

# Bezpieczeństwo i konfiguracja **eurobank online**

e-mail: [online@eurobank.pl](mailto:online@eurobank.pl)

pomoc telefoniczna: 0801 700 100

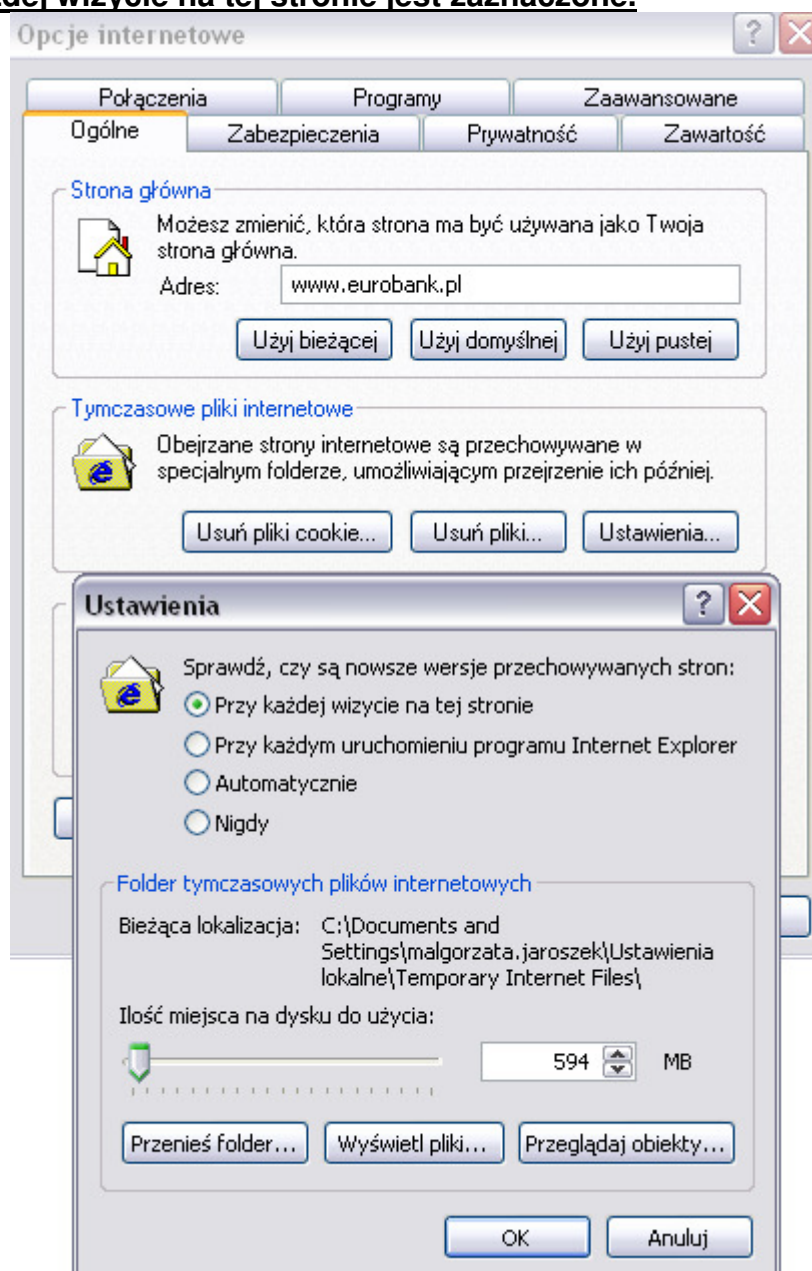
## **Spis treści:**

Twoja przeglądarka i jej konfiguracja.....	3
Internet Explorer.....	3
Mozilla Firefox.....	8
Zasady bezpieczeństwa.....	11
Metody logowania i autoryzacji transakcji w serwisie .....	19

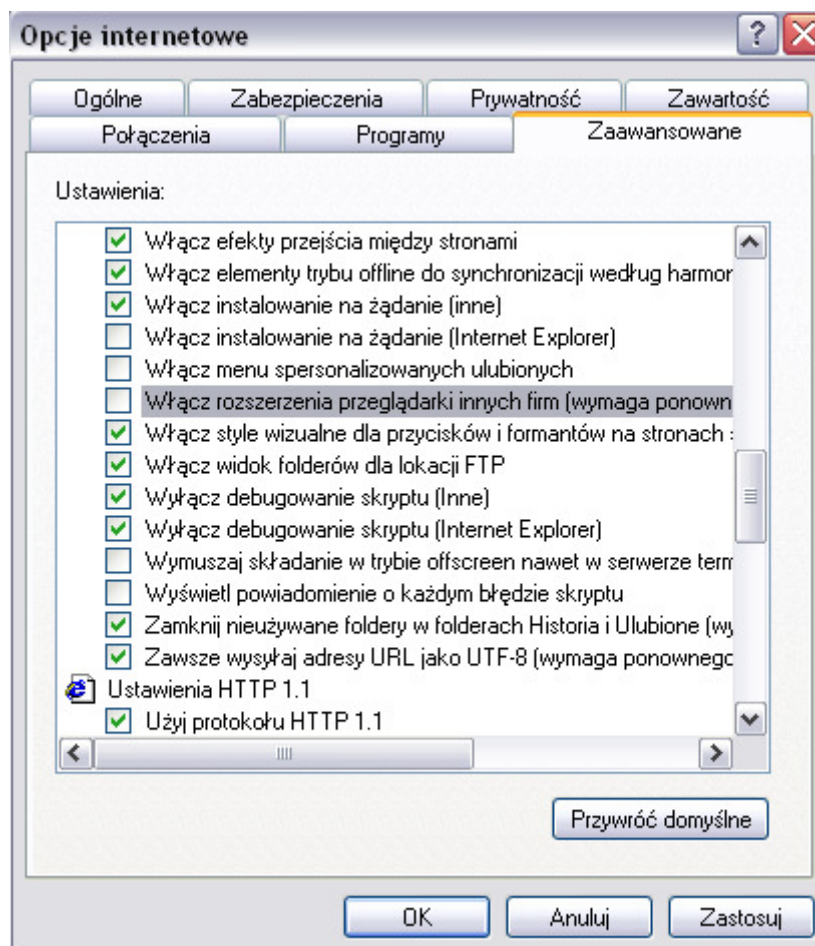
## Twoja przeglądarka i jej konfiguracja

