Warszawa, 2015

Raport

Biometria w bankowości – kluczowe aspekty

Związek Banków Polskich

FTB FORUM TECHNOLOGII BANKOWYCH

CENTRUM PRAWA NOWYCH TECHNOLOGII

Redakcja:

Tadeusz Woszczyński

Współautorzy:

Michał Czechowski, Łukasz Hnatkowski, Artur Krystosik, Zbigniew Marcinkowski, Mariusz Sudoł, Jarosław Wójtowicz

Spis treści

Spis treści 1
1. WSTĘP 2
2. REKOMENDOWANE OBSZARY ZASTOSOWANIA TECHNOLOGII BIOMETRYCZNYCH 3
3. BIOMETRIA W POLSKIM SEKTORZE BANKOWYM (UWARUNKOWANIA, WDROŻENIA) 4
3.1. WDROŻENIA, STATYSTYKI, TŁO BIZNESOWE 4
3.2. ASPEKTY PRAWNE 6
4. TECHNOLOGIE BIOMETRYCZNE W BANKOWOŚCI 7
4.1. BIOMETRIA FINGER VEIN 7
4.2. BIOMETRIA GŁOSOWA 8
4.3. BIOMETRIA PODPISU ODRĘCZNEGO 9
4.4. INNE TECHNOLOGIE BIOMETRYCZNE W BANKOWOŚCI O MNIEJSZYM STOPNIU POWSZECHNOŚCI W EUROPIE 10
5. KRYTYCZNE PARAMETRY DOBORU TECHNOLOGII DO DANEGO ZASTOSOWANIA 12
6. ODPORNOŚĆ NA FAŁSZERSTWA, ZABEZPIECZENIA, ZAGROŻENIA, WYKLUCZENIA 14
7. KORZYŚCI 16
9. ZAKOŃCZENIE 18
10. AUTORZY 19
10.1. REDAKCJA 19
10.2. WSPÓŁAUTORZY 19

1. WSTĘP

Rozwój nowoczesnych technologii stosowanych w bankowości, postępująca automatyzacja umożliwiająca uproszczenie, zwiększenie efektywności oraz transparentność procesów bankowych, ciągła konieczność minimalizacji ryzyka operacyjnego to tylko przykłady zjawisk związanych z jakże podstawowym - a nadal aktualnym i stanowiącym wyzwanie - **obowiązkiem banków**, jakim jest konieczność **zapewnienia bezpieczeństwa** zgromadzonych w nim depozytów, ochrony informacji objętych tajemnicą bankową, należytego zabezpieczenia systemów teleinformatycznych oraz dokonywanych przy ich użyciu operacji bankowych.

> Jak pokazuje praktyka rynkowa, można zaobserwować zwiększone zainteresowanie nowymi metodami zabezpieczeń

Pomimo rozwoju różnorodnych systemów zabezpieczeń, analiza ryzyka wydaje się wykazywać, iż środki stosowane dotychczas nadal nie są w pełni zadowalające. Stąd też, jak pokazuje praktyka rynkowa, można zaobserwować **zwiększone zainteresowanie nowymi metodami zabezpieczeń**.

Nasze doświadczenie pokazuje, że jeszcze 4-5 lat temu wśród bankowców panowała opinia, jakoby wykorzystywanie technologii biometrycznych było ciekawą "nowinką technologiczną", której zastosowanie mogłoby być rozpatrywane w dalekiej, bliżej nieokreślonej przyszłości. Tymczasem, w chwili obecnej, **wykorzystywanie technologii biometrycznych jest faktem**.

Okazuje się, że wybrane procesy bankowe są wykonywane przy wykorzystaniu biometrii **w ponad 30 bankach w Polsce**, a rozmowy dotyczące możliwości zastosowania technologii biometrycznych prowadzone są przez dostawców tych technologii z niemalże każdym bankiem.

Celem niniejszego *Whitepaper* jest przedstawienie zarysu najbardziej użytecznych technologii biometrycznych na potrzeby przygotowania *stricte* **praktycznego dokumentu na użytek wyższej kadry zarządzającej**. Jest to kolejny dokument przygotowany przez Grupę ds. Biometrii, która od 2007 roku funkcjonuje w Forum Technologii Bankowych ZBP. W założeniu, w przeciwieństwie do poprzednich dokumentów wydanych przez nas, nie ma to być rozbudowany, wyczerpujący raport. Tym razem, naszą intencją było przygotowanie krótkiego zestawienia prezentującego **podstawowe, lecz istotne informacje** adresowane do decydentów rozważających stosowanie metod biometrycznych w danej organizacji.

Wybór poszczególnych metod biometrycznych został dokonany na podstawie zaobserwowanych tendencji rynkowych oraz cech biometrycznych, dla których upatruje się **najszersze, najciekawsze**, czy wreszcie **najbardziej akceptowalne społecznie zastosowanie zwiększające poziom bezpieczeństwa w bankach**.

