



2020
VII EDYCJA

WYZWANIA INFORMATYKI BANKOWEJ

REDAKCJA

Andrzej Kawiński, Andrzej Sieradz

PUBLIKACJA EUROPEJSKIEGO
KONGRESU FINANSOWEGO



Mariusz Sudół, Operations Director CEE, Hitachi Europe Ltd.

Doktor nauk prawnych Uniwersytetu Warszawskiego z doświadczeniem transakcyjnym oraz regulacyjnym zdobytym w departamentach Banking & Finance międzynarodowych kancelarii prawnych. Ukończył z wyróżnieniem Wydział Prawa i Administracji Uniwersytetu Warszawskiego, uczestnicząc także w sfinansowanym przez rząd Szwajcarii stypendium naukowym na Universität Zurich. Dyrektor Operacyjny na region Europy Środkowo-Wschodniej w Hitachi Europe Limited, odpowiedzialny za sektory regulowane (bankowość, nowoczesna energetyka), w tym za praktykę prawa bankowego, praktykę prawa nowych technologii, negocjacje, przygotowywanie umów, komercjalizację i rozwój innowacyjnych produktów oraz strategię rozwoju biznesu. Wykładowca i autor wielu publikacji naukowych dotyczących prawa gospodarczego.



Tadeusz Woszczyński, Country Manager Poland, Hitachi Europe Ltd.

Od 15 lat związany z firmą Hitachi Europe, którą jako Country Manager zarządza w Polsce, Austrii, Czechach, Słowacji i krajach bałtyckich. Ekspert w zakresie nowych technologii IT w sektorze bankowym. Absolwent Politechniki Śląskiej na kierunku Elektronika i Telekomunikacja, stypendium Master Program Infotech (Informatyka) na Universität Stuttgart oraz Szkoły Głównej Handlowej (Efektywne Zarządzanie IT w Przedsiębiorstwie). Uczestnik programów szkoleniowych dla menedżerów na zagranicznych uczelniach, takich jak Wharton, Kellogg School of Management czy IESE. Od 2010 roku Członek Prezydium Forum Technologii Bankowych. Współzałożyciel, a w latach 2007-2016 przewodniczący Grupy ds. Biometrii Forum Technologii Bankowych w Związku Banków Polskich. Współautor wielu publikacji na temat biometrii, kart multiaplikacyjnych, digitalizacji przedsiębiorstw oraz regulacji. Brał udział w wielu innowacyjnych na skalę europejską projektach dotyczących pierwszych sieci bankomatów i oddziałów biometrycznych w Polsce i w Turcji, systemów „paperless”, pierwszych systemów kart multiaplikacyjnych i systemów DLP w administracji publicznej czy też wdrożeniach dotyczących rozwiązania problemu trwałego nośnika informacji.

Biometria w sektorze finansowym

Potrzeby, obszary i warunki rozpowszechnienia na rynku

Rozwój informacji, możliwości ich gromadzenia, przekazywania oraz przetwarzania, w szczególności przetwarzania elektronicznego, stanowią charakterystyczną cechę nowoczesnych technologii. Przykładem tych, których istota funkcjonowania opiera się na wykorzystywaniu indywidualnych właściwości każdego człowieka są technologie biometryczne. Wydaje się, że obecnie mogą mieć one szersze, niemal powszechne zastosowanie w bankowości.

Terminem „biometria” określa się nowoczesną technologię służącą do rozpoznawania tożsamości osób fizycznych, która ma obecnie zastosowanie zarówno w kraju, jak i za granicą. W kontekście społecznym biometria jest postrzegana m.in. jako narzędzie mogące umożliwić zwiększenie poziomu bezpieczeństwa, zapobiegania i zwalczania terroryzmu oraz ułatwiania i polepszania jakości życia obywateli, w tym klientów bankowych. Ponadto powstający wokół niej dynamicznie rozwijający się rynek produktów i usług o charakterze komercyjnym wydaje się być atrakcyjną alternatywą w stosunku do dotychczasowych, tradycyjnych metod uwierzytelniania.

