Aplikacje bankowe

Analiza obszaru logowania

softax

Spis treści

softax

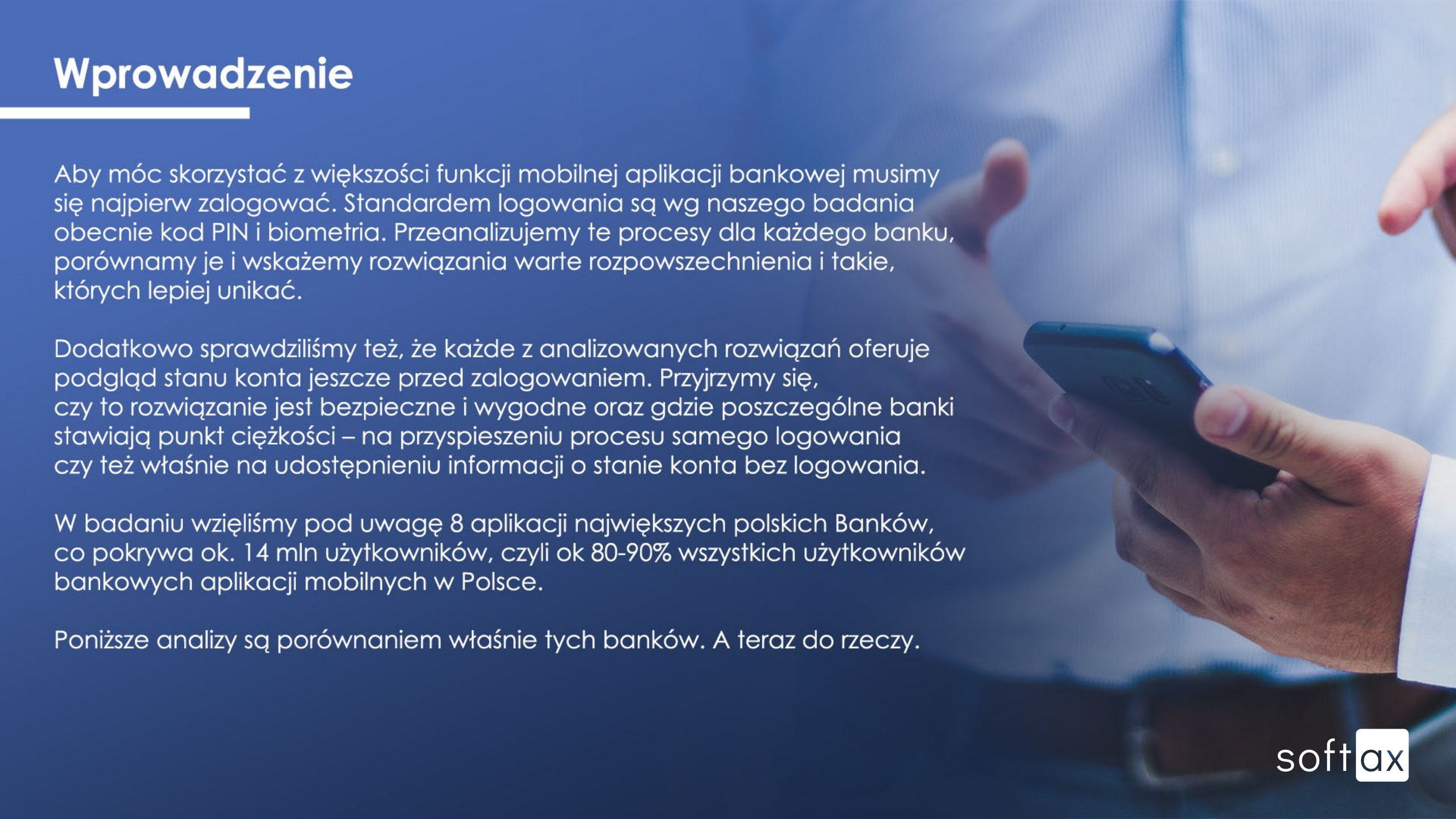
Wprowadzenie

Aby móc skorzystać z większości funkcji mobilnej aplikacji bankowej musimy się najpierw zalogować. Standardem logowania są wg naszego badania obecnie kod PIN i biometria. Przeanalizujemy te procesy dla każdego banku, porównamy je i wskażemy rozwiązania warte rozpowszechnienia i takie, których lepiej unikać.

Dodatkowo sprawdziliśmy też, że każde z analizowanych rozwiązań oferuje podgląd stanu konta jeszcze przed zalogowaniem. Przyjrzymy się, czy to rozwiązanie jest bezpieczne i wygodne oraz gdzie poszczególne banki stawiają punkt ciężkości – na przyspieszeniu procesu samego logowania czy też właśnie na udostępnieniu informacji o stanie konta bez logowania.

W badaniu wzięliśmy pod uwagę 8 aplikacji największych polskich Banków, co pokrywa ok. 14 mln użytkowników, czyli ok 80-90% wszystkich użytkowników bankowych aplikacji mobilnych w Polsce.

Poniższe analizy są porównaniem właśnie tych banków. A teraz do rzeczy.



softax

Skrót wniosków z badania

01 Największą różnicą pomiędzy Bankami jest możliwość logowania biometrią od razu na ekranie startowym. Część banków to umożliwia, inne nie, zapewne skupiając się na ułatwieniu dostępu do funkcji przed zalogowaniem.

02 Większe różnice występują w procesach służących zarządzaniu samym logowaniem i sposobem dostępu do stanu konta przed logowaniem.

03 Implementacja procesu logowania w każdym z badanych banków jest co najmniej poprawna, nie wykryliśmy poważnych błędów typu usability, niemniej żadna aplikacja nie ustrzegła się mniejszych lub większych potknięć.

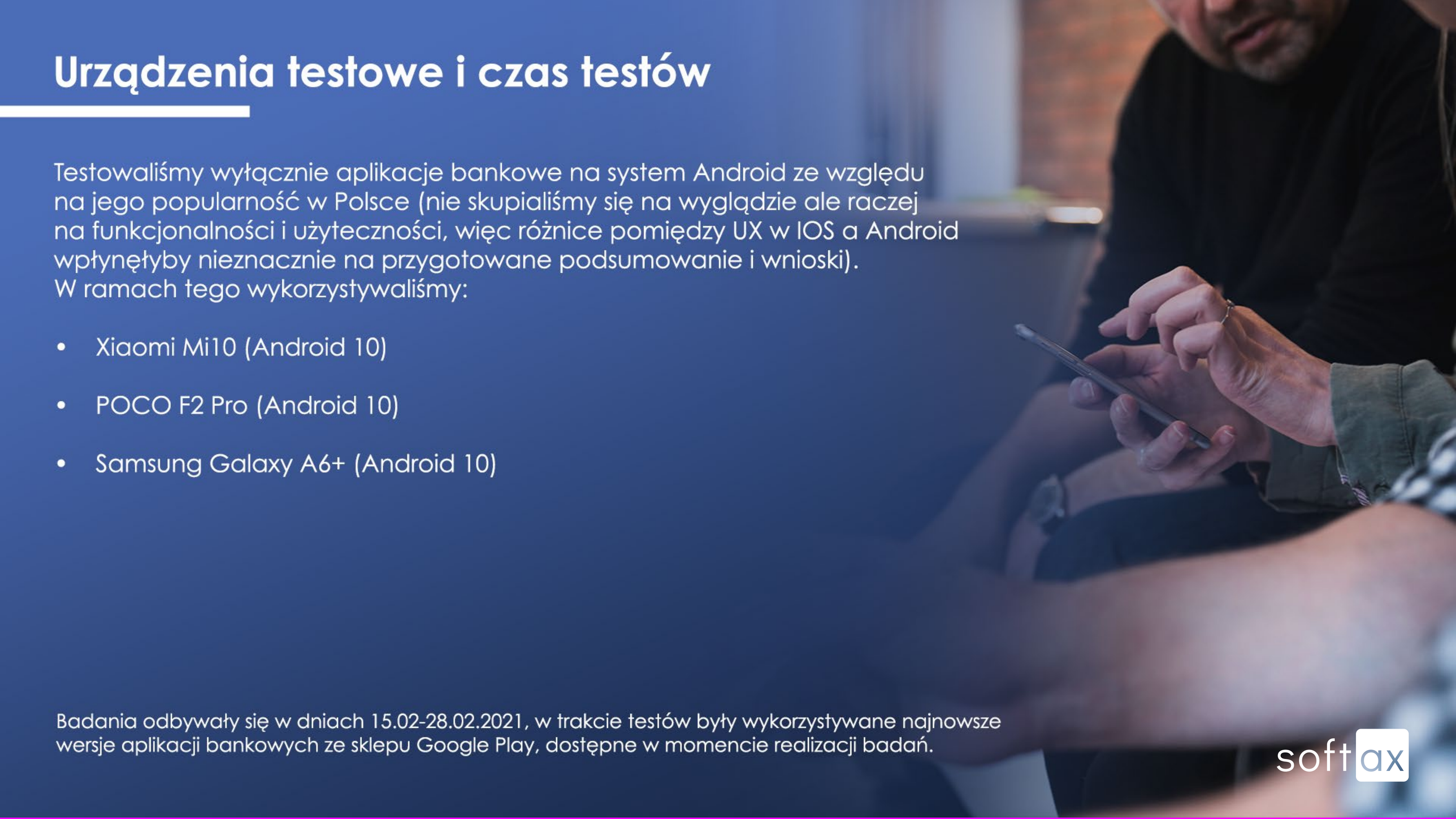
04 Wszystkie banki oferują podgląd stanu konta przez logowaniem choć ta funkcjonalność różni się zakresem i sposobem udostępniania danych.

softax

Urządzenia testowe i czas testów

Testowaliśmy wyłącznie aplikacje bankowe na system Android ze względu na jego popularność w Polsce (nie skupialiśmy się na wyglądzie ale raczej na funkcjonalności i użyteczności, więc różnice pomiędzy UX w IOS a Android wpłynęłyby nieznacznie na przygotowane podsumowanie i wnioski).
W ramach tego wykorzystywaliśmy:

- Xiaomi Mi10 (Android 10)
- POCO F2 Pro (Android 10)
- Samsung Galaxy A6+ (Android 10)



Badania odbywały się w dniach 15.02-28.02.2021, w trakcie testów były wykorzystywane najnowsze wersje aplikacji bankowych ze sklepu Google Play, dostępne w momencie realizacji badań.

softax

Analiza obszaru logowania dla każdej z aplikacji

Dla każdego banku przygotowaliśmy kilkadziesiąt slajdów ze skomentowanymi ekranami prezentującymi analizowane procesy.

softax

Proces Logowania

Ogólnie proces logowania

Proces logowania to najczęściej wykorzystywana funkcjonalność aplikacji bankowej (nawet pomimo tego, że część usług dostępna jest też bez logowania). Jak wyglądają kwestie związane z doświadczeniami klienta w zakresie zapewnienia spokoju, bezpieczeństwa i wygody (sprawności i szybkości obsługi) w analizowanych aplikacjach?

softax

Identyfikacja aplikacji

Ogólnie proces logowania

Aby mieć poczucie, że klient panuje nad sytuacją, po pierwsze musi mieć świadomość, z aplikacją jakiego banku pracuje. Wszystkie analizowane banki na stronie logowania prezentują mniejsze bądź większe logotypy swoich instytucji, ale jednak występują i tutaj pewne problemy.

softax

Identyfikacja aplikacji

Ogólnie proces logowania

mBank zamiast pełnego logotypu z nazwą stosuje tylko krótkie stylizowane logo z literką „m" oraz powitanie „Witaj w mBanku".

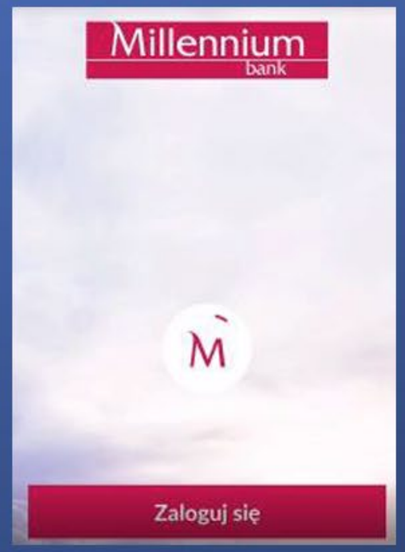
Na plus w pasku statusu (na samej górze) jest kolorowy wzór z języka wizualnego marki (który stosowany jest też na wszystkich podstronach aplikacji). To dobre rozwiązanie.

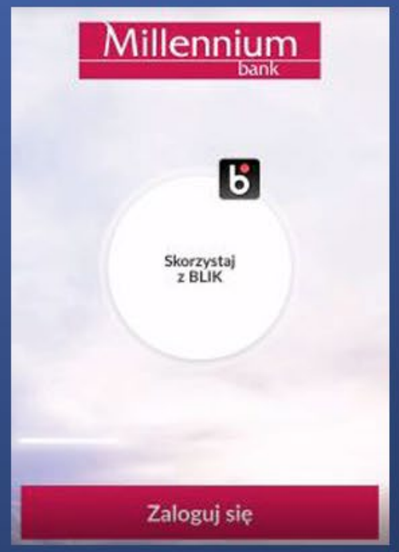
softax

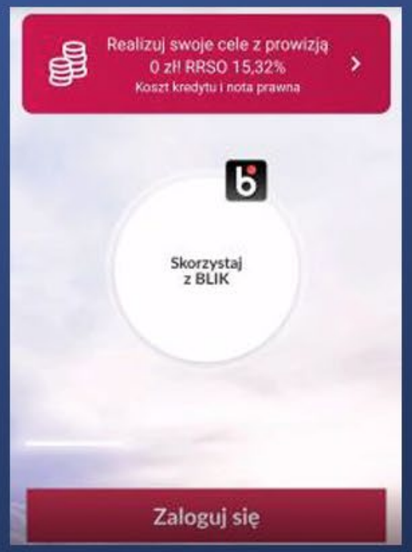
Identyfikacja aplikacji

Ogólnie proces logowania

W aplikacji banku Millennium logotyp instytucji jest po sekundzie od uruchomienia zasłonięty przez reklamę. Później do identyfikacji służy wyłącznie język kolorystyczny marki. To za mało.