2. REKOMENDOWANE OBSZARY ZASTOSOWANIA TECHNOLOGII BIOMETRYCZNYCH

Poniższy rysunek przedstawia nasze rekomendacje dotyczące zastosowania danej technologii biometrycznej w konkretnych obszarach funkcjonalnych w banku:

3. BIOMETRIA W POLSKIM SEKTORZE BANKOWYM (UWARUNKOWANIA, WDROŻENIA)

3.1. WDROŻENIA, STATYSTYKI, TŁO BIZNESOWE

Rys. Kampania reklamowa bankomatów biometrycznych sieci PlanetCash
Źródło: IT Card S.A.

W 2007 roku powstała Grupa ds. Biometrii w Forum Technologii Bankowych Związku Banków Polskich, mająca na celu edukację sektora bankowego w zakresie zastosowań biometrii. Dzięki intensywnym działaniom grupy, ZBP i dostawców w 2009 roku pierwsze banki zdecydowały się przetestować zastosowanie biometrii w obszarze bankomatów. Były to Podkarpacki Bank Spółdzielczy (PBS) oraz Bank Polskiej Spółdzielczości (BPS).

W 2010 roku PBS jako pierwszy bank w Europie wdrożył produkcyjnie biometrię (dokladnie biometrię naczyń kwrionośnych palca) w swoich bankomatach w celu usprawnienia wypłat świadczeń społecznych. Obecnie bank oferuje biometrię (Finger Vein) wszystkim swoim klientom. Biometria jest wdrożona w całej sieci bankomatów (biometryczne wypłaty bez karty) i placówek banku (autoryzacja operacji w oddziale). Sektor spółdzielczy jest obecnie największym odbiorcą biometrii w Polsce. Poza bankiem PBS, z biometrii korzystaja m.in. klienci Krakowskiego Banku Spółdzielczego, Banku Spółdzielczego w Kielcach, Powiślańskiego Banku Spółdzielczego w Kwidzynie i w wielu innych.

W czerwcu 2010 roku Bank PEKAO SA wprowadził dla swoich klientów korporacyjnych czytniki biometryczne bazujące na biometrii linii papilarny palca (FingerPrint) wraz z kartami PKI. Od tego czasu klienci korzystający z internetowej platformy transakcyjnej PekaoBIZNES24 mogą na podstawie odcisków palców logować się do systemu i autoryzować zlecenia.

We wrześniu 2012 roku Bank BPH S.A. wprowadził uwierzytelnianie biometryczne do wszystkich swoich placówek. Klienci banku mogą weryfikować swoją tożsamość i autoryzować operacje kasowe przy pomocy palca (biometria Finger Vein). Obecnie Bank BPH rozwija rozwiązanie o całą sieć franczyzową, a biometria staje się główną metodą uwierzytelniania w banku.

> W 2009 roku pierwsze banki zdecydowały się przetestować zastosowanie biometrii w obszarze bankomatów

Takie samo rozwiązanie w 2013 roku wdrożył Getin Bank we wszystkich swoich nowych oddziałach. W lutym 2014 Getin Bank wprowadził rewolucję poprzez samoobsługowe placówki Getin Point, w których klient przy pomocy biometrii naczyń krwionośnych palca (Finger Vein)

mógł zalogować się do swojej placówki, autoryzować operacje i podpisywać dokumenty. Podpis biometryczny został uruchomiony również w tradycyjnych placówkach, gdzie wcześniej funkcjonowała już biometria.

W maju 2014 roku IT Card S.A. ogłosił wprowadzenie na rynek pierwszej w Europie niezależnej sieci bankomatów biometrycznych PlanetCash. W lutym 2015 Bank Smart ogłosił wprowadzenie biometrii głosowej, jako sposób logowania do swojej bankowości mobilnej.

Biometrię głosową stosuje też Meritum Bank. Meritum Bank jak i Bank Millennium wprowadziły możliwość logowania do bankowości mobilnej przy pomocy czytnika linii papilarnych wbudowanego w smartphony.

W kwietniu 2015 roku, jeden z największych banków w Polsce - Bank Zachodni WBK, pilotażowo wprowadził do swoich oddziałów rozwiązanie podpisu biometrycznego opartego na biometrii Finger Vein. Klienci BZ WBK w Lubinie jak również w wybranych Oddziałach w Warszawie, Wrocławiu i Poznaniu mogli weryfikować swoją tożsamość i podpisywać umowy dotyczące konta osobistego z bankiem przy pomocy swojego palca.

