



BGZ BNP PARIBAS

Instrukcja instalacji urządzeń kryptograficznych

dla użytkowników rozpoczynających korzystanie z systemu Pl@net lub
BiznesPl@net



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

- 1. Instalacja komponentu do generowania podpisów elektronicznych**
- 2. Instalacja oprogramowania Comarch SmartCard do obsługi urządzeń kryptograficznych**
- 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 PI@net i BiznesPI@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).

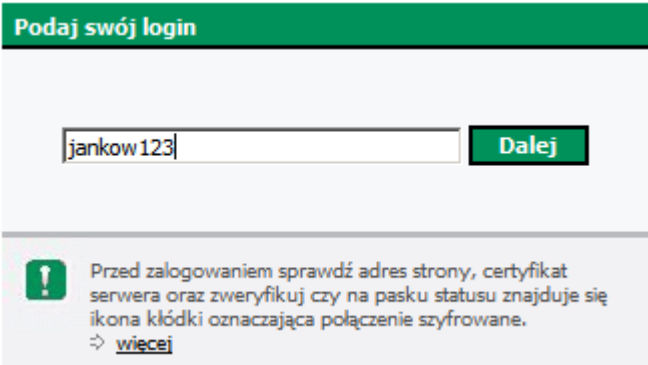
Jeżeli logujesz się do PI@net lub BiznesPI@net po raz pierwszy (a wybraną przez Ciebie metodą logowania i autoryzacji transakcji jest podpis elektroniczny), podczas pierwszego logowania system automatycznie sprawdzi czy na komputerze z którego korzystasz jest zainstalowane niezbędne oprogramowanie i, w razie wykrycia jego braku, przystąpi do ich instalacji. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie lub skorzystaj z niniejszej instrukcji.

1. Instalacja komponentu do generowania podpisów elektronicznych

Instalacja komponentu dla przeglądarki Microsoft Internet Explorer

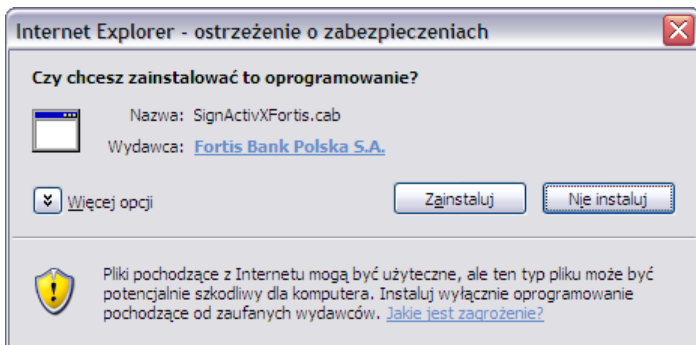
Jeżeli logujesz się do PI@net lub BiznesPI@net po raz pierwszy, lub otrzymałeś pakiet startowy z początkowym hasłem logowania, uruchom przeglądarkę i przejdź na stronę logowania systemu PI@net lub BiznesPI@net:

- logowanie do systemu PI@net: <https://planet.bgzbnpparibas.pl>
- logowanie do systemu BiznesPI@net: <https://biznesplanet.bgzbnpparibas.pl>



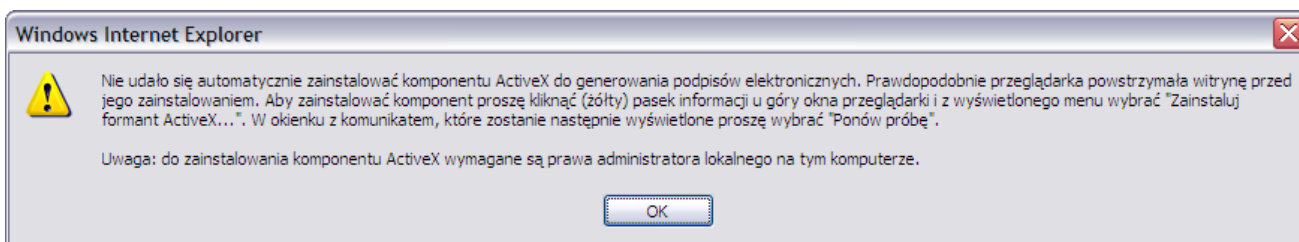
The image shows a login interface. At the top, there is a green header with the text "Podaj swój login". Below this is a text input field containing "jankow123" and a green button labeled "Dalej". Below the input field, there is a warning icon (exclamation mark in a green square) followed by the text: "Przed zalogowaniem sprawdź adres strony, certyfikat serwera oraz zweryfikuj czy na pasku statusu znajduje się ikona kłódki oznaczająca połączenie szyfrowane." Below this text is a link "wiecej" with a right-pointing arrow.

Wpisz swój login (nazwę użytkownika) i kliknij "Dalej". Przeglądarka - o ile została uruchomiona z uprawnieniami administratora - od razu zaproponuje instalację komponentu (chyba że jego najnowsza wersja jest już zainstalowana na komputerze, z którego korzystasz).