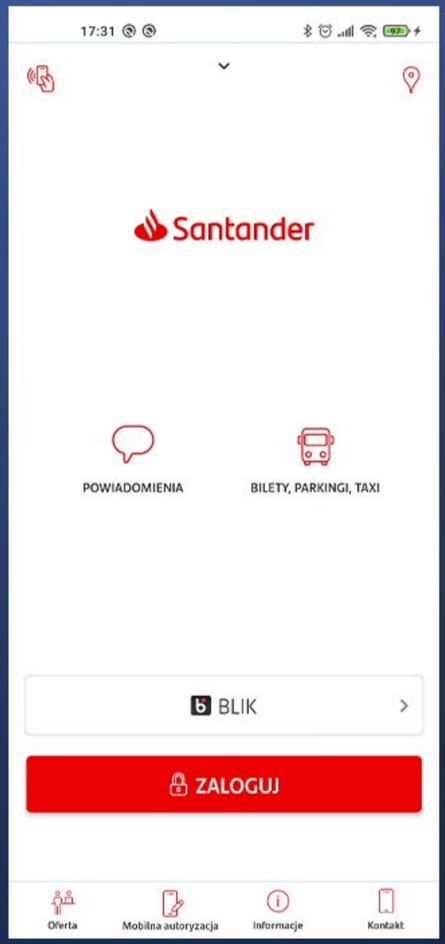




Widoczność przycisku Zaloguj

Ogólnie proces logowania

Kolejny krok to chęć zalogowania się. Przycisk Zaloguj, o ile jego użycie jest wymagane do zalogowania, powinien być łatwo widoczny i łatwo dostępny. Klient nie powinien go szukać. W większości banków (tak jak w przypadku Santander) przycisk logowania jest szeroki – w dolnej części ekranu i wyróżniający się kolorem – o to chodzi. W takiej formie jest łatwo dostępny także w przypadku korzystania jednorącz – jest w zasięgu kciuka (a to ważne dla szybkiego logowania). Dodatkowo jest wygodny zarówno dla osób lewo- jak i praworęcznych.

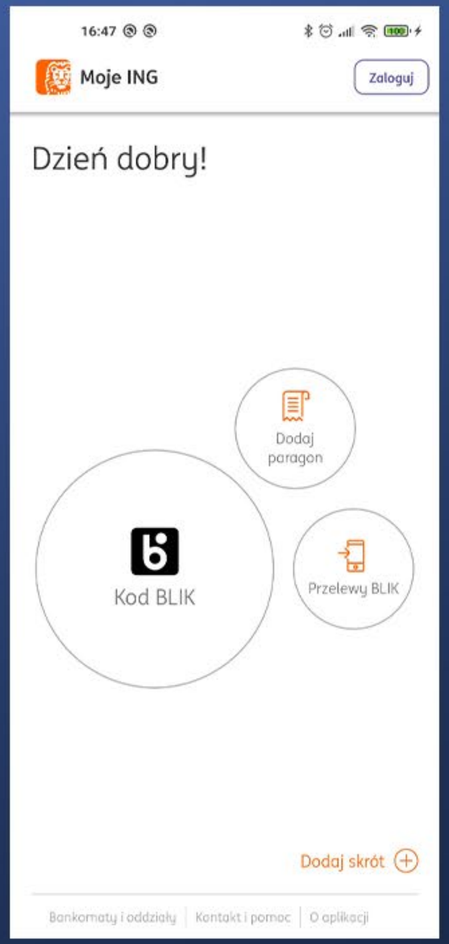


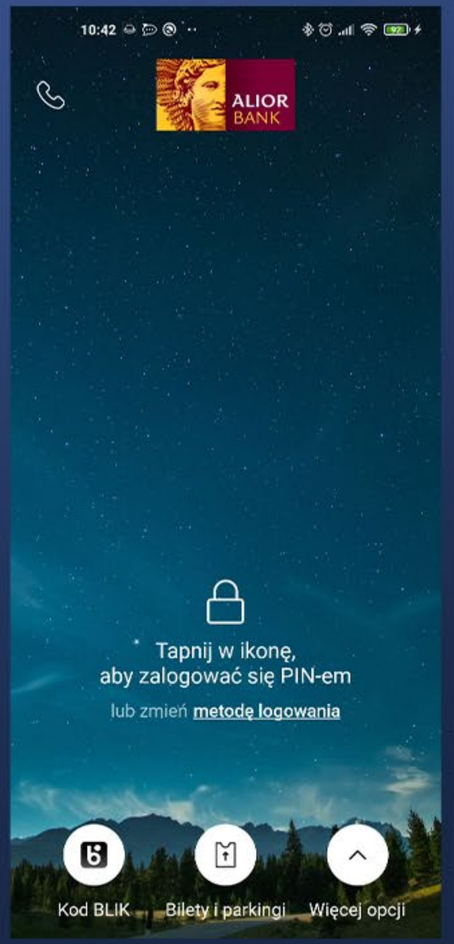
Widoczność przycisku Zaloguj

Ogólnie proces logowania

Niestety w dwóch przypadkach są z tym przyciskiem kłopoty. Najsłabiej wygląda to w aplikacji banku ING – przycisk Zaloguj jest w prawym górnym rogu, jest niewielki, także wizualnie się nie wyróżnia. Dodatkowo jest dosyć trudno dostępny, przy jednoręcznej obsłudze jest praktycznie poza zasięgiem.

W aplikacji Alior Banku z kolei przycisk logowania jest w dobrym miejscu, ale jest zrealizowany w formie ikony kłódki, której aktywność nie jest oczywista. Dlatego Bank stosuje tekstową wskazówkę „Tapnij w ikonę, aby zalogować się PIN-em".





softax

Logowanie kodem PIN

Wszystkie analizowane banki obsługują domyślnie logowanie kodem cyfrowym PIN. Różnią się jednak w kwestii dopuszczalnej liczby znaków, jaką kod PIN musi posiadać. Część Banków stawia na wygodę jako priorytet i dopuszcza kod PIN o stałej liczbie znaków (cyfr) – 4. Tak jest w przypadku Peopay, Millennium, IKO (PKOBP) i ING. Pozostałe analizowane instytucje decydują się na zwiększenie poziomu bezpieczeństwa i dopuszczają kod PIN o zmiennej długości – od 4 do 8 cyfr w przypadku Alior Banku i Santander, od 5 do 8 cyfr w przypadku mBanku. Na uwagę zasługuje aplikacja BNP Paribas, gdzie PIN może mieć od 6 do 20 znaków (zapamiętanie ciągu 20 cyfr jest praktycznie niemożliwe dla większości osób).

Trzeba wziąć pod uwagę, że dłuższy kod PIN zwiększa bezpieczeństwo, ale wyzwanie może stanowić kwestia wygody i zapewnienia klientowi odpowiedniego poczucia kontroli nad procesem logowania.

softax

Liczba znaków kodu PIN

Logowanie kodem PIN

Banki, które wymagają stałego 4-cyfrowego kodu PIN

ING

Millennium bank

Bank Pekao

Bank Polski

Banki, które pozwalają na określenie kodu PIN o długości od 4-5 do 8 znaków

ALIOR BANK

mBank

Santander

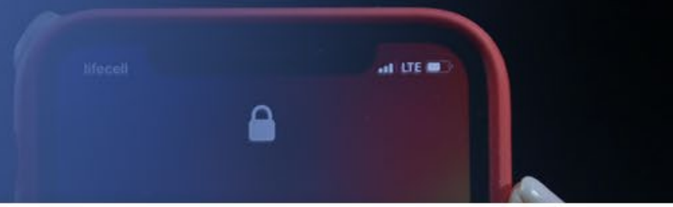
Bank, który pozwala na określenie kodu PIN o długości od 6 do 20 znaków

BNP PARIBAS

softax

Klawiatura dedykowana/systemowa

Logowanie kodem PIN



Aplikacje, które stosują dedykowaną klawiaturę kodu PIN

Aplikacje, które stosują klawiaturę systemową

softax

Czy wprowadzenie kodu PIN możliwe jest od razu po włączeniu aplikacji?

Logowanie kodem PIN

Banki stosują w swoich aplikacjach dwa podejścia. Albo strona startowa ma służyć prezentacji pewnych danych i udostępnieniu funkcji.
Albo też jest głównie przeznaczona do logowania. Z perspektywy wygody użytkownika i przyspieszenia procesu logowania lepsze jest podejście z ekranem startowym, gdzie od razu jest możliwość wprowadzenia kodu PIN. Takie podejście spośród badanych instytucji stosuje tylko mBank.

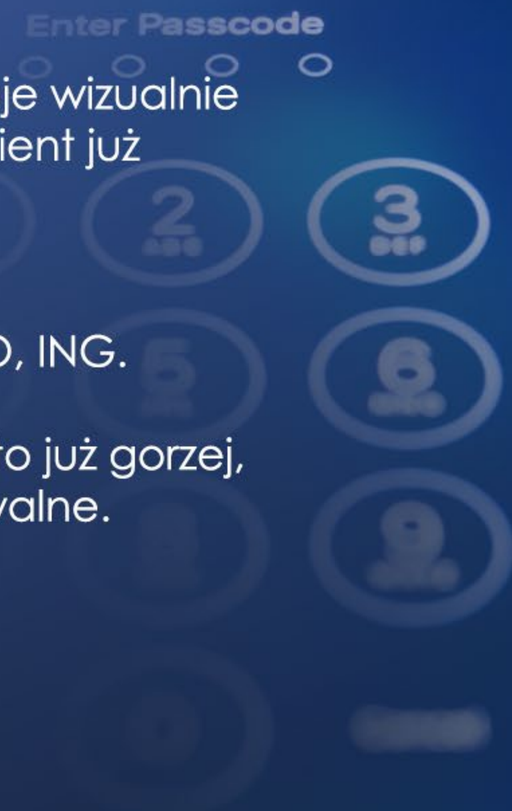
Pozostałe banki skupiają się na udostępnianiu, czasem naprawdę sporej funkcjonalności bez konieczności logowania. Część z nich – PKOBP (IKO), Santander i Millennium pozwala jednak na uruchomienie logowania biometrią od razu na ekranie startowym aplikacji.

Z naszej perspektywy rozpowszechnienie logowania biometrią zmniejsza znaczenie funkcji dostępnych bez logowania. Logowanie biometrią jest szybkie i proste (ma tutaj dużą przewagę nad kodem PIN), także wszystkie instytucje powinny przynajmniej jako konfigurowalną opcję dać możliwość zalogowania się nią od razu na ekranie startowym. Bez konieczności tapnięcia Zaloguj. W przypadku logowania kodem PIN jest to już kwestia indywidualnego podejścia.

softax

Wizualne wskazówki odnośnie długości kodu PIN

Logowanie kodem PIN



Kolejna sprawa dotycząca pewności korzystania z aplikacji dotyczy kwestii, czy system pokazuje wizualnie akceptowaną długość kodu PIN – i czy w szczególności pozwala łatwo ocenić, ile cyfr kodu klient już wprowadził, ale ile jeszcze mu zostało do wprowadzenia.

Problemu nie ma z reguły, jeśli dany bank obsługuje kod PIN o stałej liczbie znaków – 4.
Wtedy widzimy dopracowane wizualnie ekrany. I tak jest w przypadku Peopay, Millennium, IKO, ING.

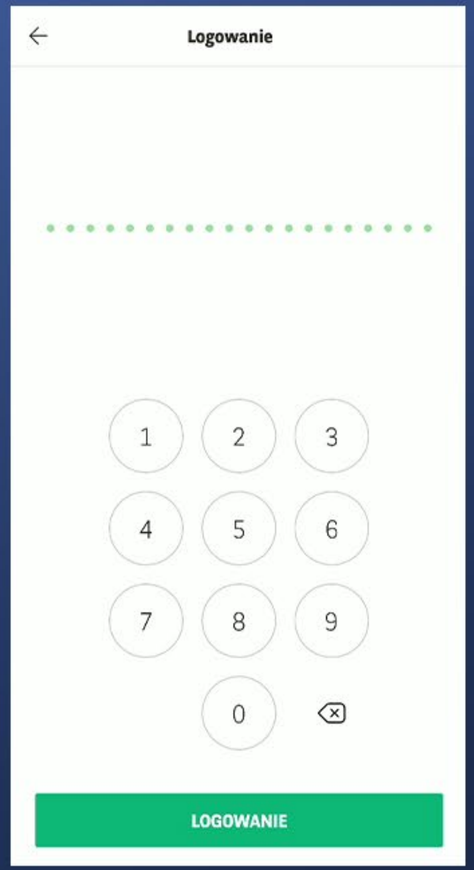
Inne banki pozwalają klientowi wybrać PIN o zmiennej długości. W takim przypadku wygląda to już gorzej, ale o ile faktycznie wprowadzone dane są ograniczone do 8 znaków, jest to jeszcze akceptowalne.

softax

Wizualne wskazówki odnośnie długości kodu PIN

Logowanie kodem PIN

Z perspektywy spokoju klienta, negatywnym przykładem jest tutaj aplikacja Banku BNP Paribas, która dopuszcza kod PIN o długości 20 znaków. Prezentacja wizualnie nie ułatwia kontroli wprowadzanych znaków. Zastosowanie tak długiego kodu jest dobrowolne.

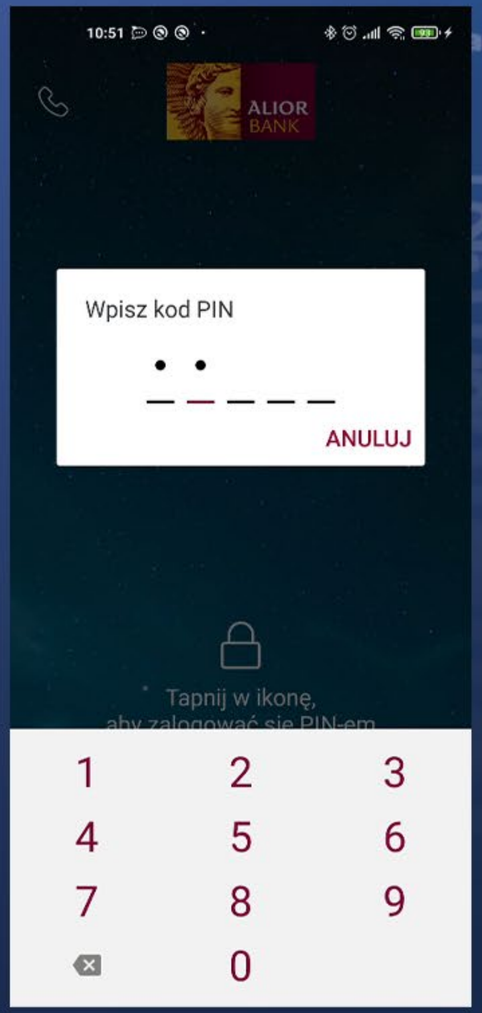


Wizualne wskazówki odnośnie długości kodu PIN

Logowanie kodem PIN

Takie podejście jednak ma pewne swoje usprawiedliwienie w kwestii bezpieczeństwa. Nie ograniczając wprowadzanych znaków teoretycznie dajemy więcej możliwości i utrudniamy włamanie. Jest to jednak w naszej ocenie zbyt daleko idące podejście.