W czerwcu 2015 swój projekt badawczy przygotowywany wspólnie z Politechniką Gdańską, ogłosiło PKO BP. Bank chce opracować rozwiązanie, w którym klienci PKO BP zamiast PIN-em czy hasłem będą mogli potwierdzać swoją tożsamość głosem, dłonią lub wizerunkiem twarzy. Pierwsze rezultaty mają być znane w 2018 roku.

W Polsce zaimplementowanych jest już ponad 1700 bankomatów biometrycznych, z czego ponad 300 należy do sektora spółdzielczego (Grupa BPS i SGB), a 1400 do niezależnej sieci PlanetCash. W ciągu najbliższych miesięcy sieć PlanetCash zwiększy liczbę bankomatów biometrycznych do 1780 maszyn.

> Im większa jest popularność biometrii wśród klientów, tym bardziej bank może ograniczyć wyłudzenia

Bank BPH posiada 256 placówek wyposażonych w czytniki biometryczne (ok 1700 czytników). Liczba ta rozszerzy się o 172 placówki partnerskie już w 2015 roku. Bank BPH posiada już ponad 160 tysięcy aktywnych klientów biometrycznych, a bank PBS ok. 20 000 klientów. Biometria jest wdrożona w Polsce w 6 bankach komercyjnych oraz ponad 30 bankach spółdzielczych. Przewiduje się, że liczba ta może co najmniej podwoić się w 2016 roku. Banki ogłosiły szereg postępowań zakupowych oraz programów pilotażowych na zastosowanie biometrii w call center, bankowości mobilnej, bankowości internetowej i w oddziałach. Wg. badań opinii społecznych przeprowadzonych na zlecenie dwóch czołowych banków komercyjnych w Polsce (w 2010 oraz 2013 roku), akceptowalność biometrii (dokł. Biometrii Finger Vein) do zastosowań w oddziałach bankowych wyniosła ok. 85%.

Przyczyn wzrostu popularności biometrii w Polsce należy szukać przede wszystkim we wzroście zagrożeń i liczby fraudów w bankach. Wykorzystując biometrię w oddziałach bankowych do uwierzytelniania operacji zarówno przez klientów jak i pracowników oddziałów, bank jest w stanie ograniczyć praktycznie całkowicie fraudy wewnętrzne w oddziałach, które stanowią coraz dotkliwszy problem. Im większa jest popularność biometrii wśród klientów, tym bardziej bank może ograniczyć wyłudzenia przy pomocy skradzionych dokumentów lub fraudy wynikające z fałszywej tożsamości (np. podrobiony dowód). Przy zastosowaniu biometrii

> Projekty prowadzone w Polsce odbiły się szerokim echem nie tylko w kraju, ale i na całym świecie

wraz z podpisem elektronicznym do podpisywania dokumentów znacząco można ograniczyć ich koszt (w tym papieru, wydruków i archiwizacji). Banki Spółdzielcze usprawniły pracę oddziałów przenosząc wypłaty zasiłków społecznych do bankomatów biometrycznych oraz ograniczyły koszty wypłat kartami dzięki wprowadzeniu „wypłat na palec". Biometria głosowa daje dużą wygodę w kontaktach z Bankiem poprzez call center, redukując jednocześnie zagrożenie fraudami. Należy wspomnieć też aspekcie marketingowym wprowadzenia biometrii. Projekty prowadzone w Polsce odbiły się szerokim echem nie tylko w kraju, ale i na całym świecie.

3.2. ASPEKTY PRAWNE

Niezwykle istotną rolę w zakresie możliwości wykorzystania i implementacji technologii biometrycznych stanowi proces przygotowywania analiz dopuszczalności stosowania tych technik przez obowiązujące normy prawne. Należy je przygotować indywidualnie pod każdy przypadek planowanego wdrożenia.

Ze względu na istotę i charakter danych biometrycznych dotychczasowe prace obejmowały analizy przeprowadzone w zakresie sfery administracyjno-prawnej związanej m.in. z przepisami o ochronie danych osobowych, jak i cywilno-prawnej – przy bardziej zaawansowanych projektach - związanej z koniecznością zapewnienia prawnej skuteczności oświadczeń woli składanych przy wykorzystaniu danej technologii.

Zebrane dotychczas doświadczenia w zakresie wykonanych prac projektowych pozwalają stwierdzić o pozytywnym ustosunkowaniu się zarządów banków do przeprowadzonych dotychczas analiz. Według najlepszej wiedzy autorów, wybrany zakres wdrożenia jednej z technologii biometrycznych w banku działającym w Polsce stanowił także przedmiot kontroli przeprowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych, zakończonej pozytywnym rezultatem dla tego banku.