Wykorzystywanie technologii biometrycznych od dłuższego czasu wydaje się być przedmiotem zainteresowania banków i firm technologicznych. Początkowo koniecznym było zaznajomienie się z niuansami technologicznymi proponowanych rozwiązań (w tym kwestiami bezpieczeństwa), następnie

kluczowe okazało się opracowanie aspektów prawnych, warunkujących jakiekolwiek ich zastosowanie na potrzeby banków i ich klientów. Nie bez znaczenia była też konieczność odpowiedniej aranżacji procesów bankowych.

Rodzaje danych biometrycznych

Biometria oznacza „technikę automatycznego pomiaru cech istot żywych i porównywania ich ze wzorcem zawartym na nośniku danych w celu rozpoznania tożsamości człowieka”¹, rozumianą w sensie prawnym, a nie psychologicznym². Rozpoznawanie to odbywa się z wykorzystaniem właściwości fizycznych lub behawioralnych człowieka³. Do właściwości fizycznych zaliczane są m.in.: układ naczyń krwionośnych palca oraz dłoni, a także linie papilarne palca lub kształt wybranych części ciała, np. dłoni czy twarzy. Cechy behawioralne dotyczą natomiast sposobu zachowania się człowieka, a ich przykładem jest charakter pisma odręcznego lub sposób pisania na klawiaturze komputera.

Biorąc pod uwagę kwestie funkcjonalne, przez biometrię można rozumieć technologię lub metodę, za pomocą której dokonywany jest pomiar możliwych do zmierzenia cech człowieka. Efekt tego pomiaru jest następnie porównywany z utworzonym uprzednio wzorcem biometrycznym zawartym na nośniku danych, np. na karcie z mikroprocesorem, w czytniku biometrycznym, w centralnej bazie danych czy na smartfonie. System biometryczny potrafi rozpoznać nasze immanentne, wrodzone cechy, przetworzyć je na dane, stworzyć z nich wzorzec i po dokonaniu porównań odpowiedzieć na pytanie „kim jesteśmy” (identyfikacja) lub potwierdzić naszą tożsamość (weryfikacja).

Dla możliwości zastosowania danych cech biometrycznych koniecznym, choć niewystarczającym, jest, aby cechy biometryczne charakteryzowały się następującymi właściwościami:

- występowały u większości osób (czyli były powszechne),
- były możliwe do zmierzenia,

1 Por. R. Kaszubski, M. Sudoł, T. Woszczyński, Z. Marcinkiewicz, J. Ratajczak, A. Czajka, *Prawne Aspekty Biometrii*, s. 4, Warszawa 2011.

2 B. Miller, *Everything You Need to Know About Automated Biometric Identification*, Security Technology & Design, April 1997; G. Roethenbaugh, *Biometrics Explained*, 1998. Available at: <http://www.ncsa.com/services/consortia/cbdc/explained.html>

3 *Ibidem*, s. 4.

- dostatecznie odróżniały od siebie poszczególne jednostki, a przy tym były dostatecznie trwałe, stałe,
- były łatwo rozpoznawalne (łatwe do zastosowania) i trudne do podrobienia.

