

Bankier.pl

**Bezpieczeństwo
w bankowości internetowej
raport Bankier.pl**



październik 2009

Bezpieczeństwo w bankowości internetowej - Raport Bankier.pl



*Michał Macierzyński
analityk Bankier.pl*

Korzystanie z bankowości internetowej nieodmiennie wywoływało w potencjalnych klientach obawy związane z bezpieczeństwem. Podstawowe pytanie brzmiało i brzmi - czy moje pieniądze są odpowiednio zabezpieczone? Bankier.pl postanowił bliżej przyjrzeć się temu zagadnieniu by ostatecznie rozwiać wątpliwości, a jednocześnie sprawdzić, które banki proponują najlepsze zabezpieczenia chroniące skutecznie przed internetowymi złodziejami.

Raport Bankier.pl to dokładny przegląd stosowanych przez banki zabezpieczeń. Według przyjętej metodologii oceniliśmy wszystkie działające na polskim rynku banki komercyjne, a także pięć największych banków spółdzielczych i system udostępniony klientom SKOK. Badaliśmy przede wszystkim zabezpieczenie systemów transakcyjnych przed najpopularniejszymi metodami ataków – phishingu, atakiem man-in-the-middle, a także man-in-the-browser.

Z naszych analiz wynika, że obecnie najnowocześniejsze zabezpieczenia bankowości internetowej stosuje wrocławski Euro Bank. Drugie miejsce zajął BNP Paribas Fortis. Tuż za nim, na miejscu trzecim plasują się ex aequo Raiffeisen Bank Polska i BZ WBK, który na początku października wdrożył nowy system transakcyjny, z nowymi zabezpieczeniami. Te cztery banki mogą pochwalić się naszym zdaniem najlepiej zabezpieczonymi systemami bankowości internetowej dla klientów detalicznych.

Wstęp

Zdaniem Bankier.pl stosowane przez polskie banki zabezpieczenia kanału internetowego należą do jednych z najbardziej zaawansowanych i najnowocześniejszych na świecie. W efekcie można śmiało stwierdzić, że korzystanie z bankowości internetowej w Polsce jest bardzo bezpieczne. Znacznie bardziej niż chociażby w USA, Wielkiej Brytanii czy innych krajach. Dlaczego? Po części jest to efekt zapóźnienia rodzimego systemu bankowego. Dzięki temu w polskich bankach wdrażano od razu najnowocześniejsze rozwiązania, które nie musiały być zgodne z systemami z lat 80-tych. Chociaż początkowo nie było to być może rozsądne biznesowo, ale rodzime banki od razu postawiły na bezpieczeństwo wykonywanych transakcji. Co prawda utrudniło to na początku rozwój i podwyższało koszt wdrożenia i utrzymania systemów, ale ostatecznie okazało się, że dzięki temu uniknięto błędów popełnionych w innych krajach, które postawiły na łatwość korzystania, kosztem bezpieczeństwa.

Obecnie wszystkie polskie banki stosują dwustopniowy poziom zabezpieczeń – jeden do logowania do rachunku, drugi do potwierdzenia transakcji. Do najpopularniejszych sposobów autoryzacji należy zaliczyć hasła jednorazowe, hasła SMSowe, czy tokeny. Wszystkie te sposoby oferują bardzo silne zabezpieczenie. W praktyce od czasu do czasu okazuje się, że może to nie wystarczyć. Łańcuch bezpieczeństwa jest bowiem tak silny, jak jego najsłabsze ogniwo. W tym przypadku jest nim końcowy użytkownik. Większość zabezpieczeń staje się bezwartościowa, jeśli klient dobrowolnie przekazuje hasła złodziejowi lub niedostatecznie zadba o zabezpieczenie swojego komputera.

Banki próbują tej prostej zasadzie przeciwdziałać, ale każde zwiększenie bezpieczeństwa odbywa się kosztem wygody użytkownika, a przede wszystkim kolejnymi wydatkami,

które ostatecznie przerzucane są na klienta. Dlatego instytucje finansowe próbują wypośrodkować te dwa elementy – wygodę i bezpieczeństwo, chociaż mają świadomość, że przy obecnej masie klientów, zwykle prawdopodobieństwo sprawa, że może dojść do kradzieży hasła. W każdym takim przypadku jest to jednak wciąż atak na klienta, a nie na bank. Okradziony jest konkretny klient lub grupa klientów, a nie instytucja w wyniku swoich zaniedbań. Tak czy inaczej zarówno stosowane zabezpieczenia, procedury, jak i praktyka funkcjonowania, stawia zabezpieczenia wykorzystywane przez polskie banki na najwyższym światowym poziomie. Pod tym względem nasz kraj wyróżnia się na tle innych rynków.

Bankier.pl postanowił sprawdzić, w jaki sposób polskie banki chronią pieniądze swoich klientów. Z raportu wynika, że porównując nasze banki do tych zagranicznych, można śmiało orzec, że stosują najwyższe standardy bezpieczeństwa, ale także cały czas pracują nad ulepszeniem już istniejących zabezpieczeń. W kwestiach bezpieczeństwa, cały czas trwa nieustanny wyścig. Przestępcy doskonałą swój warsztat i obok tak powszechnych metod jak phishing, stosują coraz bardziej wyrafinowane sposoby kradzieży, którym czasami nie oprą się nawet najsilniejsze wydawałoby się zabezpieczenia. Oczywiście takie przypadki występują zazwyczaj tylko w teorii, ale światowa i niestety rodzima praktyka pokazuje, że w odpowiednich warunkach istnieje możliwość przekucia teorii w praktykę. Przestępcy coraz częściej znajdują sposoby na obejście mniej zaawansowanych zabezpieczeń. I chociaż w skali kilku milionów klientów problem jest praktycznie niezauważalny, to jednak może podważyć zaufanie nie tylko do konkretnego banku, czy sposobu autoryzacji transakcji, ale również do samej bankowości internetowej. Z tego też powodu banki coraz częściej zmieniają sposoby zabezpieczeń na lepsze, bardziej bezpieczne. Taki los na przykład spotyka obecnie hasła jednorazowe, które zamieniane są na hasła SMSowe. W przeszłości może się zdarzyć, że również one mogą zostać zamienione na kolejne. Wyścig nie ma bowiem jak na razie mety.