Niemniej jednak, podkreślenia wymaga fakt, że przy każdorazowej ocenie dopuszczalności stosowania danej technologii biometrycznej - oprócz szczegółowej analizy norm prawnych - wymagana jest dogłębna analiza stanu faktycznego, wyrażającego się m.in. w szczegółowym opisie rodzaju mających mieć zastosowanie danych biometrycznych, określeniu zakresu i sposobu wykorzystywania biometrii, procesów do których ma być ona stosowana, wpływu wybranej metody biometrycznej na prywatność użytkowników systemu biometrycznego, aspektów technicznych i zagadnień z zakresu bezpieczeństwa, czy też sposobu implementacji przez danego dostawcę takiej technologii.

Wydaje się, że dopiero suma przeprowadzonych analiz, obejmujących m.in. wszystkie wskazane obszary istotne dla dokonania oceny prawnej dopuszczalności danego wdrożenia i związana z tym konieczność ścisłej i stałej współpracy z dostawcą technologii biometrycznej, pozwala na zakończenie implementacji z pełnym sukcesem.

Dlatego też przy ocenie ryzyk prawnych uzasadnionym wydaje się oprócz oceny prawnej (regulacyjnej) dopuszczalności zastosowania danej technologii biometrycznej, efektywności kosztowej danego rozwiązania, konieczność rozważenia dotychczasowego doświadczenia i zasobów danego dostawcy technologii biometrycznej i dokonanie oceny jego wdrożeń. Przy

dokonywaniu zmian tak istotnych procesów dla działalności banku jak chociażby uwierzytelnianie tożsamości, nie sposób bowiem pomiąć i kształtować te procesy bez skorzystania z praktyk proponowanych przez dostawców.

Ponadto, kompleksowe podejście do projektu i analizy prawnej pozwala powziąć dużo większe przekonanie banku, iż zobowiązania wynikające z umów wdrożeniowych łączących bank z dostawcą zostaną należycie i terminowo wykonane, co wydaje się kluczowe pełnej analizy i dla sukcesu wdrożenia.

4. TECHNOLOGIE BIOMETRYCZNE W BANKOWOŚCI

Technologie biometryczne zyskują coraz większą popularność i obszary zastosowań. Z roku na rok przedstawiane są coraz nowsze technologie biometryczne wykorzystujące różne unikalne cechy fizyczne bądź behawioralne człowieka. Najbardziej znanymi technologiami biometrycznymi na świecie są niewątpliwie: biometria tęczówki oka oraz biometria linii papilarnych palca. Jednakże obie te technologie nie znalazły powszechnego zastosowania w bankowości zarówno w Europie jak i w Polsce. Aby zastosować biometrię w sektorze bankowym musi ona łączyć następujące cechy:

- Wysokie bezpieczeństwo
- Ochronę prywatności
- Wysoką akceptowalność społeczną
- Praktyczność i wygodę użytkowania
- Uniwersalność

Na podstawie tendencji z rynku polskiego, do opisania w niniejszym rozdziale zostały wybrane i szczegółowo opisane 3 technologie, w tym:

- Technologię najczęściej wdrażaną w Polsce w oddziałach i bankomatach (biometria Finger Vein)
- Technologię, którą szereg banków w Polsce planuje wdrożyć lub wdrożyło w rozwiązaniach call center i bankowości mobilnej (biometria głosowa)
- Technologię, które wzbudza zainteresowanie banków jednakże dalej wzbudza wiele pytań (biometrię podpisu odręcznego).

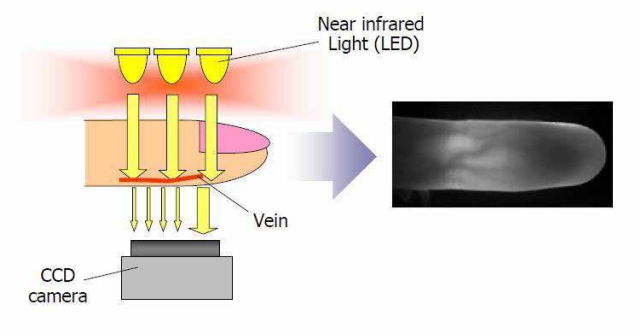
Należy zwrócić uwagę, iż powyżej wybrane technologie są rozważane w kontekście relacji klient – bank.

