

**Instrukcja instalacji
czytników, kart
procesorowych, certyfikatów
kwalifikowanych oraz
generowania podpisu
elektronicznego**

SPIS TREŚCI:

1. Instalacja czytnika kart procesorowych	3
2. Instalacja oprogramowania kart procesorowych ComArch Smart Card.....	6
3. Przygotowanie podpisu elektronicznego na karcie procesorowej ComArchSmartCard	9
3.1 Tworzenie kluczy podpisu elektronicznego na karcie procesorowej ComArch Smart Card w procesie logowania	9
3.2 Tworzenie kluczy podpisu elektronicznego na karcie procesorowej ComArch Smart Card po zalogowaniu do Systemu.....	13
4. Certyfikaty kwalifikowane.....	16
4.1 Proces dodawania certyfikatu kwalifikowanego do systemu bankowości internetowej dla Klientów biznesowych (BusinessPro).....	16
5. Doradztwo i wsparcie techniczne.....	17

1. Instalacja czytnika kart procesorowych

System bankowości internetowej dla Klientów biznesowych (BusinessPro) obsługuje praktycznie każdy dostępny na rynku czytnik kart procesorowych.

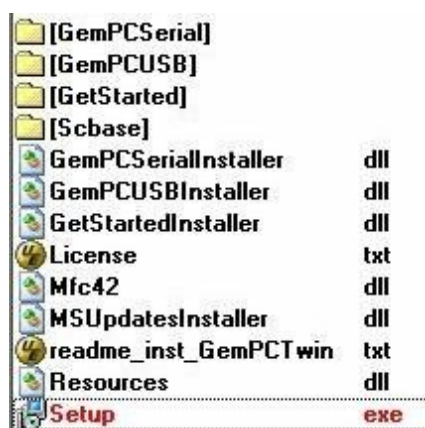
W przypadku, gdy w systemie operacyjnym komputera jest już zainstalowany dowolny czytnik kart procesorowych nie należy instalować kolejnego czytnika. Należy wykorzystać obecnie zainstalowany.

W przypadku, gdy w systemie operacyjnym zainstalowany jest dowolny czytnik, lecz jest on odłączony od komputera i niewykorzystywany, należy odinstalować jego sterowniki w „Dodaj usuń programy”, zrestartować komputer, a następnie podłączyć nowy czytnik i zainstalować jego sterowniki. W przypadku konieczności instalacji czytnika kart należy skorzystać ze sterowników dostarczonych przez producenta czytnika.

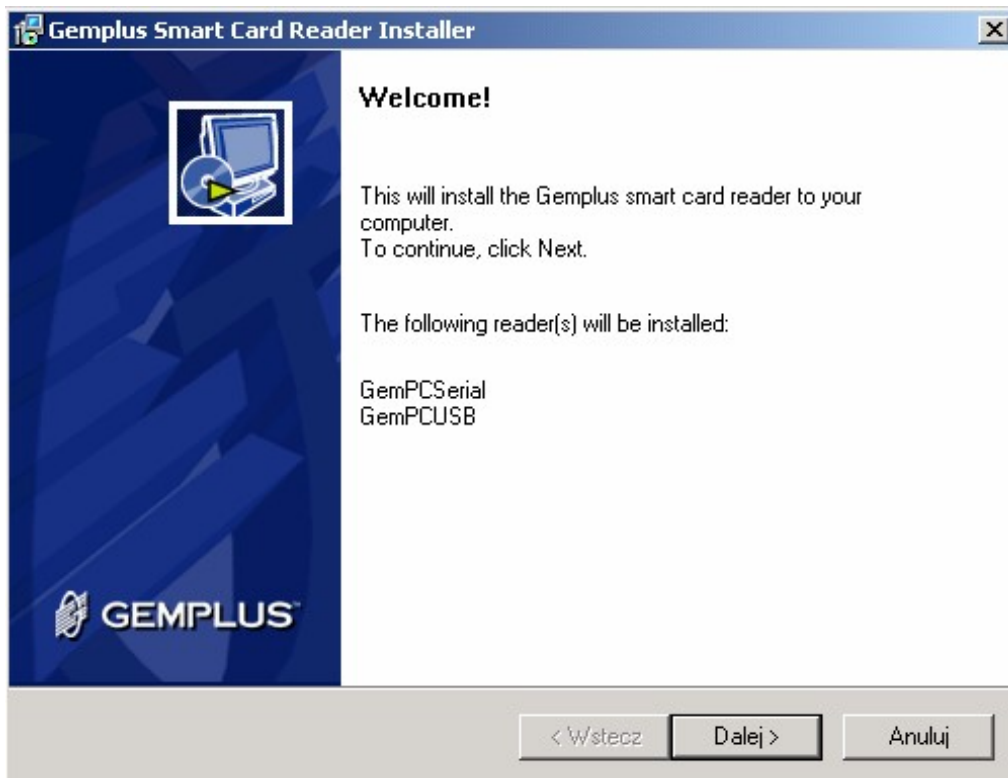
Karta procesorowa zintegrowana z czytnikiem 'gemalto' nie wymaga instalacji sterowników czytnika, a wyłącznie oprogramowania do obsługi karty Comarch SmartCard (patrz: Rozdział 2, strona: 6). Do jej poprawnego działania wymagany jest system Windows XP z poprawką SP2 lub wyższą.

