PRACA INŻYNIERSKA

IMPLEMENTACJA MOBILNEGO KLIENTA BANKU ZABEZPIECZONEGO TOKENEM

Autor:

Piotr Marek Ciecierski

Kierujący pracą:

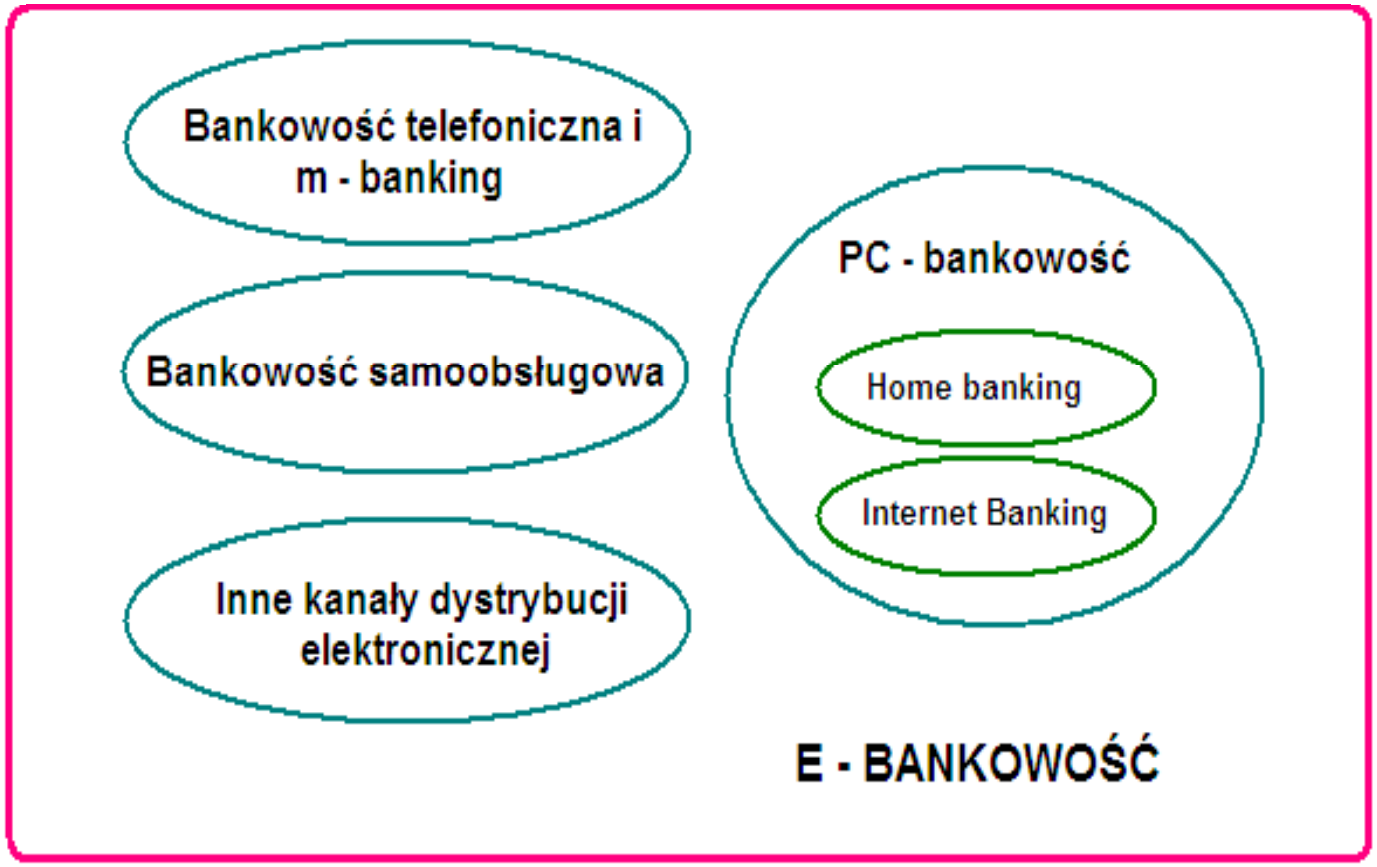
prof. dr hab. inż. Zbigniew Kotulski

Plan prezentacja

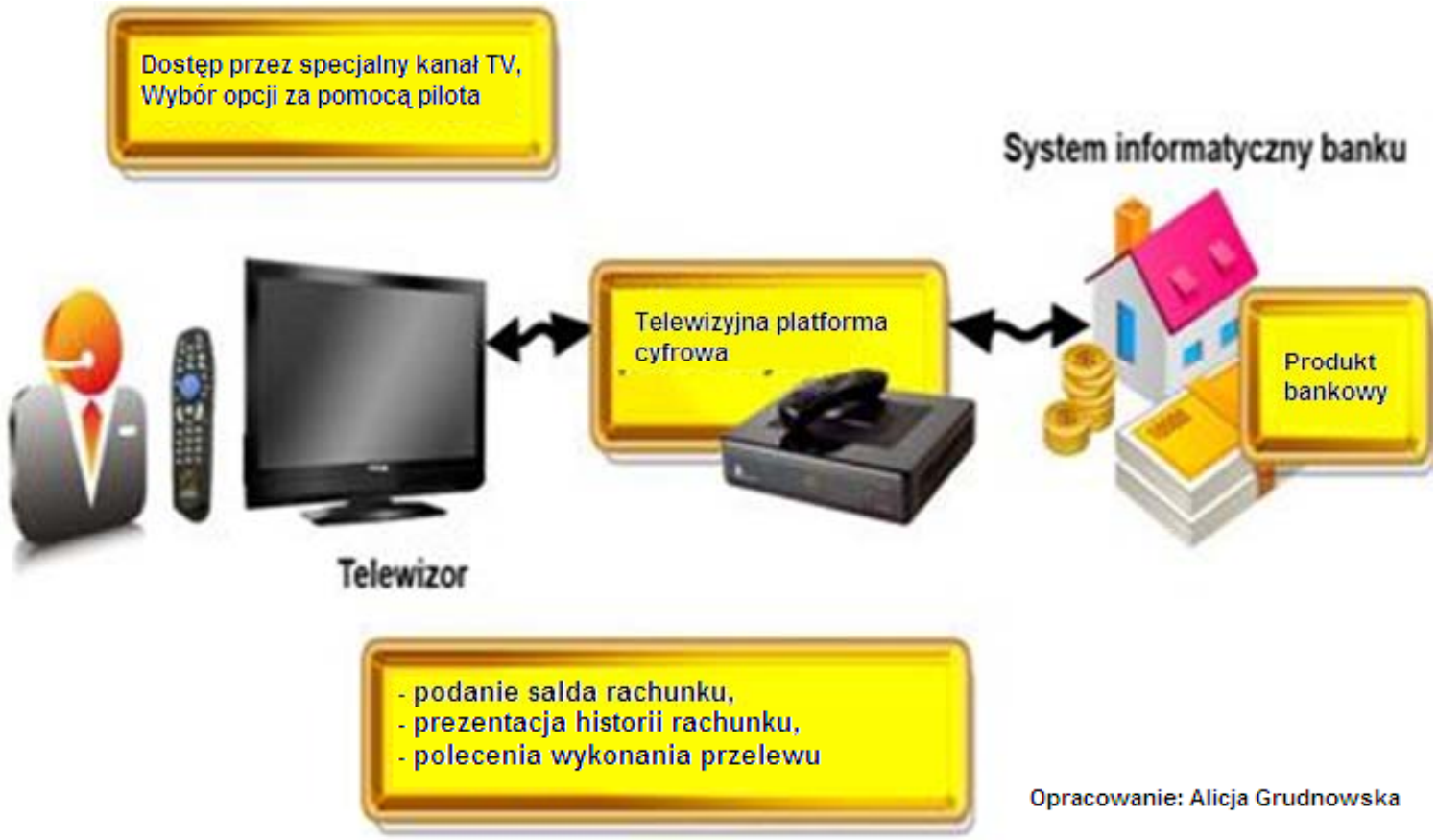
Spis treści:

1) Wprowadzenie - podział w elektronicznej bankowości
2) Usługa docelowa - bankowość mobilna
3) Założenia projektowe
   - token kryptograficzny
   - istniejące rozwiązania
4) Moja koncepcja
   - opis komponentów
   - metody zabezpieczeń
   - środowisko programistyczne
5) Osiągnięte rezultaty
6) Podsumowanie
7) Literatura

Podział elektronicznej bankowości



Bankowość telewizyjna



Opracowanie: Alicja Grudnowska

Bankowość mobilna

Definicja:

Usługa bankowości mobilnej jest to usługa znajdująca się na pograniczu bankowości i telekomunikacji, gdzie użytkownik ma dostęp do swojego rachunku z każdego miejsca na Ziemi przy wykorzystaniu urządzenia mobilnego podłączonego do sieci telefonicznej lub Internetu. [1]

Podział bankowości mobilnej:

- usługa SMS (ang. SMS banking);
- protokół WAP (ang. Wireless Application Protocol);
- bankowość internetowa (ang. i-banking)