Kliknij "Zainstaluj", co spowoduje zainstalowanie komponentu. Podczas kolejnych logowań komunikat ten nie będzie się już pojawiać.

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:



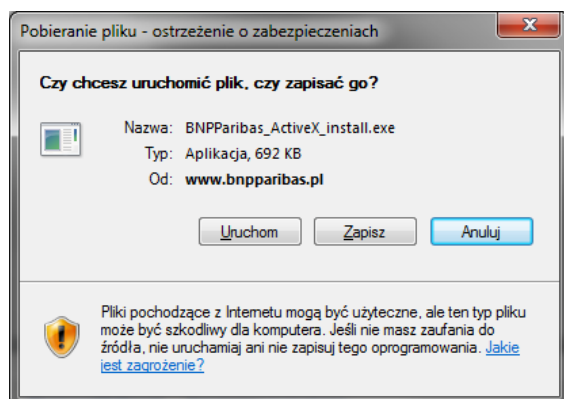
Ten sam komunikat pojawi się również, jeżeli użytkownik ma uprawnienia administratora, ale kliknie "Nie instaluj".

Istnieje również inna możliwość zainstalowania komponentu, jaką jest użycie instalatora dostępnego na stronach internetowych Banku BGŻ BNP Paribas S.A., w dziale "Bankowość internetowa", w sekcji "Do pobrania" (z prawej strony ekranu), pod adresem:

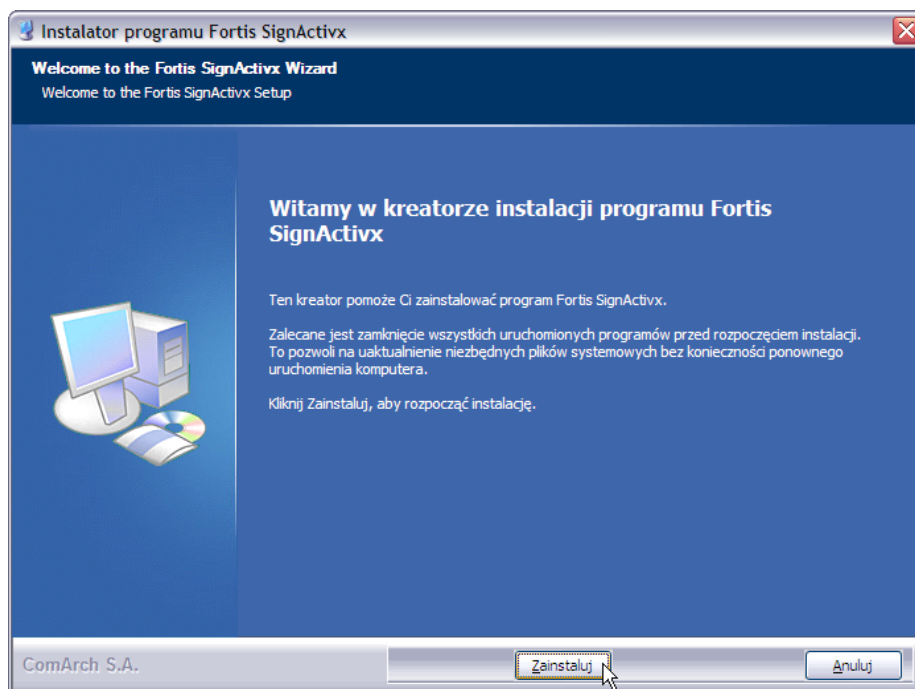
bgzhttp://www.bgzbnpparibas.pl/files/BNPParibas_ActiveX_install.exe lub

http://www.bnpparibas.pl/files/BNPParibas_ActiveX_install_x64.exe

\W tym przypadku komponent należy pobrać na dysk komputera:



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

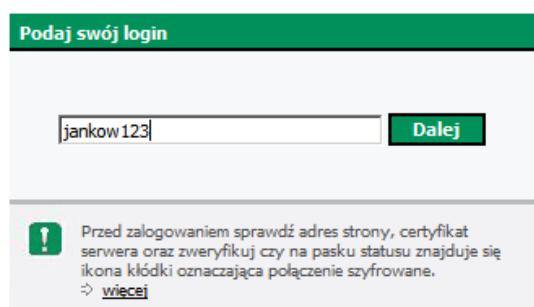


W kolejnych krokach należy wybrać przyciski "Zainstaluj" , "Dalej" , a następnie "Zakończ".