Poniżej przedstawiamy działania, jakie należy wykonać w celu poprawnej instalacji sterowników do czytnika:

1. W zależności od posiadanego rodzaju czytnika (podłączenie USB, PCMCIA) pobieramy oprogramowanie z wyżej wskazanego źródła.
2. Rozpakowujemy pobrany plik ze sterownikami.
3. Po rozpakowaniu do osobnego katalogu, uruchamiamy plik **setup.exe**. (UWAGA: czytnik powinien być odłączony w czasie instalacji oprogramowania).



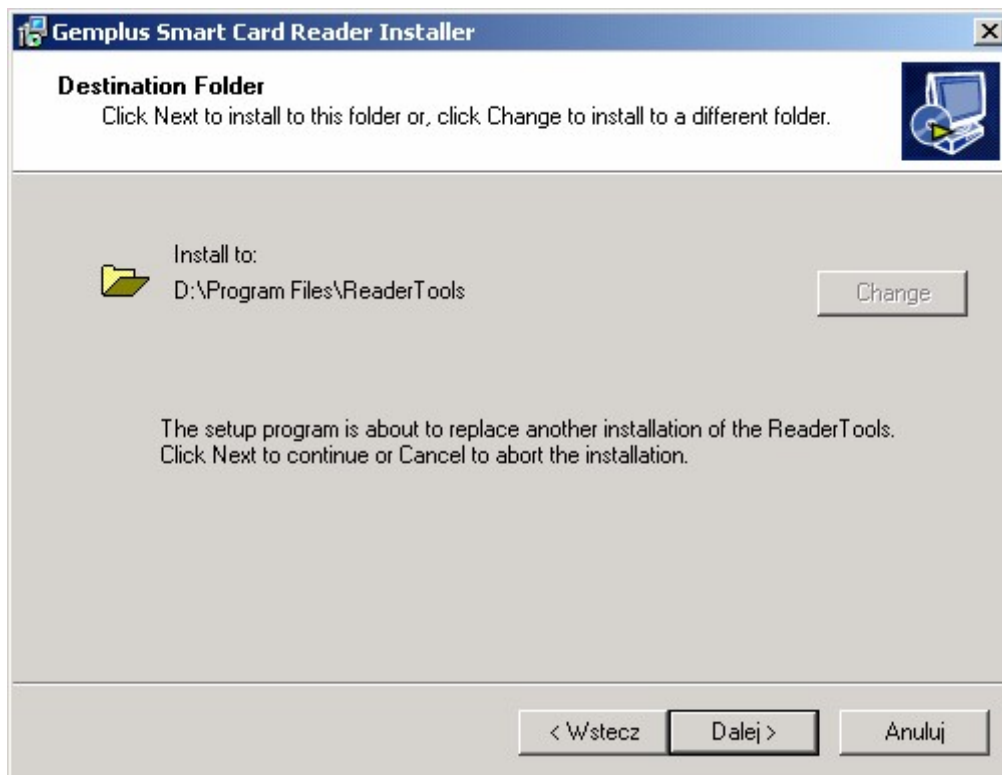
Na pytania instalatora odpowiadamy zgodnie z wytycznymi:



Następnie po zapoznaniu się z Umową Licencyjną akceptujemy ją.



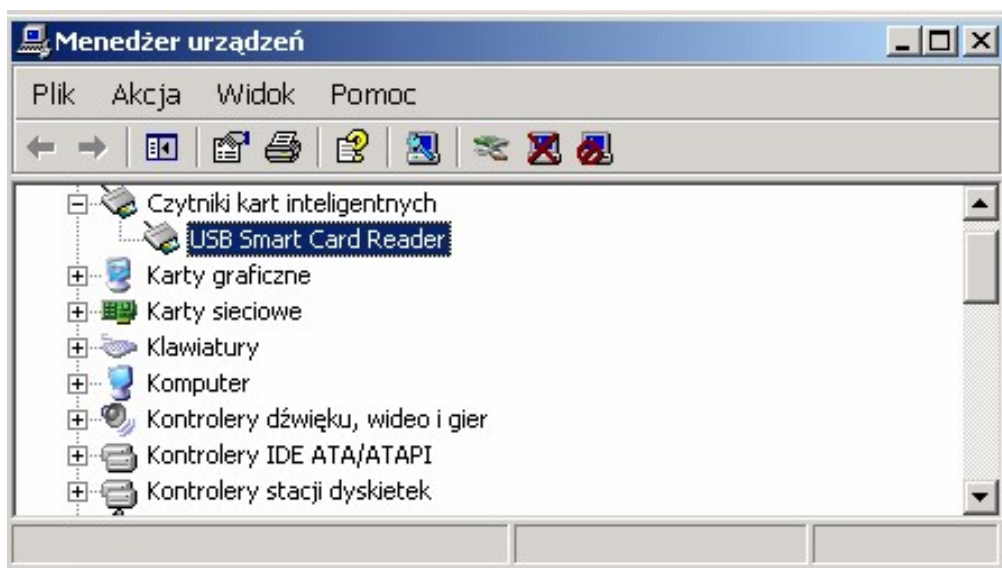
Kolejnym krokiem jest wybór miejsca docelowej instalacji.