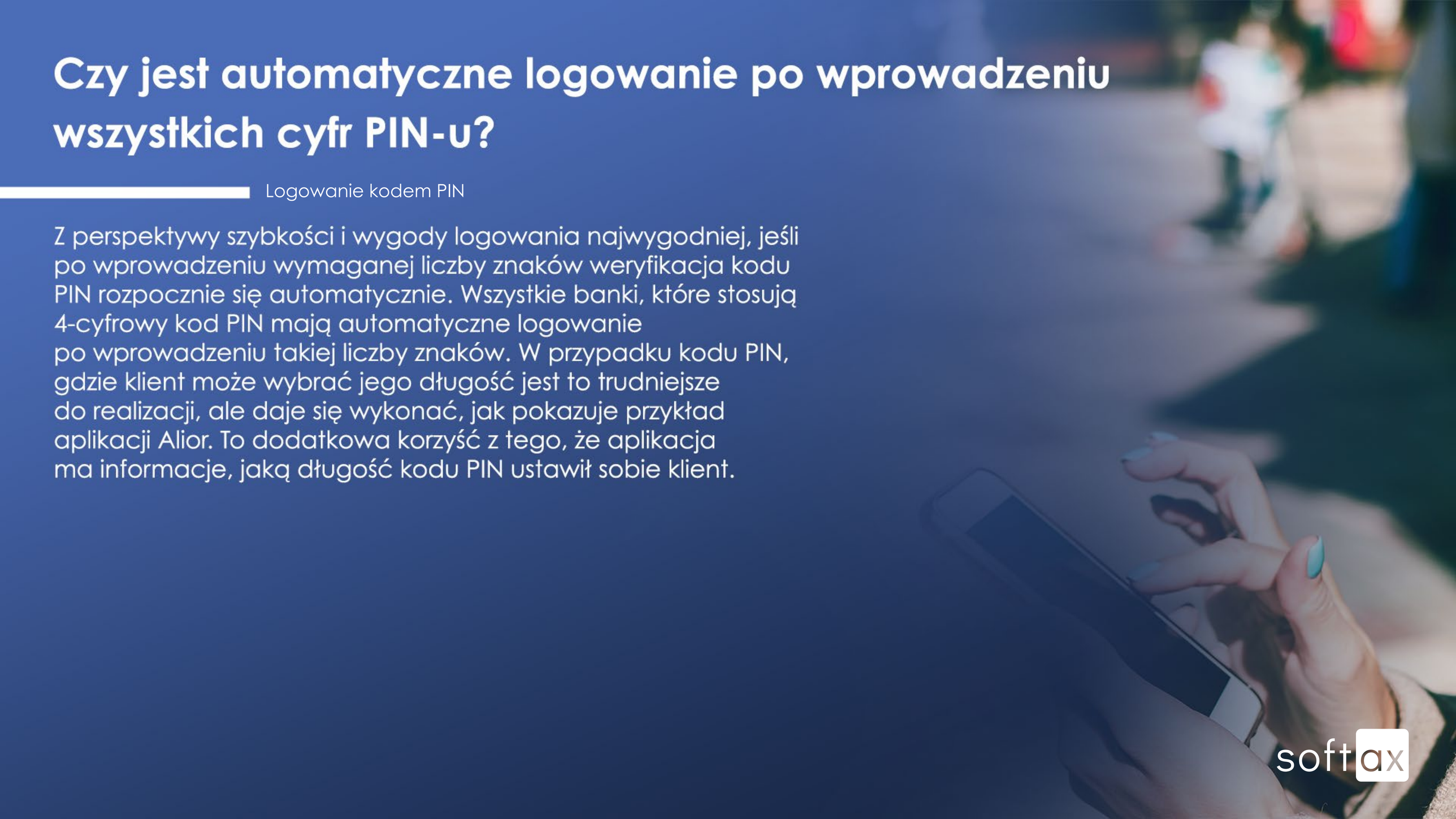
Godnym naśladowania rozwiązaniem jest za to mechanizm w Alior Banku. Kod PIN może tam mieć zmienną długość (4-8 cyfr), ale system prezentuje tyle pól na wprowadzenie kodu ile faktycznie zawiera kod PIN klienta.



Czy jest automatyczne logowanie po wprowadzeniu wszystkich cyfr PIN-u?

Logowanie kodem PIN

Z perspektywy szybkości i wygody logowania najwygodniej, jeśli po wprowadzeniu wymaganej liczby znaków weryfikacja kodu PIN rozpocznie się automatycznie. Wszystkie banki, które stosują 4-cyfrowy kod PIN mają automatyczne logowanie po wprowadzeniu takiej liczby znaków. W przypadku kodu PIN, gdzie klient może wybrać jego długość jest to trudniejsze do realizacji, ale daje się wykonać, jak pokazuje przykład aplikacji Alior. To dodatkowa korzyść z tego, że aplikacja ma informacje, jaką długość kodu PIN ustawił sobie klient.

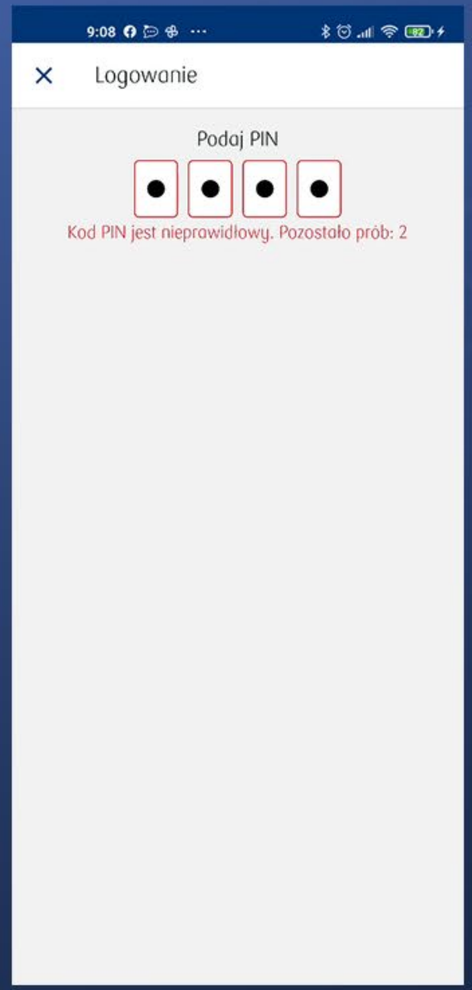


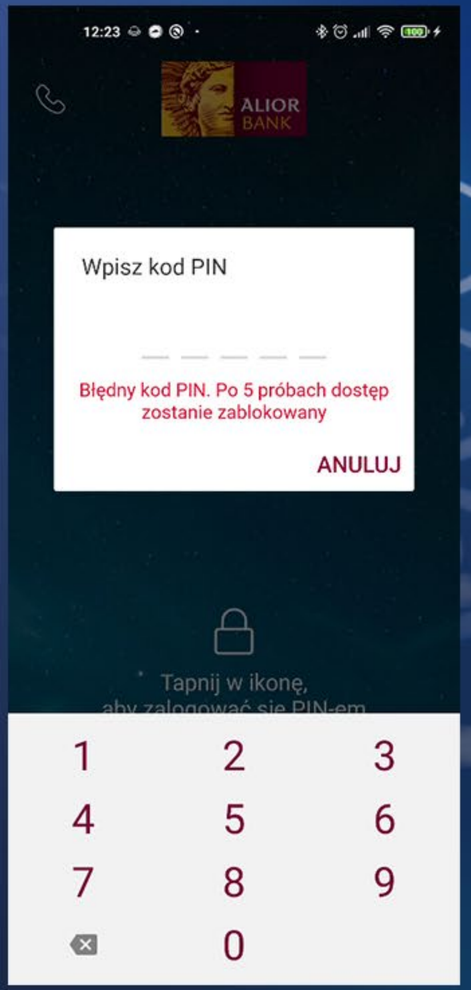
softax

Informacja o liczbie błędnych prób do zablokowania dostępu

Logowanie kodem PIN

Banki mają polityki bezpieczeństwa skutkujące blokadą dostępu w przypadku zbyt dużej liczby nieudanych prób zalogowania. Słusznie. Jednak z perspektywy klienta, który nie może sobie przypomnieć kodu PIN istotne jest, by aplikacja prezentowała informacje o tym, ile jeszcze prób do zablokowania zostało.





softax

Informacja o liczbie błędnych prób do zablokowania dostępu

Logowanie kodem PIN

Banki, które informują o pozostałej liczbie prób logowania

- ALIOR BANK
- PKO Bank Polski

Banki, które o tym nie informują

- ING
- BNP PARIBAS
- Millennium bank
- mBank
- Bank Pekao
- Santander

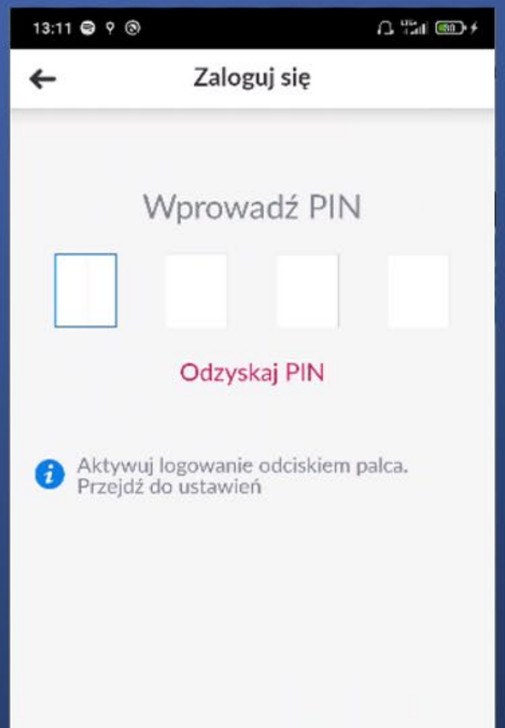
softax

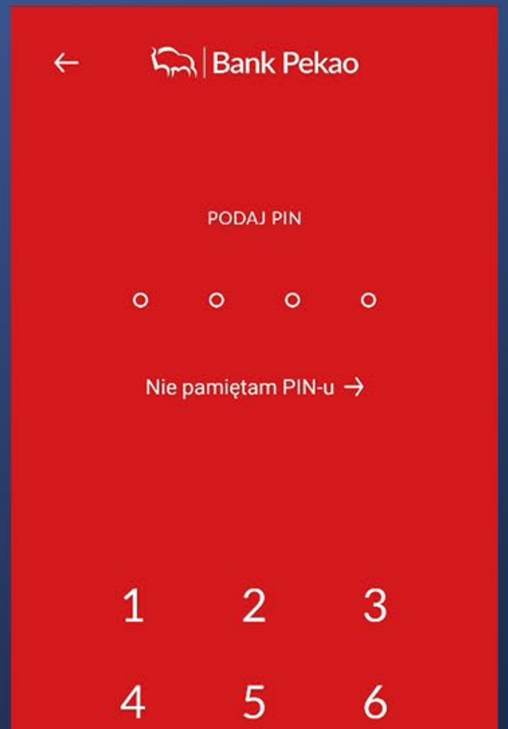
Instrukcja „Nie pamiętam PIN-u”

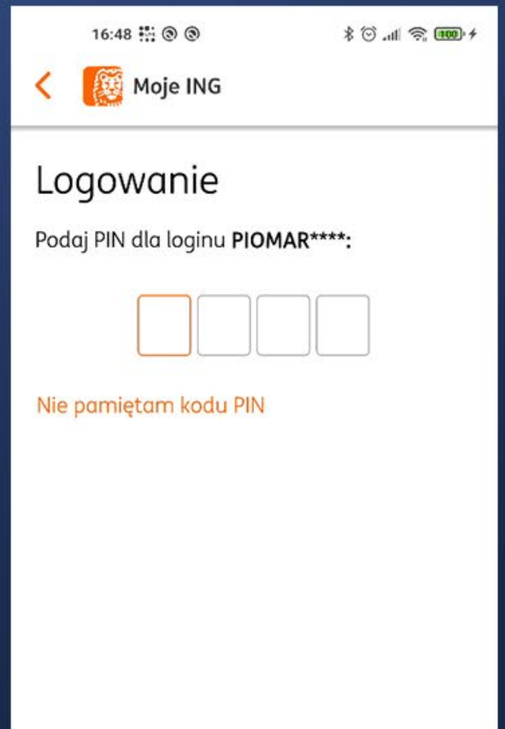
Logowanie kodem PIN

Logowanie kodem PIN wymaga od klienta pewnego wysiłku. Nie tylko chodzi o jego wprowadzanie, ale o samą konieczność pamiętania kodu. Niestety, niezależnie jak się staramy, może się zdarzyć, że zapomnimy swój kod PIN. Szczególnie, jeśli klient zazwyczaj loguje się biometrią i nie korzysta z często kodu PIN. Bank powinien dawać wsparcie klientowi w takiej sytuacji. Niestety mało banków tak robi w swoich aplikacjach.