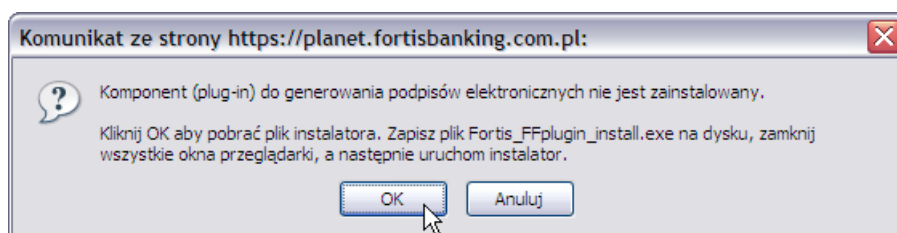
Instalacja komponentu dla przeglądarek Mozilla Firefox i Netscape Browser

Jeżeli logujesz się do PI@net lub BiznesPI@net po raz pierwszy, lub otrzymałeś pakiet startowy z początkowym hasłem logowania, uruchom przeglądarkę i przejdź na stronę logowania systemu PI@net lub BiznesPI@net:

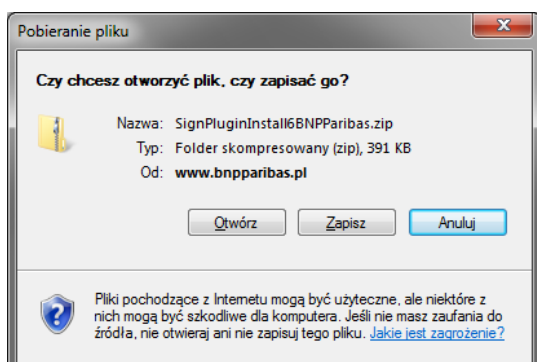
- logowanie do systemu PI@net: <https://planet.bgzbnpparibas.pl>
- logowanie do systemu BiznesPI@net: <https://biznesplanet.bgzbnpparibas.pl>



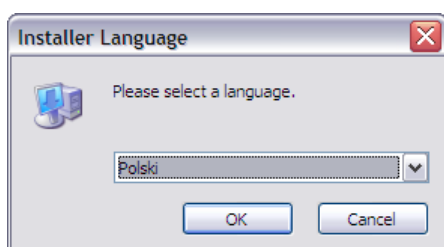
Wpisz swój login (nazwę użytkownika) i kliknij "Dalej". Przeglądarka od razu zaproponuje pobranie komponentu (chyba że jego najnowsza wersja jest już zainstalowana na komputerze, z którego korzystasz).



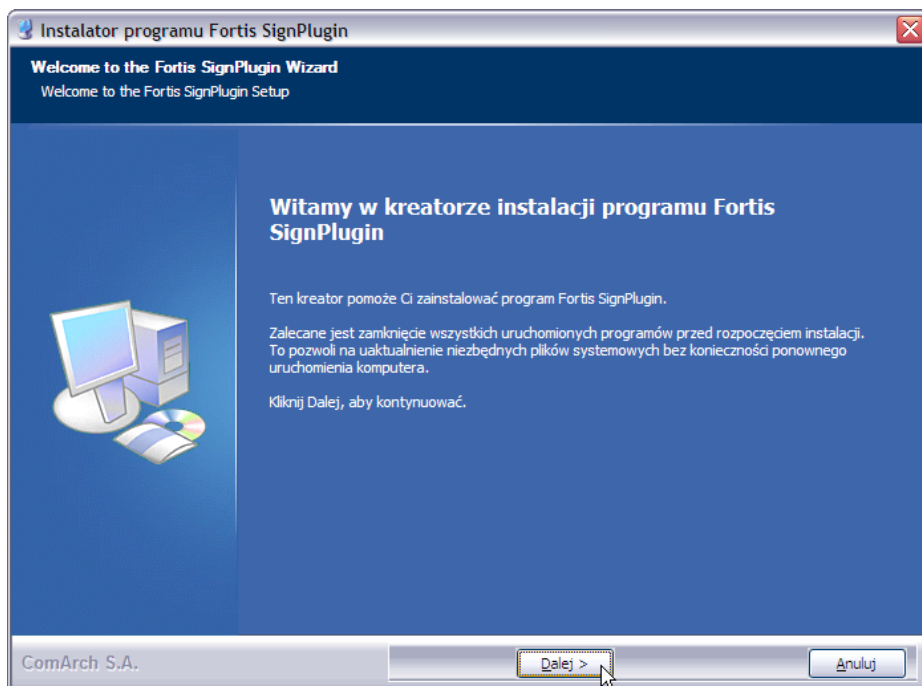
Kliknij "OK", a następnie zapisz plik instalatora na dysku.