Ranking - punktacja

Miejsce	Nazwa banku	Suma Punktów
1	Euro Bank S.A.	33,5
2	BNP Paribas Fortis S.A.	29
3	Raiffeisen Bank Polska S.A.	28,5
3	Bank Zachodni WBK S.A.	28,5
4	Alior Bank S.A.	26
5	Millennium Bank S.A.	25,5
5	Konto Xelion	25,5
5	Bank Pekao S.A.	25,5
6	MultiBank (BRE Bank S.A.)	25
6	mBank (BRE Bank S.A.)	25
6	Krakowski Bank Spółdzielczy	25
6	ING Bank Śląski S.A.	25
6	Bank Ochrony Środowiska S.A.	25
6	Bank Handlowy w Warszawie S.A.	25
6	Allianz Bank S.A.	25
7	Nordea Bank Polska S.A.	24
8	Bank BPH S.A.	21
9	Bank Gospodarki Żywnościowej S.A.	20,5
10	Volkswagen Bank Polska S.A.	18
10	Toyota Bank Polska S.A.	18
10	Podkarpacki Bank Spółdzielczy w Sanoku	18
10	Lukas Bank S.A.	18
10	Gospodarczy Bank Wielkopolski	18
10	Bank Polskiej Spółdzielczości	18
11	HSBC Polska S.A.	17
12	Polbank EFG (Euro Bank Ergasis S.A.)	16
12	Kredyt Bank S.A.	16
12	Invest-Bank S.A.	16
13	Mazowiecki Bank Regionalny w Warszawie	12
14	PKO BP S.A.	7
14	Inteligo (PKO Bank Polski S.A.)	7
14	Getin Bank S.A.	7
14	eskok.pl	7
14	DnB NORD Polska S.A.	7
14	Deutsche Bank PBC S.A.	7
14	Bank Pocztowy S.A.	7

Metodologia raportu

W poniższych punktach opisana została metodologia wykorzystana przy opracowywaniu naszego raportu:

➔ Pod uwagę zostały wzięte zabezpieczenia wykorzystane wyłącznie przy kontaktach dla klientów indywidualnych;

➔ Analizie poddane zostały wszystkie banki komercyjne oraz pięć największych banków spółdzielczych i system dostępny dla klientów SKOK-ów;

➔ Do rankingu brane były pełne, występujące w danym banku metody zabezpieczeń, często stanowiące kompozycję kilku mechanizmów np. hasło statyczne wsparte dodatkowym identyfikatorem lub token sprzętowy wsparty PINem oraz hasłem statycznym.

➔ Analizowano tylko najlepsze metody zabezpieczeń dostępne w danym banku i możliwe do wykorzystania zarówno przy logowaniu jak i potwierdzaniu transakcji, np. mBank proponuje karty kodów jednorazowych lub hasła SMS, więc w rankingu brane są pod uwagę tylko hasła wysyłane w wiadomościach SMS. W przypadku Euro Banku gdzie można wybrać token sprzętowy lub aplikację na telefon, ocenie poddano tylko aplikację na telefon, zarówno do logowania jak i potwierdzania transakcji – aplikacja jest bezpieczniejsza od tokenów w zakresie autoryzacji transakcji co jednocześnie determinuje jej wykorzystanie podczas logowania);

➔ Badano metody zabezpieczające proces logowania oraz proces autoryzacji transakcji aktywnych;

➔ Każda z metod uzyskała odpowiednią liczbę punktów w skali od 1 do 10.

➔ Punktacja zależała przede wszystkim od ochrony przed najpopularniejszymi obecnie atakami czyli przed:

➤ atakiem phishingowym, czyli zorganizowanym atakiem polegającym na wyciągnięciu od wielu użytkowników haseł i możliwość wykorzystania ich w przyszłości. Najczęściej atak wygląda tak, że nieświadomy użytkownik dostaje maila, z prośbą o wejście na stronę swojego banku, na której będzie zobowiązany do reaktywacji konta np. po ostatnio wykonanej aktualizacji oprogramowania banku. Nieświadomy użytkownik wchodzi na podstawioną stronę gdzie proszony jest np. o podanie swoich haseł jednorazowych, lub wręcz przepisanie całej zawartości karty z hasłami. Najczęściej łatwo zauważyć, że to jest atak ponieważ adres strony nie jest zgodny ze znanym nam adresem banku. Zdarzają się jednak ataki bardziej skomplikowane, które swym zasięgiem obejmują również serwery DNS (tzw. pharming) lub modyfikują pliki systemowe tak, że faktyczne wpisanie do przeglądarki poprawnego adresu skutkuje wejściem na stronę „podstawioną”. Taki atak jest już trudniejszy do wykrycia, ale świadomy użytkownik powinien zobaczyć niezgodności w certyfikacie.

➤ atakiem man-in-the-middle. Atak ten jest atakiem aktywnym tj. w pierwszym kroku następuje przejście

sesji użytkownika (podczas próby połączenia ze stroną banku) lub też z wykorzystaniem mechanizmów phishingowym użytkownika za sprawą kliknięcia w link przesłany mailem zostaje przekierowany na „podstawioną” stronę, która jest wierną kopią właściwej strony banku. Podaje tam hasło do logowania oraz w sytuacji gdy chce dokonać przelewu dane transakcji oraz hasło potwierdzające. W tym czasie informacje te przechwycone zostają przez atakującego i już na właściwej stronie banku są wykorzystane do popełnienia kradzieży. W tym przypadku również czujne oko świadomego użytkownika powinno zauważyć błędy w certyfikacie.

Warto podkreślić, że w niniejszym raporcie atak phishingowy został oddzielony od man-in-the-middle oraz man-in-the-browser i traktowany jest jako wyłudzenie haseł i wykorzystanie ich w w przyszłości, a nie w czasie rzeczywistym. Często zdarza się jednak, że te ataki są połączone.

➤ atakiem man-in-the-browser. Tak jak poprzednie ataki mogą, lecz nie muszą być powiązane ze ściąganiem złośliwego oprogramowania, tak atak man-in-the-browser na tym właśnie polega i przez to jest atakiem najniebezpieczniejszym. Z wykorzystaniem dobrze przygotowanego malware'u można tak naprawdę wykonać wszelkie czynności na komputerze ofiary. Dzięki temu można przedstawić poprawność certyfikatów, można podsłuchać hasła, można również podmienić dane, które trafiają do podpisu elektronicznego. Ten atak opiera się większości metod dostępnych na rynku.