4. Po zakończeniu instalacji wymagany jest restart komputera.

5. Po restartowaniu komputera należy podłączyć czytnik do komputera.

Czytnik powinien być widoczny w „Menedżerze urządzeń” (Panel sterowania -> System -> Sprzęt)

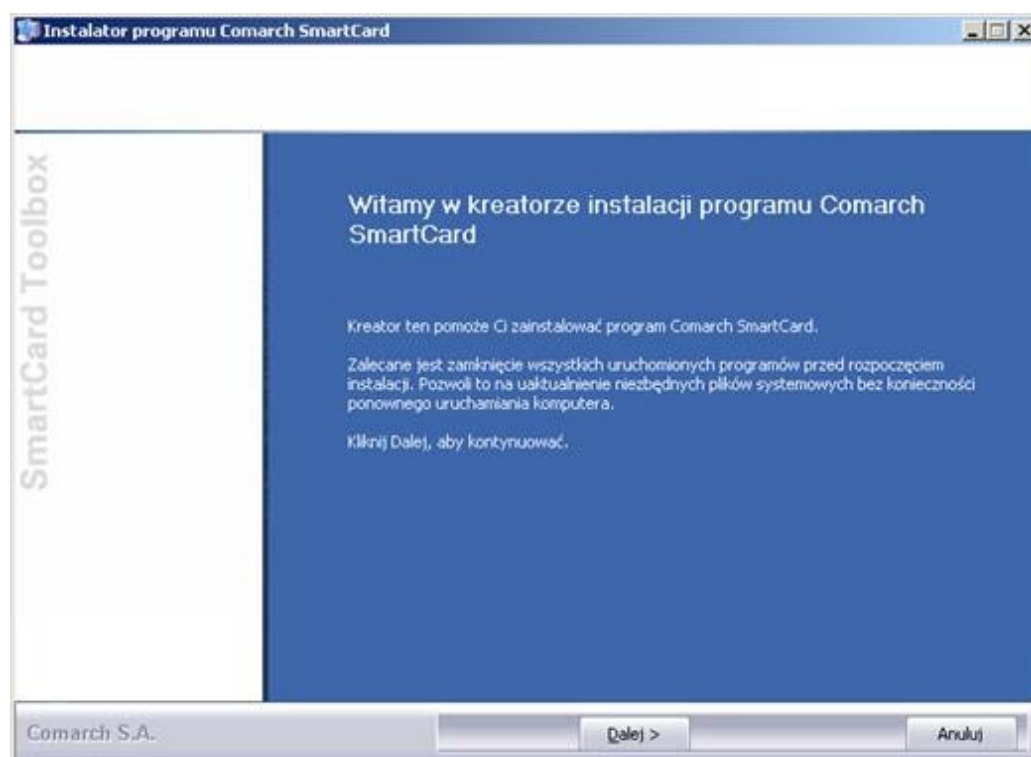


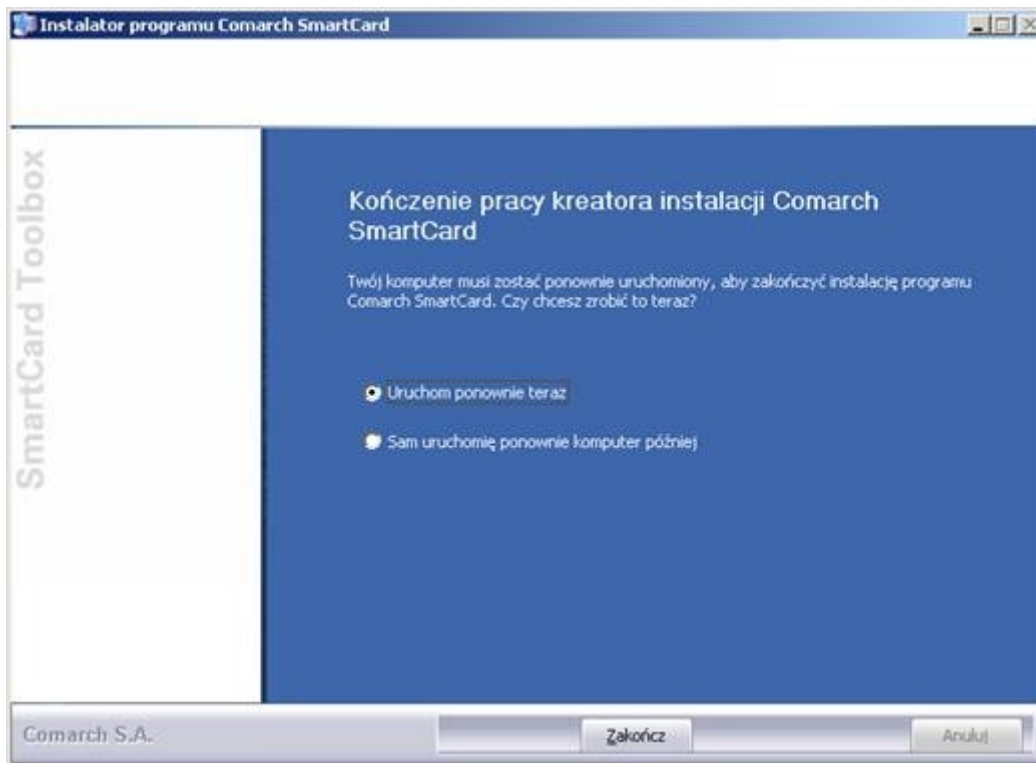
2. Instalacja oprogramowania kart procesorowych ComArch Smart Card