Przegląd projektów

a) Bankomaty

Pierwsze projekty biometryczne w Polsce związane były z procesami weryfikacji tożsamości i autoryzacji wypłat gotówkowych z bankomatów, generalnie przez wiele lat najważniejszym i najpopularniejszym zastosowaniem biometrii w bankowości. Do dzisiaj bankomaty biometryczne są bardzo popularne w Japonii (ok. 50 tys. bankomatów biometrycznych w użyciu), Turcji (banki IS Bankasi, Ziraat) oraz Ameryce Południowej (m.in. w Brazylii). Pionierem w Europie w tym obszarze była Polska. W 2009 r. Podkarpacki Bank Spółdzielczy (PBS) zastosował technologię biometryczną Finger Vein (biometria naczyń krwionośnych palca) w sieci bankomatów własnych. Umożliwiają one wypłaty świadczeń społecznych bez konieczności posiadania konta i karty płatniczej, od pewnego czasu z wykorzystaniem biometrii naczyń krwionośnych palca. Równolegle do PBS biometrię w bankomatach na pewien okres czasu wprowadził Bank BPS. Biometria Finger Vein została wdrożona w 30 bankach spółdzielczych Grupy BPS i Grupy SGB, m.in. w Powiślańskim Banku Spółdzielczym w Kwidzynie czy też w Banku Spółdzielczym w Radzynie Podlaskim. Biometrię FV wdrożył także największy bank niezrzeszony – Krakowski Bank Spółdzielczy (KBS). Niektóre banki spółdzielcze, np. BS Toruń, BS Kolno czy też BS w Szumowie zdecydowały się wdrożyć rozwiązanie oparte o naczyniach krwionośnych dłoni. W 2014 r. firma ITCard zdecydowała się wdrożyć biometrię Finger Vein w 2 000 bankomatów sieci PlanetCash. Bankomaty biometryczne można też spotkać m.in. na lotnisku Chopina w Warszawie. Biometria do dzisiaj zostaje wygodną opcją wypłat bezkartowych, szczególnie chętnie używaną przez klientów bankowości spółdzielczej. Popularność tego rodzaju wypłat została dopiero przystopowana przez popularyzację i rozwój płatności bezstykowych oraz Blik.

b) Stacjonarne oddziały bankowe

Istotny dla europejskiego sektora bankowego projekt został zrealizowany przez Bank BPH S.A., a dotyczył wykorzystywania biometrycznej weryfikacji tożsamości klienta w oddziale banku bez konieczności użycia dowodu osobistego. Dzięki temu uproszczono proces obsługi klienta oraz zapewniono obiektywną, technologiczną ocenę jego tożsamości, minimalizując skutki subiektywnej oceny dokonywanej przez pracownika banku, która czasami była błędna. Równocześnie system biometryczny służył do uwierzytelniania operacji przez pracowników banku w oddziale, aby uniemożliwić nieautoryzowany dostęp do profilu klienta. W kulminacyjnym momencie z systemu biometrycznego opartego na Finger Vein korzystało ponad 266 tys. klientów, którzy dokonywali biometrycznie 16 tys. operacji dziennie⁴. Kolejnym bankiem, który zastosował tę technologię w nowych placówkach był Getin Bank. Niektóre inne banki pilotażowo wdrażały w swoich placówkach biometrię podpisu odręcznego. Powszechne zastosowanie biometrii w celu zwiększenia bezpieczeństwa transakcji i redukcji papieru było planowane przez większość w banków w Polsce. Niestety, projekty zostały wstrzymane ze względu na redukcję liczby oddziałów oraz inwestycji w sieć sprzedaży na rzecz kanałów zdalnych.

c) Zdalne oddziały bankowe oraz biometryczny podpis elektroniczny

Najbardziej zaawansowanym projektem w Polsce był, zrealizowany w 2014 r. przez Getin Bank S.A., projekt wirtualnych oddziałów bankowych (z ang. VTM). Oddziały te, ustawione w kilku centrach handlowych w Polsce, wykorzystywały technologie biometryczne i mechanizmy kryptograficzne do powiązania biometrycznej tożsamości człowieka z jego oświadczeniem woli. Zostały stworzone prawnie skuteczne podpisy biometryczne, a także dokumenty utworzone i zabezpieczone biometrycznie. Był to pierwszy projekt w Europie, w którym wykorzystano biometrię Finger Vein jako uwierzytelnienie do klucza prywatnego (BioPKI). W 2015 r. koncepcja ta była kontynuowana przez Bank Zachodni WBK S.A., który przeprowadził z sukcesem pilotaż w wybranych placówkach w Warszawie, Wrocławiu, Poznaniu i Lublinie. W trakcie pilotażu 61% osób zdecydowało się zostawić swoje wzorce biometryczne, a 95% z nich uznało wzrost wygody za główny powód decyzji o wyborze biometrii⁵.