➔ Przy podobnej ochronie przed w/w atakami analizie poddawane były dodatkowe utrudnienia występujące przy danej metodzie (za co była przyznawana nieznacznie wyższa ocena) a także badano podatności na warunki zewnętrzne w tym np. możliwość przechwycenia SMSa. Warto w tym miejscu przywołać atak polegający na kradzieży tożsamości, w celu uzyskania duplikatu karty SIM, wykorzystywanej do otrzymywania wiadomości SMS, w tym naszych haseł potwierdzających transakcję. Poziom weryfikacji dokumentów u operatorów telekomunikacyjnych jest znacznie niższy niż w bankach, dzięki temu możliwość otrzymania kolejnej karty twierdząc, że stara uległa zniszczeniu jest możliwy po przedstawieniu podrobionego dowodu osobistego. Ponadto SMSy są podatne na przechwycenie ze względu na fakt, że muszą przejść dosyć długą drogę od wygenerowania treści w banku, poprzez bramkę wyjściową, system brokera, operatora, urządzenia nadawcze by ostatecznie trafić na telefon użytkownika.

➔ Wzór, który został zastosowany do niniejszego rankingu wygląda następująco:

„suma punktów za bezpieczeństwo = 1 x punkty za logowanie + 3 x punkty za transakcje aktywne“

Z punktu widzenia bezpieczeństwa środków przechowywanych na rachunku ważniejsze jest zabezpieczenie operacji aktywnych tj. przelewów, zamykania lokat itp. – stąd też trzykrotnie większa waga metod chroniących transakcje aktywne.

Podsumowanie

W październiku tego roku mija 11 lat od momentu, kiedy Polacy po raz pierwszy mogli zarządzać swoimi pieniędzmi w banku przez internet. Od tego momentu wiele się zmieniło. Z technologicznej ciekawostki, bankowość internetowa stała się obowiązującym standardem praktycznie we wszystkich komercyjnych instytucjach, dużej części banków spółdzielczych, a nawet SKOK-ów. Rada Bankowości Elektronicznej przy Związku Banków Polskich przewiduje, że jeszcze do końca tego roku liczba aktywnych klientów bankowości elektronicznej przekroczy 8 milionów. Oznacza to, że już około 40 proc. posiadaczy kont bankowych obsługuje swój rachunek przez internet. To ogromny sukces polskich banków i ich klientów. Oszczędności wynikające z korzystania z bankowości elektronicznej można szacować na setki milionów złotych rocznie. Co najważniejsze zyskują na tym nie tylko banki, ale przede wszystkim klienci. Płacą mniej za prowadzenie rachunków, za przelewy, szybciej zarządzają swoimi pieniędzmi, zakładając lokaty, czy wpłacając pieniądze na rachunki oszczędnościowe. Trudno wyliczyć mniej wymierne korzyści w postaci oszczędności czasu, które normalnie trzeba było poświęcić na dojazd do placówki i stanie w bankowych kolejkach. Chociaż nikt się tego początkowo nie spodziewał, to bankowość po tych 11 latach zmieniła się na zawsze i nie do poznania. Można śmiało stwierdzić, że zyskał na tym przede wszystkim klient. W zamian jednak banki przerzuciły na niego sporo obowiązków. Żeby skorzystać z bankowości internetowej nie tylko trzeba nauczyć się korzystać z komputera i internetu, ale również odpowiednio zadbać o bezpieczeństwo. Koszty te musi oczywiście ponieść klient.

Bezpieczeństwo bankowości internetowej leży przede wszystkim w rękach samych klientów. Teoretycznie do zabezpieczenia własnych pieniędzy mogłoby wystarczyć samo hasło. Tak przecież chronimy zdecydowaną większość aplikacji i usług w internecie. Problem w tym, że tam gdzie pojawiają się pieniądze, pojawiają się przestępcy. I to właśnie w ochronie przed nimi banki wprowadzają wyrafinowane sposoby zabezpieczeń. Mają one być odporne na znane i jeszcze niewykryte metody włamań i wyłudzeń. Cały system bezpieczeństwa ma chronić wszystkich klientów – zarówno zaawansowanych internautów, jak również tych czyniących swoją przygodę z siecią. Po części jest to zatem łączenie ognia z wodą. Czy tak rzeczywiście jest? Trudno na to pytanie wprost odpowiedzieć. Faktem jest jednak, że chociaż można stwierdzić, że polskie banki są dobrze zabezpieczone przed potencjalną kradzieżą z kont klientów, to niektóre instytucje wyróżniają się pod tym względem.

Naszym zdaniem najlepsze zabezpieczenia bankowości internetowej stosuje wrocławski Euro Bank. Tuż za nim plasuje się Raiffeisen Bank Polska i BZ WBK z niedawno wdrożonym systemem. W ścisłej czołówce są wszystkie banki stosujące do autoryzacji transakcji SMSy. Znajdują się one przed bankami wykorzystującymi podpis elektroniczny czy tokeny. Na końcu znajdują się banki wykorzystujące do autoryzacji transakcji TANy, czyli hasła jednorazowe. Ich pozycja w raporcie oczywiście nie powinna być utożsamiana z faktem, że są one słabo zabezpieczone. To raczej stwierdzenie, że w ich przypadku znacznie częściej może dojść do skutecznie przeprowadzonych ataków – zarówno wykorzystujących prosty phishing, jak również inne przestępcze techniki. Chociaż

ostatnie miesiące pokazały, że nie jest to tylko teoretyczne zagrożenie, to jednak skala problemu wciąż jest na tyle mała, że nie ma powodu do większego niepokoju. Mimo to, wszystkie instytucje stosujące tego rodzaju zabezpieczenia, powinny zwrócić większą uwagę na prewencję, czyli chociażby edukację klientów. Nawet jednak w takim przypadku nie można wykluczyć sytuacji, kiedy na komputerze klienta zainstalowany jest trojan, który przekazuje wszystkie informacje przestępcom. Pokazuje to, że chociaż założenia systemu zabezpieczeń postają niezmiennie takie same, to przestępcy nieustannie próbują znaleźć luki, które umożliwią im nielegalny transfer pieniędzy z rachunków klientów. Niestety trudno stworzyć takie systemy, które dają 100 procentową pewność zabezpieczenia, a które jednocześnie będą łatwe w użyciu dla przeciętnego klienta. To właśnie największa bolączka branży bankowej – stworzyć takie rozwiązanie, które dadzą największy możliwy do osiągnięcia poziom zabezpieczenia, przy jednoczesnym zachowaniu wygody korzystania i co nie mniej istotne przy rynku masowym – niskich kosztach wdrożenia, utrzymania i rozwoju. Pod tym względem zawsze jest to pewnego rodzaju kompromis. W pewnym sensie stosowanie zbyt skomplikowanych i drogich zabezpieczeń nie ma sensu, bo bank radykalnie musiałby ograniczyć liczbę potencjalnych użytkowników gotowych korzystać ze skomplikowanych lub drogich zabezpieczeń.