### Internet Explorer (na przykładzie IE w wersji 6.0)

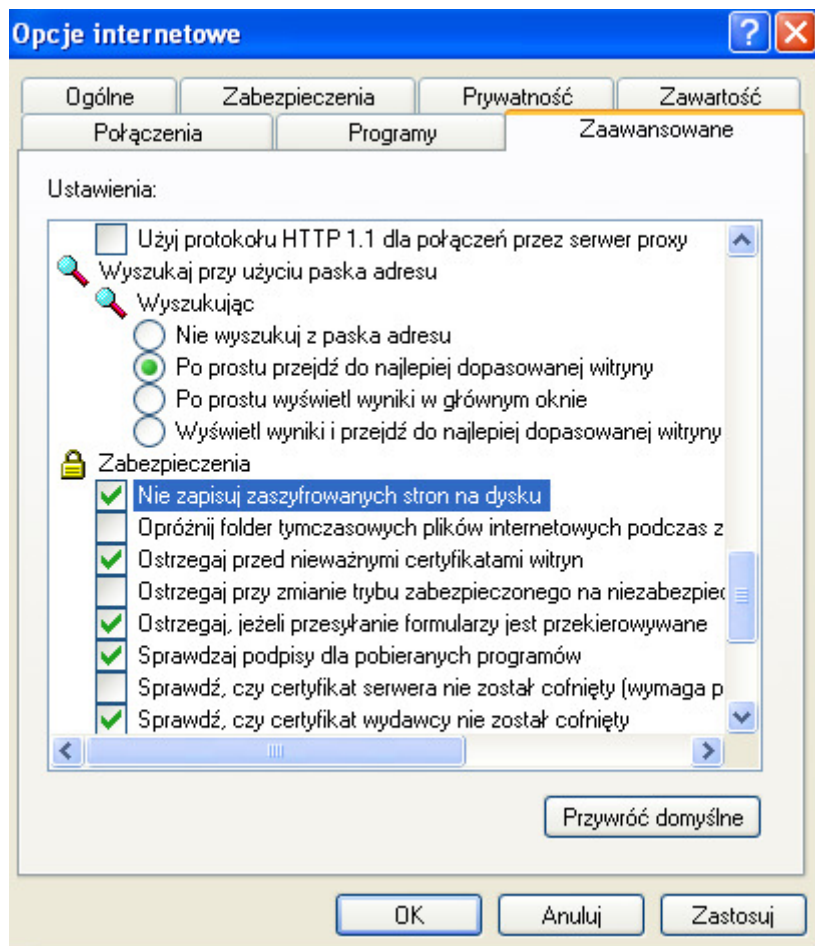
1. W menu Narzędzia wybierz Opcje internetowe / Ogólne / Tymczasowe pliki internetowe/ Ustawienia i upewnij się, że na liście Sprawdź, czy są nowsze wersje przechowywanych stron: pole **Przy każdej wizycie na tej stronie jest zaznaczone**.



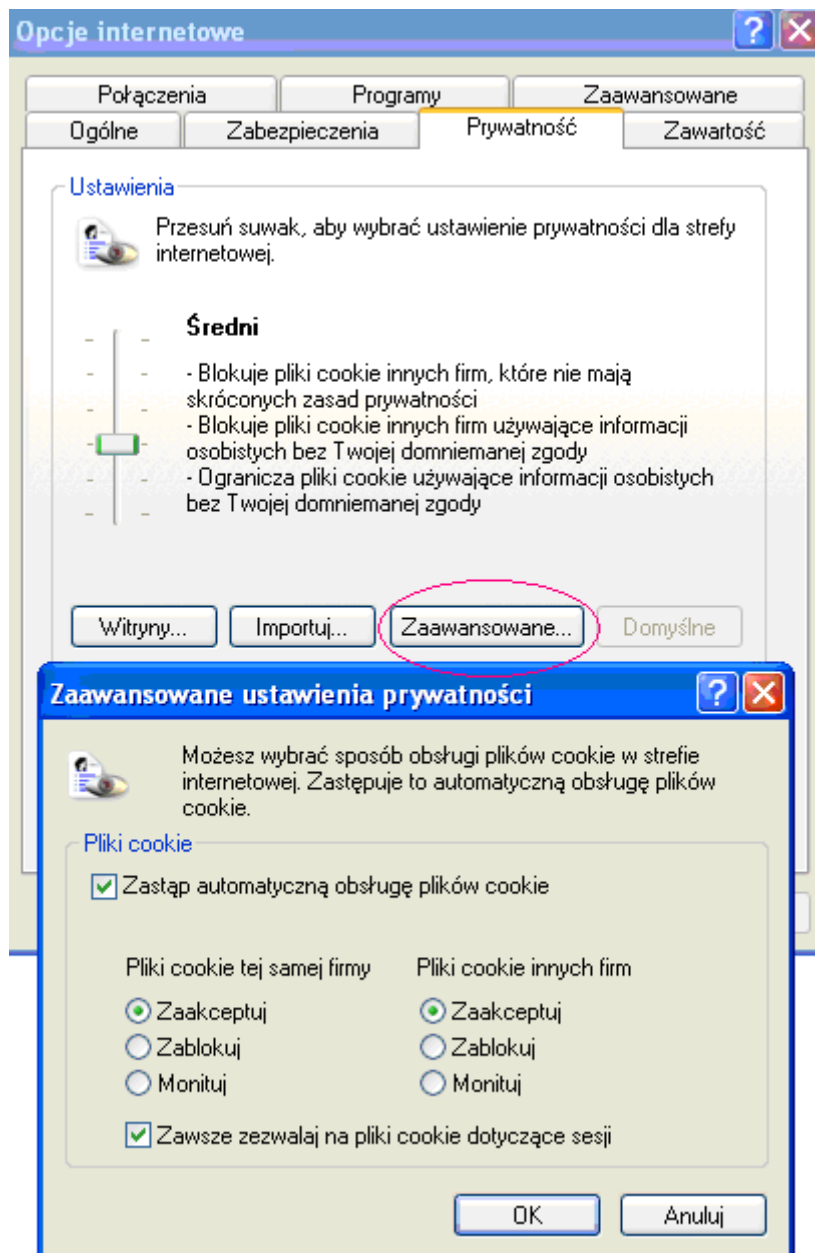
2. Następnie w menu Narzędzia / Opcje internetowe / Zaawansowane / część **Przeglądanie** upewnij się, że pole **Włącz rozszerzenia przeglądarki innych firm** nie jest zaznaczone.