4 Źródło: Bank BPS S.A. (05.2016)

5 Źródło: Oddziały Paperless w Banku Zachodni WBK S.A., International Biometric Congress, 22.09.2015

d) Contact Center

Biometria głosowa jest naturalnym narzędziem do weryfikacji klientów w Contact Center, czyli tam gdzie dana osoba musi być uwierzytelniona na odległość. Można ją wdrożyć w różny sposób, np. jako system zależny od treści (treść hasła jest z góry ustalona i każda osoba ma takie samo hasło) lub jako system od niej niezależny, czyli uwierzytelnienia osoby podczas zwykłej rozmowy telefonicznej. Od 2015 r. klienci Santander Bank Polska mogą potwierdzać swoją tożsamość na infolinii za pomocą głosu⁶. Identyfikacja biometryczna znacznie przyspieszyła i ułatwiła proces logowania do bankowości telefonicznej. Pomimo iż biometria głosu nie wymaga inwestycji w specjalistyczne urządzenia, ta metoda biometryczna mimo wszystko nie zyskała wielkiej popularności w Polsce.

e) Urządzenia mobilne

Zastosowanie biometrii w urządzeniach mobilnych stało się obecnie najpopularniejszym zastosowaniem biometrii i niewątpliwie wpłynęło na zmianę nastawienia wielu osób do tej technologii. Logowanie biometryczne jest dzisiaj standardem do logowania do bankowości mobilnej i stosuje je praktycznie większość banków w Polsce. Do tego celu wykorzystuje się mechanizmy biometryczne wbudowane w smartfony, takie jak biometria linii papilarnych (np. TouchID) czy też twarzy (np. FaceID). Niektóre banki wprowadziły możliwość założenia konta poprzez telefon na tzw. „selfie”. Od 2020 r. Bank Pekao S.A. umożliwia założenia go poprzez aplikację mobilną PeoPay. Weryfikacja tożsamości odbywa się za pomocą selfie i biometrii⁷. Już w 2017 r. Bank Zachodni WBK (obecnie Santander Bank Polska) umożliwił klientom indywidualnym oraz prowadzącym jednoosobową działalność gospodarczą założenie konta bankowego przy pomocy wideoweryfikacji wykorzystującej metody biometrii twarzy⁸. Aby wykorzystać wielki potencjał popularności biometrii w bankowości mobilnej i rozszerzyć jej zastosowanie, konieczne jest opracowanie biometrii zgodnej z wymaganiami PSD2.0, które dotyczą silnego uwierzytelniania, oraz umożliwiającej zastosowanie w większości urządzeń mobilnych, czyli niezależnie od platformy sprzętowej.

⁶ Źródło: „BZ WBK rozpozna swoich klientów po głosie”, prnews.pl, 30.04.2015

⁷ Źródło: „Konto w Banku Pekao bez wychodzenia z domu. Wystarczy zdjęcie dowodu i selfie”, Spider’s Web, 19.02.2020

⁸ Źródło: „Ruszyła wideoweryfikacja w Banku Zachodnim WBK”, Santander Bank Polska, 19.10.2017

f) Bankowość korporacyjna

Dokonując przeglądu projektów, należy zwrócić uwagę, że adresowane są one głównie do klienta detalicznego i służą przede wszystkim zabezpieczeniu jego własnych interesów. Należy dodać, że dane biometryczne pracowników mogą zabezpieczać interesy firm. Jako przykład można podać projekt zrealizowany przez Barclays Bank w Wielkiej Brytanii. Został on wdrożony w dużej skali (na ponad 30 000 czytników biometrycznych) pod kątem potrzeb bankowości korporacyjnej, tj. do potwierdzania przez przedstawicieli poszczególnych firm zlecenia przelewów znacznej wartości.

