Wymagania funkcjonalne i pozafunkcjonalne dla banku internetowego

Michał *198361* Przyłuski

6 listopada 2006

SŁOWNIK

przelew Przekazanie środków pieniężnych między dwoma rachunkami bankowymi, prowadzonymi w tym samym lub w różnych bankach w Polsce.

identyfikator Nadany każdemu użytkownikowi systemu (w szczególności klientowi banku), unikalny ciąg cyfr służący do identyfikacji klienta.

hasło Ustalony przez użytkownika systemu (w szczególności przez klienta banku) ciąg cyfr, liter oraz znaków specjalnych służący do autoryzacji użytkownika, do użytku wraz z identyfikatorem. Hasło jest tajne i nie powinno być ujawniane.

hasło jednorazowe Przekazany użytkownikowi drogą nieelektroniczną ciąg cyfr. Każde hasło jednorazowe może być wykorzystane tylko raz. Z tego względu należy użytkownikowi przekazać wiele haseł.

autoryzacja Zapewnienie, że użytkownik systemu jest osobą, za którą się podaje, oraz że ma odpowiednie uprawnienia do korzystania z systemu (konto aktywne).

ID	Nazwa	Opis	Pri
		Wymagania funkcjonalne	
1	Autoryzacja użytkownika	System przeprowadza dialog z użytkownikiem (np. pyta o login i hasło) w celu sprawdzenia czy użytkownik jest tym użytkownikiemm, za którego się podaje. Dane wprowadzone przez użytkownika są porównywane z danymi w bazie danych. Od rezultatu tej operacji zależy realizowalność wszystkich pozostałych.	1
2	Sprawdzenie stanu konta	Użytkownik ma możliwość sprawdzenia stanu swojego rachunku bankowego, a także historii operacji przeprowadzonych na nim.	1
3	Przelew	Użytkownik może dokonać przelew ze swojego rachunku na rzecz innego. Może to być zarówno przelew uprzednio zdefiniowany, jak i spontaniczny. W przypadku przelewu spontanicznego wymagana dodatkowa autoryzacja. Po wykonaniu operacji z rachunku klienta schodzi na rzecz Banku prowizja. Analogicznie na rzecz rachunku użytkownika może dość do przelewu (z wewnątrz lub z innego banku).	1
4	Definicja przelewu	Użytkownik zapamiętuje w systemie dane (numer rachunku, odbiorca, i ew. kwotę) przelewu, tak aby móc go wielokrotnie realizować. Wymagana dodatkowa autoryzacja. Po wykonaniu operacji z rachunku klienta schodzi na rzecz Banku prowizja.	2
5	Zlecenie stałe	Użytkownik zapamiętuje w systemie dane (numer rachunku, odbiorca, kwota) przelewu, który będzie automatycznie realizowany przez system z zadaną częstotliwością. Wymagana dodatkowa autoryzacja. Po wykonaniu operacji z rachunku klienta schodzi na rzecz Banku prowizja.	2
6	Zmiana hasła	Użytkownik może zmienić hasło dostępu do systemu. Wymagana dodatkowa autoryzacja.	2
7	Dodatkowa autoryzacja	Użytkownik podaje hasło jednorazowe o zadanym przez system numerze. Służy to ograniczeniu dostępu do rachunku osobie, która podejrzała dane autoryzacyjne użytkownika, gdyż podejrzenie hasła jednorazowego nic nie daje, z uwagi na to, iż jest ono jednorazowe.	2
8	Realizacja przelewu	Po złożeniu przez użytkownika zlecenia przelewu system zgłasza ten przelew do realizacji do KIR, w ramach systemu Eliskir.	1
9	Kontakt z hotline	Użytkownik może poprosić hotline o kontakt z nim. Podaje wtedy preferowany numer telefonu, pod który hotline powinien się zgłosić. System zapisuje prośbę użytkownika.	3
10	Zakładnie konta	Użytkownik zakłada konto, do bazy są wprowadzane jego dane, zostaje mu nadany numer klienta oraz numer rachunku. Przekazana do realializacji zostaje jego karta płatnicza, a odpowiedni dział sprawdza jego dokumenty.	1
11	Wypłata w bankomacie	Użytkownik autoryzuje się przed bankomatem przy pomocy kodu PIN, bankomat po upewnieniu się o dostępności srodków wypłaca odpowiednią kwotę. W ramach innej operacji dokonuje się rozliczenia faktycznego.	2
12	Płatność w sklepie	Bank autoryzuje prośbę autoryzacyjną ze strony operatora karty i blokuje odpowiednie środki na rachunku klienta umożliwiając klientowi dokonanie płatności w sklepie. W ramach odrębnej operacji bank rozlicza się z operatorem karty.	2
13	Usunięcie konta	System przyjmuje dyspozycję usunięcia konta wraz z przekazaniem srodków na określony rachunek.	1