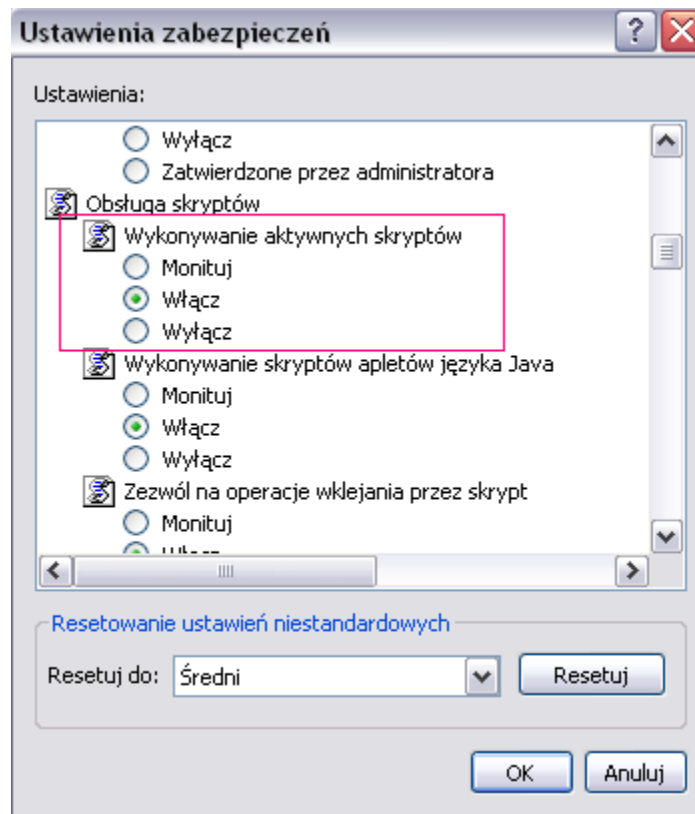
3. W części Zabezpieczenia upewnij się, że pole **Nie zapisuj zaszyfrowanych stron na dysku** jest zaznaczone.



4. W menu Narzędzia / Opcje internetowe / Prywatność / Zaawansowane / **zaznacz** opcję: **Zastąp automatyczną obsługę plików cookie** oraz opcję **Zawsze zezwalaj na pliki cookie dotyczące sesji**.

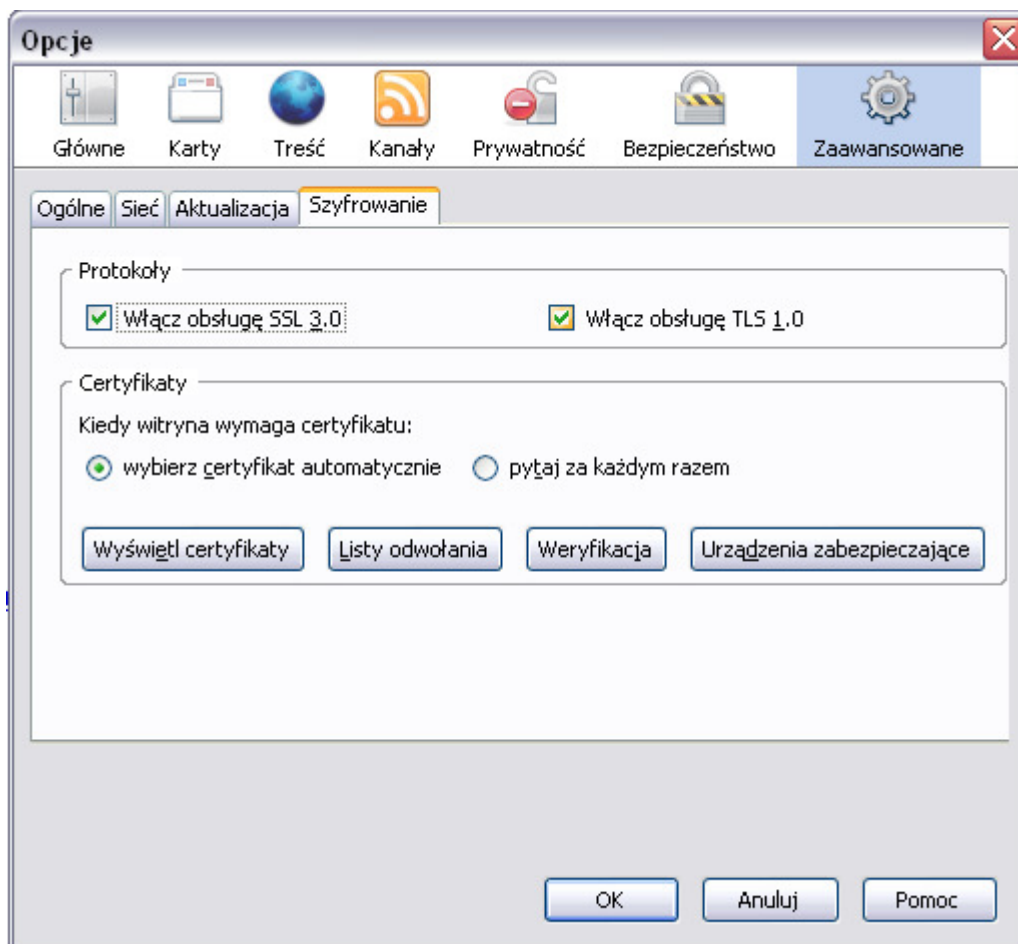


5. W menu **Narzędzia / Opcje internetowe / Zabezpieczenia** wybierz **opcję Poziom niestandardowy...** i **włącz Wykonywanie aktywnych skryptów**.