Warto zwrócić uwagę, że podczas gdy wszystkie projekty realizowane w Polsce dotyczyły relacji z poszczególnymi osobami fizycznymi, ten zrealizowany w Wielkiej Brytanii wymagał wykorzystania cechy biometrycznej danej osoby fizycznej działającej w imieniu osoby prawnej. Oznaczało to, że immanentnie przypisana cecha biometryczna jednostki ludzkiej staje się niezbędna do działalności profesjonalnego biznesu, najczęściej pracodawcy osoby fizycznej. Co ważne, bank nie przechowuje danych biometrycznych centralnie, tylko na kartach PKI, które są wydawane pracownikom klienta korporacyjnego. Z badań przeprowadzanych przez Barclays wynika, że wszyscy klienci uznali korzystanie z czytnika biometrycznego za łatwe w użyciu i obecnie preferują użycie tej metody uwierzytelniania. W listopadzie 2019 r. Barclays Bank rozszerzył swój system biometryczny o nowej generacji mobilne urządzenia biometryczne oparte na biometrii Finger Vein⁹.

g) Dokonywanie płatności

Latem 2016 r. uruchomiono pierwszy w Wielkiej Brytanii pilotażowy system płatności biometrycznych, FingoPay¹⁰, w którym po raz pierwszy wykorzystano tryb pełnej identyfikacji biometrycznej. Klient nie musi wykorzystywać jakiegokolwiek danej identyfikacyjnej, wystarczy przyłożyć palec do czytnika. Obecnie system jest w trakcie rolloutu w całej Wielkiej Brytanii. W 2019 r. władze Manchesteru ogłosiły, że będzie ono pierwszym miastem na świecie, gdzie zostaną powszechnie wprowadzone płatności biometryczne. Pilotaż płatności ruszył latem 2019 r. w dzielnicach: Spinningfields, Ancoats i King Street. Od stycznia 2019 r. płatności są dostępne na Etihad Stadium, na którym gra klub piłkarski Manchester City. W lutym FingoPay ruszył z pierwszymi

⁹ Źródło: „Barclays and Hitachi launch next-generation finger vein scanner”, Barclays Bank, 22.11.2019

¹⁰ Źródło: „FingoPay” to launch this summer”, Planetbiometrics, 20.07.2016

płatnościami biometrycznymi typu bank-to-bank wspólnie z firmą Reflow. W marcu 2020 r. firma Sthaler, twórca system płatniczego Fingopay, została uznana za 9. najszybciej rozwijającą się firmę w rankingu World's Most Innovative Companies for 2020¹¹.

Wiele banków i instytucji płatniczych umożliwia przeprowadzenie płatności w sklepie telefonem, która jest uwierzytelniana poprzez wykorzystanie mechanizmów biometrycznych wbudowanych w telefon, np. za pomocą FaceID. Z takiej możliwości można skorzystać m.in. w przypadku ApplePay czy Revoluta.

Na podstawie najnowszych badań VISA, 90% badanych osób w Polsce jest pewnych, że w ciągu trzech lat będzie płacić smartfonem i czułoby się bezpieczniej, gdyby do autoryzacji takich transakcji wykorzystywano rozwiązania biometryczne. 83% konsumentów uważa przy tym, że biometria jest bezpieczną formą uwierzytelnienia, a to wzrost o 23 p.p. w stosunku do ubiegłorocznej edycji raportu¹².

Potrzeby i warunki rozpowszechnienia na rynku

Wydaje się, że biometria staje się jednym z czynników koniecznych do bezpiecznego prowadzenia biznesu przez banki, w szczególności jeżeli jest rozważana całościowa transformacja wybranych procesów bankowych do postaci cyfrowej. Sytuacje kryzysowe, takie jak obecny stan epidemii spowodowany przez COVID-19, pokazują potrzebę, jak i potęgę gospodarki cyfrowej. Przy prawidłowo potwierdzonej tożsamości użytkownika systemu teleinformatycznego i bezpiecznym transferze danych wiele czynności możemy wykonać zdalnie. Nie chodzi zatem tylko o działania zwiększające efektywność dotychczasowych procesów, ale też o stworzenie alternatywnych, jak najbardziej bezpiecznych procesów funkcjonowania społeczeństwa i biznesu.