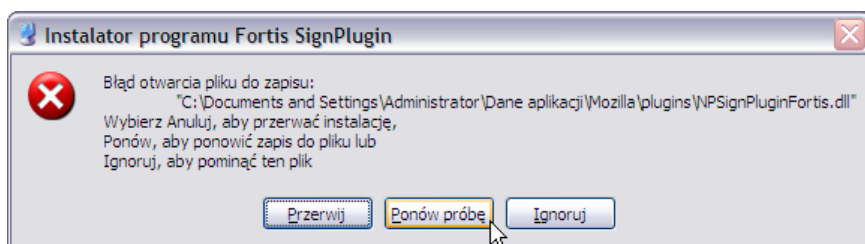
Uruchom plik instalatora (uprawnienia administratora nie są wymagane do instalacji):



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

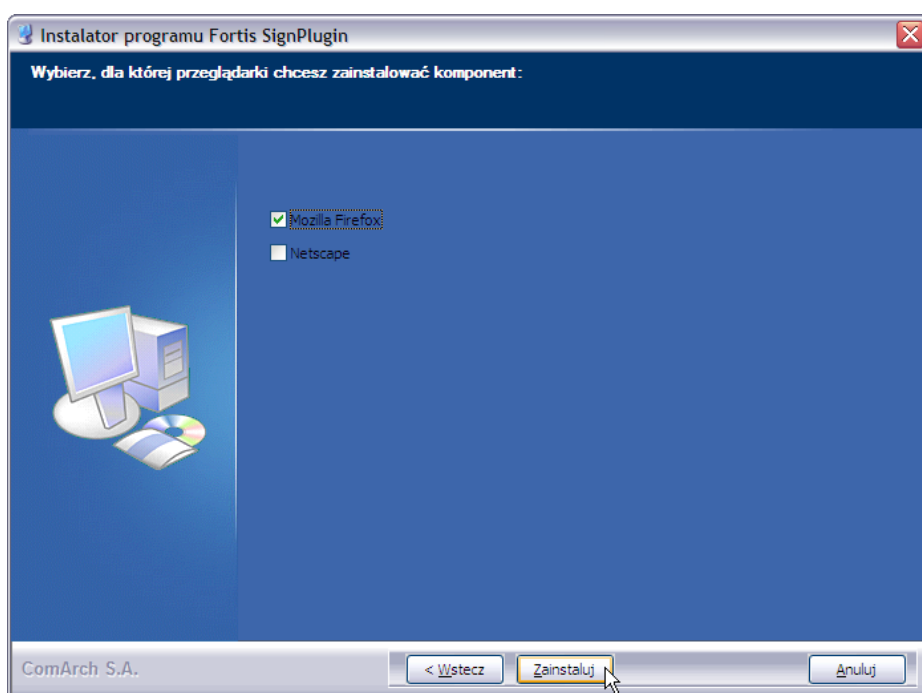


Jeżeli przed uruchomieniem instalatora nie zostały zamknięte wszystkie okna przeglądarki, instalator może zgłosić błąd:



W takiej sytuacji należy zamknąć przeglądarkę, a następnie kliknąć "Ponów próbę".

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".

Komponent można pobrać również ze stron internetowych Banku BGŻ BNP Paribas SA - jest on dostępny w dziale "Bankowość internetowa", w sekcji "Do pobrania" (z prawej strony ekranu), pod adresem:

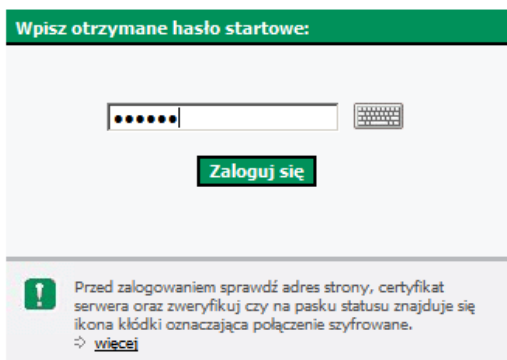
<http://www.bgzbnpparibas.pl/files/SignPluginInstall6BNPParibas.zip>

Teraz **powróć do strony logowania systemu PI@net lub BiznesPI@net**. Wpisz swój login i kliknij "Dalej".

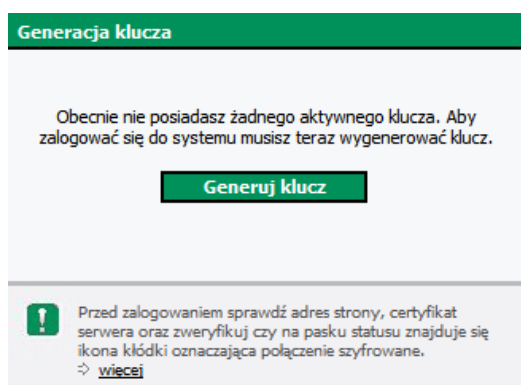
2. Instalacja oprogramowania Comarch SmartCard do obsługi urządzeń kryptograficznych

Kolejną czynnością, którą należy wykonać, jest zainstalowanie oprogramowania Comarch SmartCard - jest ono niezbędne, aby móc korzystać z urządzeń kryptograficznych - kart kryptograficznych oraz nośników USB.