ID	Nazwa	Opis	Pri
		Wymagania pozafunkcjonalne	
51	Bezpieczeństwo	System powinien gwarantować najwyższy możliwy system bezpieczeństwa. Wszystkie dane zgromadzone w systemie należy traktować jako objęte tajemnicą bankową w rozumieniu ustawy „Prawo Bankowe" (z dnia 29 sierpnia 1997, Dz. U. 1997.140.939 ze zmianiami, art. 104 i nast.). Oznacza to także konieczność zapewnienia poufności danych podczas transferu w otwartch sieciach (internet).	1
52	Dostępność	System powienien być dostępny dla użytkowników przez 24 godziny na dobę, 7 dni w tygodniu. Dopuszcza się przerwy konserwacyjne, jednakże tylko w okresach najmniejszej aktywności użytkownika, i nie trwające więcej niż godzinę.	1
53	Niezawodność	W przypadku wystąpienia krytycznej awarii czas przywrócenia systmu do pełnej funkcjonalności nie może przekroczyć 4 (czterech) godzin. Za krytyczną awarię uznaje się kataklizm dotyczący przynajmniej 15% powierzchni Polski, lub conajmniej 20% ludności. Dopuszcza się także uznanie za krytyczną awarię jednoczesnych zniszczeń o charakterze katastrofy na obszarze w promieniu 25 km od wszystkich centrów danych Banku. Krytyczna awaria może wystąpić tylko w sytuacji ogłoszenia przez władze stanu klęski żywiołowej lub innej sytuacji wyjątkowej o charakterze ogólnokrajowym.	1
54	Skalowalność	W początkowej fazie system powienien być w stanie obsłużyć 2 000 000 użytkowników bez żadnych modyfikacji systemu. Za obsługę użytkownika uznaje się gwarantowaną reakcję w czasie poniżej 0,5 s na jego działania, ze średnim czasem poniżej 0,2 s. System powinien być w stanie po dokonaniu odpowiednich modyfikacji do obsługi 50 000 000 użytkowników przy zachowaniu powyższych parametrów czasu reakcji.	1
55	Integralość	Należy dołożyć wszelkich starań, aby dane przechowywane w systemie zachowały swoją integralność. Celem nadrzędnym jest uniemożliwienie dowolnej modyfikacji danych przez użytkownika lub osoby trzecie.	1
56	Przenośność	Z punktu widzenia użytkownika (interfejs WWW) system powienin być kompatybilny z przeglądarką internetową, niezleżnie od systmu operacyjnego stosowanego przez użytkownika. Zarówno przeglądarki graficzne, jaki tekstowe powinny dostarczać pełną funkcjonalność systemu. Ten sam moduł systemu powinien udostępniać interfjes WWW, który będzie akceptowaly dla użytkownika korzystającego z systemu przy użyciu telefonu komórkowego lub palmtopa.	2
57	Dokumentacja	System powienin być odpowiednio udokumentowany. Przewidywany okres eksploatacji systmu (30 lat) powoduje, iż może zajść konieczność dokonania pewnych modyfikacji w systemie (patrz wymaganie 58). Dokumentacja powinna być pełna i jednoznaczna.	2
58	Modyfikowalność	System powinien być łatwo modyfikowalny, a więc silnie zmodularyzowany. Zmiany popełnione w jednym module nie mogą pod żadnym pozorem wpłynąć na działanie niezmienianych modułów (patrz wymaganie 59).	2
59	Odporność	Każdy moduł powienien samodzielnie zapewniać poprawność danych wejściowych, a nie polegać na wyjściu innego modułu. Błędy nie mogą się propagować, powinny zostać przez system wychwycone na wczesnym etapie.	2