Sterowniki do kart procesorowych są dostępne na stronie www bankowości internetowej dla Klientów biznesowych (BusinessPro) w sekcji **Karty ComArch SmartCard**. Poniżej przedstawiamy działania, jakie należy wykonać w celu poprawnej instalacji sterowników do kart procesorowych:

1. Rozpakowujemy pobrany plik ze sterownikami.
2. Po rozpakowaniu uruchamiamy plik **ComarchSmartCard.exe**.
3. Na pytania instalatora odpowiadamy zgodnie z wytycznymi domyślnymi:

Należy zainstalować oprogramowanie do czytnika, a następnie podłączyć czytnik do komputera.

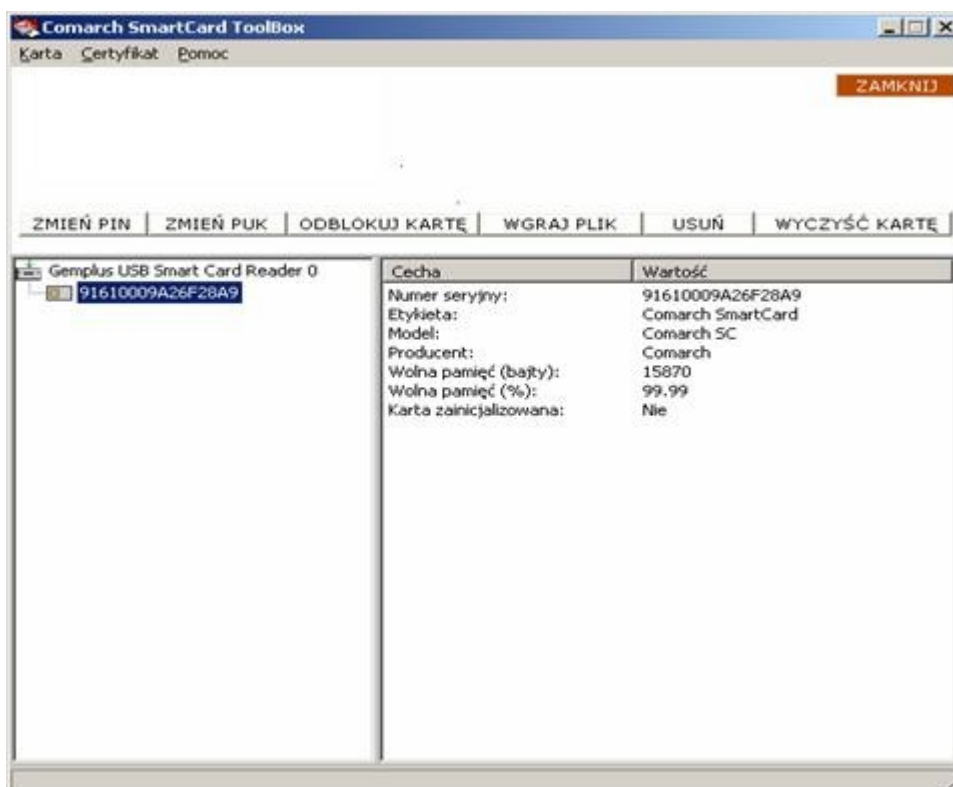




4. Po zakończeniu instalacji wymagany jest restart komputera.

5. Po restartowaniu komputera karta procesorowa powinna działać już poprawnie.

6. W menu Start -> Programy -> Comarch SmartCard powinien być widoczny program **SmartCard Toolbox** służący do zarządzania kartą.



Przykładowy wygląd karty procesorowej zintegrowanej z czytnikiem:

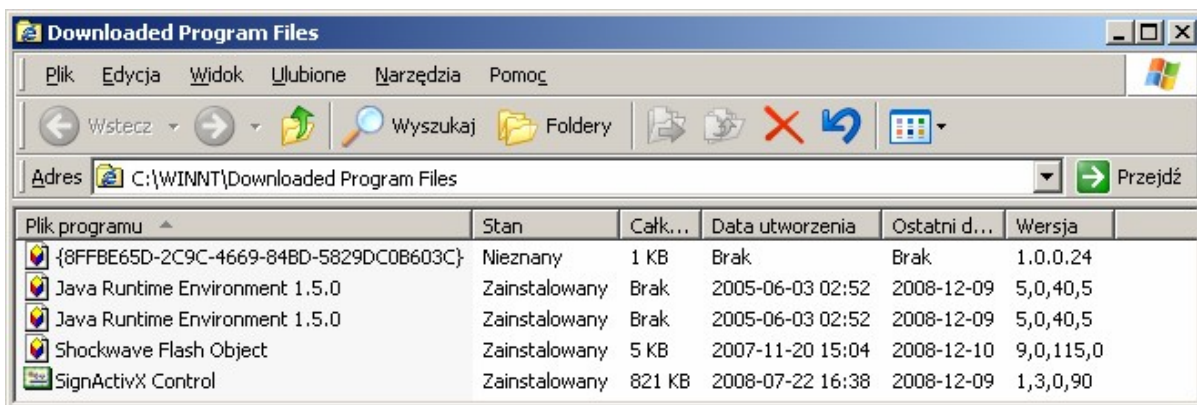


3. Przygotowanie podpisu elektronicznego na karcie procesorowej ComArch Smart Card

Uwaga!

