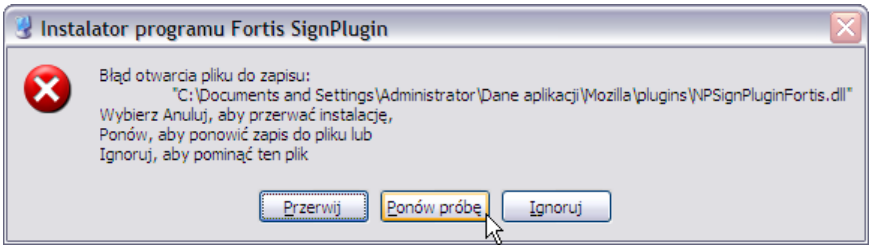



Na kolejnym ekranie instalatora należy wybrać, dla której przeglądarki zainstalować komponent (instalator jest wspólny dla Firefoxa i Netscape):



Następnie kliknij "Zainstaluj", a na kolejnych ekranach "Dalej" i "Zakończ".

**Uwaga**: Jeżeli instalator zgłosi "Błąd otwarcia pliku do zapisu":



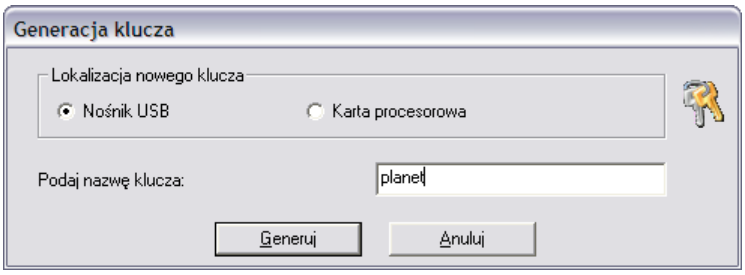

wówczas należy wylogować się z Pl@net lub BiznesPl@net, zamknąć przeglądarkę, a następnie kliknąć "Ponów próbę".

**Komponent można pobrać również ze stron internetowych BNP Paribas Bank Polska SA** - jest on dostępny w dziale "Bankowość internetowa", w sekcji "Do pobrania" (z prawej strony ekranu), pod adresem: http://www.bgzbnpparibas.pl/files/SignPluginInstall6BNPParibas.zip

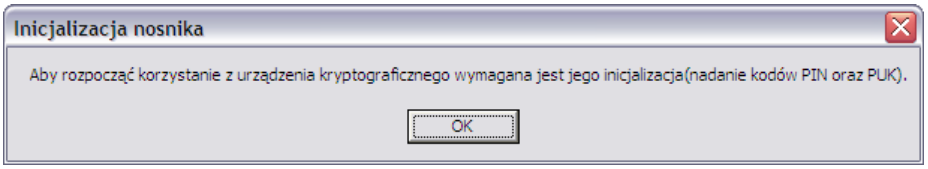
## 3. Inicjalizacja karty lub nośnika USB i wygenerowanie klucza

Po zainstalowaniu komponentu, powracamy do przerwanego wcześniej generowania klucza. Wyświetlony zostanie ekran wyboru rodzaju urządzenia kryptograficznego, na którym ma zostać wygenerowany klucz. Wskaż rodzaj urządzenia z którego korzystasz (nośnik USB bądź karta procesorowa - kryptograficzna), a w polu poniżej wpisz nazwę, pod jaką zostanie zapisany nowo generowany klucz (możesz nadać dowolną nazwę).

Upewnij się że Twój nośnik USB jest podłączony do komputera, a jeśli korzystasz z karty kryptograficznej - czy podłączony jest czytnik, a karta włożona do czytnika.




Jeżeli urządzenie kryptograficzne (nośnik USB lub karta) jest nowe, nieużywane, wymagane jest jego zainicjalizowanie, tzn. zdefiniowanie kodu PIN, który będzie go zabezpieczał, oraz kodu PUK, czyli tzw. kodu odblokowującego. Kliknij "OK" aby przejść do inicjalizacji urządzenia kryptograficznego.