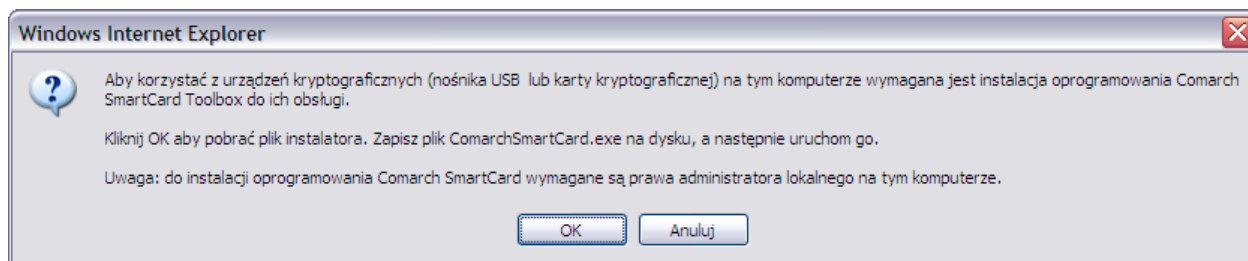
Powróć do strony logowania systemu PI@net lub BiznesPI@net i wpisz hasło z pakietu startowego:



...a następnie kliknij "Zaloguj się". System zaproponuje teraz wygenerowanie klucza - kliknij "Generuj klucz".

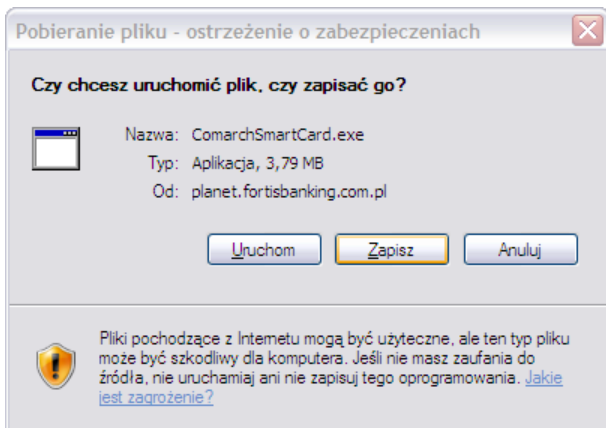


Zanim jednak możliwe będzie wygenerowanie klucza, niezbędna jest instalacja oprogramowania Comarch SmartCard do obsługi urządzeń kryptograficznych. Jeżeli na komputerze z którego korzystasz nie zostało ono zainstalowane, system automatycznie wykryje to i zaproponuje instalację:



Instalacja odbywa się za pomocą łatwego w obsłudze kreatora. Kliknij "OK" aby pobrać plik instalatora. Zapisz plik ComarchSmartCard.exe na dysku komputera, a następnie uruchom go.

Uwaga: Instalacja wymaga posiadania uprawnień administratora na danym komputerze.

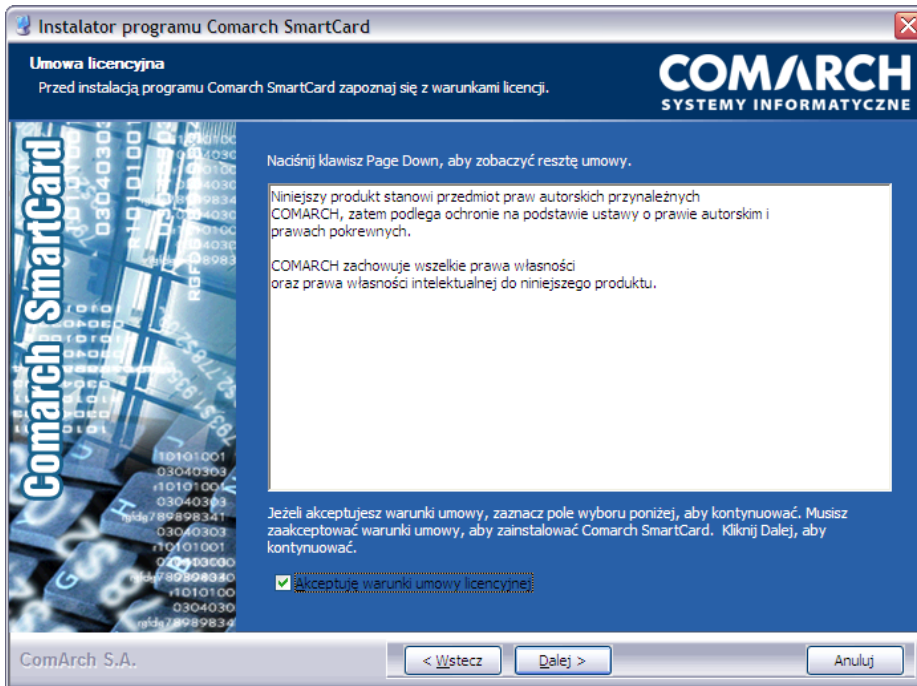


Plik instalacyjny ComarchSmartCard.exe możesz również pobrać ze stron internetowych BNP Paribas Bank Polska SA - jest on udostępniony w dziale "Bankowość internetowa", w sekcji "Do pobrania" (z prawej strony ekranu), pod adresem: http://www.bgzbnpparibas.pl/files/comarchsc_bnpparibas.exe (rozmiar pliku: 20.5 MB).