> Technologie biometryczne zyskują coraz większą popularność i obszary zastosowań

4.1. BIOMETRIA FINGER VEIN

Biometria naczyń krwionośnych palca *(ang. Finger Vein)* wykorzystuje **unikalny wzór naczyń krwionośnych znajdujących się wewnątrz ludzkiego palca**. Unikalność technologii została udowodniona kompleksowymi badaniami medycznymi. Badania te udowodniły uniwersalność biometrii naczyń krwionośnych palca, co oznaczało, że może ona być wykorzystana przez wszystkich, bez względu na rasę i wiek, co było problemem wśród innych technologii biometrycznych (np. biometrii tęczówki oka). Wzór naczyń krwionośnych wykorzystany w procesie uwierzytelniania nie zmienia się przez całe życie, chyba iż ma na niego wpływ choroba. Wzór naczyń krwionośnych jest pobierany poprzez naświetlenie palca światłem bliskiej podczerwieni, które jest nieszkodliwe i powszechnie stosowane w medycynie. Podczas rejestracji

powstaje unikalny, referencyjny wzorzec biometryczny. Wzorzec biometryczny powstaje w sposób jednokierunkowy i nie zawiera żadnych danych wrażliwych. Podczas weryfikacji biometrycznej, żywy palec jest porównywany w czasie rzeczywistym z zapisanym wcześniej wzorcem referencyjnym. Dzięki temu, że dana biometryczna znajduje się wewnątrz ludzkiego ciała, technologia ta zapewnia ochronę prywatności użytkowników, co zostało potwierdzone przez szereg organizacji ochrony danych osobowych (np. CNIL we Francji). Kluczową przewagą tej technologii jest wysoka akceptowalność społeczna wynoszą w Polsce ok 85%, co zostało potwierdzone licznymi badaniami.



Rys. Unikalny wzór naczyń krwionośnych palca wykorzystany w technologii Finger Vein

Technologia Finger Vein powstała pod koniec lat 90-tych w Japonii. Została ona stworzona i opatentowana przez japońską firmę Hitachi. Głównym celem tej technologii było stworzenie alternatywy dla biometrii linii papilarnych palca, która ze względu na wiele wad i kontrowersji z nią związanych nie przyjęła się w społeczeństwie japońskim. Biometria Finger Vein została wykorzystana w największych projektach bankowych na świecie. W Japonii biometria Finger Vein jest wykorzystana w 293 bankach (m.in. Mizuho Bank, SMBC, Japan Post Bank, Bank of Kyoto, CITI, HSBC itd.) i wdrożona w ponad 80 tysiącach bankomatów. Korzysta z niej ponad 50 mln klientów bankowych w Japonii. W 2010 roku IS Bankasi wdrożył ponad 3000 bankomatów biometrycznych („Biyokimlik") w oparciu o technologię Finger Vein. W 2014 Bank Barclays ogłosił wdrożenie technologii Finger Vein do bankowości korporacyjnej i przekazania swoim klientom 30 000 czytników. Od 2009 roku technologia ta jest stosowana w Polsce. Wdrożyły ją i rozwijają 2 banki komercyjne (BPH SA i Getin Bank) oraz ok. 30 banków spółdzielczych. W Polsce funkcjonuje też pierwsza niezależna sieć bankomatów biometrycznych stosująca Finger Vein – PlanetCash. W 2015 Bank BZ WBK wdrożył pilotażowo czytniki biometryczne Finger Vein wraz z ekranami dotykowymi dla klienta w 6 swoich oddziałach do podpisywania dokumentów.

4.2. BIOMETRIA GŁOSOWA

"W moim banku mój głos jest moim hasłem" - tak może brzmieć hasło dostępowe w nowoczesnym bankowym IVR zamiast TelePINu. Hasło dla wszystkich jest takie samo, więc nie ma potrzeby ukrywania go.

W modzie jest ostatnio wyłączanie usług IVR i w tym przypadku również biometria głosowa może bardzo pomóc. Wystarczy, że klient wyrazi zgodę na założenie profilu głosowego i podczas kolejnych rozmów będzie uwierzytelniany automatycznie podczas zwykłej rozmowy z konsultantem bez używania hasła głosowego w IVR. Z takiej metody biometrii głosowej korzystają dziś takie banki jak Tatra Banka, Barclays czy ostatnio amerykański bank Eastern Bank.

Rys. Biometria głosowa

Biometria głosowa chętnie jest też wykorzystywana w aplikacjach mobilnych jako alternatywne do pinów lub dodatkowe zabezpieczenie dostępu do bankowości mobilnej. Najlepsze rozwiązania pozwalają wykorzystać jeden profil biometryczny w kilku kanałach np. zakładając profil w IVR można wykorzystać go w bankowości mobilnej.

> Ilość nadużyć stale rośnie, a do Call Center dzwonią nie tylko nasi klienci, ale również i oszuści

Banki na świecie coraz częściej stosują weryfikację klientów po głosie, gdyż ten jest unikalny i zapewnia jednocześnie wysokie bezpieczeństwo oraz wygodę dostępu do usług. Przykładami mogą być Bank ING w Rumunii, Tatra Banka na Słowacji czy choćby Barclays w Wielkiej Brytanii.