Aby karty procesorowe ComArch Smart Card było poprawnie obsługiwane w systemie bankowości internetowej dla Klientów biznesowych (BusinessPro), musi być zainstalowana najnowsza wersja komponentu podpisującego.

Wersję zainstalowanego komponentu możemy sprawdzić w Internet Explorer -> Narzędzia -> Opcje internetowe -> Zakładka „Ogólne” -> Ustawienia -> Przeglądaj obiekty.



Na ekranie widać, że wersja zainstalowanego komponentu to 1.3.0.90. Do poprawnej obsługi kart Comarch SmartCard wymagana jest wersja 1.3.0.90.

3.1 Tworzenie kluczy podpisu elektronicznego na karcie procesorowej ComArch Smart Card w procesie logowania

W celu wygenerowania kluczy podpisu elektronicznego na karcie procesorowej należy zalogować się do systemu bankowości internetowej dla Klientów biznesowych (BusinessPro).

Dla logowania z kartą generacja kluczy wymuszana jest automatycznie w procesie logowania do Systemu.

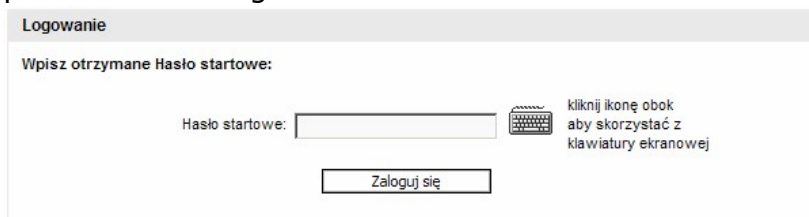
1. Proces logowania rozpoczynamy w sposób standardowy, podając identyfikator Użytkownika i wybierając przycisk „Dalej”.

Logowanie

Wpisz swój Identyfikator:

Identyfikator:

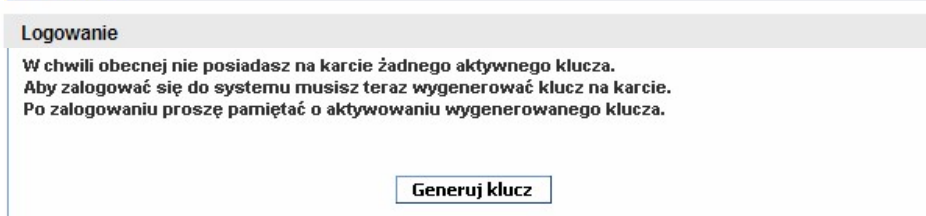
2. Następnie, w zależności czy już korzystaliśmy z Systemu, podajemy hasło z pakietu startowego



lub hasło maskowane i przycisk „Zaloguj się”.



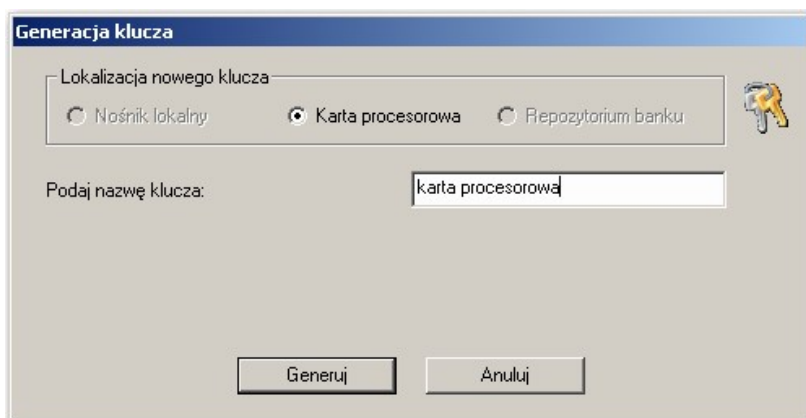
3. Kolejny ekran informuje o braku aktywnego klucza na karcie procesorowej i potrzebie jego wygenerowania. Wybieramy przycisk „Generuj klucz”.



4. W oknie **Generacja klucza** podajemy nazwę klucza, pod jaką będzie widziany w Systemie (UWAGA: nie używamy polskich znaków w nazwie klucza).

Uwaga!