Polskie banki stosują wiele różnych sposobów zabezpieczeń, zarówno przy logowaniu, jak i późniejszej autoryzacji operacji. W przypadku logowania najczęściej wystarczy login i hasło, często w wersji maskowanej. Z punktu widzenia klienta, najważniejsze jest jednak zachowanie bezpieczeństwa przy operacjach aktywnych, czyli na przykład wykonania przelewu na zewnętrzny rachunek. Tutaj wszystkie banki dbają o zabezpieczenie, chociaż postęp technologiczny sprawił, że nie wszystkie ze stosowanych obecnie sposobów oferują taki sam poziom bezpieczeństwa. Do najbezpieczniejszych, dostępnych obecnie w Polsce zabezpieczeń, zaliczyliśmy TokenGSM, czyli token w telefonie z funkcją prezentacji i podpisu transakcji w trybie challenge-response. Chroni on przed wszystkimi najważniejszymi sposobami ataku na klientów bankowości internetowej. Podobna idea zabezpieczenia przyświeca hasłom SMSowym, jednak w ich przypadku w niektórych, na całe szczęście w bardzo ograniczonych przypadkach, może dojść do przerwania łańcucha bezpieczeństwa. Pokazuje to, że żadna metoda zabezpieczeń nie daje gwarancji bezpieczeństwa na zawsze. Być może za jakiś czas pojawi się również atak na TokenGSM. Czas pokaże.

Systemy zabezpieczeń stosowane w polskich bankach cały czas ewoluują, trudno zatem obecnie stwierdzić, w którym kierunku rozwinię się rynek. W tym momencie widać wyraźną przewagę rozwiązań opartych na SMSach, przede wszystkim ze względu na połączenie wysokiego bezpieczeństwa i łatwości używania. Rozwiązanie wdrożone przez Euro Bank jest jak na razie jedynym takim przykładem w Polsce, a do tego sam bank proponuje równoległy sposób zabezpieczeń oparty na tradycyjnym tokenie. Można się jednak spodziewać, że w przyszłości podobne rozwiązanie może zostać wdrożone do innych banków, jako jeszcze jedna możliwa do wybrania opcja zabezpieczenia transakcji.

czytaj dalej na stronie 6 ▶

Wszystkie sposoby zabezpieczeń mają swoje wady i zalety. Dużo zależy od przyzwyczajeń klientów, którzy akceptują tylko sposoby, do których się przyzwyczaili. Jest to odwieczny dylemat banków, które chcąc ulepszyć dotychczasowy poziom bezpieczeństwa, muszą zmierzyć się z falą krytyki płynącej ze strony części dotychczasowych użytkowników. Bezpieczeństwo jest jednak bardzo istotne i nie warto na nim oszczędzać. Przekonały się o tym amerykańskie czy australijskie banki, które przez lata lekcewały problem, wprowadzając miesięczne i dzienne limity przelewów i ubezpieczając się na wypadek przypadków włamań na konta klientów. Po kilku latach okazało się, że w sumie nawet kilka milionów klientów przestało korzystać z bankowości internetowej lub ograniczyło swoją aktywność do operacji pasywnych, takich jak sprawdzanie salda. Właśnie ze względu na zbyt małe bezpieczeństwo dokonywanych w internecie operacji. To ryzyko, na które już nikt nie chce sobie pozwolić. Dlatego rodzime banki bardzo dbają o bezpieczeństwo. Mają świadomość, że ewentualne problemy będą rzutowały nie tylko na konkretny bank, ale również na bankowość internetową jako taką.

Czy klient, który posiada rachunek w banku, którego zabezpieczenie zostało przez nas ocenione jako słabsze, po-

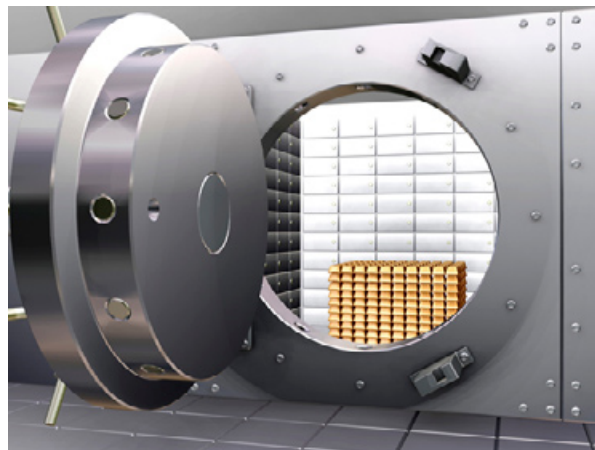
winien się czegoś obawiać lub zmieniać banki? W żadnym przypadku. Powinien przede wszystkim zapoznać się ze słabymi stronami danego sposobu logowania czy autoryzacji. Zazwyczaj to w zupełności wystarczy. Bardzo często zdarza się, że bank udostępnia kilka metod autoryzacji. Jeśli nie jest to związane z wysokimi dodatkowymi kosztami, należy pomyśleć o migracji na bezpieczniejsze rozwiązanie. Tak jest na przykład w bankach, które umożliwiają zamianę z papierowych TANów na SMSy. W końcu chodzi tu o bezpieczeństwo własnych pieniędzy. Dlatego też poza możliwościami oferowanymi przez bank, każdy klient powinien dbać o bezpieczeństwo swoich danych i komputera. Jeśli jest to możliwe, warto wprowadzić limity transakcyjne, powiadomienia o zalogowaniu czy wykonaniu operacji. To ostatnie dotyczy zarówno bankowości internetowej jak i operacji wykonywanych kartą płatniczą. W takim przypadku możemy mieć pewność, że z należytą starannością zadbałoby o bezpieczeństwo własnych pieniędzy. Jak to w życiu bywa – lepiej bowiem zapobiegać, niż potem się martwić i wyjaśniać wątpliwości z bankiem. Nawet najlepsze zabezpieczenia nie zwalniają nas z odpowiedzialności i o tym zawsze powinni pamiętać klienci banków, korzystający z usług przez internet. Wówczas można mieć pewność, że będziemy korzystać z samych zalet bankowości internetowej – przede wszystkim z oszczędności czasu i pieniędzy.