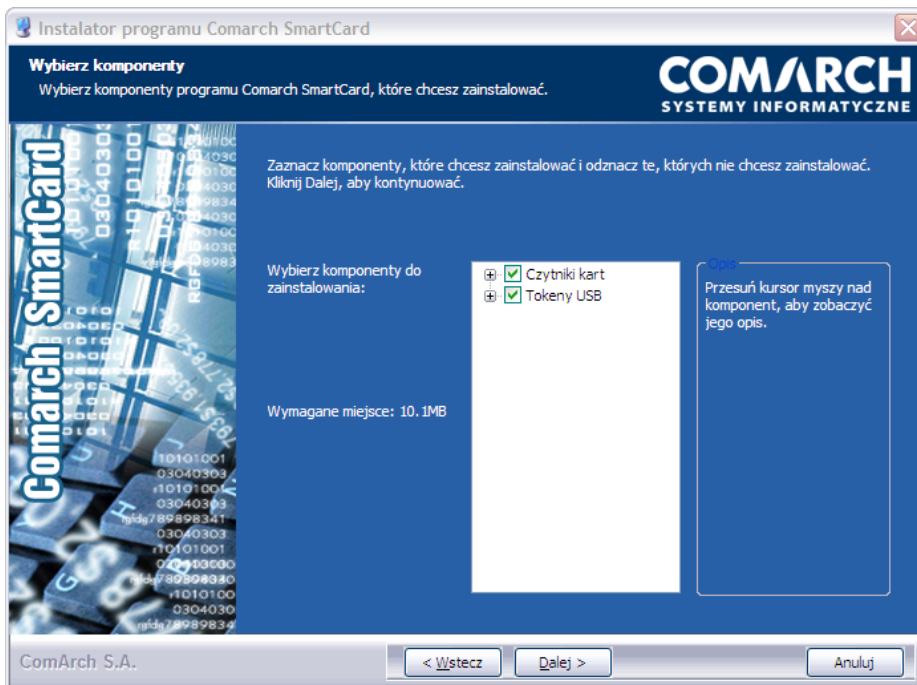
Po uruchomieniu instalatora, postępuj zgodnie ze wskazówkami wyświetlanymi na ekranie, posługując się przyciskiem "Dalej".



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

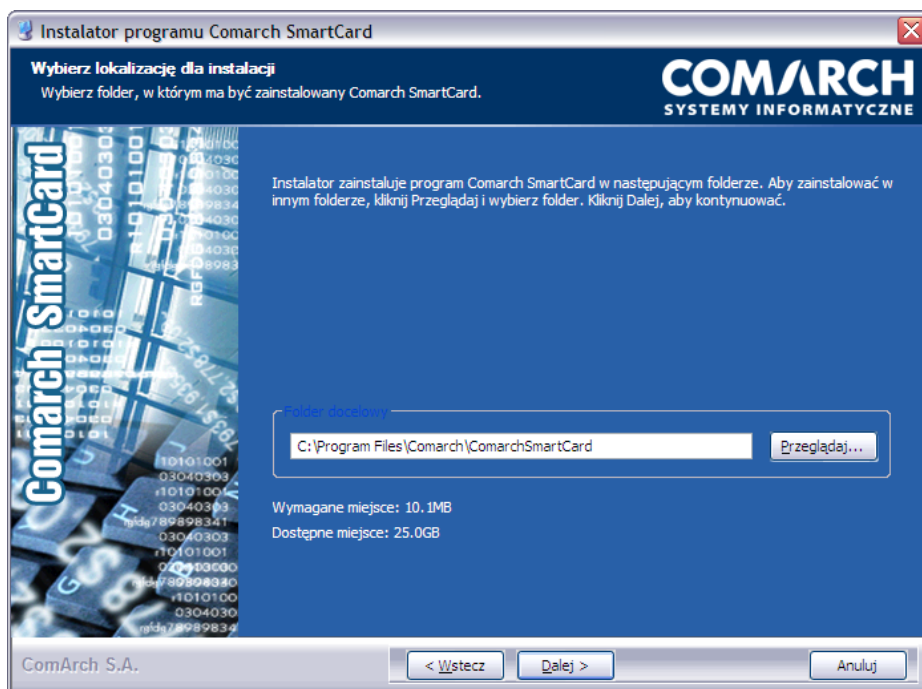


Instalator zaproponuje teraz instalację sterowników do czytnika kart oraz nośników kryptograficznych USB. Pozostaw zaznaczone pola wyboru przy obydwu komponentach (zarówno "Czytniki kart" jak i "Tokeny USB") i kliknij "Dalej".