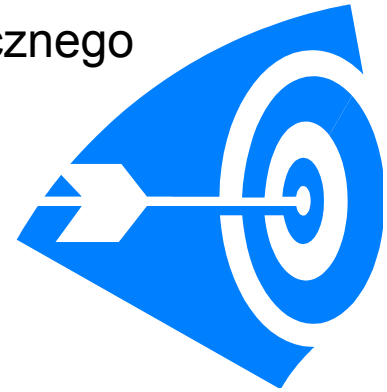
Czynniki rozwoju:

- stale rosnące zapotrzebowanie
- rozwój technologii w aparatach komórkowych
- zwiększenie gamy usług dostępnych drogą elektroniczną

Założenia projektowe

Stworzenie dedykowanej, mobilnej aplikacji do kontaktu z bankiem, która:

- zapewnieni wysoki poziom bezpieczeństwa
- będzie aplikacją user-friendly
- zapewni dostęp do podstawowych funkcji bankowości internetowej
- będzie służyła do autoryzacji operacji aktywnych - funkcja tokena kryptograficznego



Token kryptograficzny

Definicja:

Token kryptograficzny to małe urządzenie, bądź w przypadku telefonów komórkowych dedykowana aplikacja, która przy wykorzystaniu algorytmów kryptograficznych, służy m.in. do generowania haseł jednorazowych. Może być wykorzystywany w różnych systemach zabezpieczeń i pracować w kilku trybach w zależności od implementacji. [3]

Podstawowe rodzaje:

- OTP, czyli One Time Password
- karty inteligente
- tokeny software'owe

Przykłady Tokenów

Entrust OTP Identity Guard

Tryby pracy:

- hasła na bazie czasu
- hasła na bazie licznika
- hasła w trybie wyzwanie-odpowiedź

Token PPSD - Gemalto

System CERB - Wheel

RAIFFEISEN BANK POLSKA S.A. – MOBILNY BANK

Raiffeisen BANK
Raiffeisen Bank Polska S.A.

- aplikacja dedykowana na urządzenia mobilne
- integracja z funkcjami telefonu
- możliwość personalizacji
- mały transfer danych
- mała awaryjność
- małe wymagania
- wysoki poziom bezpieczeństwa

Mobilny Bank
Powered by Raiffeisen Bank Polska S.A.

RAIFFEISEN BANK POLSKA S.A. – MOBILNY BANK

Raiffeisen BANK
Raiffeisen Bank Polska S.A.

Bezpieczeństwo:

- odporność na phishing oraz atak main-in-the-middle
- odporność na ataki z grupy client site attack
- podpisany kod aplikacji
- szyfrowana transmisja danych przy pomocy protokołu SSL
- poufne dane nie są przechowywane na telefonie użytkownika
- automatyczne zamknięcie sesji użytkownika
- wykorzystanie identyfikatora urządzenia

Mobilny Bank
Powered by Raiffeisen Bank Polska S.A.

PEKAO S.A. - PEAKOTOKEN

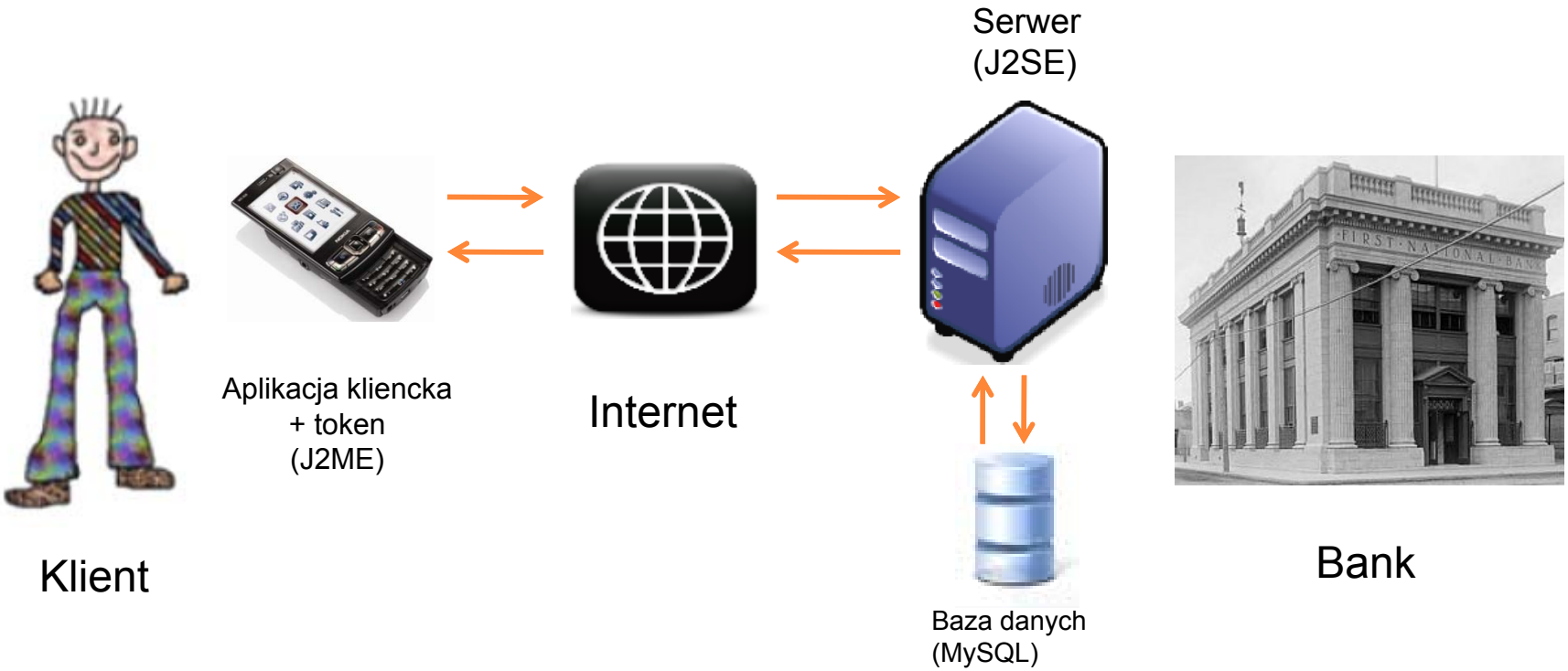
- aplikacja dedykowana na urządzenia mobilne
- innowacyjna metoda autoryzacji transakcji
- alternatywa dla listy haseł jednorazowych
- niskie wymagania
- darmowe korzystanie
- obecnie najbezpieczniejsza metoda autoryzacji transakcji