Pozytywne przykłady dotyczą aplikacji Millennium, ING Bank (gdzie przekierowuje do logowania hasłem maskowanym) oraz Banku Pekao (gdzie powoduje wywołanie dedykowanej rozmowy z CallCenter).







softax

Instrukcja „Nie pamiętam PIN-u”

Logowanie kodem PIN

Aplikacje, które dają informacje w sytuacji, gdy nie pamiętamy kodu PIN

Bank Pekao

Millennium bank

ING

Aplikacje, które takiego wsparcia nie oferują

ALIOR BANK

BNP PARIBAS

Bank Polski

mBank

Santander

softax

Logowanie PIN-em przy włączonej biometrii

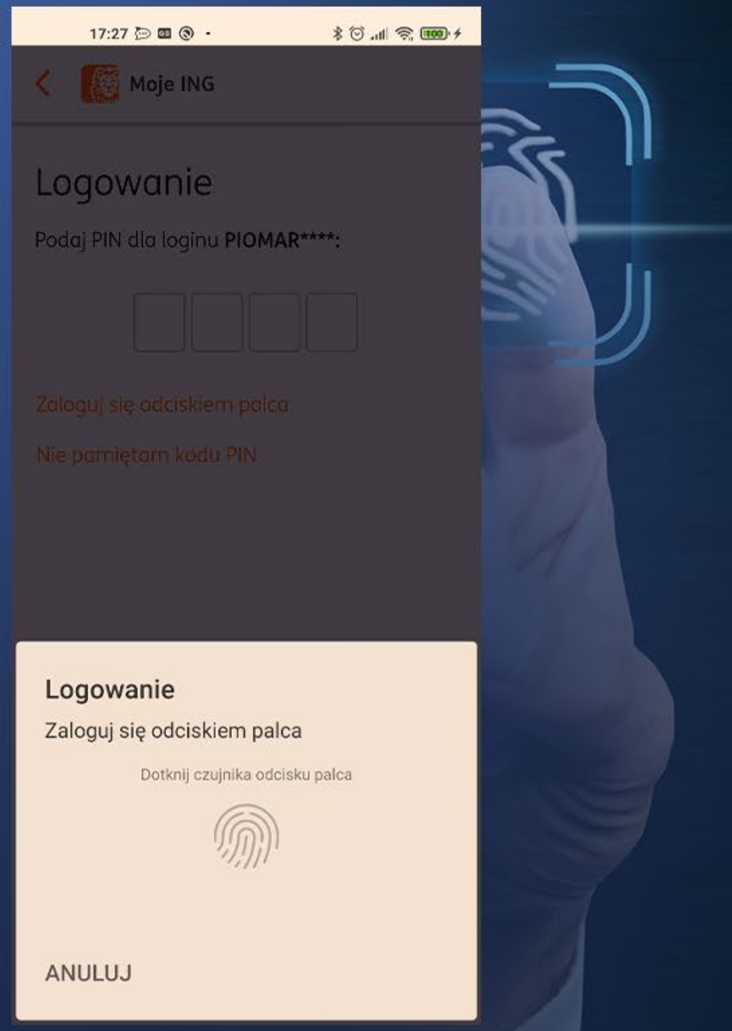
Logowanie kodem PIN

Przy logowaniu kodem PIN mamy potencjalnych kilka kwestii, które mogą zburzyć spokój klienta.

Pierwsza sprawa to w ogóle dostęp do logowania PIN-em w sytuacji, kiedy włączone jest domyślne logowanie biometrią. Każdy bank na to pozwala. Klient czasem nie chce lub nie może skorzystać z weryfikacji odciskiem palca i musi mieć prosty dostęp do standardowego rozwiązania – kodu PIN. Jak to wygląda w różnych bankach?

Generalnie po tapnięciu przycisku Zaloguj przy włączonej biometrii pojawia się panel biometrii. Po kliknięciu na ekran poza nim, lub na przycisk Anuluj/Zamknij zazwyczaj trafiamy na ekran do podania kodu PIN. I to jest ok.

O ile w tle widzimy ekran do podania kodu PIN takie podejście nie wydaje się rodzić problemów. Tak jest oprócz ING także w IKO, mBanku i BNP Paribas



softax

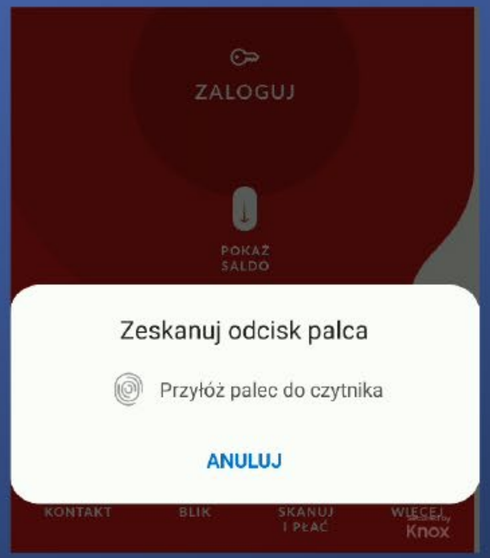
Logowanie PIN-em przy włączonej biometrii

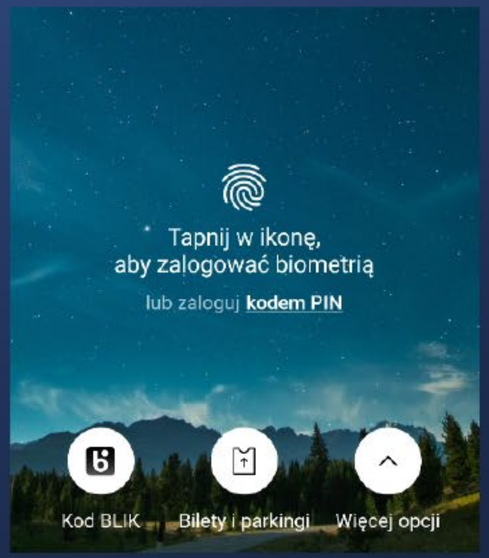
Logowanie kodem PIN

W przypadku Peopay pod wyświetlanym panelem autoryzacji biometrią niestety nie widzimy ekranu do wprowadzenia kodu PIN. Tapnięcie Anuluj rzeczywiście do niego prowadzi, ale nie jest to oczywiste.

Inne pozytywne przykłady to Millennium i Alior – przy włączonej biometrii można zalogować się kodem PIN dzięki dedykowanej nazwanej opcji.

Zalecamy, by stosować takie rozwiązanie także na standardowym panelu biometrii, gdzie tzw. negatywny przycisk może nosić etykietę „Lub zaloguj się kodem PIN", zamiast typowego Zamknij lub Anuluj.

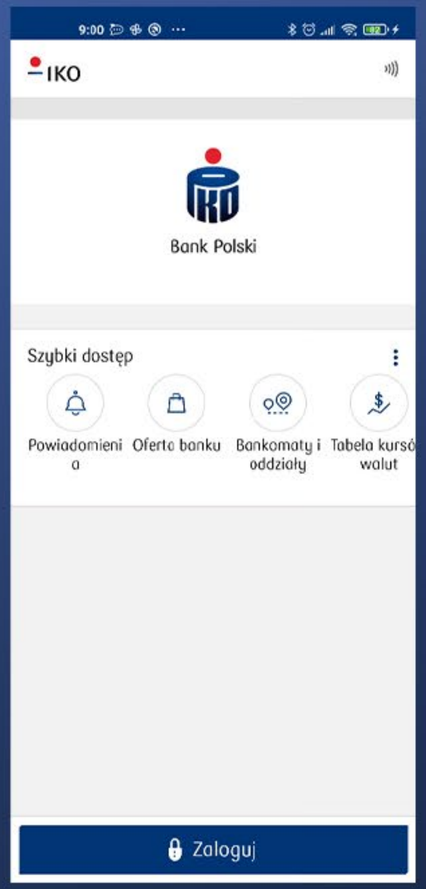




Logowanie PIN-em przy włączonej biometrii

Logowanie kodem PIN

Pewien problem pojawia się też w IKO, gdy mamy dodatkowo włączone uruchamianie logowania biometrią już na ekranie startowym. Wtedy, aby dotrzeć do kodu PIN potrzebne jest dwukrotne anulowanie logowania biometrią (najpierw na starcie, a potem po kliknięciu Zaloguj).



softax

Możliwość logowania hasłem (jako alternatywa dla PIN)

Logowanie kodem PIN

Wszystkie banki oferują możliwość logowania numerycznym kodem PIN. Część banków – Pekao SA (Peopay) i Santander oferują możliwość ustawienia logowania się hasłem maskowanym. ING Bank oferuje taki sposób logowania jako tryb zapasowy w przypadku, gdy klient zapomni swojego kodu PIN.

Tego typu mechanizmy są jednak, w naszej opinii, skazane na bycie pewną niszą. Klienci oczekują przede wszystkim wygody – logowanie za pomocą hasła maskowanego jest trudne (szczególnie na telefonie), nawet, jeśli utrudnia przechwycenie wpisywanych danych. Niemniej jako opcja dla pewnych grup klientów lub tryb zapasowy może to być dopuszczalne.

softax

Logowanie biometrią

Wszystkie analizowane aplikacje pozwalają na logowanie się biometrią. Z perspektywy klienta logowanie biometrią, co oczywiste, zwiększa wygodę i szybkość procesu logowania.

Kwestie bezpieczeństwa są tutaj sprawą nieco skomplikowaną. Logowanie biometrią zapobiega zdalnemu przechwyceniu kodu PIN czy hasła, więc można powiedzieć, że z jednej strony zwiększa bezpieczeństwo. Z drugiej strony jednak naraża na sytuacje nieautoryzowanego dostępu w przypadku nieświadomości posiadacza telefonu i wykorzystania takiego stanu przez nieuprawnione osoby (przykłady jakie podają media: córka odblokowała telefon śpiącej matki korzystając z jej odcisku palca czy studenci w tracie imprez alkoholowych uzyskujący dostęp do telefonu upojonego kolegi).

Zalecane jest zatem monitorowanie, za pomocą systemu antyfraudowego, sytuacji dostępu do danych klienta i zleceń realizowanych z aplikacji w zależności od sposobu logowania (kodem PIN lub biometrią).

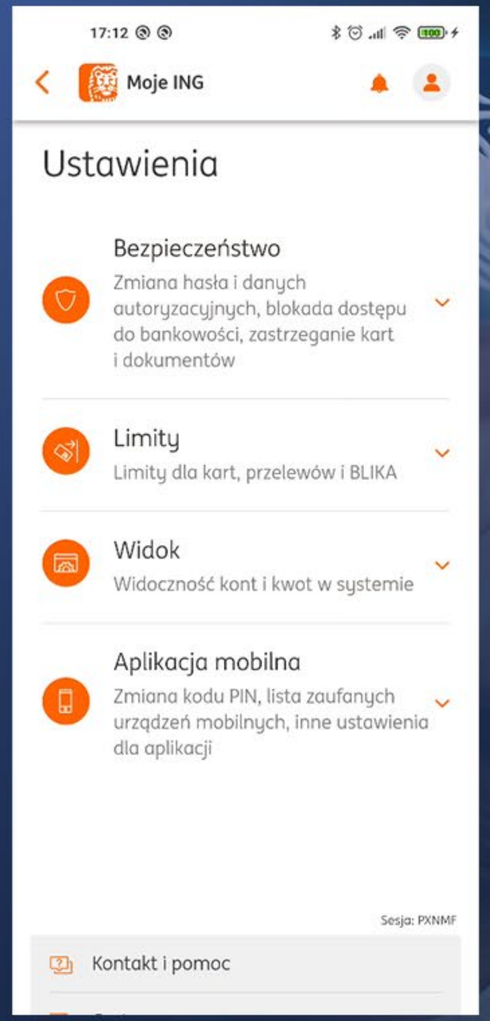
softax

Dostęp do konfiguracji biometrii w ustawieniach

Logowanie biometrią

Sprawdziliśmy, jak trudno jest znaleźć w Ustawieniach miejsce pozwalające na włączenie biometrii. W większości aplikacji jest to łatwe, na głównym poziomie ustawień lub w takiej sekcji, która wydaje się jednoznacznie określać miejsce, gdzie należy szukać odpowiedniej opcji. Pewien problem mieliśmy w aplikacji ING, gdzie dwie sekcje pasowały: „Bezpieczeństwo" i „Aplikacja mobilna". Pomimo tego, że sekcje mają swój opis, logowanie biometryczne nie zostało wymienione w żadnej z nich, wiec potrzebne było zgadywanie (w tym przypadku właściwa była ta druga opcja).

W naszej ocenie aplikacje bankowe już na stronie startowej lub stronie logowania powinny zachęcać do włączenia logowania biometrią poprzez odpowiednią informację i przekierowanie od razu do odpowiedniej sekcji w Ustawieniach. Alior Bank proponuje przekierowanie do zmiany metody logowania (to dobrze, ale brakuje konkretnej informacji o włączeniu logowania biometrią), natomiast Millennium Bank proponuje aktywację logowania odciskiem palca w ustawieniach, ale bez przejścia od razu do odpowiedniego miejsca w aplikacji.

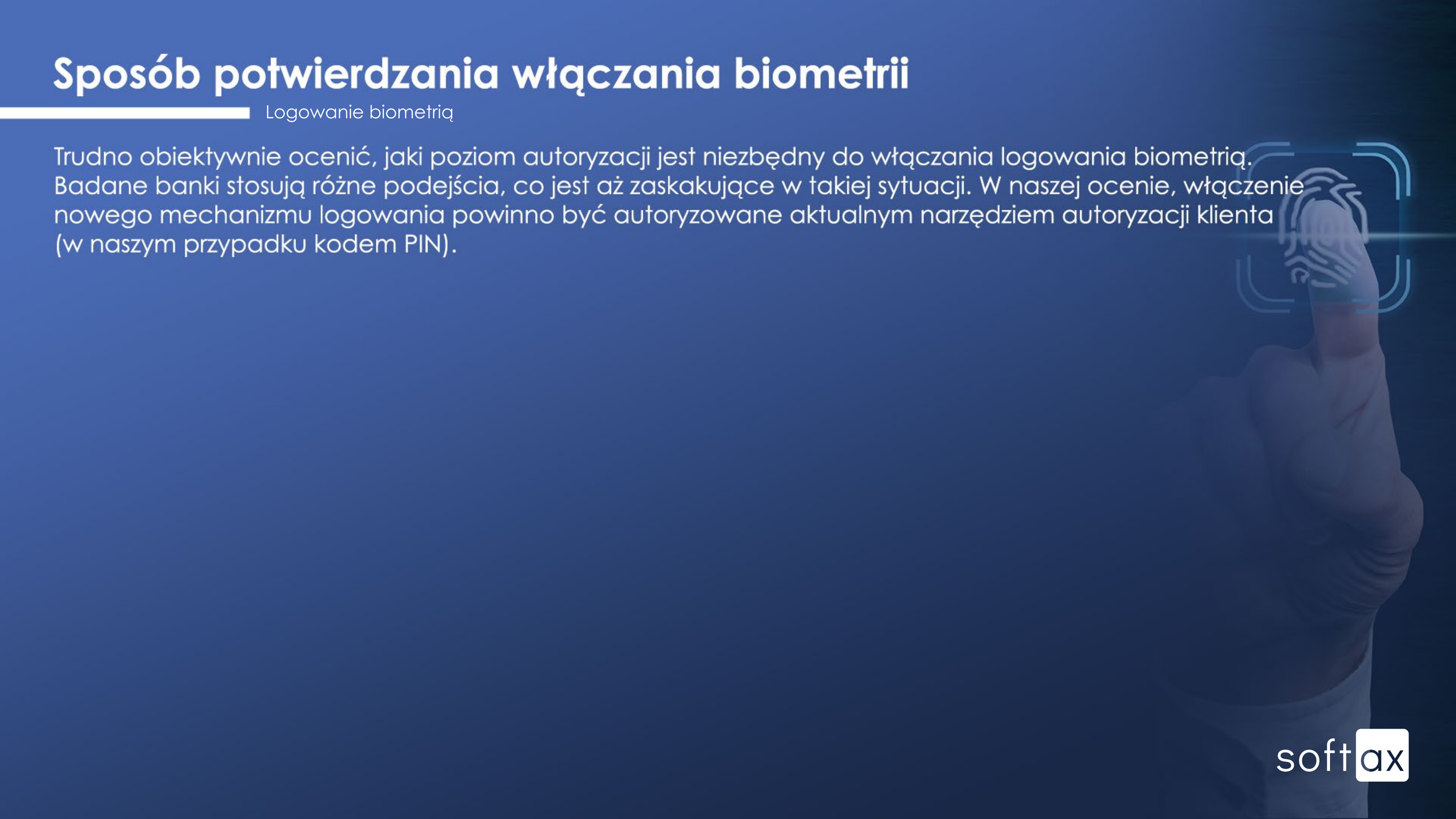


softax

Sposób potwierdzania włączania biometrii

Logowanie biometrią

Trudno obiektywnie ocenić, jaki poziom autoryzacji jest niezbędny do włączania logowania biometrią. Badane banki stosują różne podejścia, co jest aż zaskakujące w takiej sytuacji. W naszej ocenie, włączenie nowego mechanizmu logowania powinno być autoryzowane aktualnym narzędziem autoryzacji klienta (w naszym przypadku kodem PIN).