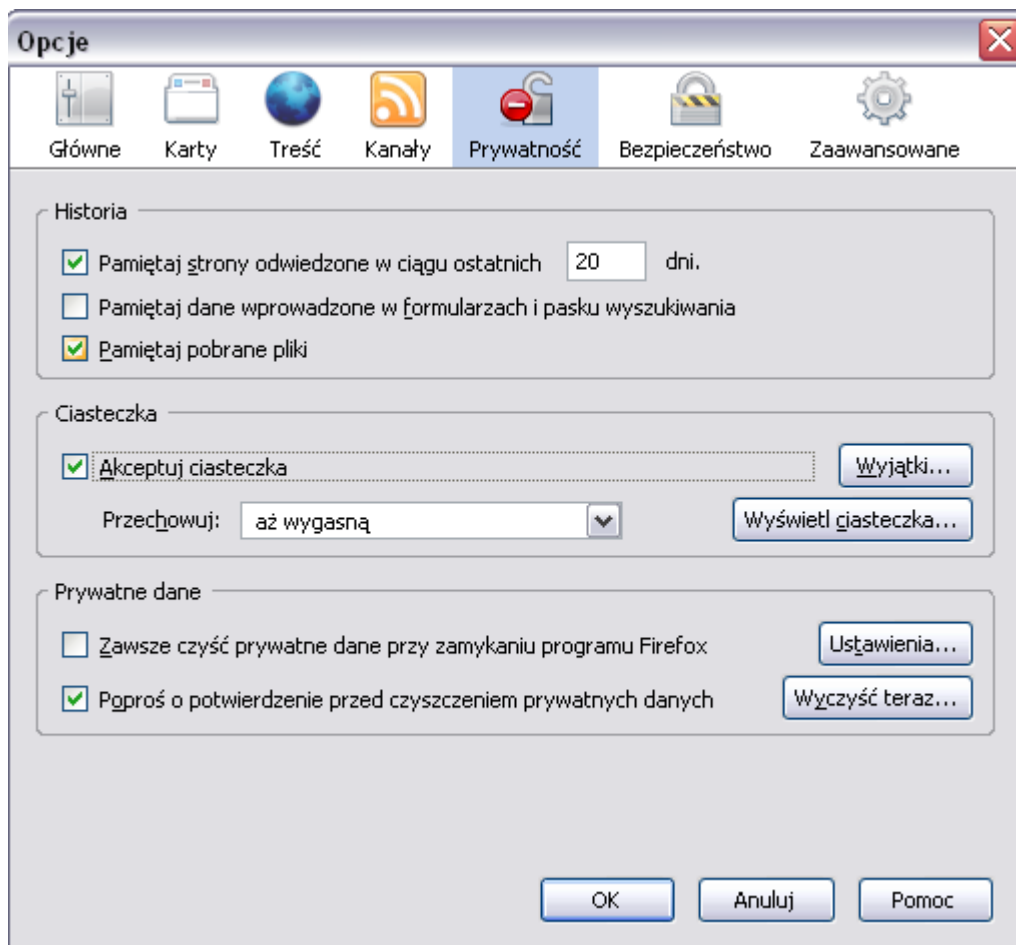


## Mozilla Firefox (na przykładzie MF w wersji 2.0.)

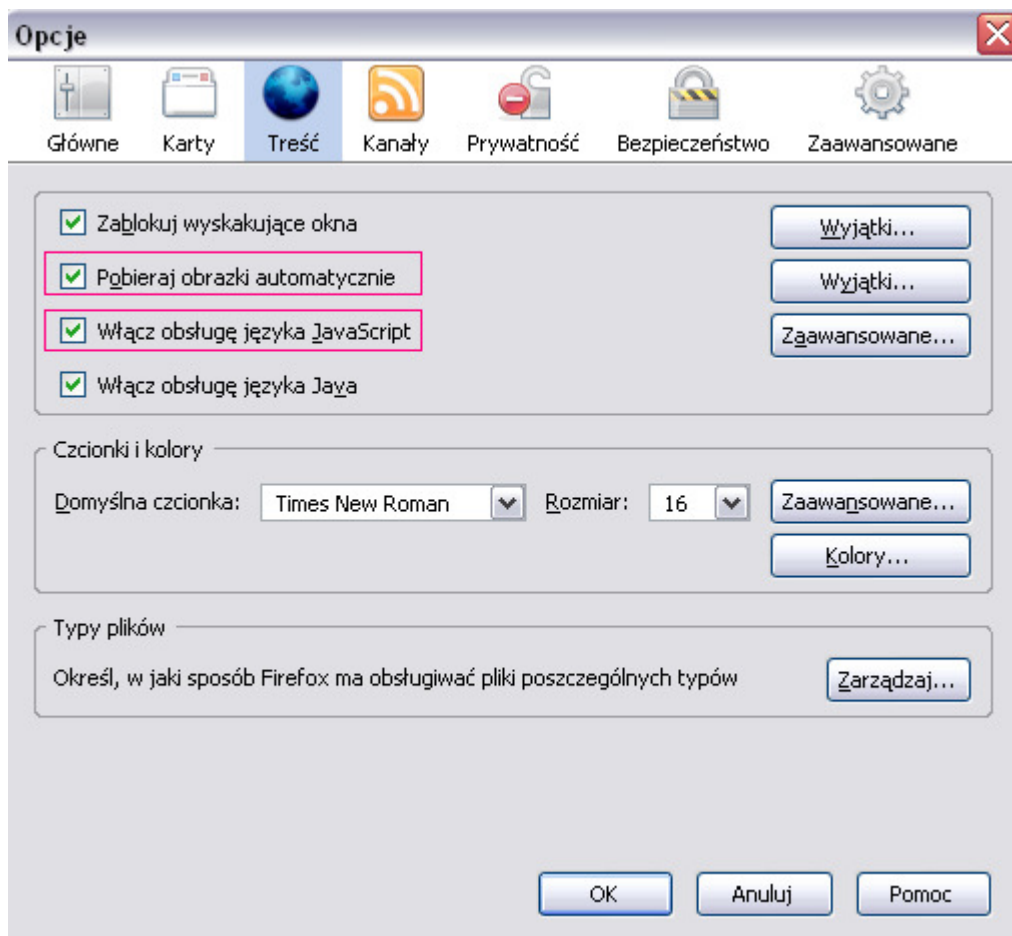
1. W menu Narzędzia / Opcje / Zaawansowane / Szyfrowanie **Włącz obsługę SSL 3.0.**



2. W menu Narzędzia / Opcje / Prywatność / Ciasteczka zaznacz opcję **Akceptuj ciasteczka**.



3. W menu Narzędzia / Opcje/ Treść zaznacz **Pobieraj obrazki automatycznie** oraz **Włącz obsługę języka JavaScript**.



## Zasady bezpieczeństwa

Aby bezpiecznie korzystać z serwisu **eurobank online oraz serwisu telefonicznego**, pamiętaj o kilku podstawowych zasadach.

- **Stosuj dobre praktyki bezpieczeństwa**
  - zwracaj uwagę na komunikaty przeglądarki
  - chroń swój identyfikator i hasło przed niepowołanymi osobami
  - używaj funkcji wyloguj się zawsze przed zakończeniem pracy
  - zamykaj wszystkie okna przeglądarki przed odejściem od komputera.
  
- **Używając tokena sprzętowego:**
  - nie udostępniaj nikomu tokena
  - w wypadku utraty – niezwłocznie zgłoś to w placówce lub telefonicznie
  
- **Używając Tokena GSM:**
  - ustaw PIN do tokena inny niż PIN do telefonu
  - zawsze sprawdzaj czy informacje o transakcji wyświetlone przez token są zgodne z operacją jaką zamierzasz wykonać.