PEKAO S.A. - PEAKOTOKEN

Bezpieczeństwo:

- aplikacja zabezpieczona kodem PIN
- dodatkowa weryfikacja poprawności kodu PIN
- praca w dwóch trybach:
  - znacznik czasowy
  - wyzwanie-odpowiedź
- generowanie całkowicie w trybie off-line
- dla operacji „wysokiego ryzyka” kod powiązany z transakcją
- automatyczne wylogowanie użytkownika

Opis komponentów



Schemat środowiska testowe

Metody zabezpieczeń

Aplikacja kliencka:

- uruchomienie - kod PIN aplikacji
- logowanie do serwisu - hasło statyczne + hasło jednorazowe na bazie czasu (token – tryb znacznika czasowego)
- autoryzacja transakcji – hasło jednorazowe na podstawie kilku cyfr z numeru PESEL użytkownika (token – tryb wyzwanie-odpowiedź)

Połączenie pomiędzy aplikacją klienta, a serwerem banku:

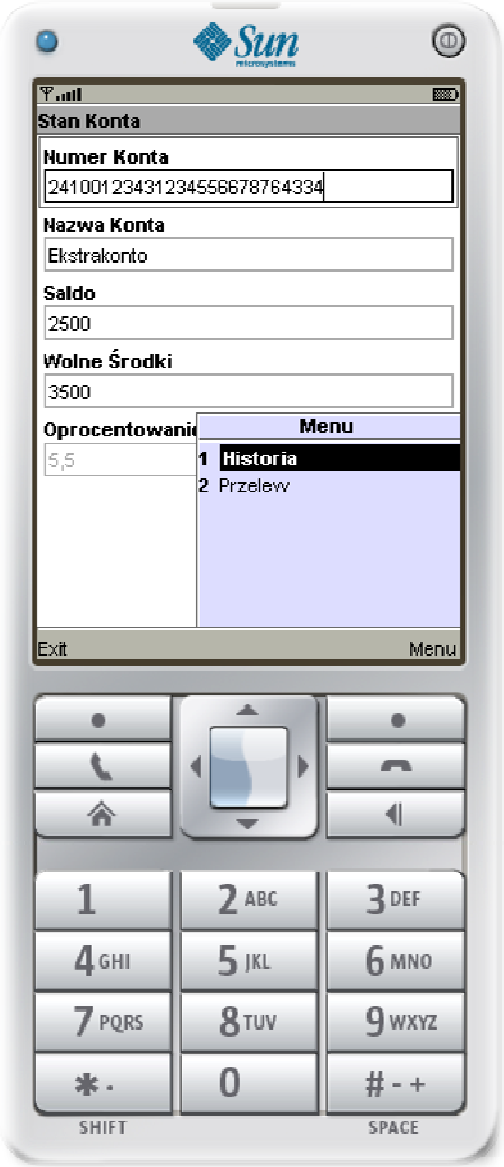
- transmisja szyfrowana np. SSL

Osiągnięte rezultaty

Aplikacja kliencka Mobilny Bank:

- napisana w języku Java w wersji dla urządzeń mobilnych (J2ME)
- możliwość sprawdzenia stanu konta, historii operacji oraz wykonania przelewu
- implementacja tokena służącego do logowania oraz autoryzacji operacji
- funkcjonalność 2 w 1
- niskie wymagania sprzętowe

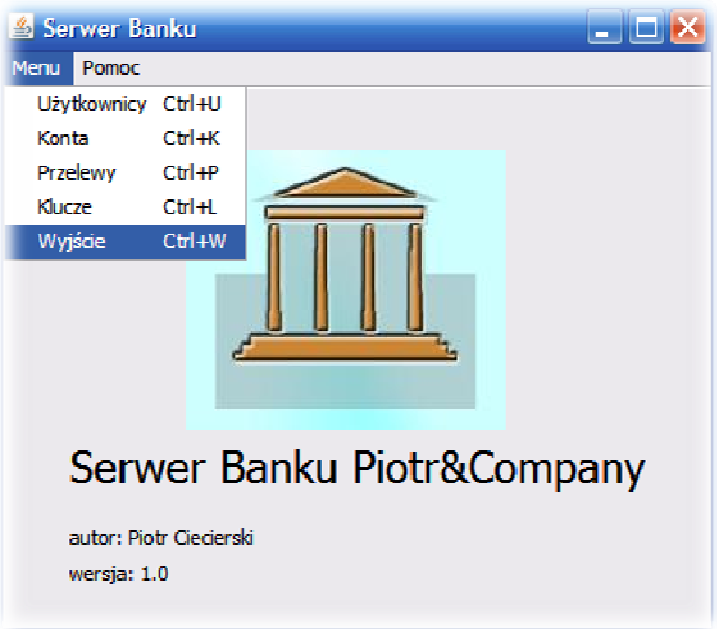
Osiągnięte rezultaty



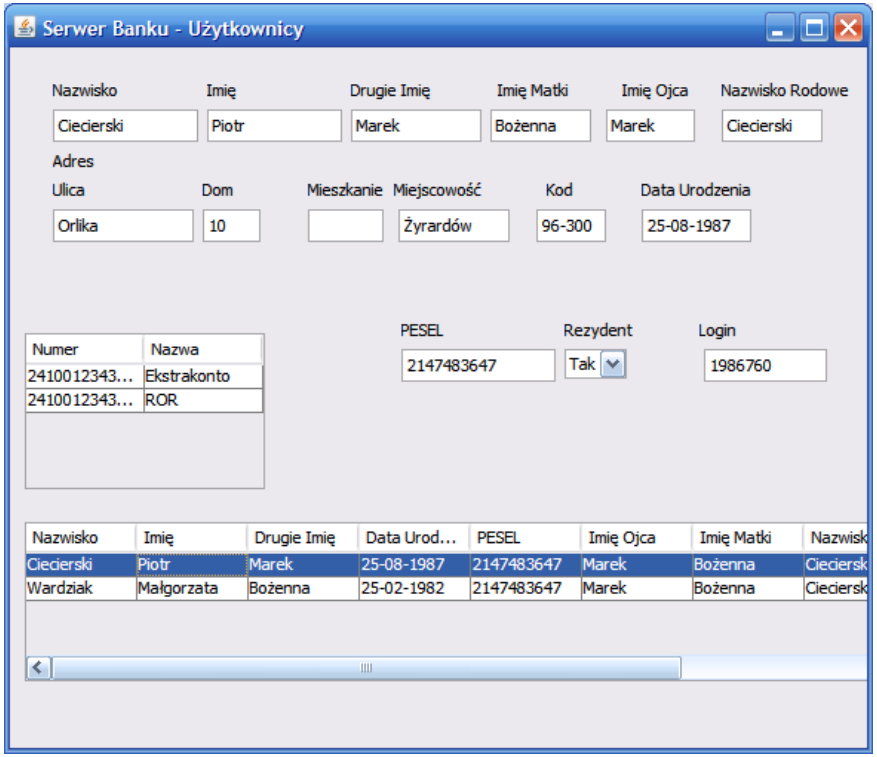
Osiągnięte rezultaty

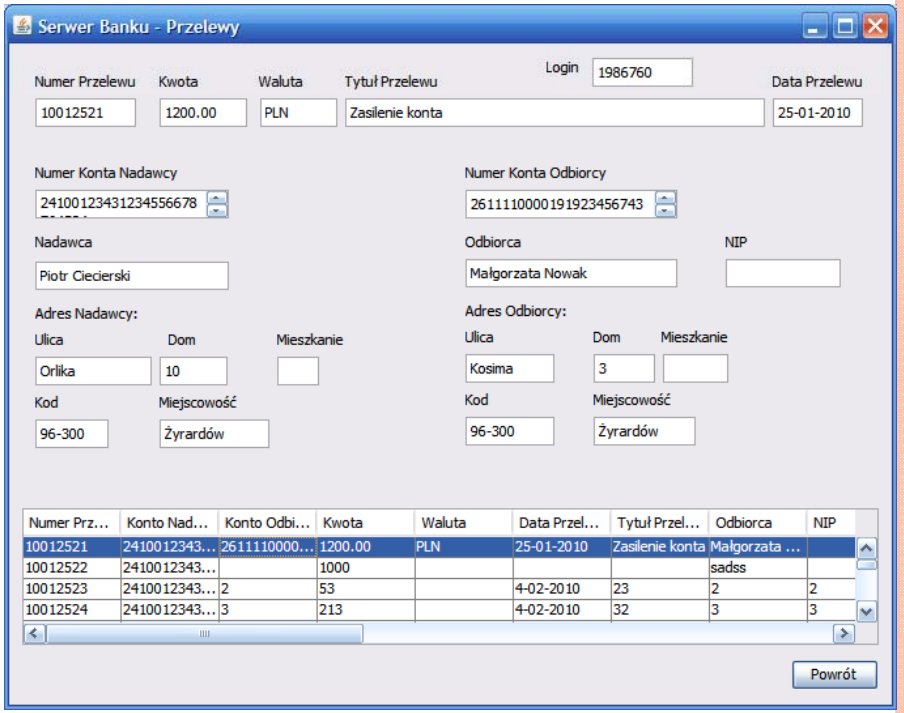
Aplikacja serwerowa banku:

- napisana w języku Java w wersji standardowej (J2SE)
- implementacja algorytmów weryfikujących poprawność haseł przy logowaniu oraz autoryzacji transakcji
- monitorowanie aktywności klientów