Z punktu widzenia warunków rozwoju istotne są następujące kwestie: prawna możliwość lub nawet konieczność stosowania zabezpieczeń biometrycznych, akceptowalność i przyjazność ich stosowania przez użytkowników, a także decyzyjność i prawidłowe wykonanie systemów biometrycznych.

11 Źródło: „Fingopay named 9th in Europe's most innovative companies 2020”, Fintech TIMES, 16.03.2020

12 Źródło: „Raport Visa: Polacy otwarci na innowacyjne płatności, również z wykorzystaniem biometrii”, 13.02.2018

O ile kwestia akceptowalności społecznej i decyzyjności dotyczącej wdrożeń wydają się uwarunkowane kwestiami faktycznych potrzeb, o tyle warto przybliżyć warunki związane z normami prawnymi. Prawo polskie pod wpływem zmian wynikających z przepisów prawa UE zostało uzupełnione regulacjami coraz bardziej nadążającymi za obecnymi potrzebami i stanem rozwoju bankowości biometrycznej. Jest to widoczne na przykładzie RODO, gdzie zastąpiono przepisy obowiązujące w poprzednim brzmieniu ustawy o ochronie danych osobowych. W nowych regulacjach wprowadzono definicję legalnych danych biometrycznych, a także określono jako dane biometryczne przesłanki kwalifikacji cech fizjologicznych, fizycznych i behawioralnych. Uregulowano także, że dane biometryczne są danymi osobowymi, różnymi od ogólnej kategorii danych osobowych, stanowiąc szczególną kategorię danych osobowych. Ustanowiony też został zakaz przetwarzania szczególnej kategorii danych osobowych, jak również przesłanki jego zniesienia i możliwości przetwarzania danych biometrycznych.

Ponadto regulacje prawne dotyczące bankowości zostały uzupełnione przez przepisy PSD II. Zawierają one postanowienia analogiczne do regulacji SecuRePay, wskazując na możliwość spełnienia wymogów silnego uwierzytelniania w przypadku wykorzystywania danych biometrycznych. W tym obszarze ustanowiono definicję silnego uwierzytelniania, przypadki jego obligatoryjnego stosowania, a także zasady odpowiedzialności odszkodowawczej oraz sposób rozliczania roszczeń wynikających z braku jego stosowania pomiędzy dostawcami usług płatniczych.

Zgodnie z PSD2 „silne uwierzytelnianie” oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów spośród trzech należących do następujących kategorii:

- wiedza (coś, co wie wyłącznie użytkownik),
- posiadanie (coś, co posiada wyłącznie użytkownik),
- inherencja (cecha klienta – coś, czym jest użytkownik).

Powyżej wskazane cechy powinny być niezależne od siebie w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, bo tylko wtedy uwierzytelnianie mogłoby być zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.

Oprócz samej definicji istotne jest doprecyzowanie statuuje kiedy dostawca usług płatniczych powinien wymagać silnego uwierzytelnienia klienta.

Ma to mieć miejsce co najmniej przy dokonywaniu przez użytkownika następujących czynności:

- uzyskiwaniu dostępu do rachunku płatniczego online (np. przez kanały bankowości internetowej lub mobilnej),
- inicjowaniu elektronicznej transakcji płatniczej,
- przeprowadzaniu za pomocą kanału zdalnego czynności, które mogą wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć.

Obszary rozpowszechnienia na rynku

Wydaje się, że zapytania kierowane w ostatnim czasie do firm technologicznych wskazują na trzy nowe obszary szczególnego zastosowania metod biometrycznych: wykorzystaniu precyzyjnych cech biometrycznych (np. Finger Vein) w celu uwierzytelniania transakcji w bankowości korporacyjnej, stworzeniu systemów płatności biometrycznych dostępnych dla klienta masowego (w tym tych zapewniających mechanizmy silnego uwierzytelniania) przy wykorzystaniu infrastruktury klienta (np. smartfonów) oraz wykorzystaniu metod biometrycznych w realizacji idei „paperless”.