Do generacji klucza system bankowości internetowej dla Klientów biznesowych (BusinessPro) wymaga zainstalowanego komponentu podpisującego. W celu uzyskania pomocy przy instalacji komponentu prosimy o kontakt z Infolini



5. Karta dostarczana jest w stanie pre-inicjalizowanym, co oznacza, że posiada ona odpowiednie funkcjonalności dla podpisu elektronicznego, ale nie jest jeszcze gotowa do użycia, ponieważ brakuje kodu PIN oraz PUK. Kartę należy aktywować poprzez ustawienie własnych kodów PIN i PUK. Można ją również reinicjalizować w przypadku jej całkowitego zablokowania (blokada PIN i PUK), powoduje to wyczyszczenie zawartości karty (usunięcie wszystkich kluczy podpisu) i wymóg nadania nowych kodów PIN i PUK. Jeżeli system wykryje, że karta jest niezainicjalizowana lub jest całkowicie zablokowana (zablokowany PIN i PUK) zostanie wyświetlone okno inicjalizacji karty. Należy w nim wprowadzić kod PIN: 4-16 znaków oraz kod PUK: 8-16 znaków.

Inicjalizacja karty

Kod PIN - osobisty numer identyfikacyjny. Uniemożliwia nieuprawnionym i przypadkowym osobom korzystanie z Twojej karty procesorowej, a tym samym wykonywania dyspozycji na Twoim rachunku wymagających podpisu elektronicznego znajdującego się na karcie. Jest on całkowicie poufny i powinien być znany tylko Tobie jako właścicielowi karty.

Kod PUK - osobisty kod odblokowujący. Powinieneś go przechowywać w bezpiecznym miejscu i chronić przed zgubieniem. Może być bowiem przydatny w przypadku, gdy zapomnisz Twojego osobistego numeru identyfikacyjnego PIN lub jeżeli trzy razy pod rząd zostanie wprowadzony błędny numer identyfikacyjny PIN. W takich sytuacjach kod PUK pozwoli na odblokowanie numeru identyfikacyjnego PIN.

Należy pamiętać, że nie wolno przechowywać numeru identyfikacyjnego PIN oraz kodu odblokowującego PUK razem z kartą procesorową. Może to bowiem umożliwić osobom niepowołanym dostęp do Twojego rachunku w sytuacji zaginięcia lub kradzieży karty.

PIN
Podaj nowy PIN

Powtórz nowy PIN

PUK
Podaj nowy PUK

Powtórz nowy PUK

OK Anuluj

6. Po zatwierdzeniu wprowadzonych danych system zapyta, czy wydrukować kod PUK.

BPHBPH

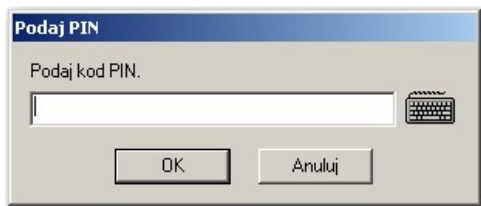
Wydrukować PUK?

Tak Nie

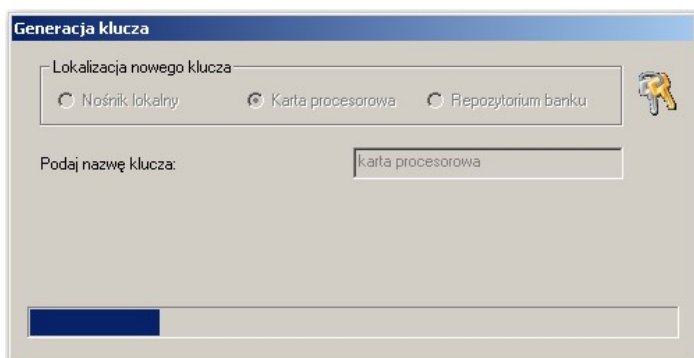
Uwaga!

Należy pamiętać, że nie wolno przechowywać numeru identyfikacyjnego PIN oraz kodu odblokowującego PUK razem z kartą procesorową. Może to bowiem umożliwić osobom niepowołanym dostęp do rachunku bankowego w sytuacji zaginięcia lub kradzieży karty.

7. Kolejny ekran służy do generacji klucza na karcie ComArch SmartCard. Podajemy wprowadzony uprzednio kod PIN do karty i wybieramy przycisk „OK”.



8. Po wybraniu przycisku „OK” rozpoczyna się tworzenie kluczy na karcie procesorowej.



9. Po utworzeniu kluczy na karcie klucz publiczny jest zapisywany w systemie bankowym i następuje logowanie do systemu bankowości internetowej dla Klientów biznesowych (BusinessPro).

Uwaga!

Należy pamiętać, że wygenerowany na karcie procesorowej klucz jest jeszcze nieaktywny. Należy pamiętać o aktywowaniu klucza poprzez poprawną autoryzację poprzez Infolinię.

10. Po zalogowaniu w Systemie i przejściu do księgi Administracja -> Bezpieczeństwo -> Klucze widoczny jest wygenerowany wcześniej klucz w stanie „Nieaktywny”.