- **Korzystaj z programów antywirusowych**

Jeśli korzystasz z Internetu, zalecamy używanie programu antywirusowego. Wirusy, robaki i inne złośliwe programy pojawiają się w systemie operacyjnym m.in. poprzez zainfekowane załączniki poczty elektronicznej, niesprawdzone dyskietki i płyty CD oraz programy ściągane z nieznanego źródła. Wirusy działają niepostrzeżenie, a straty spowodowane infekcją bywają duże. Wirusy mogą przechwytywać poufne dane znajdujące się w serwisie bankowości elektronicznej (dane adresowe, stan środków na karcie itp.). Niektóre programy potrafią nawet podmieniać informacje jakie przesyłasz do Banku – np, zmienić kwotę przelewu.

Na rynku dostępnych jest wiele różnych programów antywirusowych, które mogą uchronić komputer przed tym zagrożeniem. Programy te skanują komputer pod kątem szkodliwych programów i porównują z bazą znanych wirusów. Bardzo ważne jest aktualizowanie posiadanego programu i bazy wirusów – codziennie powstają nowe odmiany złośliwego oprogramowania, dlatego jak najczęściej należy skanować zasoby komputera.

- **Używaj osobistej zapory firewall**

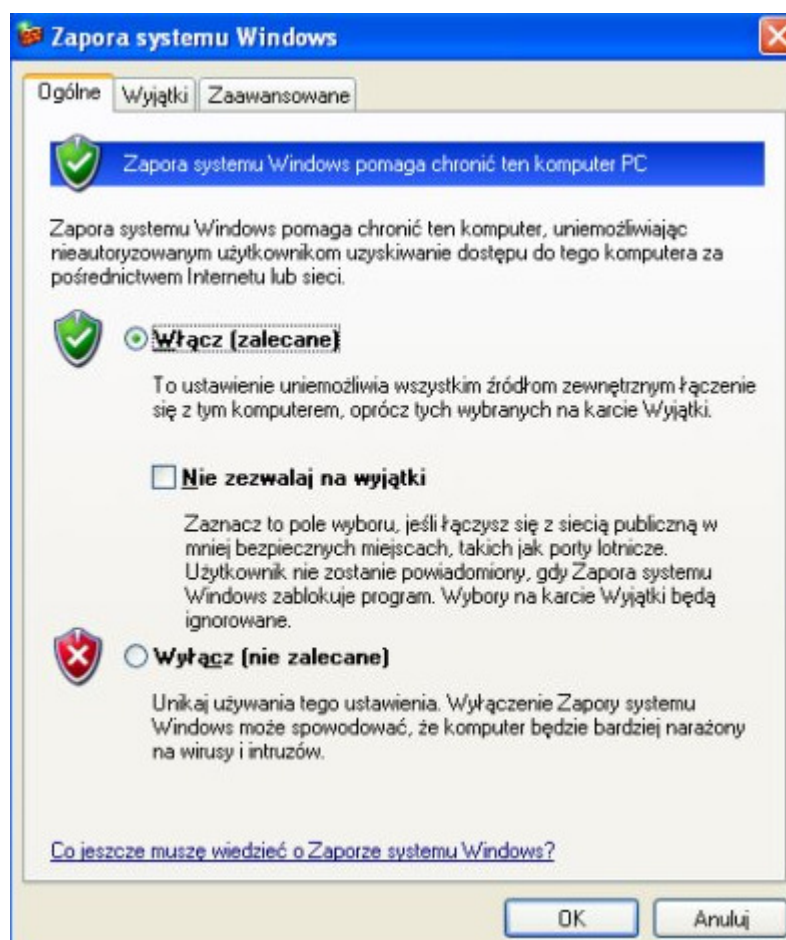
Zapora firewall pełni funkcję strażnika, który kontroluje każdy ruch na styku komputera z Internetem, ograniczając przychodzące i wychodzące połączenia

sieciowe. Na rynku dostępnych jest wiele różnych zapór firewall. W Windows XP firewall znajduje się już w systemie operacyjnym.

- **Korzystając z serwisu telefonicznego:**
  - nie podawaj nikomu nadanego sobie telekodu
  - w przypadku podejrzenia dostania się telekodu w ręce osoby trzeciej natychmiast skontaktuj się z telefonicznym Centrum Obsługi Klienta w celu zmiany telekodu

### Aby włączyć firewall w Windows XP SP2:

- 1) otwórz Panel sterowania
- 2) kliknij dwukrotnie ikonę Połączenia sieciowe
- 3) prawym przyciskiem myszy kliknij ikonę Połączenie z internetem
- 4) z rozwijalnego menu wybierz opcję Właściwości
- 5) przejdź do zakładki Zaawansowane i kliknij przycisk **Ustawienia**
- 6) w nowym oknie w zakładce Ogólne **zaznacz** opcję **Włącz (zalecane)**



## ○ Dbaj o bezpieczeństwo połączenia

Komunikacja między komputerem użytkownika a serwerem banku szyfrowana jest protokołem SSL o długości klucza 128 bitów. Potwierdzeniem bezpiecznego (szyfrowanego) połączenia jest:

- adres URL rozpoczynający się od **https** (zamiast standardowego http), gdzie „s” oznacza „secure” – bezpieczny
- ikona kłódki na dolnym pasku przeglądarki lub pasku adresowym (miejsce zależy od rodzaju i wersji przeglądarki),



Certyfikat SSL służy do poświadczania autentyczności serwera, z którym komunikuje się dany komputer. Sprawdzenie szczegółów certyfikatu **przed zalogowaniem do serwisu** pozwala się upewnić, że strona, z którą nawiązane jest połączenie, to rzeczywiście strona eurobanku.

**Uwaga:** Jeśli przy wejściu na stronę serwisu eurobank online przeglądarka wyświetli jakikolwiek komunikat ostrzegawczy dotyczący certyfikatu, skontaktuj się telefonicznie z eurobankiem pod numerem **0801 700 100**.