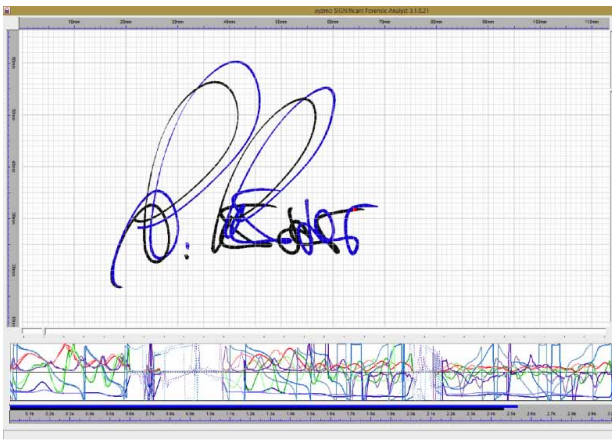
Dziś jest to jedyna dostępna i skuteczna metoda biometrycznej weryfikacji osób na odległość.

W listopadzie 2014 roku TNS przeprowadził w Polsce badania, z których wynika, że 54% osób chętnie skorzystałoby z biometrii głosowej zamiast haseł czy pinów a kolejne 23% nie ma zdania na ten temat, co oznacza, że stosując odpowiednią edukację można i takich użytkowników przekonać do weryfikacji głosowej. To bardzo pozytywna wiadomość dla wszystkich instytucji w Polsce planujących wykorzystanie biometrii głosowej. Porównując te badania z badaniami przeprowadzonymi w innych krajach europejskich, Polska wypada na ich tle dużo lepiej.

Rozwiązania biometrii głosowej sprawdzają się nie tylko w obszarze uwierzytelniania klientów, ale coraz częściej wykorzystywane są w procesach antyfraudowych. Ilość nadużyć stale rośnie a do Call Center dzwonią nie tylko nasi klienci, ale również i oszuści. Równolegle z zagrożeniami ze strony zorganizowanych grup przestępczych, działających w obszarze bankowości elektronicznej, działają również takie, które atakują Call Center. Dzięki biometrii głosowej możemy skutecznie przeciwdziałać tego typu atakom, wykorzystując nagrane rozmowy telefoniczne w Call Center.

4.3. BIOMETRIA PODPISU ODRĘCZNEGO

Podpis odręczny był i będzie jeszcze długo stosowany w kontaktach z wieloma instytucjami. Każdy z nas ma swój indywidualny charakter pisma, inaczej trzymamy pióro, piszemy z różną szybkością i każdy z nas z inną siłą naciska na podłoże. To tylko kilka indywidualnych cech wykorzystywanych przez grafologa, a ma on do dyspozycji kilkadziesiąt parametrów podczas pracy nad podpisem.



Rys. Dane biometryczne dla biometrii podpisu odręcznego

Rozwiązania biometrii podpisu odręcznego zwykle wykorzystują jedynie kilka cech takich jak siła nacisku, ruch pióra nad podłożem, prędkość pisania, przyspieszenie, kąt pisania, zmiana kąta. Zestaw tych parametrów jest na tyle rozbudowany, że możemy skutecznie tworzyć profile biometryczne podpisujących się osób.

Wykorzystanie elektronicznego podpisu odręcznego w niczym nie zaburza pracy grafologa. Może on z powodzeniem pracować na wydruku podpisu odręcznego a jeśli potrzebna będzie dokładniejsza analiza, dodatkowe wspomniane parametry zebrane elektronicznie jak siła nacisku, czy odwzorowanie ruchu pióra nad podłożem, pomagają mu jedynie w analizie podpisu.

> Coraz większe możliwości, jak również niskie koszty powodują, iż biometria podpisu odręcznego jest coraz częściej stosowana

Podpis odręczny umożliwia przede wszystkim pozbycie się papieru w procesach bankowych bez wprowadzania zmian w procesach biznesowych - zachowujemy krok, jakim jest złożenie podpisu i postępujemy zgodnie z już obecnym procesem. Dużą zmianą jest brak przetwarzania dokumentacji papierowej, co przyspiesza procesy, obniża koszty i dodatkowo zabezpiecza transakcję przez weryfikację biometryczną osób w czasie rzeczywistym. Jedną z wielu zalet tej metody jest standaryzacja dokumentów, gdyż wykorzystuje się w tym celu otwarty format dokumentu PDF opatrzony znacznikami czasu i zabezpieczony przed wprowadzaniem zmian. Taki dokument ma wszelkie cechy oryginalnego dokumentu papierowego.

Jednym z banków, który wykorzystał z powodzeniem elektroniczny podpis odręczny jest Tatra Banka na Słowacji. Głównym celem banku była automatyzacja weryfikacji klientów na podstawie podpisu odręcznego w oddziale i zwiększenie przez to bezpieczeństwa transakcji. Ważny dla zarządu banku był również aspekt łatwości wprowadzenia tej metody w oddziałach i szkolenie kadry obsługującej klientów.