Włączanie biometrii

Logowanie biometrią

Aplikacje, które wymagają podania kodu PIN i odcisku palca

Aplikacje, które wymagają jedynie kodu PIN

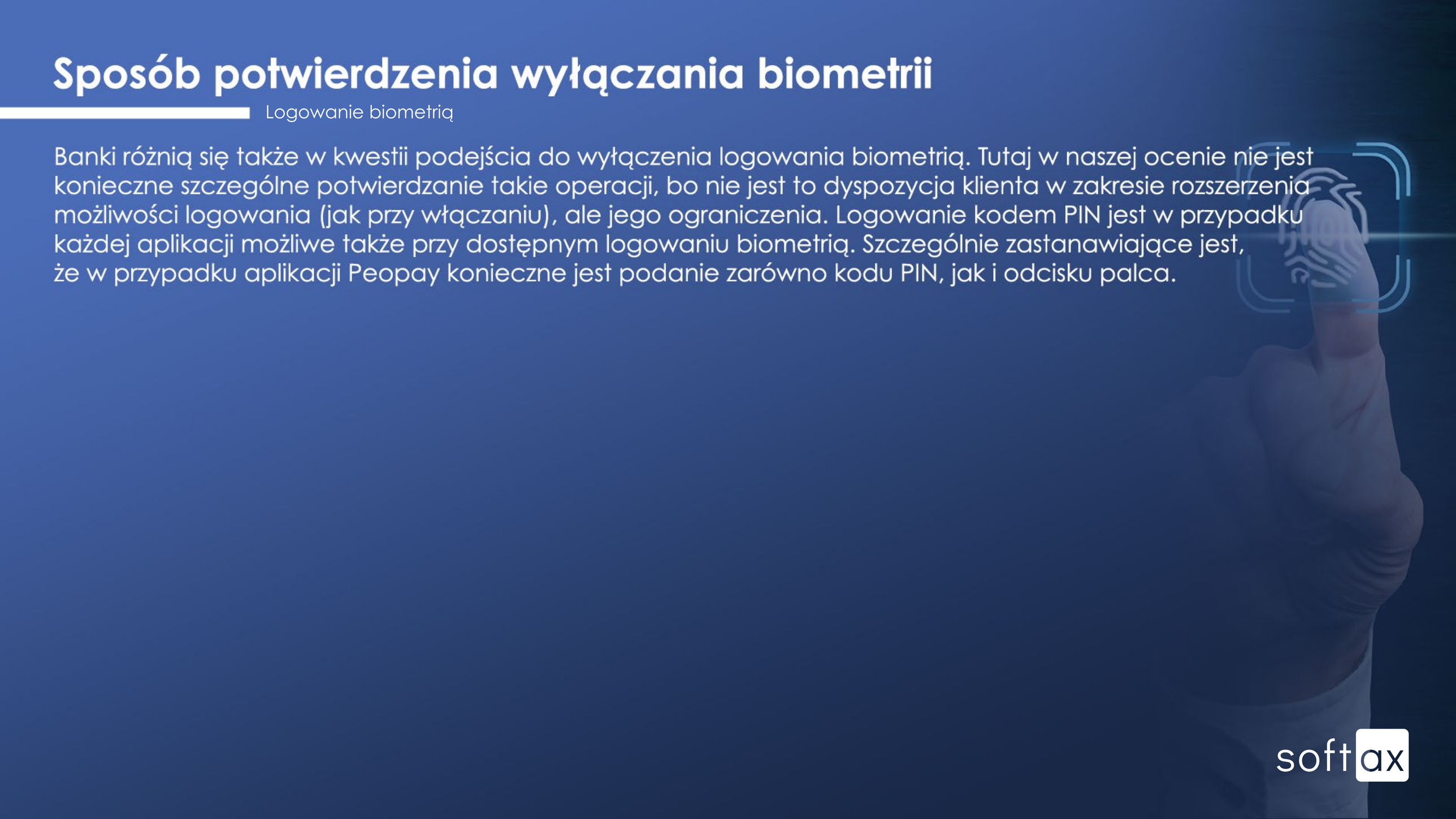
Aplikacje, które wymagają jedynie odcisku palca

softax

Sposób potwierdzenia wyłączania biometrii

Logowanie biometrią

Banki różnią się także w kwestii podejścia do wyłączenia logowania biometrią. Tutaj w naszej ocenie nie jest konieczne szczególne potwierdzanie takie operacji, bo nie jest to dyspozycja klienta w zakresie rozszerzenia możliwości logowania (jak przy włączaniu), ale jego ograniczenia. Logowanie kodem PIN jest w przypadku każdej aplikacji możliwe także przy dostępnym logowaniu biometrią. Szczególnie zastanawiające jest, że w przypadku aplikacji Peopay konieczne jest podanie zarówno kodu PIN, jak i odcisku palca.



Wyłączanie biometrii

Logowanie biometrią

Aplikacje, które nie wymagają dodatkowej autoryzacji

ING

mBank

Millennium bank

BNP PARIBAS

Santander

Aplikacje, które wymagają jedynie kodu PIN

ALIOR BANK

Bank Polski

Aplikacje, które wymagają podania kodu PIN i odcisku palca

Bank Pekao

softax

Czy jest możliwość logowania biometrią od razu po włączeniu aplikacji

Logowanie biometrią

Jeśli włączamy aplikację, by wykonać jakąś akcję wymagającą zalogowania, to chcemy to logowanie przejść jak najszybciej. Dlatego bardzo dobrą opcją jest możliwość włączenia logowania biometrią od razu na stronie startowej aplikacji.

softax

Czy jest możliwość logowania biometrią od razu po włączeniu aplikacji

Logowanie biometrią

Aplikacje pozwalające na włączenie logowania biometrią na ekranie startowym

Bank Polski

mBank

Millennium bank

Santander

Aplikacje, które takiej możliwości nie oferują

ALIOR BANK

ING

BNP PARIBAS

Bank Pekao

softax

Zakres obsługiwanej biometrii

Logowanie biometrią

Standardowym rodzajem biometrii dla systemu Android jest odcisk palca. Czytniki są umieszczane z przodu (na dole), na plecach lub z boku urządzenia a także w ekranie. Inne mechanizmy autoryzacji biometrycznej są rzadziej spotykane, jednak istnieją. Istotne jest jednak by miały odpowiednio wysoki poziom zabezpieczeń. Za taki nie uważa się prostego rozpoznawania twarzy z użyciem zwykłego aparatu. Za odpowiednio bezpieczny można uznać skan tęczówki oka, a także przestrzenną weryfikację twarzy (3D). Tego typu mechanizmy w środowisku Android mają jednak bardzo nieliczne telefony.

Wsparcie aplikacji bankowych, które są dedykowane na system Android w zakresie zastosowania innej biometrii niż odcisk palca jest niezadowalające. Według oficjalnych deklaracji, jedynie aplikacja mBank umożliwia wykorzystanie tęczówki oka i skanu twarzy 3D.

Z naszych testów wynika jednak, że aplikacje IKO (PKOBP), Peopay (Pekao SA) i ING Banku także pozwalają na wykorzystanie tych typów biometrii w telefonie (jednak bez dedykowanych tekstów informacyjnych). Jest to możliwe dzięki wykorzystaniu standardowych API systemu Android (gdzie z różnych rodzajów biometrii korzysta się w ten sam sposób od wersji 9.0) i braku kontroli faktycznego rodzaju stosowanej biometrii.

softax

Wsparcie dla skanu twarzy 3D i tęczówki oka w systemie Android

Logowanie biometrią

Oficjalne wsparcie

mBank

Brak oficjalnego wsparcia, ale działa

ING

PKO Bank Polski

Bank Pekao

Nie jest dostępne

ALIOR BANK

BNP PARIBAS

Santander

Millennium bank

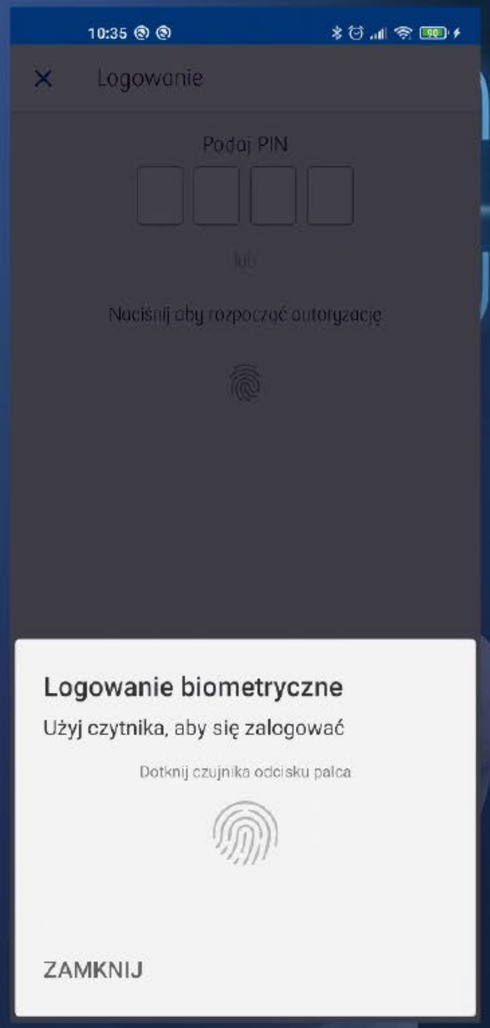
softax

Wizualizacja logowania biometrią

Logowanie biometrią

Klient nie powinien się zastanawiać. Logowanie biometrią (za pomocą odcisku palca) wydaje się bardzo proste i wygodne. Niestety także i tutaj pojawiły się kłopoty w aplikacjach. Związane najprawdopodobniej z rodzajem wykorzystywanego API Android i faktycznym dostosowaniem interfejsu.

Zgodnie z zaleceniami od wersji Android 9.0 powinno się korzystać z dedykowanego systemowego, wyjeżdżającego z dołu panelu logowania biometrią (który może wyglądać delikatnie inaczej w zależności od producenta telefonu). Stosowanie własnych rozwiązań w tej kwestii może powodować problemy, zwłaszcza w przypadku nowych telefonów z czytnikiem odcisku palca wbudowanym w ekran. Poprawny i zalecany sposób wizualizacji stosują: IKO, mBank, ING, PeoPay. Jak to powinno wyglądać pokazuje przykład IKO (PKOBP).



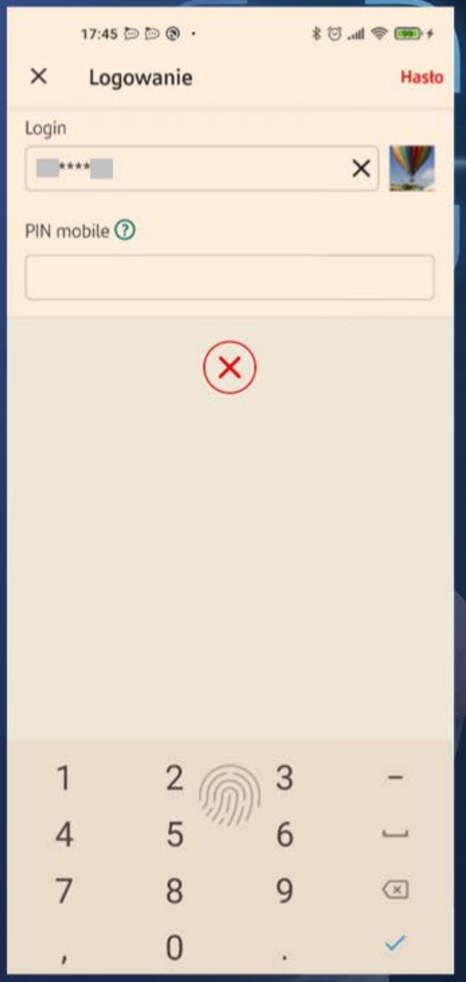
softax

Wizualizacja logowania biometrią

Logowanie biometrią

Aplikacja Santander ma nawet dwa problemy. Pierwszy polega na tym, że przedwcześnie uruchamia weryfikację odcisku palca – od razu po włączeniu aplikacji, nie czekając na przyłożenie palca do czytnika. To oczywiście się nie udaje i wita nas na starcie czerwony krzyżyk.

Druga sprawa w przypadku czytników w ekranie, kiedy czytnik jest aktywny pojawia się ikona, gdzie przyłożyć palec. Niestety zasłania ona inne wizualne elementy na ekranie i wprowadza konfuzję. Co prawda działa, ale właśnie burzy spokój w korzystaniu z aplikacji.