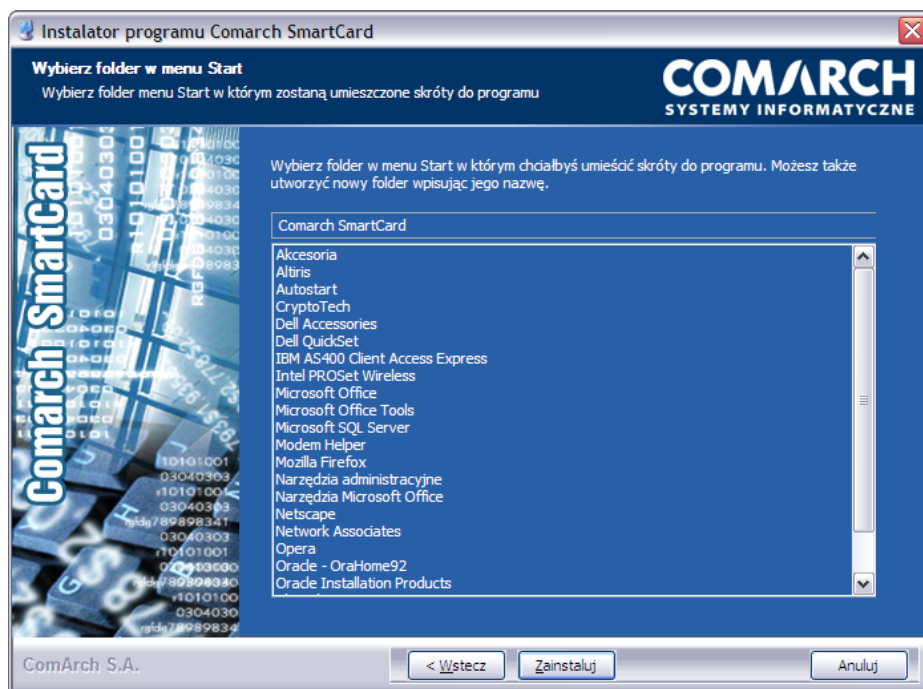


Jeżeli nie chcesz instalować nadmiarowych sterowników, możesz odznaczyć pole wyboru przy urządzeniach, z których nie będziesz korzystał - jeśli zamierzasz używać tylko nośnika kryptograficznego USB, wystarczy że zainstalujesz sterowniki Gem e-Seal z grupy "Tokeny USB". Z kolei, jeśli będziesz korzystał 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.

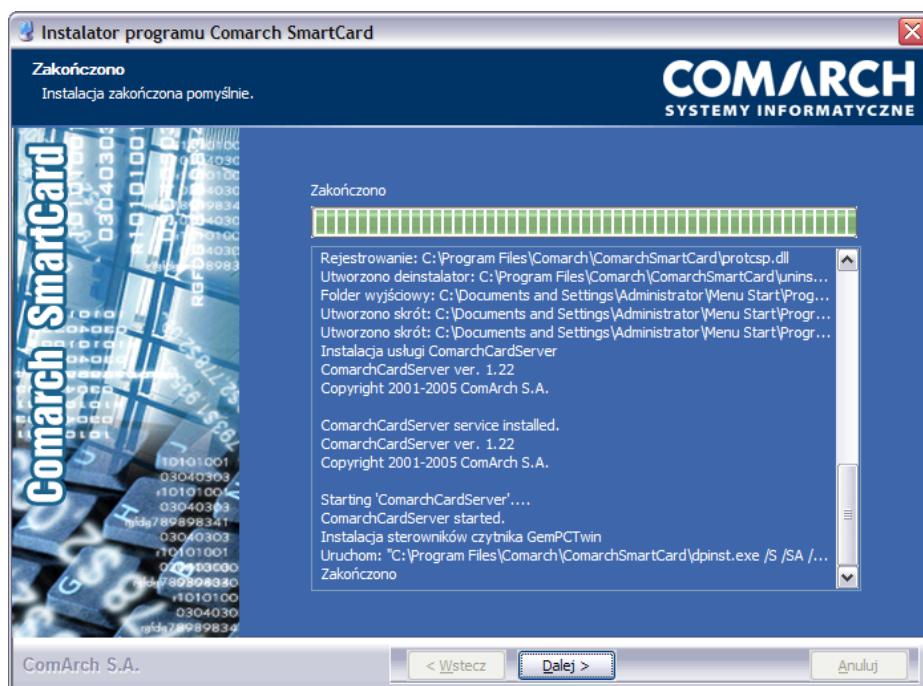
Następnie, określ miejsce instalacji aplikacji - zaakceptuj domyślnie proponowany folder lub zmień go korzystając z przycisku "Przełączaj...":