Koszt i wygoda użytkowania - komentarz

Przy okazji analizy bezpieczeństwa warto poruszyć temat wygody użytkowania oraz kosztu wdrożenia i utrzymania w/w mechanizmów. Jeszcze parę lat temu rozwiązania uchodzące za najbardziej bezpieczne były bardzo drogie jak np. tokeny sprzętowe czy podpis elektroniczny, a także mało poręczne – użytkownik by zapewnić silną ochronę dla swoich pieniędzy musiał dysponować dodatkowym urządzeniem. Poza tym np. korzystając z czytnika i karty był ograniczony tylko do jednego komputera. By wykonać operacje w kawiarence internetowej, o ile administrator wyraził zgodę, musiał nastąpić proces instalacji biblioteki oraz czytnika. To było bardzo uciążliwe i kosztowne. Nawet jeśli klient nie ponosił bezpośrednio opłat za wydanie np. tokena, musiał liczyć się z wyższymi opłatami za konto lub inne usługi. Z tego też względu pewną rewolucją stały się hasła jednorazowe – drukowane na kartce lub karcie-zdrapce. Na ówczesne standardy było to rozwiązanie bardzo wygodne i tanie. Można powiedzieć, że dzięki niemu bankowość internetowa mogła w Polsce osiągnąć masę krytyczną. W pewnym momencie był to standard obowiązujący praktycznie w całym sektorze.

Niestety, praktyka pokazała, że przestępcy szybko wykryli luki poszczególnych zabezpieczeń. Wyścig zbrojeń cały czas trwa. Obecnie metody oparte o dodatkowe urządzenia nie są już tak bezpieczne, jak kiedyś. Ataki man-in-the-middle pokazały słabość tokenów sprzętowych (również tokenów challenge-response bez prezentacji danych), natomiast różnego rodzaju złośliwy malware obnażył podpis elektroniczny, również ten sprzętowy. Warto zaznaczyć, że ani jakość obsługi ani koszt w tym samym czasie się nie zmienił. Rynek szuka rozwiązań bezpiecznych, łatwych w obsłudze oraz opłacalnych pod względem kosztowym. Bardzo dobrym rozwiązaniem, które od kilku lat dostępne

jest na polskim rynku jest rozwinięcie pomysłu hasel jednorazowych - są to hasła wysyłane w wiadomości SMS, razem z informacjami o transakcji. Są w miarę bezpieczne oraz łatwe w użyciu. Problemem w ich przypadku jest jednak stosunkowo wysoki koszt, który banki zaczynają przerzucać na klientów. Właśnie koszty wpłyną prawdopodobnie również na poszukiwanie tańszych, a równocześnie równie bezpiecznych alternatyw. Jedną z nich wydaje się, zamiana hasel SMSowych na aplikacje podobne do tych, które w tym momencie oferuje Euro Bank. Wygoda użytkowania jest co prawda niższa od obsługi SMS (trzeba włączyć program), ale sam fakt, że nie trzeba nosić zdrapek, tokenów, kart kryptograficznych nie jest bez znaczenia. Poza tym rozwiązanie jest z pewnością tańsze (licencja, a nie koszt poszczególnych wiadomości) w utrzymaniu przez bank oraz jak wykazał niniejszy raport jest też na dzisiaj rozwiązaniem najbezpieczniejszym.



Dodatek do metodologii - dostępne metody zabezpieczeń

Hasło statyczne (HS)

Najprostsza, ale zarazem najmniej bezpieczna metoda uwierzytelnienia użytkowników w systemach bankowości elektronicznej. Klient logując się do banku musi podać sobie tylko znany ciąg znaków. Banki korzystają z tej metody ponieważ powszechnie uważa się, że zalogowanie na konto i weryfikacja salda jest procesem mało inwazyjnym i atakujący nie jest w stanie wyrządzić wielu szkód. Jest to nieco błędne założenie, ponieważ atak polegający na przelaniu wszystkich oszczędności na konta ZUS, US oraz innych zdefiniowanych odbiorców może być również bardzo odczuwalny dla posiadacza rachunku.

Metoda wykorzystywana przede wszystkim podczas logowania.

Bezpieczeństwo

Metoda całkowicie nieodporna na phishing, ataki man-in-the-middle, man-in-the-browser. Poza tym narażona na podejrzenie oraz odgadnięcie, ponieważ większość haseł jest bardzo prosta by nie stwarzały problemów w zapamiętaniu.

Ocena bezpieczeństwa: 1

Hasło statyczne + dodatkowy identyfikator (HS + DI)

Hasło statyczne jest wzbogacone o dodatkowy (również statyczny) identyfikator w postaci np. numeru PESEL. Dla utrudnienia przejścia system prosi o wybrane cyfry/litery z hasła.

Bezpieczeństwo

Metoda nieodporna na phishing, ataki man-in-the-middle, man-in-the-browser. Identyfikator jest jedynie utrudnieniem i atak musi być prowadzony dłużej niż w przypadku zwykłego hasła statycznego - podczas jednej sesji atakujący dostanie tylko niektóre znaki. Atak musi być powtarzany do momentu uzyskania znaków o które system pyta atakującego (rzadko musi być to pełny identyfikator).

Atak phishingowy może również polegać na tym by klient podał swój numer PESEL w całości, razem z hasłem statycznym. Wtedy wystarczy jedna sesja.

Ocena bezpieczeństwa: 1,5

Hasło maskowane (HM)

Metoda polegająca na wprowadzaniu wybranych znaków z hasła statycznego. System za każdym razem losowo wybiera o które znaki zapyta.

Bezpieczeństwo

Ten sam poziom bezpieczeństwa i taka sama podatność na ataki co w przypadku hasła statycznego wspartego dodatkowym identyfikatorem.

Ocena bezpieczeństwa: 1,5

Hasło maskowane plus obrazek identyfikujący właściwą stronę (HM + O)

Po wprowadzaniu i akceptacji loginu, pojawia się obrazek, który sami wybraliśmy podczas rejestracji. Poprawny obrazek ma za zadanie upewnić klienta, że korzysta z prawidłowej strony bankowej. Jeżeli obrazek jest zgodny z naszymi oczekiwaniami podajemy wybrane znaki z hasła statycznego (te o które w danej sesji system zapyta).

Obrazek może się również pojawić już po zalogowaniu do systemu bankowego (po podaniu hasła).