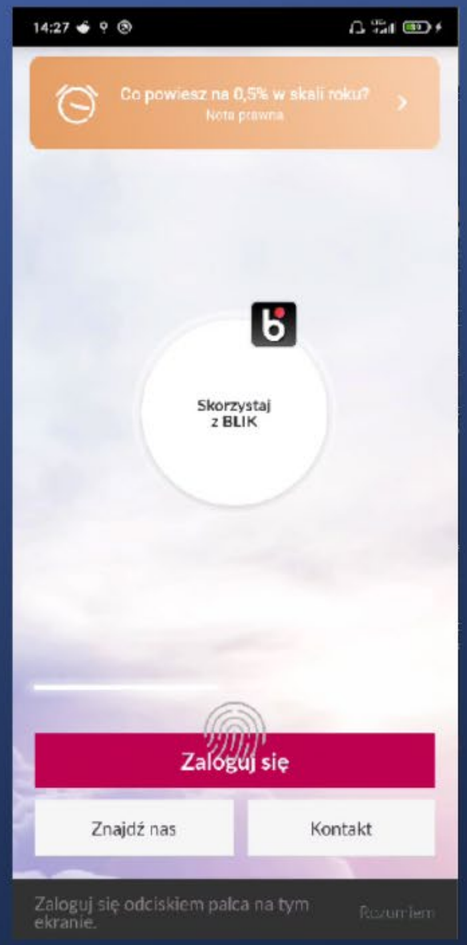


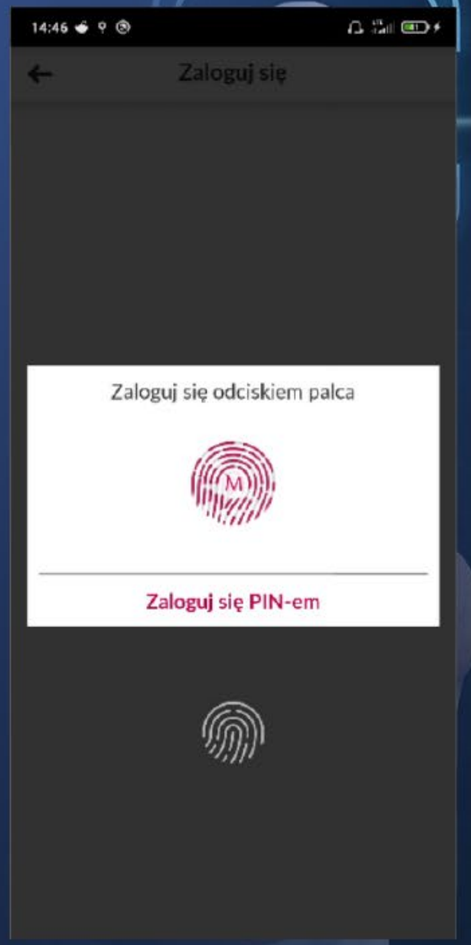
softax

Wizualizacja logowania biometrią

Logowanie biometrią

W aplikacji banku Millennium mamy możliwość logowania się od razu na ekranie startowym lub na dedykowanym.
W przypadku telefonów z czytnikiem odcisku palca w ekranie także tutaj wizualizacja czytnika nakłada się na elementy ekranowe, a to wprowadza niepokój. Klient nie ma pewności, że robi wszystko tak jak powinien.



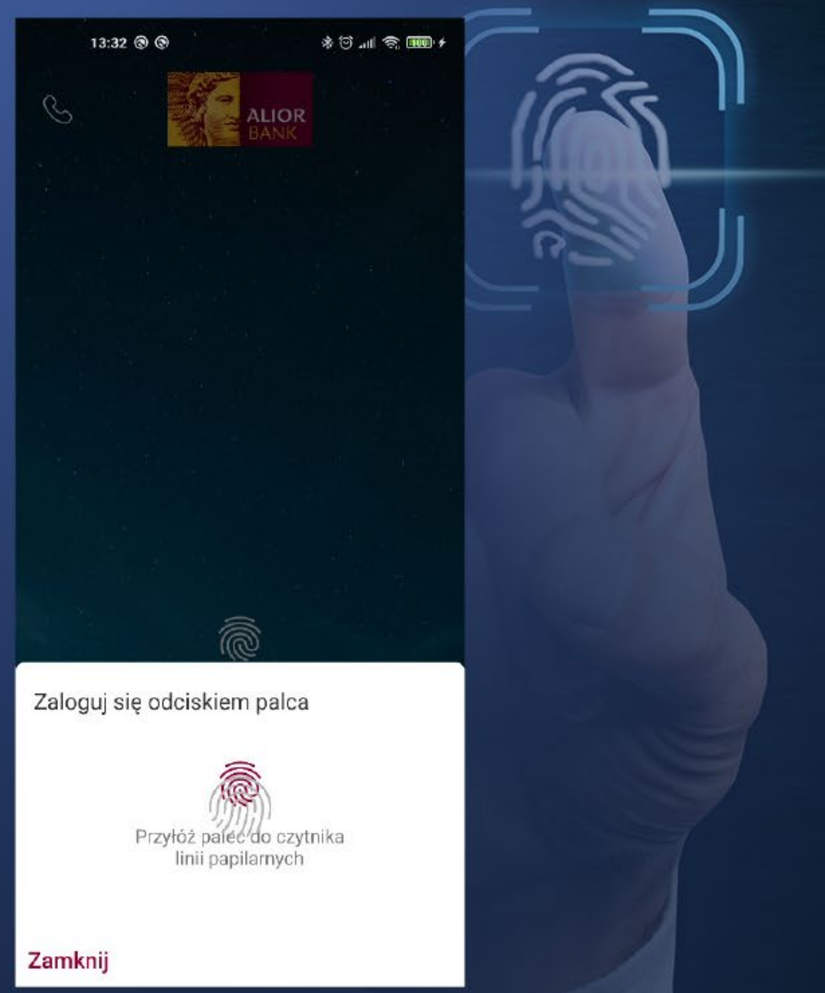


softax

Wizualizacja logowania biometrią

Logowanie biometrią

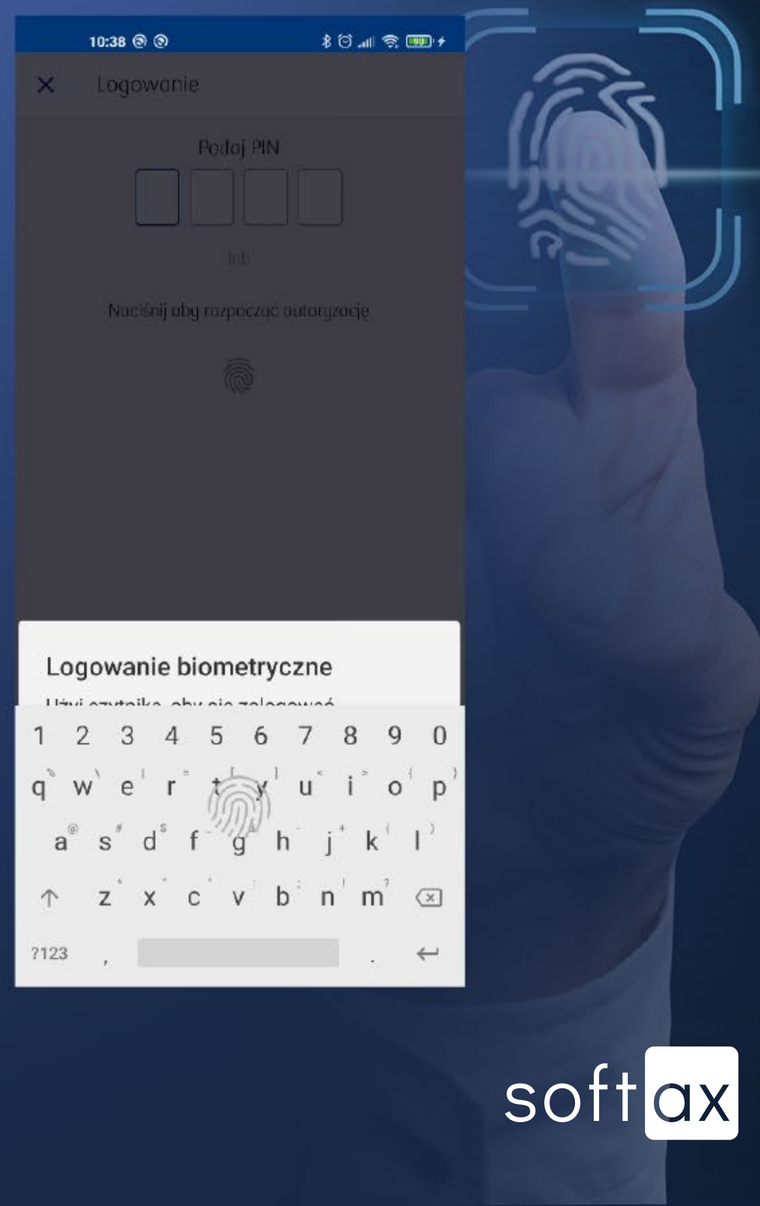
Aplikacja Alior Banku ma na tym tle tylko drobne problemy – ikonki się częściowo nakładają. Ale w sumie mamy trzy ikonki odcisku palca (jedna w tle). To także nie jest najlepsze rozwiązanie.



Wizualizacja logowania biometrią

Logowanie biometrią

W specyficznej sytuacji, także aplikacja IKO (PKO BP) ma problemy – nie w prostym scenariuszu, ale w przypadku przełączania się między logowaniem kodem PIN i biometrią. Ale jednak. To pokazuje jak istotne są testy tej funkcjonalności na różnych rodzajach urządzeń i w różnych scenariuszach.

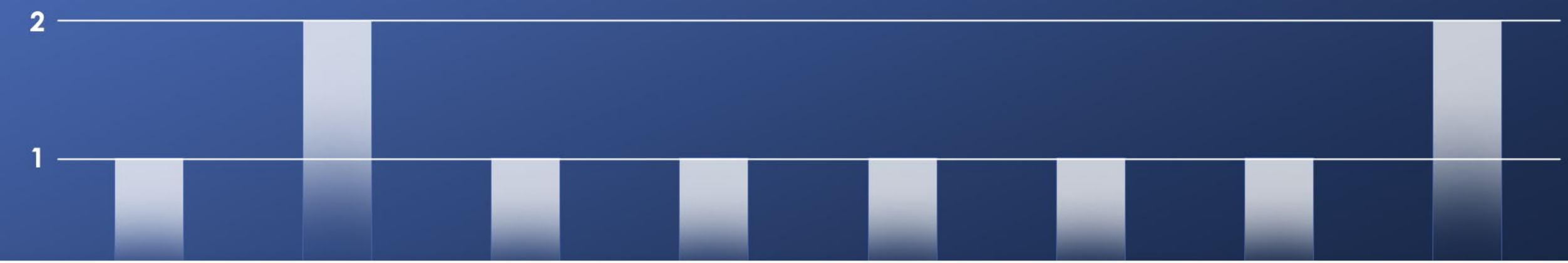


softax

Szybkość i wygoda logowania - Liczba tapnięć

Z perspektywy wygody korzystania z logowania im mniej jest wymaganych tapnięć tym lepiej.
Jak to zatem wygląda w różnych bankach.

Liczba tapnięć wymaganych do zalogowania kodem PIN
(nie licząc wprowadzania samego kodu)



ALIOR BANK
BNP PARIBAS
ING
mBank
Millennium bank
Bank Polski
Bank Pekao
Santander

softax

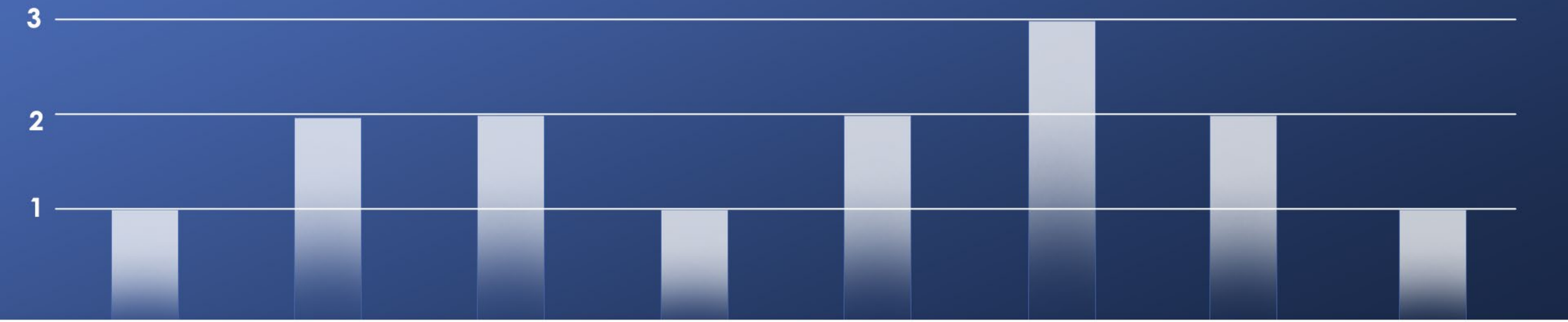
Szybkość i wygoda logowania - Liczba tapnięć

Liczba tapnięć przy logowaniu biometrią (nie licząc weryfikacji biometrii)

softax

Szybkość i wygoda logowania - Liczba tapnięć

Przejście do logowania PIN przy włączonym logowaniu biometrią



ALIOR BANK | BNP PARIBAS | ING | mBank | Millennium bank | Bank Polski | Bank Pekao | Santander

Jeśli chodzi o czas logowania to trudno powiedzieć o istotnych różnicach. Wszystkie badane aplikacje można było uznać za szybkie w działaniu. Cały proces logowania, oczywiście kiedy wymagał większej liczby tapnięć był oczywiście nieco dłuższy, ale nadal były to czasy bardzo krótkie.

softax

Podsumowanie logowania

Wszystkie badane instytucje dają możliwość logowania się zarówno kodem PIN, jak i biometrią. Kod PIN jest wciąż nieodzowny, nawet przy włączonej biometrii czasem może być wymagane logowanie PIN-em (np. po zmianie/dodaniu odcisku palca na telefonie). Także w niektórych sytuacjach klienci mogą nie mieć możliwości skorzystania z biometrii (mają np. założone rękawiczki). Dlatego istotne jest, by proces logowania kodem PIN był jak najprostszy.

Polecamy zatem wizualizację ułatwiającą ocenę liczby wprowadzanych znaków w kodzie, a także zachęcamy do przedstawienia klientowi liczby cyfr, które musi wprowadzić. Przy takim podejściu możliwe jest też automatyczne rozpoczęcie logowania po wprowadzeniu wszystkich cyfr z kodu.

Aplikacje powinny także prezentować dedykowane informacje w przypadku problemów klienta, gdy zrobi on błąd w kodzie PIN lub nie pamięta hasła.

Z perspektywy bezpieczeństwa polecamy też stosowanie specjalizowanej klawiatury (zamiast systemowej) dla wprowadzania tak wrażliwej danej jak kod PIN klienta.