Osiągnięte rezultaty



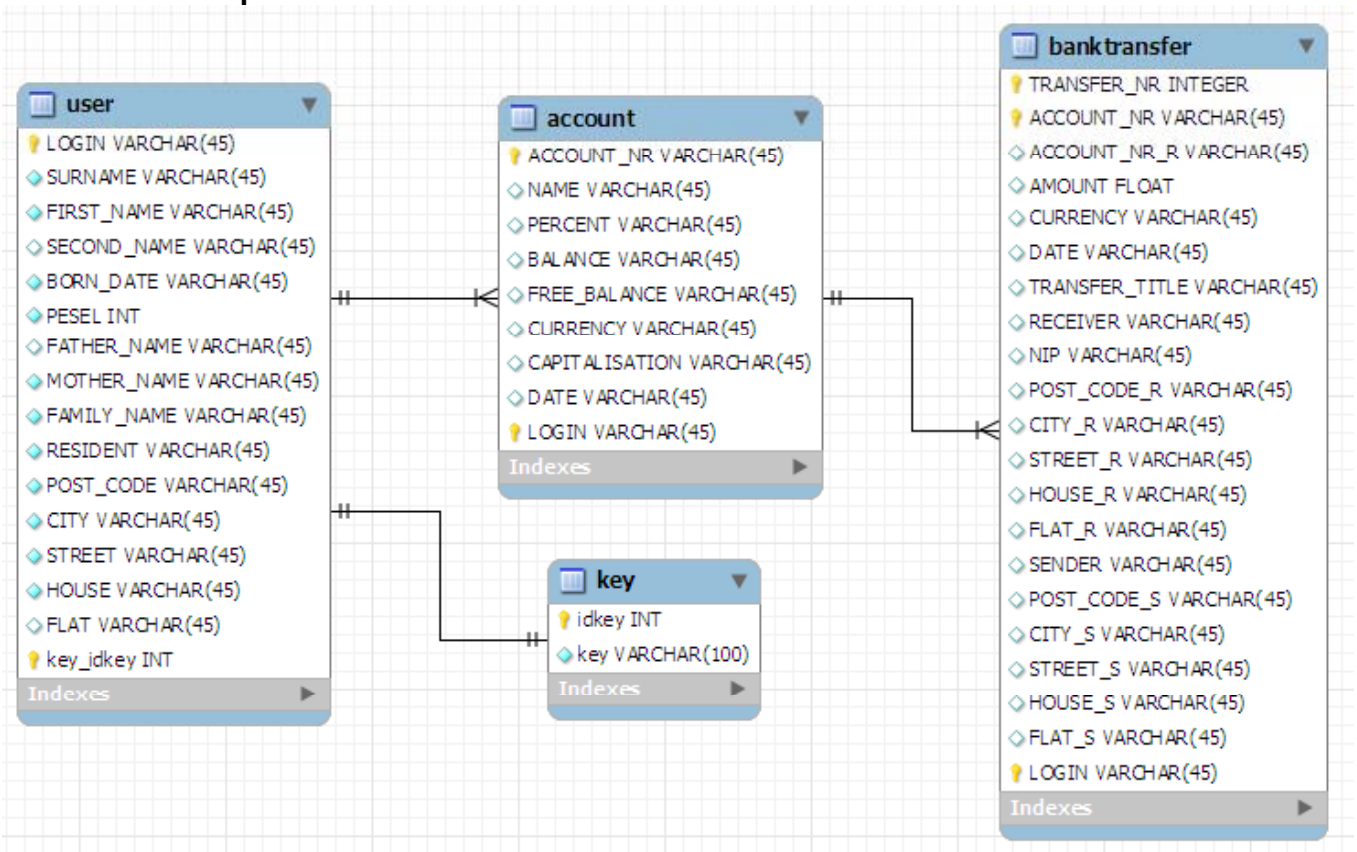


Aplikacja serwera banku