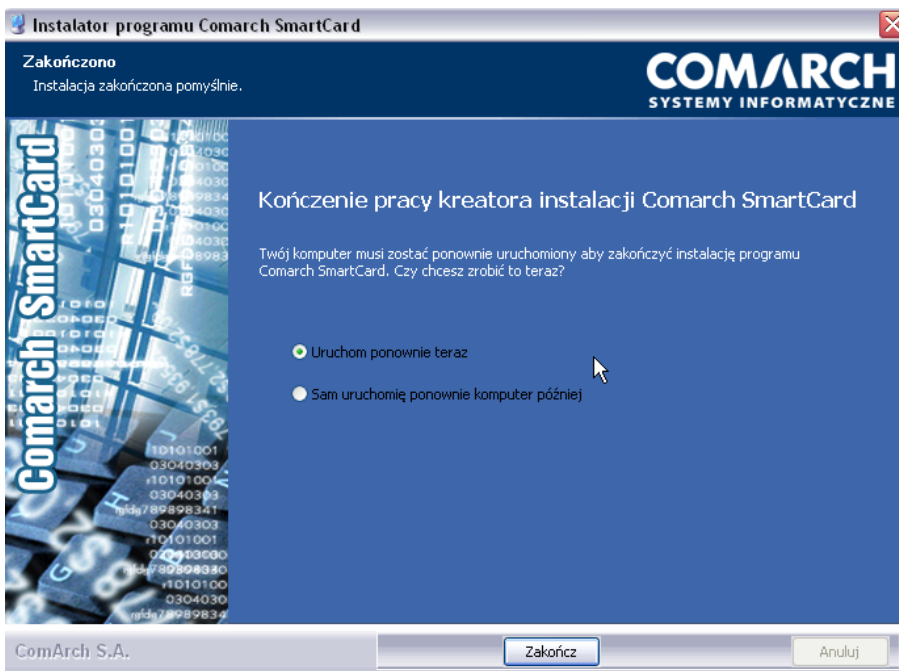
W kolejnym kroku instalator poprosi o wybranie foldera w menu Start, w którym umieszczony zostanie skrót uruchamiający aplikację. Wskaż folder i kliknij "Zainstaluj":



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



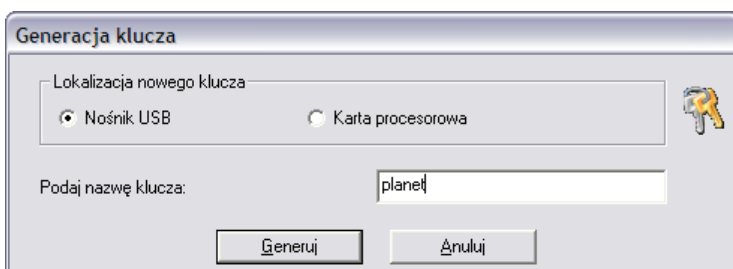
Instalacja dobiegła końca. Jeśli korzystasz z systemu Windows 98 lub Windows ME konieczne będzie jeszcze zrestartowanie komputera - zaznacz opcję "Uruchom ponownie teraz" i kliknij "Zakończ". W przypadku nowszych wersji systemu Windows (Vista, XP lub Windows 2000) restart nie jest konieczny - zaznacz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



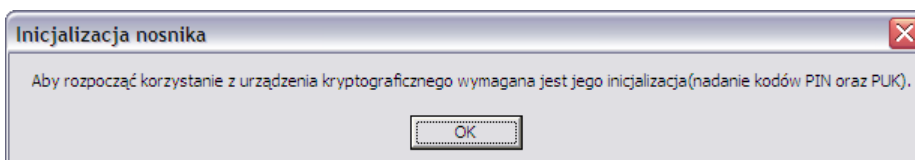
3. Inicjalizacja karty lub nośnika USB i wygenerowanie klucza

Po zainstalowaniu oprogramowania Comarch SmartCard możesz powrócić do przerwanej wcześniej generowania klucza. Podłącz teraz nośnik USB do komputera lub podłącz czytnik kart i włóż kartę do czytnika. Następnie, powróć do przeglądarki i kliknij przycisk "Generuj klucz".

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).



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".

Inicjalizacja nośnika

Kod PIN jest 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 3-krotnym z rzędu podaniu nieprawidłowego kodu PIN. Kod PUK powinieneś przechowywać w bezpiecznym miejscu i chronić przed zgubieniem.

Należy pamiętać, że nie wolno przechowywać numeru PIN ani kodu odblokowującego PUK razem z urządzeniem kryptograficznym. Może to bowiem umożliwić osobom niepowołanym dostęp do Twojego rachunku w sytuacji zaginięcia lub kradzieży karty bądź nośnika USB.

PIN

Podaj nowy PIN

xxxxxx

Powtórz nowy PIN

xxxxxx

PUK

Podaj nowy PUK

xxxxxxxxxx

Powtórz nowy PUK

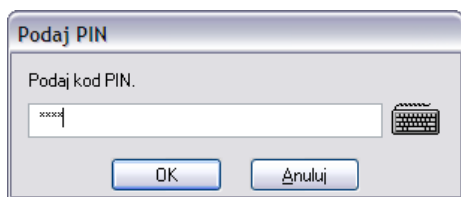
xxxxxxxxxx

OK Anuluj

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.

Po zakończeniu generowania klucza, zostaniesz zalogowany do systemu PI@net lub BiznesPI@net.