Bezpieczeństwo

Wprowadzenie obrazka nieznacznie zwiększa bezpieczeństwo i jest dodatkowym, wizualnym elementem wskazującym na to, że znajdujemy się na prawidłowej stronie. Musimy jednak wiedzieć, że złożone ataki man-in-the-middle są w stanie sobie z tym poradzić, podobnie ataki man-in-the-browser. Ponieważ nadal metoda opiera się de facto na hasle statycznym, możliwe jest przeprowadzenie ataku phishingowego.

Ocena bezpieczeństwa: 2

Karta zdrapka / lista haseł jednorazowych (TAN)

Istnieje od początku polskiej bankowości internetowej. Lista haseł jednorazowych lub karta zdrapka (hasło dostępne po starciu warstwy ochronnej) uwierzytelniają użytkownika lub/i służą do potwierdzania transakcji. Na rynku istnieją różne systemy oparte o tę metodę – począwszy od prostej listy haseł, które są drukowane po kolei i tak też wprowadza się je do systemu, poprzez hasła nie układane w kolejności – po karty typu „szachownica“ / „macierz“ gdzie kod buduje się z wartości umieszczonych pod konkretnymi polami typu A3B4.

Bezpieczeństwo

Teoretycznie najbezpieczniejsze są karty typu „szachownica“, lecz i ta metoda jest narażona na popularny phishing – nieświadomy użytkownik może przepisać całą macierz podobnie jak w przypadku wszystkich innych rodzajów kart. Metoda nie jest również odporna na ataki man-in-the-middle i man-in-the-browser.

Ocena bezpieczeństwa: 2

SMS z hasłem jednorazowym plus hasło maskowane (SMS HJ + HM+O)

Metoda łącząca opisywane wcześniej hasło maskowane z dodatkowymi zabezpieczeniami. W tym przypadku po wprowadzeniu i zaakceptowaniu wybranych znaków z hasła na wskazany wcześniej numer telefonu przychodzi wiadomość SMS z hasłem jednorazowym. Ponadto po zalogo-

czytaj dalej na stronie 8 ▶

► ze strony 7

waniu pojawia się obrazek identyfikujący stronę. Obrazek wcześniej ustala użytkownik.

Bezpieczeństwo

Hasło jednorazowe wysłane na telefon komórkowy zabezpiecza przed popularnymi atakami phishingowymi polegającymi na przekierowaniu użytkownika na fałszywą stronę, która prosi o podanie haseł, nie zabezpiecza jednak przed atakami man-in-the-middle i man-in-the-browser.

Ocena bezpieczeństwa: 5

SMS z hasłem jednorazowym plus hasło statyczne plus obrazek identyfikujący właściwą stronę (SMS HJ + HS + O)

Tym razem hasło jednorazowe, które zostaje przesłane na SMS jest wsparte hasłem statycznym. SMS przychodzi po podaniu identyfikatora i hasła statycznego. Cała metoda wzbogacona jest o wyświetlenie obrazka, który pojawi się po zalogowaniu.

Bezpieczeństwo

Bezpieczeństwo na podobnym poziomie co hasło wysłane SMS wzbogacone o hasło maskowane.

Ocena bezpieczeństwa: 4,5

SMS z hasłem jednorazowym plus hasło statyczne plus mechanizm „captcha” (SMS HJ + HS + C)

Metoda podobna do poprzedniej z tą różnicą, że obrazek pojawiający się po zalogowaniu został zastąpiony przez mechanizm „captcha”, tj. trzeba przepisać dodatkowe znaki z pojawiającej grafiki.

Bezpieczeństwo

Bezpieczeństwo na tym samym poziomie co poprzednia metoda. Warto jednak zaznaczyć, że mechanizm „captcha” służy do innej ochrony niż „obrazek”. Ten ostatni służy poinformowaniu użytkownika, że jest na niewłaściwej stronie, „captcha” natomiast ma chronić przed automatami próbującymi łamać hasła metodą brute-force.

Oba mechanizmy są jednak tylko dodatkami i nie zabezpieczają przed głównymi wektorami ataków.

Ocena bezpieczeństwa: 4,5

SMS z opisem transakcji i hasłem jednorazowym powiązanym z tą transakcją (SMS Transakcja)

Obecnie najpopularniejsza metoda na rynku służąca do potwierdzenia transakcji. Po wprowadzeniu danych np. do przelewu, bank wysyła do użytkownika wiadomość SMS zawierającą informacje o właśnie dokonanej czynności (np. wybrane cyfry z numeru rachunku, kwotę, datę) oraz hasło służące do potwierdzenia tej transakcji. Klient przepisuje hasło z SMSa i w ten sposób akceptuje transakcję.

Bezpieczeństwo

Do niedawna najbezpieczniejsza metoda na rynku. Odporna na phishing, ataki man-in-the-middle i man-in-the-

browser - o ile użytkownik czyta skrupulatnie dane transakcji. Największą bolączką pod kątem bezpieczeństwa jest fakt, że ta metoda zależna jest nie tylko od samego banku, ale również od operatora GSM oraz ewentualnie od brokera. Przez wszystkie te „dodatkowe” punkty przechodzą informacje o transakcji oraz samo hasło. Ponadto weryfikacja tożsamości u operatorów telefonii komórkowej podlega znacznie niższym restrykcjom niż w banku. To powoduje, że pojawiły się ataki personalizowane na konkretną osobę, gdzie atakujący podszywał się pod właściwego użytkownika i dzięki fałszywym danym wyłudzał od operatora drugą kartę SIM twierdząc, że poprzednia została zgubiona. Takie ataki miały już miejsce na polskim rynku. Mimo wszystko na tle innych metod hasła wysyłane SMS'em wraz z opisem transakcji póki co pozostają bardzo silnym mechanizmem potwierdzającym.

Ocena bezpieczeństwa: 8

Token sprzętowy generujący hasła na bazie czasu. (T (czas))

Token to małe urządzenie generujące hasła jednorazowe. Klient wykorzystuje je w procesie logowania lub/i do potwierdzenia transakcji. Generowane hasło za każdym razem jest inne, i w niniejszym przypadku jest ograniczone czasowo tj. klient ma na przykład 5 minut by je wykorzystać. Po tym czasie hasło traci ważność.

Token bez dodatkowego elementu zabezpieczającego wystąpił w rankingu tylko raz i był zabezpieczeniem transakcji - tj. hasło z tokena klient podaje po akceptacji wprowadzonych danych.

Bezpieczeństwo

Podobnie jak w przypadku haseł jednorazowych wysyłanych w postaci wiadomości SMS token sprzętowy zabezpiecza przed popularnymi atakami mającymi na celu wyłudzenie haseł do logowania/potwierdzenia transakcji ale również podobnie nie zabezpiecza przed man-in-the-middle i man-in-the-browser.