Elektroniczny podpis odręczny stosowany jest również w takich instytucjach jak: Poczta Włoska, Unicredit Włochy, Intesa San Paolo Bank, GE Money Bank w Czechach, Raiffeisen Bank, T-Mobile USA, KPN, Vodafone. To tylko niektóre przykłady.

Technologia rozwija się tak szybko, że dziś możemy wykorzystać nie tylko specjalizowane pady do zbierania podpisów odręcznych, ale wykorzystać również urządzenia mobilne i tablety. Coraz więcej urządzeń posiada wbudowane matryce czułe nie tylko na dotyk ale również na siłę nacisku. Jeśli urządzenie nie ma takiej funkcjonalności, to możemy wykorzystać również specjalne elektroniczne pióro, które zarejestruje nacisk pisania. Coraz większe możliwości, jak również niskie koszty powodują, iż biometria podpisu odręcznego jest coraz częściej stosowana. Na tą chwilę główną przeszkodą w powszechnym zastosowaniu tej biometrii jest wciąż niskie bezpieczeństwo (współczynnik fałszywej akceptacji FAR wynosi ok 1,2%).

4.4. INNE TECHNOLOGIE BIOMETRYCZNE W BANKOWOŚCI O MNIEJSZYM STOPNIU POWSZECHNOŚCI W EUROPIE

Na świecie wykorzystuje się też inne technologie biometryczne w bankowości, które jednak nie zyskały znaczącej popularności w projektach bankowych w Europie, w tym w Polsce. Przykładem takiej technologii jest biometria linii

> Biometria linii papilarnych to jedna z najdłużej wykorzystywanych metod weryfikacji tożsamości

papilarnych (Finger Print), która jest powszechnie stosowana w brazylijskim sektorze bankowym. W Indiach i krajach afrykańskich wdraża się odcisk palca do uniemożliwienia zakładania rachunków bankowych na podstawie fałszywej tożsamości. W Europie oraz Japonii odcisk palca jest jednak odrzucany ze względu na kontrowersje związane z ochroną prywatności i niską akceptowalność społeczną. Kolejnym przykładem jest biometria naczyń krwionośnych dłoni (Palm Vein). Technologia ta jest stosowana przez jedne z największych banków Japonii (Bank of Tokyo Mitsubishi), Brazylii (Banco de Bradesco) i Turcji (Ziraat Bankasi). Mimo to, przede wszystkim ze względów praktycznych, nie rozpowszechnia się ona w Europie. Poniżej krótko opisano obie te technologie:

- **Biometria linii papilarnych** *(ang. Finger Print)*

  Jest to jedna z najdłużej wykorzystywanych metod weryfikacji tożsamości. Opiera się na wykorzystaniu analizy wzorca odcisku linii papilarnych, który jest unikalny i różny dla każdego palca każdej dłoni dla każdej osoby. Pomiar linii papilarnych, jako cechy biometrycznej może być wykonany przy użyciu czytnika linii papilarnych (ultradźwiękowego, pojemnościowego lub optycznego), który pozwala na stwierdzenie identyczności odcisków palców na podstawie zbieżności 12 elementów (zwanych detalami lub minucjami).

  Metoda biometryczna oparta o badanie linii papilarnych jest wygodna i cechuje się względnie wysoką niezawodnością (czytniki niewielkich rozmiarów rejestrują obraz linii z dużą dokładnością), a co więcej jest powszechnie znana. Z drugiej natomiast strony przy dokonywaniu pomiaru mogą nastąpić błędy na skutek mechanicznych uszkodzeń (np. wysuszenie, pęknięcie) lub zabrudzeń palca(np. tłuszcz), zmiany jego kształtu z upływem lat lub chociażby przesunięcia palca na skanerze. Technologia ta jest hamowana m.in. przez jej negatywne postrzeganie w kontekście historycznym oraz obawy przed możliwością kradzieży tożsamości. Wykorzystanie danych biometrycznych w oparciu o linie papilarne palca wzbudza też kontrowersje prawne związane z możliwością identyfikacji człowieka bez jego wiedzy. W ostatnich latach technologia biometryczna przeżywa jednak swego rodzaju „reinkarnację" ze względu na powszechność smartphonów i tabletów w których umożliwiono logowanie właśnie poprzez tą technologię biometryczną.

- **Biometria naczyń krwionośnych dłoni** *(ang. Palm Vein)*

  Metoda ta opiera się na badaniu danych ludzkiej dłoni, wykorzystuje jednak nie zewnętrzną powierzchnię, a znajdujące się w wewnątrz organizmu naczynia krwionośne, których układ jest unikalny i stały. Dana biometryczna weryfikowana jest za pomocą światła bliskiej podczerwieni, które naświetla dłoń i uzyskuje informację dzięki właściwościom hemoglobiny. Pozyskany wzorzec nie może stanowić podstawy do odtworzenia naczyń krwionośnych. Technologia ta jest uznawana za nieinwazyjną i nienaruszającą prywatność użytkowników ze względu na niebezpośrednie badania danej znajdującej się wewnątrz organizmu weryfikowanej osoby.