Bankowość korporacyjna będzie jednym z głównych odbiorców rozwiązań biometrycznych w najbliższym czasie. Pionier w tym zakresie, Barclays PLC, zdecydował właśnie o rozszerzeniu projektu o kilkadziesiąt tysięcy urządzeń mobilnych Finger Vein. A do grona użytkowników biometrii dołączają kolejne wielkie instytucje finansowe w Unii Europejskiej. Jako główną przyczynę takiego stanu rzeczy należy wskazać ciągły wzrost zagrożenia cyberatakami. Od kilku lat cyberprzestępczość, w tym ataki phishingowe, sięją spustoszenie w sektorze bankowym. W październiku 2017 r. firma analityczna EY podała, że co druga instytucja finansowa deklaruje, iż wystąpiło w niej zjawisko nadużycia popełnione przez cyberprzestępcę. To o 35% więcej niż w 2016 r. i aż o 160% więcej niż w 2016 r.¹³ Potencjalny fraud podczas transakcji korporacyjnej mógłby spowodować nieodwracalne straty finansowe i reputacyjne dla banku. Dlatego też uwierzytelnianie biometryczne w połączeniu z technologiami kryptograficznymi (PKI) wydaje się najlepszym rozwiązaniem dostępnym na rynku w celu zabezpieczenia transakcji korporacyjnych.

¹³ Źródło: „Cyberprzestępczość najszybciej rosnącym zagrożeniem według branży finansowej”, EY, Warszawa, 24.10.2017 r

Bankowość mobilna

Wykorzystanie biometrii w bankowości mobilnej jest bardzo popularne. Wpływ na to miało wyposażenie smartfonów w czytniki linii papilarnych lub dobrej jakości kamer. Niestety, ze względu na niski poziom bezpieczeństwa, jak również brak kontroli nad danymi biometrycznymi, biometria nie jest obecnie wykorzystywana do autoryzacji operacji. Czytnik biometryczny jest kolejną „usługą” w telefonie – bank nie ma możliwości kontroli nad procesem uwierzytelniania, a jedynie otrzymuje wynik tej operacji. Kolejnym problemem jest brak ujednoliconej metody uwierzytelniania, co ma związek z różnorodnością modeli telefonów i wbudowanych mechanizmów biometrycznych. Właśnie w tym zakresie widać największy potencjał. Wg. danych podanych przez Prnews.pl pod koniec 2017 r., banki miały blisko 9 mln użytkowników bankowości mobilnej, co oznacza wzrost o 2 mln w porównaniu do 2016 r.¹⁴ W październiku 2016 r. japońska firma Hitachi podała do wiadomości, iż opracowała prototyp nowej technologii biometrycznej opartej na biometrii naczyń krwionośnych palca umożliwiającą wykorzystanie jej w dowolnym smartfonie. Rozwiązanie to korzysta bowiem z kamery wbudowanej w smartfon i nie potrzebuje żadnych dodatkowych urządzeń. W celu zwiększenia bezpieczeństwa bazuje ono na czterech palcach, a nie na jednym, a dodatkowo poza strukturą naczyń krwionośnych wykorzystuje również wzór struktury skóry. Rozwiązanie produkcyjne ma być wprowadzone na rynek w drugiej połowie 2020 r. i być dostępne na platformach iOS, Android i Windows.

Paperless

Transformacja cyfrowa jest jednym z najważniejszych zagadnień w świecie papieru. Jednakże wg światowych badań 80% dokumentów jest dalej procesowana w formie papierowej. Rozwiązaniem tego problemu miało być zastosowanie podpisu elektronicznego, do stosowania którego przez wiele lat konieczne było posiadanie karty mikroprocesorowej. Regulacja eIDAS pozwala jednak na upowszechnienie podpisów zdalnych i popularyzację idei samego podpisu. Należy jednak zwrócić uwagę na aspekt bezpieczeństwa i zadać sobie pytanie, czy kod PIN lub token jest odpowiednim zabezpieczeniem