W opisywanej metodzie nie ma dodatkowego elementu, jakim może być hasło statyczne czy PIN do tokena.

Ocena bezpieczeństwa: 4,5

Token sprzętowy generujący hasła na bazie czasu plus hasło statyczne (T (czas) + HS)

Metoda polegająca na wprowadzeniu jednocześnie hasła jednorazowego wygenerowanego przez token oraz hasła statycznego. Obie części stanowią tzw. Passphrase i są wprowadzane w celu zalogowania się (po podaniu identyfikatora/loginu) lub do potwierdzenia transakcji.

Bezpieczeństwo

Nieznacznie wyższe niż w przypadku samego tokena sprzętowego.

Ocena bezpieczeństwa: 4,5

czytaj dalej na stronie 9 ►

Token sprzętowy generujący hasła na bazie czasu plus hasło statyczne plus pytanie (T (czas) + HS + P)

Kolejna wariacja metody opartej o token sprzętowy. W tym przypadku poza hasłem statycznym system prosi o podanie odpowiedzi na wcześniej przygotowane pytanie.

Bezpieczeństwo

Nieznacznie wyższe od tokena z hasłem statycznym.

Ocena bezpieczeństwa: 5

Token sprzętowy generujący hasła na bazie czasu (zabezpieczony dodatkowym PINem) plus hasło statyczne plus obrazek (T (czas) z PIN + HS + O)

Kolejna wariacja metody opartej o token sprzętowy. W tym przypadku token posiada zabezpieczający PIN a jako dodatkową ochronę zastosowano hasło statyczne oraz obrazek.

Bezpieczeństwo

Ponieważ jest PIN oraz obrazek, ocena nieznacznie wyższa niż w przypadku poprzedniej metody.

Ocena bezpieczeństwa: 5,5

Token sprzętowy generujący hasła na bazie licznika. Token z PINem (T (licznik) z PINem)

Urządzenie podobne do wcześniej opisywanych tokenów. Posiada jednak klawiaturę służącą do wprowadzenia PINu. Poza tym zasadniczą różnicą jest fakt, że hasła generowane są z wykorzystaniem licznika (nie są ograniczone czasowo).

Bezpieczeństwo

Token generujący hasła z wykorzystaniem licznika jest mniej bezpieczny niż urządzenie generujące hasła ograniczone czasowo. Klient korzystający z tej metody narażony jest na wszystkie analizowane w raporcie ataki włącznie z phishingiem. Atakujący może wyłudzić określoną liczbę haseł od ofiary by wykorzystać je w dowolnym czasie – z zastrzeżeniem, że wcześniej klient nie skorzysta z kolejnego wygenerowanego hasła. To jest przewaga tej metody nad kartami zdrapkami, ponieważ w przypadku phishingu zorientowanego na TAN okres czasu w którym atakujący może wykorzystać hasła jest zazwyczaj bardzo duży (ofiara podała hasła z których sama będzie chciała korzystać, w przypadku tokena Klient nie wróci do wygenerowanych już tokenów, które podał podczas ataku).

Dodatkowym zabezpieczeniem i przewagą nad TANem jest PIN.

Ocena bezpieczeństwa: 3

Token sprzętowy generujący hasła w trybie Challenge-Response. Token z PINem (T (CHR) z PIN)

Token z klawiaturką służącą do podania PINu a także do wprowadzenia kodu transakcji (tzw. challenge), który wyświetla się po akceptacji danych np. do przelewu. Po wprowadzeniu tego kodu urządzenie generuje odpowiedź tj. kod potwierdzający

(tzw. response), który klient wpisuje pod transakcją.

Bezpieczeństwo

Poziom bezpieczeństwa większy niż w przypadku tokenów generujących hasła jednorazowe. Hasło potwierdzające jest przypisane do konkretnej transakcji i wymaga reakcji użytkownika. Nie można przeprowadzić ataku phishingowego polegającego na wcześniejszym zdobyciu hasła. Metoda nie chroni jednak przed atakami typu man-in-the-middle i man-in-the-browser.

Ocena bezpieczeństwa: 5

Token w telefonie generujący hasła na bazie licznika (token zabezpieczony PINem) plus hasło statyczne (TokenGSM (licznik) z PINem + HS)

Metoda zabezpieczająca logowanie do banku polegająca na generowaniu haseł jednorazowych z wykorzystaniem aplikacji instalowanej na telefonie komórkowym. Hasło generowane jest na bazie licznika. Aplikacja zachowuje się dokładnie jak token sprzętowy. Dodatkowymi składnikami uwierzytelnienia są PIN do aplikacji oraz hasło statyczne, które podaje się razem z wygenerowanym hasłem jednorazowym).

Bezpieczeństwo

Bezpieczeństwo porównywalne z tokenem sprzętowym generującym hasła na bazie licznika i zabezpieczonego PINem. Metoda wzbogacona o dodatkowe hasło statyczne.

Ocena bezpieczeństwa: 3,5

Token w telefonie z funkcją Challenge-Response (token zabezpieczony PINem) (TokenGSM (Transakcja))

Ta sama aplikacja, która potrafi generować hasła jednorazowe odpowiada również za potwierdzanie transakcji. W momencie gdy klient wprowadza dane np. do przelewu i zatwierdza je, system bankowy generuje kod transakcji (tzw. challenge), kod ten wpisuje do aplikacji. Następnie aplikacja na telefonie wyświetla mu dane z tej transakcji (dane zostały przesłane w kodzie challenge, całkowicie w trybie offline) i klient musi je zatwierdzić. Po ich akceptacji aplikacja generuje kod potwierdzający (tzw. response), który to kod klient wpisuje pod przelewem. Jeżeli kod się zgadza transakcja jest realizowana.