Aby sprawdzić dane dotyczące certyfikatu SSL:

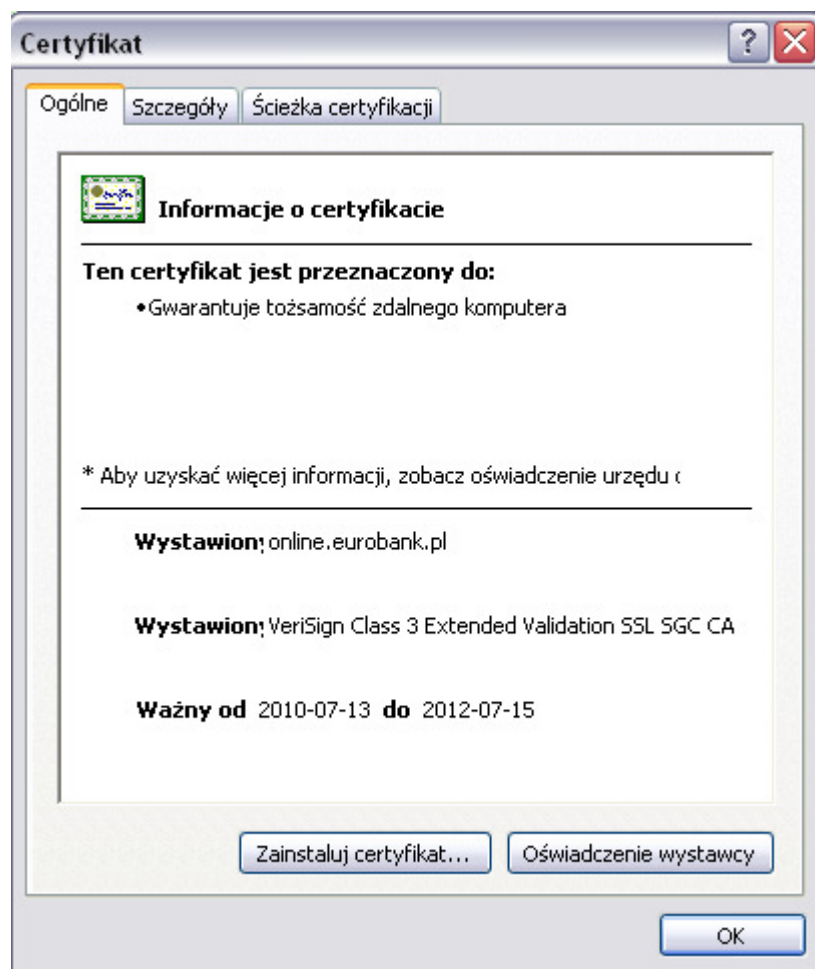
- kliknij ikonkę kłódki w lewym dolnym rogu paska przeglądarki lub
- z menu Plik (*File*) wybierz Właściwości (*Properties*).

Następnie po wybraniu przycisku Certyfikaty sprawdź następujące pozycje:

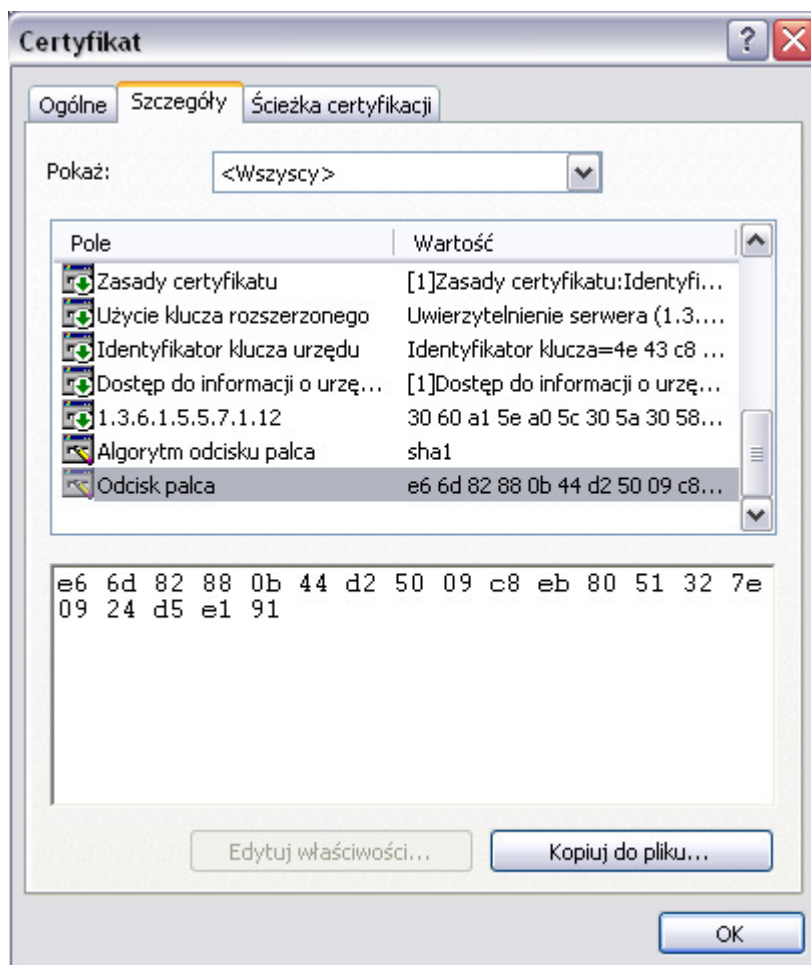
- Ogólne (*General*)
- Szczegóły (*Details*)
- Ścieżka certyfikacji (*Certification path*)