¹⁴ Źródło: „Raport PRNews.pl: Rynek bankowości mobilnej – IV kw. 2017”, Prnews.pl, 27.02.2018

operacji składania podpisu. Naturalnym wyborem wydaje się być biometria, bo dotychczas to właśnie ona, poprzez analizę naczyń krwionośnych bądź podpisu odręcznego, zastępowała nam właśnie kod PIN. Sama operacja składania podpisu odbywała się za pomocą karty bądź poprzez HSM (Hardware Security Module) w infrastrukturze banku. Od wielu lat zastanawiano się jednak czy dana biometryczna nie mogłaby zastąpić klucza prywatnego. Barierą był fakt zmieniających się próbek biometrycznych, bo podczas pomiaru istotną rolę odgrywa poziom natężenia światła, oraz konsekwencje ewentualnej utraty klucza. Naukowcy z Japonii opracowali jednak nowe rozwiązanie, które może stać się prawdziwą rewolucją w świecie biometrii i motorem napędowym idei „Paperless”, jak i stosowania samego podpisu elektronicznego. Tą technologią jest Public Biometric Infrastructure (PBI). Jego koncepcja polega na tym, aby klucz prywatny jest powiązany z uśrednioną wartością biometryczną uwzględniającą wszelkiego rodzaju wahania podczas pomiaru. Z otrzymanej w ten sposób danej nie da się ekstrahować danej biometrycznej, podobnie jak klucza prywatnego bez obecności użytkownika posiadającego tę daną. Pierwsze wdrożenia pilotażowe tej technologii zostały wdrożone w Japonii w latach 2018-2019, m.in. przez drugiego największego operatora telekomunikacyjnego w Japonii, firmę KDDI¹⁵. Do płatności i podpisywania transakcji została wykorzystana technologia PBI. Dane transakcji były przechowywane w sieci blockchainowej opartej o Hyperledger Fabric.

Uwierzytelnianie na stacjach roboczych

Logowanie do stacji roboczych lub systemów i domeny było swego czasu jednym z podstawowych zastosowań biometrii. W niektórych laptopach były zaimplementowane podstawowe czytniki linii papilarnych, ale bardziej w formie gadżetu niż do profesjonalnych zastosowań. Niektóre firmy, np. Hitachi, Fujitsu czy Morpho, wprowadziły na rynek czytniki biometryczne USB do zastosowania w komputerach PC. Były one stosowane przez wiele instytucji do logowania do systemów krytycznych ze względu na wysokie bezpieczeństwo, jak i wygodę, chociażby ze względu na brak konieczności pamiętania haseł. Jednakże w rozpowszechnieniu biometrii przeszkadzał wysoki koszt inwestycji związanej z zakupem dodatkowych urządzeń biometrycznych.

¹⁵ Źródło: „Hitachi and KDDI trial biometric payments on blockchain”, FintechFutures, 26.07.2018

W najbliższym czasie może jednak nastąpić rewolucja w tej dziedzinie. We wrześniu 2019 r. firma Hitachi ogłosiła wprowadzenie nowej technologii biometrycznej, tzw. „hand gesture biometric”¹⁶. Umożliwia ona zalogowanie do stacji roboczych poprzez proste podniesienie dłoni. System bazuje na technologii Finger Vein i wykorzystuje kamerę wbudowaną w laptopach. Biorąc pod uwagę masowe przejście na tzw. „pracę zdalną”, zabezpieczenie laptopów służbowych uwierzytelnianiem biometrycznym wydaje się być naturalnym kierunkiem.

W związku z powyższym wydaje się, że biometria może być narzędziem zwiększającym poziom bezpieczeństwa transakcji finansowych spełniającym wymogi prawne, a przy możliwości zastosowania jej na powszechnie używanych telefonach komórkowych czy tabletach, może w najbliższym czasie wyznaczyć kolejne standardy obsługi klienta i narzędzia dla kanałów dystrybucji produktów bankowych.

16 Źródło: „Hitachi’s new hand gesture biometric technology raises the bar for computer security”, Hitachi, 10.09.2019