Bezpieczeństwo

Obecnie najsilniejsza metoda potwierdzania transakcji dostępna na polskim rynku. Challenge-response pokazujący dane transakcji na zewnętrznym urządzeniu jakim jest telefon, ponadto w sposób całkowicie offline'owy, jest obecnie optymalnym zabezpieczeniem przed phishingiem oraz atakami man-in-the-middle i man-in-the-browser. Ponadto porównując aplikację TokenGSM do wiadomości SMS ta wyświetla dane w sposób bardzo przejrzysty i czytelny (nie sposób jest przeoczyć ważne informacje) i dane te muszą zostać zatwierdzone zanim wygenerowane zostanie hasło potwierdzające. Sam fakt, że hasło generowane jest po akceptacji danych oraz na telefonie jest również lepszym rozwiązaniem od hasła wysyłanego SMSem, które generowane jest już na serwerze razem z danymi o transakcji. Dzięki temu, że cały proces podpisu transakcji dzieje się

czytaj dalej na stronie 10 ►

w trybie offline (tj. nie jest niezbędna karta SIM) odchodzi również ryzyko ataku poprzez kradzież tożsamości. Teoretycznym zagrożeniem są wirusy na komórki, jednak wbrew powszechnej opinii aplikacje Java są na nie odporne a inne platformy również bardzo dbają by możliwość napisania na nie wirusa była jak najmniejsza. Atakujący szybciej stworzy złośliwe oprogramowanie na platformy stacjonarne niż mobilne. Podsumowując powyższe aplikacja TokenGSM została przez nas oceniona najwyżej.

Ocena bezpieczeństwa: 10.

Podpis elektroniczny programowy tj. z certyfikatem i kluczami przechowywanymi na komputerze klienta (lub na dowolnym nośniku) (PE (SOFT)).

Klient banku podczas pierwszego logowania inicjuje na swoim komputerze generację kluczy służących do podpisu oraz uzyskuje certyfikat, który zostaje zapisany w systemie. Podczas dokonywania transakcji klient podaje hasło statyczne, które odblokowuje klucz, którym dane są podpisywane. Następnie podpisana informacja trafia do systemu bankowego.

Bezpieczeństwo

Mogłoby się wydawać, że rozwiązania oparte o PKI (infrastruktura klucza publicznego, podpis elektroniczny) powinny być rozwiązaniami najbezpieczniejszymi. Zabezpieczają one jednak tylko przed phishingiem i atakami man-in-the-middle. Są całkowicie bezbronne wobec zagrożeń typu man-in-the-browser. Obecnie spotykane ataki potrafią modyfikować dane przekazywane do podpisu przy jednoczesnym prezentowaniu na ekranie „właściwych” informacji. PKI oparte o zaufane centra certyfikacji chroni przed man-in-the-middle i chroni przed phishingiem.

Ocena bezpieczeństwa: 5

Podpis elektroniczny sprzętowy (PE (HARD))

Klient zostaje wyposażony przez Bank w zestaw do składania podpisu tj. w czytnik, kartę z certyfikatem oraz odpowiednią bibliotekę do obsługi zestawu. Może być to również urządzenie typu USB łączące w sobie czytnik z kartą. Istnieje możliwość by klient korzystał z zestawu do podpisu kwalifikowanego. W momencie dokonywania transakcji użytkownik zostaje poproszony o podanie PINu do karty, która zawiera stosowne klucze służące do podpisania wrażliwych informacji.

Bezpieczeństwo

Ponieważ dochodzą dodatkowe elementy, które są niezbędne do dokonania transakcji poziom bezpieczeństwa oceniony został nieco wyżej niż w przypadku podpisu programowego. Ocena nie może być jeszcze wyższa ponieważ ta metoda również nie zabezpiecza przed atakami man-in-the-browser.

Ocena bezpieczeństwa: 6

Podpis elektroniczny sprzętowy i SMS z hasłem jednorazowym (PE + SMS (HJ))

Jest to podpis elektroniczny zgodny z opisem poprzedniej metody wzbogacony o hasło jednorazowe przesłane w wiadomości SMS.

Bezpieczeństwo

Nieznacznie większe niż sam podpis sprzętowy. Podobnie zabezpiecza przed phishingiem i atakami man-in-the-middle lecz nie zabezpiecza przed man-in-the-browser.

Ocena bezpieczeństwa: 6,5



Zestawienie banków i wspieranych metod – ranking

Nazwa banku	Logowanie	Autoryzacja transakcji
Euro Bank S.A.	TokenGSM (licznik) + HS	T o k e n G S M (Transakcja)
BPN Paribas Fortis S.A.	SMS (HJ) + HM + O	SMS (Transakcja)
Raiffeisen Bank Polska S.A.	SMS (HJ) + HS + C	SMS (Transakcja)
Bank Zachodni WBK S.A.	SMS (HJ) + HS + O	SMS (Transakcja)
Alior Bank S.A.	HM + O	SMS (Transakcja)
Bank Pekao S.A.	HM	SMS (Transakcja)
Konto Xelion	HM	SMS (Transakcja)
Millennium Bank S.A.	HS + DI	SMS (Transakcja)
Allianz Bank S.A.	HS	SMS (Transakcja)
Bank Handlowy w Warszawie S.A.	HS	SMS (Transakcja)
Bank Ochrony Środowiska S.A.	HS	SMS (Transakcja)
ING Bank Śląski S.A.	HS	SMS (Transakcja)
Krakowski Bank Spółdzielczy	HS	SMS (Transakcja)
mBank (BRE Bank S.A.)	HS	SMS (Transakcja)
MultiBank (BRE Bank S.A.)	HS	SMS (Transakcja)
Nordea Bank Polska S.A.	PE (HARD)	PE (HARD)
Bank BPH S.A.	HM	PE (HARD) + SMS (HJ)
Bank Gospodarki Żywnościowej S.A.	T (czas) z PIN + HS + O	T (CHR) z PIN
Bank Polskiej Spółdzielczości	T (czas) + HS	T (czas) + HS
Gospodarczy Bank Wielkopolski	T (czas) + HS	T (czas) + HS
Lukas Bank S.A.	T (czas) + HS	T (czas) + HS
Podkarpacki Bank Spółdzielczy w Sanoku	T (czas) + HS	T (czas) + HS
Toyota Bank Polska S.A.	T (czas) + HS	T (czas) + HS
Volkswagen Bank Polska S.A.	T (czas) + HS	T (czas) + HS
HSBC Polska S.A.	T (czas) + HS + Pytanie	T (czas)
Invest-Bank S.A.	HS	PE (SOFT)
Polbank EFG (Euro Bank Ergasis S.A.)	HS	PE (SOFT)
Kredyt Bank S.A.	HS	T (CHR) z PIN
Mazowiecki Bank Regionalny w Warszawie	T (licznik) z PIN	T (licznik) z PIN
Bank Pocztowy S.A.	HS	TAN
Deutsche Bank PBC S.A.	HS	TAN
DnB NORD Polska S.A.	HS	TAN
eskok.pl	HS	TAN
Getin Bank S.A.	HS	TAN
Inteligo (PKO Bank Polski S.A.)	HS	TAN
PKO BP S.A.	HS	TAN