**W poszczególnych zakładkach zwróć uwagę na:**

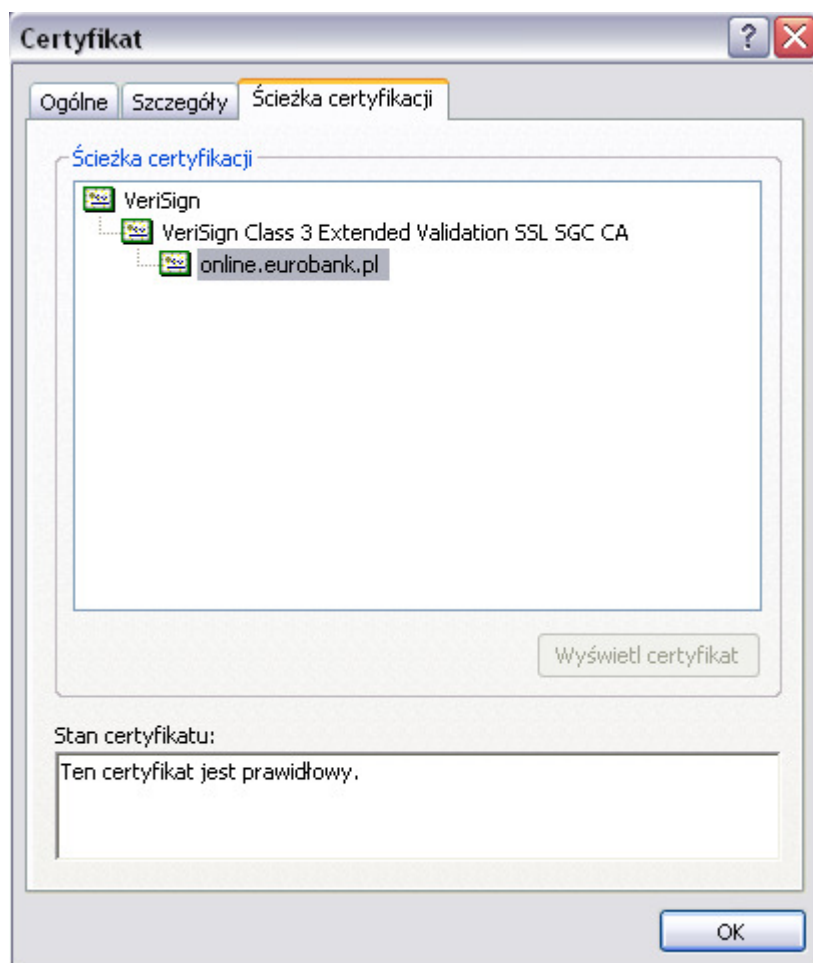
- Ogólne – w polu **Wystawiony** powinien być adres: **online.eurobank.pl**



- Szczegóły: **Odcisk palca** (*Details* → *Thumbprint*). Pole to powinno mieć określoną, niżej podaną wartość:



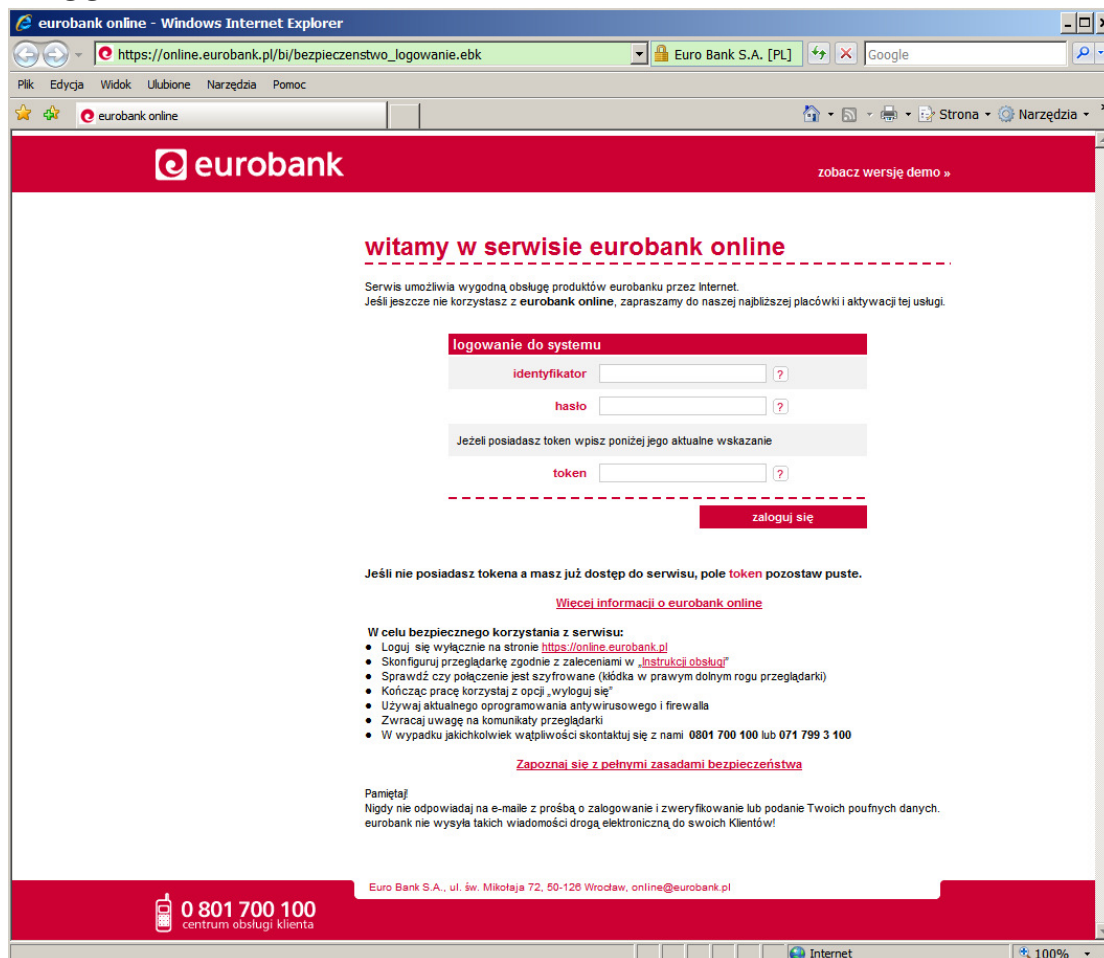
- o Ścieżka certyfikatu – adres **online.eurobank.pl**



Eurobank stosuje nowoczesny certyfikat EV SSL, który dodatkowo ułatwia zweryfikowanie autentyczności strony:

- gdy strona zabezpieczona jest certyfikatem EV SSL, informacje w pasku adresowym przeglądarki są podświetlone na zielono (podświetlone elementy różnią się w zależności od przeglądarki),
- obok paska adresu zostanie od razu wyświetlona informacja o instytucji dla której został wystawiony certyfikat (w wypadku serwisu eurobank online jest to Euro Bank S.A.)

Ekran logowania w przeglądarce Internet Explorer 7 obsługującej certyfikaty EV SSL:



Zalety certyfikatów EV SSL dostępne są w nowych wersjach przeglądarek. Z pośród przeglądarek rekomendowanych przez eurobank są to:

- Microsoft Internet Explorer 7,
- Mozilla Firefox 3.

Na starszych wersjach tych przeglądarek (od Internet Explorer 6 i FireFox 1.5), serwis eurobank online, będzie działał prawidłowo. Jednak ułatwienia wynikające z certyfikatu EV SSL nie będą dostępne (pasek adresowy nie będzie podświetlany na zielono, a aby zobaczyć instytucję dla której wystawiony jest certyfikat, konieczne będzie sprawdzenie jego szczegółów zgodnie z powyższym opisem).