Logowanie biometrią jest dostępne we wszystkich bankach, ale nie wszędzie można włączyć możliwość logowania biometrią od razu na ekranie startowym. Zachęcamy, by taką opcję klientom udostępnić. Wybór dostępnej metody logowania (kodem PIN lub biometrią) powinien być w każdym wypadku jasny i łatwo dostępny.

softax

Informacje o koncie przed logowaniem

Dostęp do informacji o koncie

Informacje przed zalogowaniem

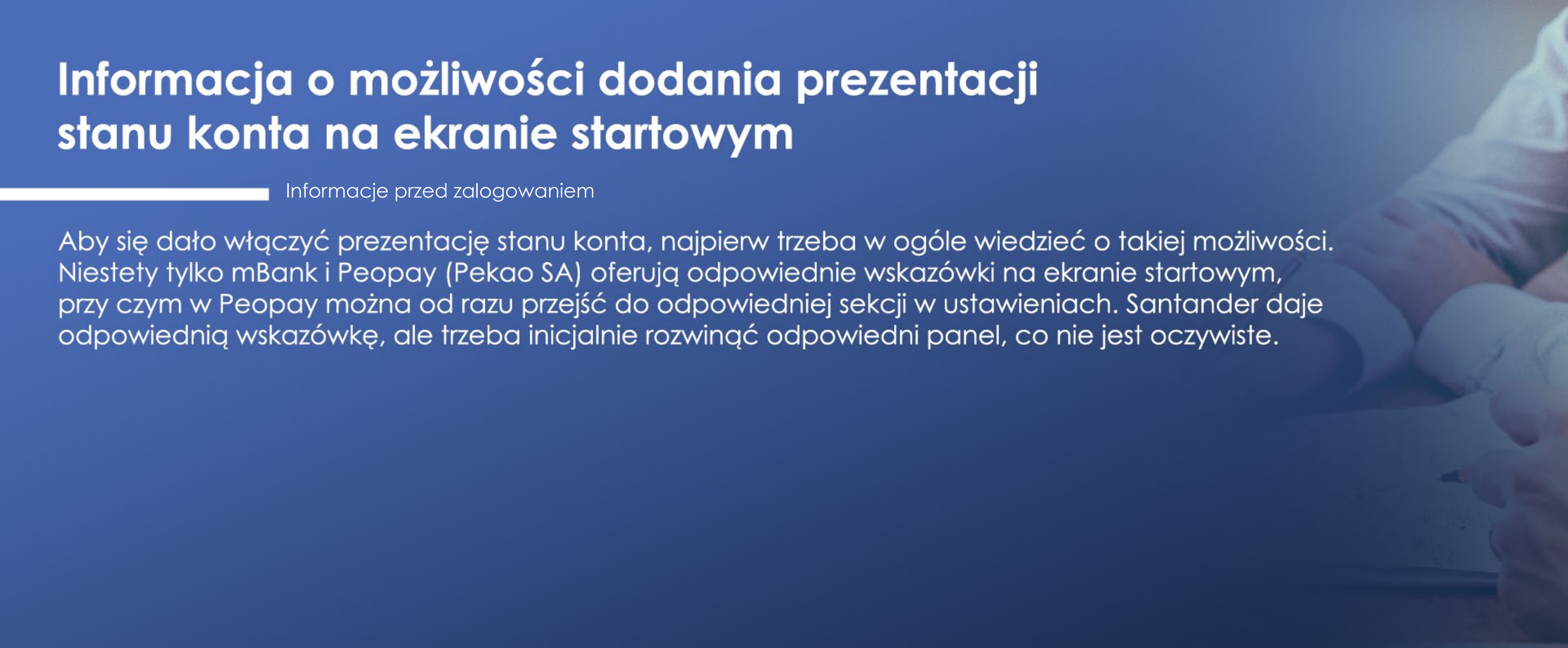
Drugą częścią naszej bieżącej analizy były kwestie związane z prezentacją danych o stanie konta klienta bez konieczności logowania. Wszystkie badane instytucje dały taką możliwość w swoich aplikacjach. I chociaż logowanie biometrią jest bardzo szybkie, niektórzy klienci mogą preferować dostęp do najbardziej podstawowej informacji bez konieczności przejścia procesu logowania.

softax

Informacja o możliwości dodania prezentacji stanu konta na ekranie startowym

Informacje przed zalogowaniem

Aby się dało włączyć prezentację stanu konta, najpierw trzeba w ogóle wiedzieć o takiej możliwości. Niestety tylko mBank i Peopay (Pekao SA) oferują odpowiednie wskazówki na ekranie startowym, przy czym w Peopay można od razu przejść do odpowiedniej sekcji w ustawieniach. Santander daje odpowiednią wskazówkę, ale trzeba inicjalnie rozwinąć odpowiedni panel, co nie jest oczywiste.



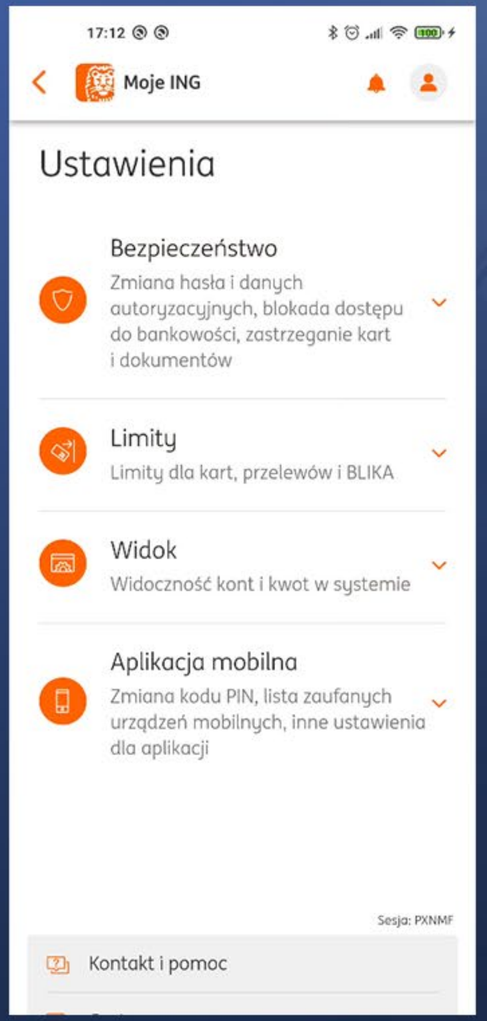
softax

Dostęp do konfiguracji prezentacji stanu konta w ustawieniach

Informacje przed zalogowaniem

Przyjmijmy, że wiemy jednak o możliwości konfiguracji prezentacji stanu konta przez logowaniem. I szukamy takiej opcji w ustawieniach. Okazuje się, że w przypadku aplikacji ING Banku takiej opcji nie znajdziemy. Ustawienie prezentacji stanu konta jest dostępne tylko z ustawień odpowiedniego widżetu dostępnego na stronie startowej.

Jest to podejście ograniczające tzw. discoverability. Zalecamy jednak by takie opcje w ogólnych ustawieniach umieszczać. Dodatkowo można do tej opcji przejść z ekranu startowego. Jest to wygodne, ale nie powinna to być jedyna możliwość, a uzupełnienie standardowego miejsca w ustawieniach aplikacji (takie podejście stosują PeoPay, Santander i Millennium).



softax

Podgląd prezentacji stanu konta na ekranie ustawień

Informacje przed zalogowaniem

Wszystkie banki oferują podgląd stanu konta przed zalogowaniem. I to w dwóch formach – jako konkretna kwota i w wariancie procentowym, gdzie użytkownik określa wartość 100%. To drugie podejście pozwala na ukrycie przed postronnymi faktycznej wartości salda rachunku, ale pozostaje zrozumiałe dla osoby włączającej to ustawienie. Klienci mogą wybrać, które podejście bardziej im odpowiada, a w przypadku BNP Paribas mogą także wybrać prezentację jednocześnie obu opcji.

Prezentacja salda przed logowaniem

Informacje przed zalogowaniem

Różnice pojawiają się w podejściu do tego, jakie salda i ilu rachunków można podejrzeć. Część aplikacji oferuje podgląd kilku rachunków (ING Bank, Santander, Millennium), pozostałe tylko jednego wybranego rachunku. Dodatkowo część aplikacji oferuje podgląd stanu karty kredytowej (mBank, ING Bank).
Najbardziej rozbudowane podejście stosuje tutaj chyba ING Bank.

softax

Jak działa limit procentowy (czy może być więcej niż 100%)?

Informacje przed zalogowaniem

Tak, jak wspomnieliśmy, saldo może być pokazywane w postaci procentowej z ustawianą przez klienta wartością 100%. Okazuje się, jednak, że jest tutaj spora rozbieżność między aplikacjami. Część banków przyjmuje, że stan konta wartości 100% przekroczyć nie może (czyli, że maksymalny stan konta to 100%). Druga część pozwala na przekroczenie 100%, czyli np. dla stanu konta 1400 zł, i limitowi 100% ustawionemu na 100zł zostanie zaprezentowana wartość 1400%. W takim przypadku uzyskujemy więcej informacji, ale też bardziej odkrywamy wrażliwe dane.

Oczywiście to klient włącza samodzielnie taką funkcjonalność w ustawieniach, nie ma jednak wyboru, z której opcji chce skorzystać. Sytuację pogarsza fakt, że część banków nie daje żadnych wskazówek, które z tych podejść zostanie zastosowane. Konieczne jest zazwyczaj eksperymentowanie przez klienta.

Nasza rekomendacja w związku z powyższym – wprowadzenie na ekranie ustawień jasnej informacji mówiącej o przyjętej strategii odnośnie interpretacji wartości 100%.

softax

Jak działa limit procentowy (czy może być więcej niż 100%)?

Informacje przed zalogowaniem

Aplikacje, które nie pokazują więcej niż 100% jako procentowy stan konta

ING

mBank

ALIOR BANK

BNP PARIBAS

Bank Pekao

Aplikacje, które nie stosują takiego limitu

Millennium bank

PKO Bank Polski

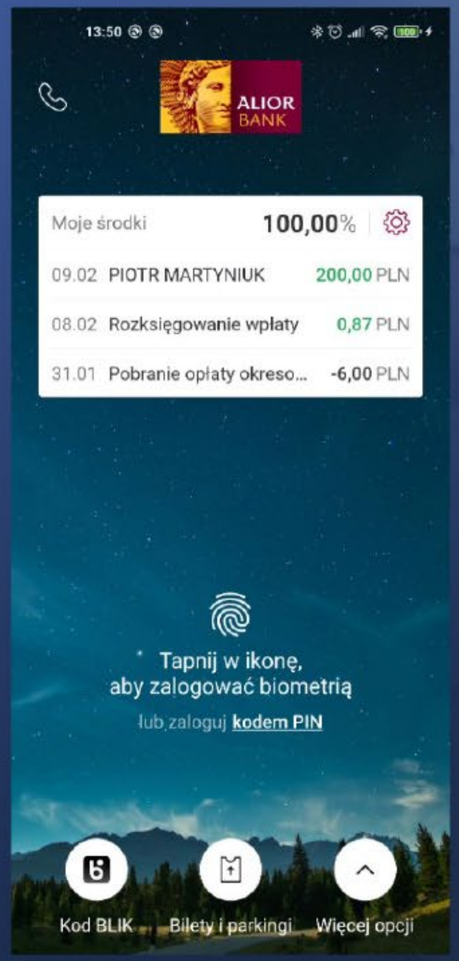
Santander

softax

Prezentacja ostatnich transakcji przed logowaniem

Informacje przed zalogowaniem

Oprócz samego salda wybranych rachunków część banków pozwala także na prezentację ostatnich transakcji przed logowaniem. Najlepsze rozwiązane w tym zakresie oferuje aplikacja Alior Banku, gdzie możliwe jest (konfigurowalne niezależnie od salda rachunku) włączenie prezentacji ostatnich 3 transakcji, dla których dostępne są najważniejsze dane: data transakcji, kontrahent (lub typ operacji) i kwota.



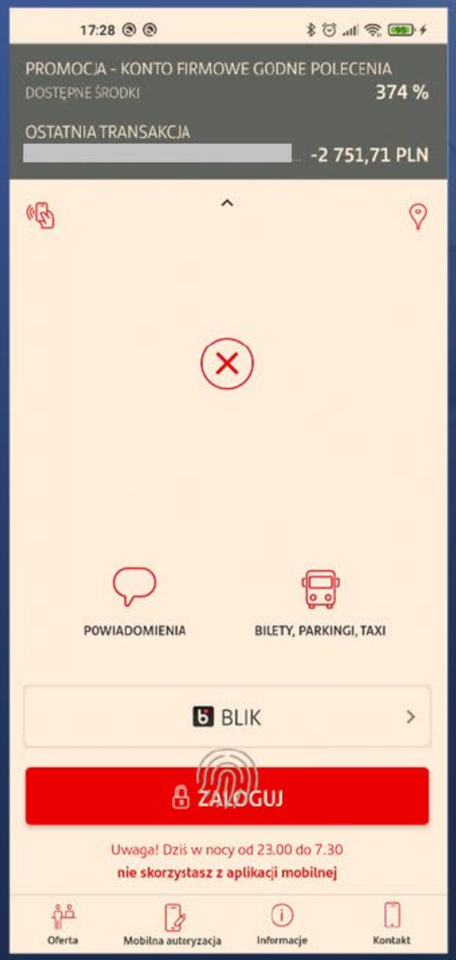
softax

Prezentacja ostatnich transakcji przed logowaniem

Informacje przed zalogowaniem

Santander Bank oferuje prezentację danych ostatniej transakcji. Ta funkcjonalność jest włączana razem z prezentacją salda i nie da się oddzielnie konfigurować. Także, jeśli chodzi o prezentowane dane nie jest idealnie – prezentowany jest tylko tytuł operacji i kwota, brak daty i kontrahenta transakcji.

Pozostałe aplikacje nie dają możliwości podglądu ostatnich transakcji. Czy taka funkcjonalność jest potrzebna? Trudno jednoznacznie odpowiedzieć. W dobie powszechnego logowania biometrią z jednej strony łatwo się zalogować i zobaczyć pełną historię. Z drugiej strony jest to opcja włączana przez klienta i może dla części użytkowników być bardzo wygodna.