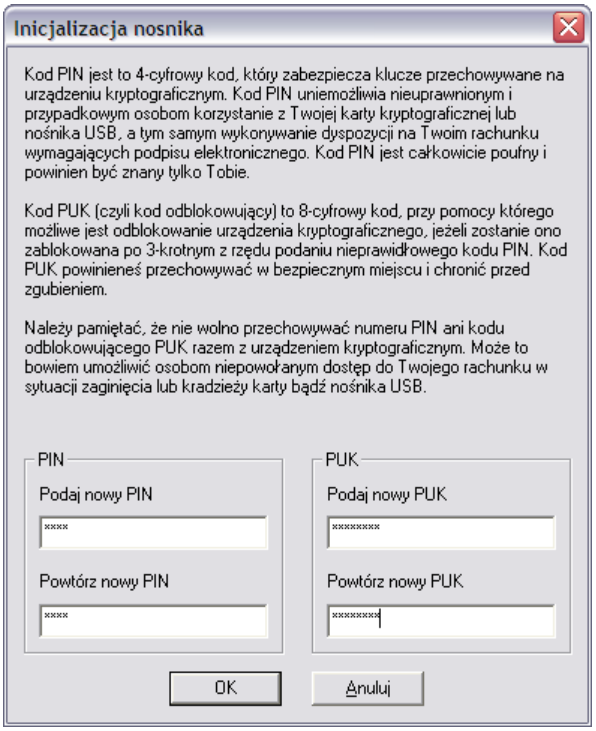

Na wyświetlonym teraz ekranie inicjalizacji urządzenia kryptograficznego zdefiniuj:
- kod PIN (4 cyfry), oraz
- kod PUK (kod odblokowujący - 8 cyfr)

Kod **PIN** to 4-cyfrowy kod, który zabezpiecza klucze przechowywane na urządzeniu kryptograficznym. Kod PIN uniemożliwia nieuprawnionym i przypadkowym osobom korzystanie z Twojej karty kryptograficznej lub

nośnika USB, a tym samym wykonywanie dyspozycji na Twoim rachunku wymagających podpisu elektronicznego. Kod PIN jest całkowicie poufny i powinien być znany tylko Tobie.

Kod **PUK**, czyli kod odblokowujący, to 8-cyfrowy kod, przy pomocy którego możliwe jest odblokowanie urządzenia kryptograficznego, jeżeli zostanie ono zablokowane po 5-krotnym z rzędu podaniu nieprawidłowego kodu PIN. Kod PUK powinieneś przechowywać w bezpiecznym miejscu i chronić przed zgubieniem.

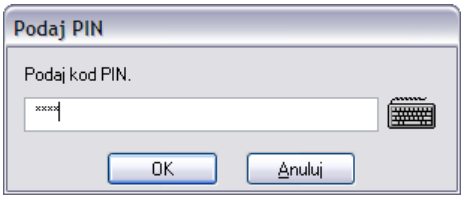
Dla uniknięcia pomyłki, każdy z kodów należy wprowadzić dwukrotnie. Zatwierdź przyciskiem "OK".




**Uwaga: pamiętaj, by nie przechowywać kodu PIN ani kodu odblokowującego PUK razem z urządzeniem kryptograficznym (nośnikiem USB czy kartą kryptograficzną). Może to bowiem umożliwić osobom niepowołanym dostęp do Twojego rachunku w sytuacji zaginięcia lub kradzieży Twojego urządzenia kryptograficznego.**

**Uwaga:** jeżeli urządzenie kryptograficzne (karta lub nośnik USB) zostanie zablokowane po 5-krotnym z rzędu podaniu nieprawidłowego kodu PIN, a nie pamiętasz kodu PUK, możesz nadal korzystać z tego urządzenia - wystarczy ponownie je zainicjalizować. Podczas inicjalizacji, zostaną jednak usunięte wszystkie klucze zapisane na danym urządzeniu.

Po zatwierdzeniu przyciskiem "OK" system zaproponuje wydrukowanie kodu PUK, po czym powróci do przerwanej wcześniej operacji generowania nowego klucza. Wyświetlone zostanie okienko z prośbą o podanie kodu PIN - wpisz kod, który zdefiniowałeś chwilę wcześniej.




Zatwierdź przyciskiem "OK". Zaczekaj aż system wygeneruje klucz i zapisze go w pamięci chipa na karcie lub nośniku USB.

**Jeśli posiadasz uprawnienia do rachunków więcej niż jednego podmiotu (np. rachunku firmowego oraz prywatnego, etc.)**, system zapyta czy chcesz aby zmiana metody logowania i autoryzacji metody dotyczyła wszystkich z nich, czy tylko tego, w kontekście którego aktualnie pracujesz. Kliknij "OK" aby zmienić metodę dla wszystkich rachunków. Jeżeli wybierzesz "Anuluj", zmiana metody na podpis elektroniczny będzie dotyczyć tylko rachunków tego podmiotu, w kontekście którego obecnie pracujesz.

Dyspozycja zmiany metody logowania i autoryzacji transakcji musi zostać potwierdzona przy pomocy dotychczas wykorzystywanej metody - kodu SMS. Wpisz otrzymany kod SMS i kliknij "Podpisz".

Zostanie wyświetlony komunikat potwierdzający zmianę metody logowania i autoryzacji transakcji na podpis elektroniczny. Zmiana odnosi skutek począwszy od następnego logowania - wyloguj się z systemu i zaloguj ponownie - tym razem już przy użyciu podpisu elektronicznego.