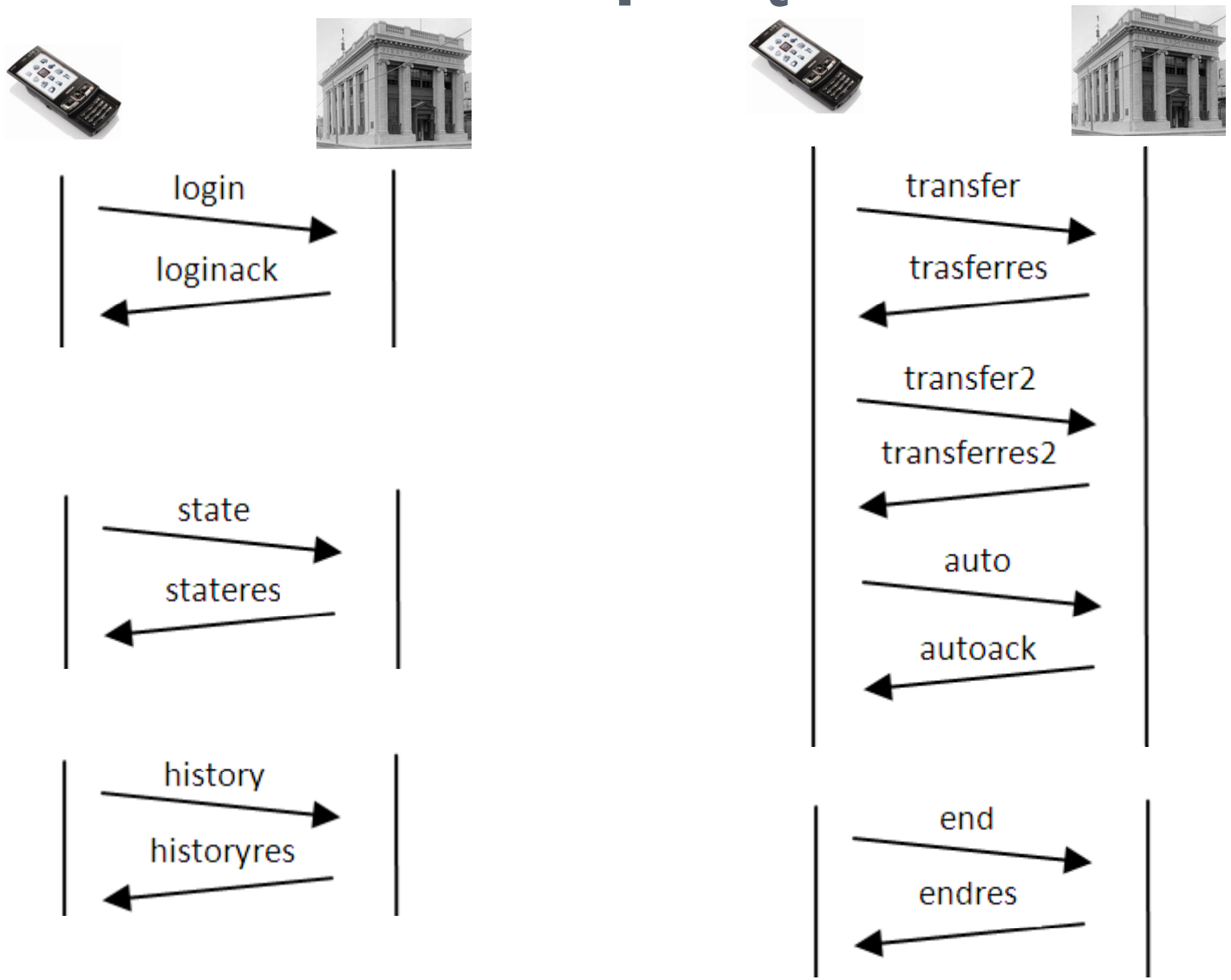
Osiągnięte rezultaty

Baza danych banku:

- baza danych MySQL
- przechowuje dane personalne oraz bankowe klientów
- brak zabezpieczenia

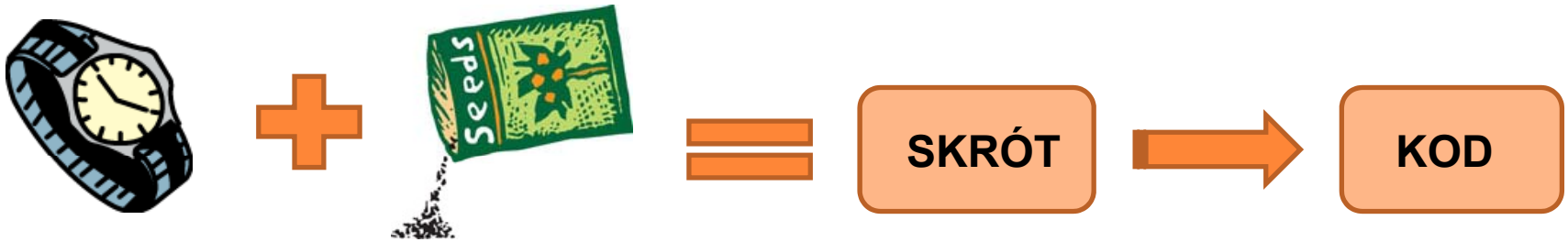


Protokół połączenia



Osiągnięte rezultaty

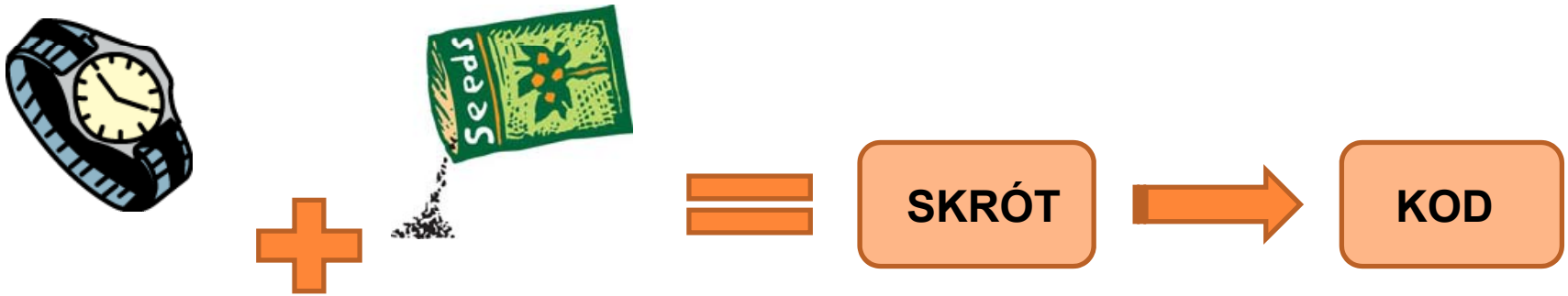
Algorytm generowania hasła na podstawie znacznika czasowego



- funkcja skrótu SHA-1 (160 bit)
- Ziarno ukryte w aplikacji (160 bit)
- 8 cyfrowe hasło
- hasło ważne 30-60 s

Osiągnięte rezultaty

Algorytm generowania hasła w trybie wyzwanie-odpowiedź



Wyzwanie

- funkcja skrótu SHA-1 (160 bit)
- ziarno ukryte w aplikacji (160 bit)
- 2 losowe cyfry z nr PESEL jako wyzwanie
- 8 cyfrowe hasło
- oczekiwanie na hasło 60-90 s

Podsumowanie

Aplikacja kliencka – Mobilny Klient:

- 2 w 1 – dedykowana aplikacja + token kryptograficzny
- duża dostępność ze względu na platformę Java
- łatwość w użyciu
- ogromna ilość potencjalnych klientów
- bezpieczeństwo

Literatura

[1] Dąbrowska A., Janoś-Kresło M., Wódkowski A.,
E-usługi a społeczeństwo informacyjne
Difin, 2009

[2] Miskiewicz M., Droździel A.,
e-Finanse rosną w siłę,
Money.pl, 2008

[3]Praca zbiorowa pod redakcją Andrzeja Gospodarowicza,
Bankowość elektronicza,
Polskie Wydawnictwo Ekonomiczne, 2005

[4] Macierzyński M.,
Bezpieczeństwo w bankowości internetowej,
Bankier.pl, 2009

[5] Raiffeisen Bank Polska S.A.,
Przewodnik użytkownika aplikacji Mobilny Bank,
2009