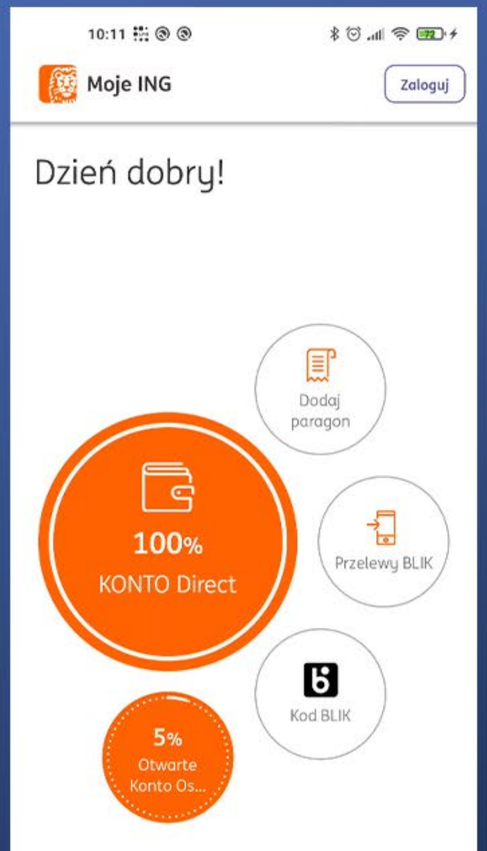


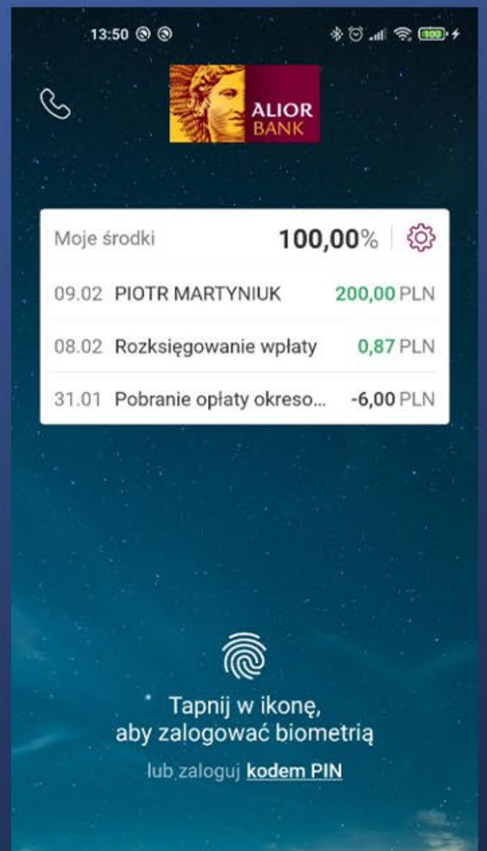
softax

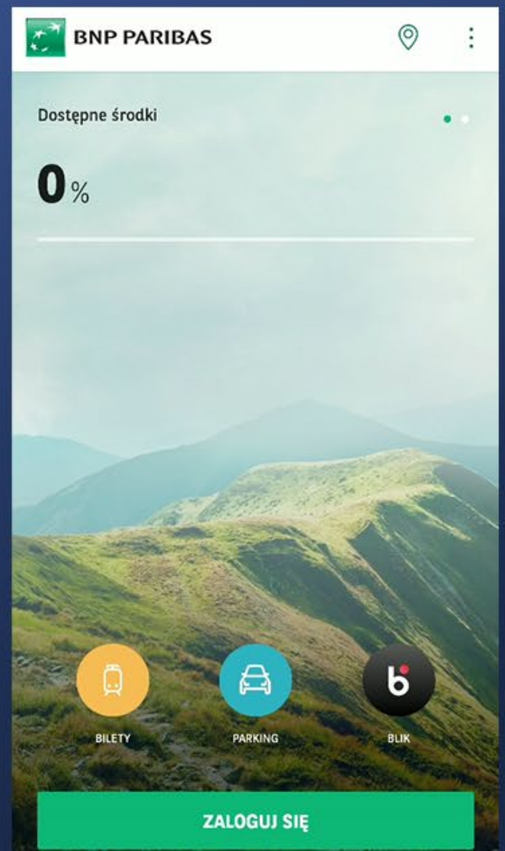
Sposób prezentacji stanu konta na ekranie startowym

Informacje przed zalogowaniem

Po włączeniu prezentacji stanu konta nie wszędzie taka prezentacja jest od razu widoczna na ekranie startowym. Banki różnią się tutaj mocno podejściem. Część z nich prezentuje podgląd od razu, część wymaga akcji klienta – tapniecia czy rozwinięcia odpowiedniej opcji by taki podgląd zobaczyć.
Najprościej więc stan rachunku zobaczyć w aplikacji ING Banku, Alior Banku i w aplikacji BNP Paribas, które prezentują stan konta od razu na ekranie startowym.





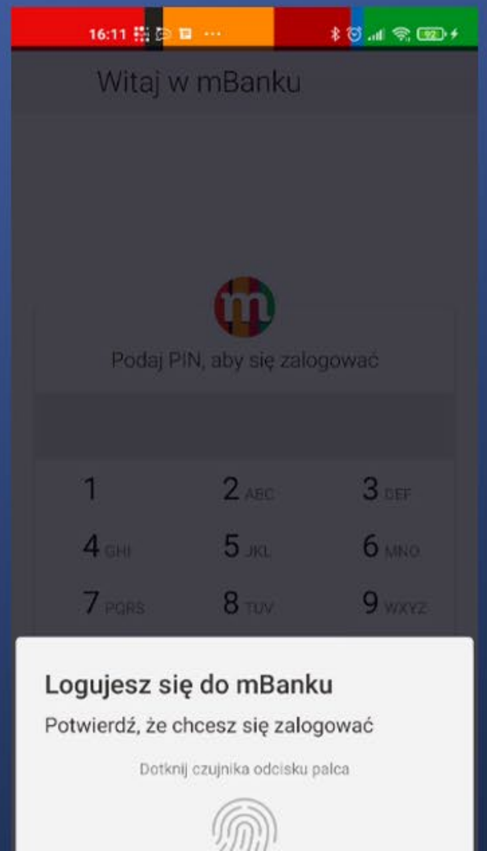


softax

Sposób prezentacji stanu konta na ekranie startowym

Informacje przed zalogowaniem

W przypadku aplikacji mBanku jest pewne potknięcie. Aplikacja ta także prezentuje podgląd stanu konta od razu, ale posiada także przydatną możliwość automatycznego uruchomienia na ekranie startowym logowania biometrią. Niestety zasłania ona całkowicie podgląd stanu konta.
W przypadku pozostałych aplikacji podgląd jest dostępny po wykonaniu odpowiedniej akcji.
W przypadku Peopay jest to opcja bardzo dobrze widoczna (Pokaż saldo).

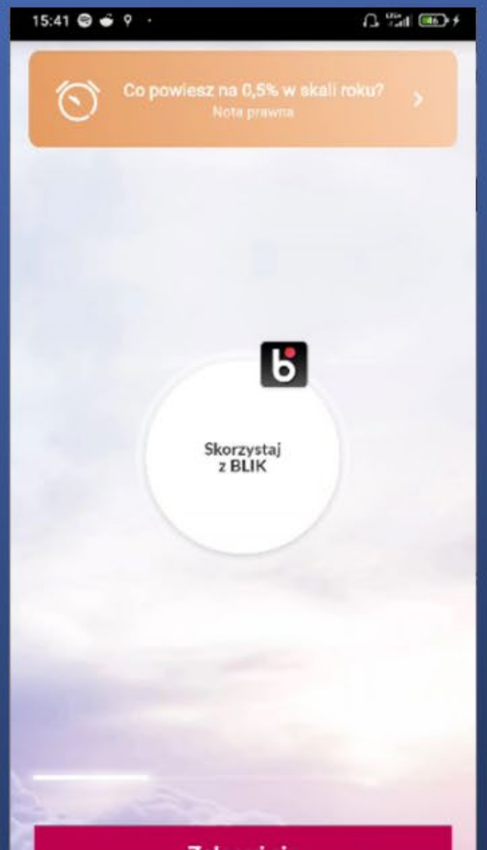


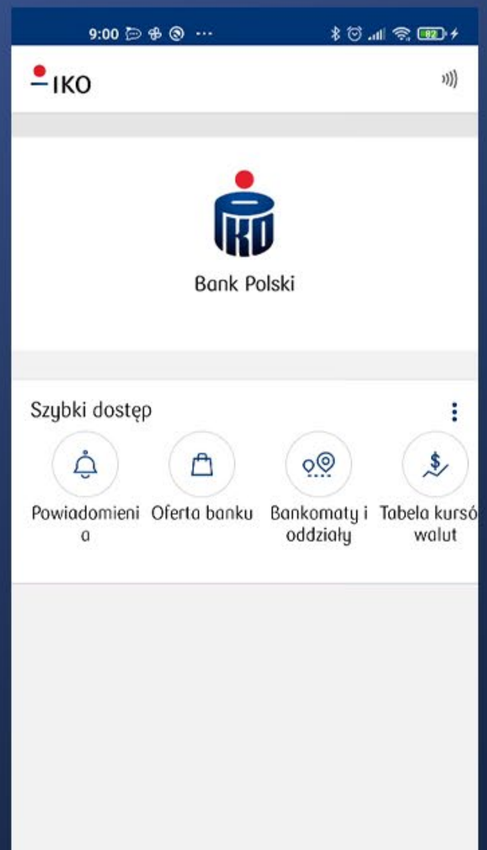
softax

Sposób prezentacji stanu konta na ekranie startowym

Informacje przed zalogowaniem

W przypadku pozostałych są tylko bardzo dyskretne i nie do końca intuicyjne wskazówki (mały znaczek rozwijania na górze w przypadku Santander czy słabo wyróżniony pasek przewijania nad przyciskiem Zaloguj jak w Millennium). Natomiast w przypadku IKO (PKO BP) konieczny jest gest pociągnięcia od góry, ale brak jest jakiekolwiek wskazówki wizualnej na ekranie startowym.





softax

Sposób prezentacji stanu konta na ekranie startowym

Informacje przed zalogowaniem

Aplikacje, które udostępniają podgląd bezpośrednio na ekranie startowym

ING

mBank

ALIOR BANK

BNP PARIBAS

Aplikacje, które wymagają interakcji do prezentacji podglądu

Millennium bank

PKO Bank Polski

Santander

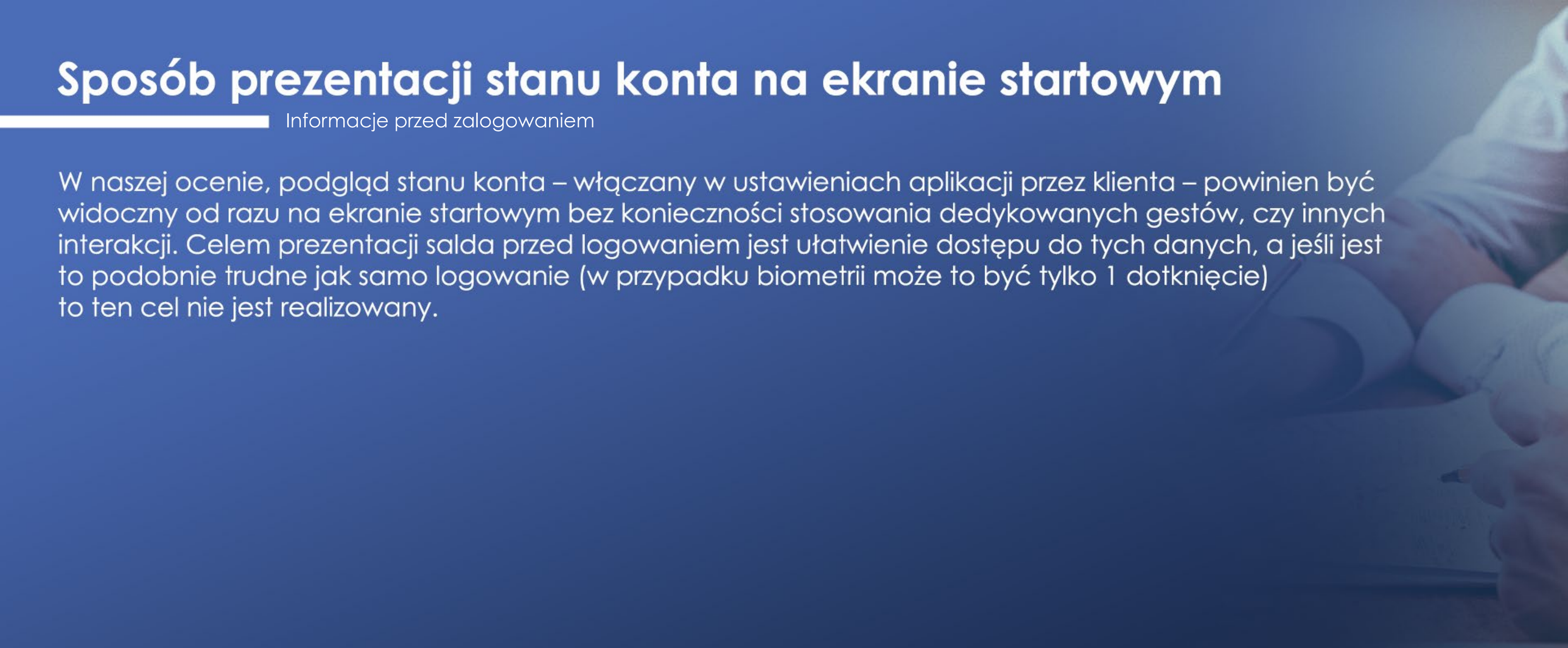
Bank Pekao

softax

Sposób prezentacji stanu konta na ekranie startowym

Informacje przed zalogowaniem

W naszej ocenie, podgląd stanu konta – włączany w ustawieniach aplikacji przez klienta – powinien być widoczny od razu na ekranie startowym bez konieczności stosowania dedykowanych gestów, czy innych interakcji. Celem prezentacji salda przed logowaniem jest ułatwienie dostępu do tych danych, a jeśli jest to podobnie trudne jak samo logowanie (w przypadku biometrii może to być tylko 1 dotknięcie) to ten cel nie jest realizowany.



softax

Podsumowanie informacji o koncie przed logowaniem

Przy zastosowaniu biometrii logowanie staje się tak szybkie, że wielu klientów może po prostu preferować zalogowanie i wygodny dostęp do pełnych danych o swoim koncie. W naszej ocenie jednak dostęp do informacji o stanie konta bez konieczności logowania może być dla części klientów przydatną funkcją. Warto jednak, by banki dawały do niej łatwy dostęp niezależnie od włączenia biometrii, czy ogólnie przede wszystkim bez utrudniania procesu logowania.

Dostęp do tej informacji jest w badanych aplikacjach konfigurowalny przez klienta – nie powinien być zatem w naszej opinii dodatkowo ukrywany – np. poprzez wymaganie wykonania dedykowanych gestów na stronie logowania.

Banki powinny także przekazywać jasne informacje odnośnie sposobu interpretacji kwoty 100% w przypadku pokazywania stanu środków na koncie w postaci procentowej. Obecnie stosowane są na rynku dwa różne podejścia w tym zakresie (kwota 100% jako pułap maksymalny lub po prostu jak wartość przeliczeniowa). Oba rozwiązania mają swoje zalety, istotne jest by informować klienta o sposobie działania tej opcji.

softax

Aplikacje bankowe

Analiza obszaru logowania

Dziękujemy

softax