## ○ Uwważaj na phishing

Phishing (od ang. *fishing*, niekiedy określane jako *password harvesting fishing* – łowienie haseł) jest szczególną formą przestępstwa informatycznego polegającego na skłonieniu użytkowników komputerów do ujawnienia swoich danych (nazwa użytkownika, hasło, numer PIN lub inne informacje o dostęпах), a następnie wykorzystaniu tych informacji. Phishing jest

szczególnie groźny dla użytkowników bankowości internetowej. Phisher zazwyczaj wysyła spam do potencjalnych ofiar i kieruje je na stronę, która udaje rzeczywistą stronę banku internetowego.

Typowe sposoby poławiania poufnych informacji to:

- informowanie o rzekomym dezaktywowaniu konta i konieczności ponownej aktywacji – z podaniem wszelkich poufnych informacji; strona przechwytyująca informacje jest wówczas łudząco podobna do prawdziwej
- tworzenie fałszywych stron serwisów z adresami bardzo przypominającymi oryginalne, a więc łatwymi do przeoczenia dla osób niedoświadczonych.

**Pamiętaj! Wszystkie wiadomości e-mail zawierające prośbę o podanie jakichkolwiek informacji lub zalogowanie się są podejrzane!**

Eurobank nigdy nie poprosi Klientów o potwierdzenie loginu lub hasła pocztą elektroniczną ani nie podaje w wiadomościach e-mail odsyłaczy do strony logowania.

Jedynie na stronie serwisu [www.eurobank.pl](http://www.eurobank.pl) mogą znajdować się odsyłacze do logowania do serwisu eurobank online. W wypadku jakichkolwiek podejrzeń, co do autentyczności strony, przed zalogowaniem prosimy o kontakt telefoniczny pod numer **0801 700 100**.

### Metody logowania i autoryzacji transakcji w serwisie

Logowanie do serwisu może się odbywać za pomocą identyfikatora oraz samego hasła lub za pomocą identyfikatora, hasła i wskazania tokena (sprzętowego lub TokenaGSM), jeśli wybrałeś token.

Już w samym serwisie transakcje możesz potwierdzać za pomocą: wskazania tokena sprzętowego lub TokenaGSM.

**Pamiętaj**, jeśli chcesz mieć do dyspozycji pełną funkcjonalność serwisu zapytaj Doradcę Klienta o jeden z rodzajów tokena. Bez tokena masz dostęp tylko do niektórych operacji.

Token sprzętowy lub TokenGSM (do wyboru) możesz otrzymać już podczas pierwszej wizyty w placówce po podpisaniu umowy o usługi Bankowości Elektronicznej. Obsługa tokenów jest opisana w **Instrukcji obsługi tokenów**.

Logowanie do serwisu bankowości telefonicznej odbywa się w serwisie IVR. System prosi o 3 losowo wybrane cyfry telekodu.

Wykonywanie operacji w serwisie bankowości telefonicznej jest możliwe na 2 sposoby:

- poprzez serwis IVR
- za pomocą Doradcy Telefonicznego

Funkcjonalności eurobank online według sposobów autoryzacji działań/transakcji w serwisie eurobank online przedstawia tabela:

Rodzaj operacji eurobank online	Dostępna dla metod autoryzacji			Czy operacja podlega limitom
	bez tokena	TokenGSM	token sprzętowy	
aktualizowanie danych osobowych		X	X	nie
zastrzeżenie dowodu tożsamości	X	X	X	nie
<b>płatności</b>				
przelew między moimi kontami	X	X	X	tak
przelew zwykły do odbiorcy zaufanego	X	X	X	tak
przelew zwykły do odbiorcy nie zaufanego		X	X	tak
przelew na rachunek ZUS		X	X	tak
przelew na rachunek US		X	X	tak
założenie zlecenia stałego na konto odbiorcy zaufanego	X	X	X	tak (kwota założonego zlecenia podlega limitom jedynie w dniu założenia zlecenia)
założenie zlecenia stałego na konto odbiorcy nie zaufanego		X	X	tak (kwota założonego zlecenia podlega limitom jedynie w dniu założenia zlecenia)
edycja zlecenia na konta odbiorcy zaufanego	X	X	X	tak (limitom podlega nowa kwota zlecenia)
edycja zlecenia na konta odbiorcy nie zaufanego		X	X	tak (limitom podlega nowa kwota zlecenia)
dodanie odbiorcy do listy		X	X	nie
edycja odbiorcy		X	X	nie
usunięcie odbiorcy z listy	X	X	X	nie
<b>lokaty</b>				
założenie lokaty	X	X	X	nie
edycja lokaty	X	X	X	nie
likwidacja lokaty		X	X	nie
porównanie oprocentowania lokat w kalkulatorze lokat	X	X	X	nie

<b>karta kredytowa</b>				
splata karty	<b>X</b>	<b>X</b>	<b>X</b>	<b>tak</b>
aktywacja karty		<b>X</b>	<b>X</b>	<b>nie</b>
wykonanie zastrzeżenia karty kredytowej	<b>X</b>	<b>X</b>	<b>X</b>	<b>nie</b>
zmiana limitów transakcji		<b>X</b>	<b>X</b>	<b>nie</b>
zmiana ubezpieczeń		<b>X</b>	<b>X</b>	<b>nie</b>
ustawienie powiadomień SMS		<b>X</b>	<b>X</b>	<b>nie</b>
<b>karta debetowa</b>				
złożenie wniosku o wydanie karty do konta Visa Electron spersonalizowanej		<b>X</b>	<b>X</b>	<b>nie</b>
zmiana limitów transakcji		<b>X</b>	<b>X</b>	<b>nie</b>
zastrzeżenie karty debetowej	<b>X</b>	<b>X</b>	<b>X</b>	<b>nie</b>
<b>wnioski</b>				
złożenie wniosku kredytowego oraz wniosku o kartę kredytową	<b>X</b>	<b>X</b>	<b>X</b>	<b>nie</b>
<b>Kredyty</b>				
przeglądanie listy posiadanych kredytów	<b>X</b>	<b>X</b>	<b>X</b>	<b>nie</b>
sprawdzenie szczegółów posiadanego kredytu oraz harmonogram	<b>X</b>	<b>X</b>	<b>X</b>	<b>nie</b>
zmiana ustawień powiadomień SMS dla wybranych produktów		<b>X</b>	<b>X</b>	<b>nie</b>

Uwaga! Maksymalna kwota jednorazowego przelewu lub zlecenia w serwisie eurobank online wynosi 999 999,99 PLN.