Klucze					
Dane z 27.10.2009, 9:36:23					
DODAJ CERTYFIKAT KWALIFIKOWANY		GENERUJ NOWY KLUCZ			
Zarządzanie kluczami					
Wybór	Nazwa klucza Data generacji	Odcisk klucza	Suma kontrolna	Typ klucza	Status Widoczny
<input type="checkbox"/>	klucz4 06-03-2009	38 0B D2 0B 2E 21 4E F3 6D 00 42 EF 78 7B 11 3F 4E DC D0 53	117110314	Klucz PGP na karcie procesorowej ważny bezterminowo bez limitu użyć	Nieaktywny TAK

11. Po aktywowaniu klucza i ponownym zalogowaniu w Systemie i przejściu do księgi Administracja -> Bezpieczeństwo -> Klucze widać wygenerowany poprzednio klucz w stanie „Aktywny”.

3.2 Tworzenie kluczy podpisu elektronicznego na karcie procesorowej ComArch Smart Card po zalogowaniu do Systemu

Dla logowania z hasłem maskowanym generowanie klucza odbywa się po zalogowaniu do Systemu i samodzielnym wybraniu funkcji: „Generuj nowy klucz”, dostępnej w Administracja -> Bezpieczeństwo -> Klucze.

Tworzenie kluczy po zalogowaniu przebiega analogicznie do opisanego powyżej:

1. Po wejściu w księgę Administracja -> Bezpieczeństwo -> Zarządzanie kartą procesorową wybieramy przycisk „Inicjalizuj kartę”, w celu nadania jej kodu PIN oraz kodu PUK.

Zarządzanie kartą procesorową	
Dane z 27.10.2009, 9:43:19	
Inicjalizacja karty	
Karta dostarczana jest w stanie pre-inicjalizowanym, co oznacza że posiada ona odpowiednie funkcjonalności dla podpisu elektronicznego ale nie jest jeszcze gotowa do użycia ponieważ brakuje kodu PIN oraz PUK. Kartę należy aktywować poprzez ustawienie własnych kodów PIN i PUK. Kartę można również reinicjalizować w przypadku jej całkowitego zablokowania (blokada PIN i PUK) powoduje to wyczyszczenie zawartości karty (usunięcie wszystkich kluczy podpisu) i wymóg nadania nowych kodów PIN i PUK. W celu aktywowania karty należy wybrać poniższy przycisk "Inicjalizacja karty"	
<input type="button" value="INICJALIZACJA KARTY"/>	
Zmiana PIN	
Personal Identification Number. Prywatny Numer Identyfikacyjny (co najmniej 4 cyfrowy) który zabezpiecza klucze przechowywane na karcie przed niepowołanym użyciem. W celu zmiany numeru PIN należy wybrać poniższy przycisk "Zmień PIN"	
<input type="button" value="ZMIANA PIN"/>	
Zmiana PUK	
Personal Unlocking Key. 8-cyfrowy numer, który służy do odblokowania karty w przypadku zablokowania numeru PIN. W celu zmiany numeru PUK należy wybrać poniższy przycisk "Zmień PUK"	

Uwaga!

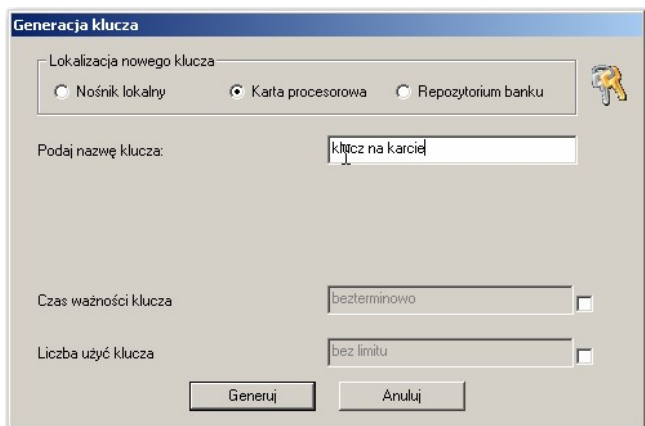
Należy pamiętać, że nie wolno przechowywać numeru identyfikacyjnego PIN oraz kodu odblokowującego PUK razem z kartą procesorową. Może to bowiem umożliwić osobom niepowołanym dostęp do rachunku bankowego w sytuacji zaginięcia lub kradzieży karty.

2. Następnie w księdze Administracja -> Bezpieczeństwo -> Klucze wybieramy przycisk „Generuj nowy klucz”.

Uwaga!

Do generacji klucza system bankowości internetowej dla Klientów biznesowych (BusinessPro) wymaga zainstalowanego komponentu podpisującego. W celu uzyskania pomocy przy instalacji komponentu prosimy o kontakt z Infolinią.

3. W oknie **Generacja klucza** wprowadzamy nazwę klucza np. „klucz na karcie”, wybieramy przycisk „Generuj” (UWAGA: nie używamy polskich znaków w nazwie klucza).



Generacja klucza

Lokalizacja nowego klucza

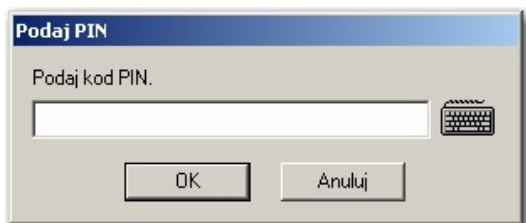
Nośnik lokalny Karta procesorowa Repozytorium banku

Podaj nazwę klucza:

Czas ważności klucza

Liczba użyć klucza

4. Następnie podajemy kod PIN i wybieramy przycisk „OK”.



Podaj PIN

Podaj kod PIN.

5. Możemy dodatkowo określić datę, do kiedy generowany klucz będzie ważny tzn. do kiedy będzie można używać go do autoryzacji. W tym umieszczamy znaczek obok pola „Czas ważności klucza” i wybieramy datę.

6. Możemy również określić liczbę sesji ważności klucza. W tym umieszczamy znaczek obok pola „Liczba użyć klucza” i wprowadzamy wartość liczbową w pole.

7. Po wybraniu przycisku „Generuj” rozpoczyna się tworzenie kluczy na karcie.

8. Po utworzeniu kluczy na karcie, klucz publiczny jest zapisywany w Systemie bankowym.

Zaraz po wygenerowaniu klucz widoczny jest na liście w stanie „**Nieaktywny**”.

Uwaga!

Należy pamiętać, że wygenerowany na karcie procesorowej klucz jest jeszcze nieaktywny. Proszę pamiętać o aktywowaniu klucza poprzez poprawną autoryzację za pośrednictwem Infolinii.

Po aktywowaniu klucza i ponownym zalogowaniu w Systemie i przejściu do księgi Administracja -> Bezpieczeństwo -> Klucze widać wygenerowany poprzednio klucz w stanie „**Aktywny**”.

4. Certyfikaty kwalifikowane

System bankowości internetowej dla Klientów biznesowych (BusinessPro) pozwala Państwu na wykorzystywanie własnego bezpiecznego podpisu elektronicznego opatrzonego certyfikatem kwalifikowanym.

W systemie bankowości internetowej dla Klientów biznesowych (BusinessPro) obsługiwane są wszystkie certyfikaty kwalifikowane polskich Zaufanych Urzędów Certyfikacji:

- SIGILLUM – Polska Wytwórnia Papierów Wartościowych S.A.,
- CERTUM – Powszechne Centrum Certyfikacji – Unizeto Technologies SA,
- SZAFIR – Krajowej Izby Rozliczeniowej.

4.1 Proces dodawania certyfikatu kwalifikowanego do systemu bankowości internetowej dla Klientów biznesowych (BusinessPro)

1. Zainstalować oprogramowanie dostarczone przez wystawcę certyfikatu według otrzymanej od niego instrukcji.
2. Postępując wg instrukcji otrzymanej od wystawcy dodać certyfikat osobisty do magazynu certyfikatów systemu Windows.
3. Dodając certyfikat **przyjazną nazwę wprowadzamy bez polskich znaków**.
4. Postępując wg instrukcji otrzymanej od wystawcy należy dodać certyfikat wystawcy oraz certyfikat roota do magazynu certyfikatów Windows jako zaufane urzędy certyfikacji.
5. Poprawnie zainstalowany w systemie certyfikat widoczny jest w Internet Explorer w Narzędzia -> Opcje internetowe -> Zawartość -> Certyfikaty -> Osobisty.
6. W celu dodania certyfikatu do systemu bankowości internetowej dla Klientów biznesowych (BusinessPro) należy zalogować się do Systemu i przejść do księgi Administracja -> Bezpieczeństwo -> Klucze.
7. W księdze klucze wybieramy przycisk „**Dodaj certyfikat kwalifikowany**”.
8. Z listy certyfikatów wybieramy certyfikat, który chcemy dodać do Systemu i nadajemy mu własną nazwę. Przy nadawaniu nazwy **nie używamy polskich znaków!**
9. Jeżeli certyfikat jest poprawny i zawiera kompletne dane, zostanie dodany do Systemu i będzie gotowy do aktywacji.

☐ Klucze [DODAJ]

Dane z 27.10.2009, 9:53:44 ?

Zarządzanie kluczami

Wybór	Nazwa klucza Data generacji	Odcisk klucza	Suma kontrolna	Typ klucza	Status Widoczny
<input type="checkbox"/>	Certyfikat	8C D5 55 F9 AC DB 7C 74 A1 2F A6 05 D3 FC 54 39 D7 7A AD 55	121415196	Certyfikat kwalifikowany ważny do 29-01-2010 bez limitu użyć	Aktywny TAK

Wybierz akcję ▼ ?

Uwaga!

Należy pamiętać, że zapisany na karcie procesorowej certyfikat jest

jeszcze nieaktywny. Proszę pamiętać o aktywowaniu certyfikatu poprzez poprawną autoryzację przez Infolinię.

5. Doradztwo i wsparcie techniczne

W przypadku dodatkowych pytań związanych z instalacją czytników, kart procesorowych, certyfikatów kwalifikowanych oraz generowaniem podpisu elektronicznego w systemie bankowości internetowej dla Klientów biznesowych (Businesspro) prosimy o kontakt z:

Infolinia:

Firmy mikro i małe:

Tel. 19 502

Firmy średnie i duże:

Tel. 0 801 274 274 (z telefonów stacjonarnych)

Tel. 22 531 8095 (z telefonów komórkowych i z zagranicy)

(koszt połączenia jak za jedną jednostkę taryfikacyjną)

<https://www.aliorbank.pl/>