  Podobnie jak biometria linii papilarnych, biometria naczyń krwionośnych dłoni jest wygodna, akceptowalna społecznie, redukuje koszty banku, jest dokładna, ale również jej stosowanie nie zagraża zdrowiu użytkownika. Jednakże przede wszystkim ze względów praktycznych nie rozpowszechniła się w instytucjach finansowych w Europie.

5. KRYTYCZNE PARAMETRY DOBORU TECHNOLOGII DO DANEGO ZASTOSOWANIA

Aby wdrożenie w banku odniosło oczekiwany sukces, należy dobrać technologię biometryczną i rozwiązanie spełniające kryteria dla danego obszaru zastosowań. Poniżej przedstawiono kluczowe kryteria wobec rozwiązań biometrycznych w stosunku do najbardziej popularnych zastosowań:

Zastosowanie	Kluczowe kryteria wyboru technologii biometrycznej
Bankomat	• Odporność czytnika na warunki atmosferyczne (nasłonecznienie, mróz, deszcz itp.) • Rozmiar czytnika umożliwiający montaż na facji bankomatu • Wysoka akceptowalność społeczna • Wandaloodporność czytnika • Możliwość integracji z aplikacją bankomatową • Wysokie bezpieczeństwo urządzenia
Oddział	• Wysoka akceptowalność społeczna • Ergonomia czytnika i łatwość w obsłudze • Rozwiązanie niewymagające modyfikacji infrastruktury sieciowej w placówkach banku • Rozwiązanie niezależne od systemów operacyjnych zainstalowanych na stacjach roboczych doradcy w placówkach • Wysokie bezpieczeństwo urządzenia
Podpisywanie dokumentów	• Zapewnienie integralności podpisywanego dokumentu poprzez integracje z infrastrukturą klucza publicznego (PKI) • Bezpieczne przechowywanie kluczy prywatnych • Wysoka akceptowalność społeczna
Placówki samoobsługowe (VTM)	• Możliwość montażu czytnika w urządzeniu samoobsługowym (z wyłączeniem biometrii głosowej) • Możliwość przeprowadzenia wygodnej i bezpiecznej rejestracji biometrycznej bez konieczności fizycznej obecności konsultanta(odporność na fałszerstwa) • Wysoka akceptowalność społeczna • Wysokie bezpieczeństwo urządzenia • Czytnik wyposażony w test żywotności
Call Center - IVR (Uwierzytelnienie w IVR)	• Stosowanie rozpoznawania mowy naturalnej • System zarządzania próbkami głosowymi • Możliwość integracji hasła głosowego z IVR w innych kanałach np aplikacja mobilna czy www • Zwracanie uwagi nie tylko na współczynnik FAR (odpowiada za bezpieczeństwo) ale również na FRR, który odpowiada za wygodę użytkowania • System raportowania biznesowego i bezpieczeństwa • Odporność na ataki z użyciem odtwarzania sklejonych nagrań lub sztuczne wytwarzanie odpowiedniej barwy głosu

Call Center bez IVR - (Uwierzytelnienie podczas rozmowy z konsultantem)	• Skuteczna weryfikacja rozmówców podczas całej rozmowy w trybie ciągłym • Wygodne zbieranie próbek głosowych podczas rozmowy z agentem • System zarządzania próbkami głosowymi • Zwracanie uwagi na wybór dostawcy z kompetencjami doradztwa biznesowego • Spójny system raportowania biznesowego i bezpieczeństwa dla wszystkich kanałów: IVR, aplikacja mobilna, www • Odporność na ataki z użyciem odtwarzania sklejonych nagrań lub sztuczne wytwarzanie odpowiedniej barwy głosu
Skrytki depozytowe	• Wygoda dla użytkownika • Wysoki współczynnik bezpieczeństwa
Bankowość internetowa	• Niska cena urządzenia umożliwiająca masowe zastosowanie przy zachowaniu wysokiej jakości • Mały rozmiar czytnika • Bezpieczna komunikacja z systemami banku, odporność na ataki • Możliwość zastosowania z technologiami typu Sign What You See • Wysoka akceptowalność społeczna • Wsparcie na najpopularniejszych przeglądarek (IE, Mozilla, Chrome) i systemów operacyjnych (Windows, MacOS, Linux)
Bankowość mobilna (głos)	• System zarządzania próbkami głosowymi • Możliwość integracji hasła głosowego z aplikacji mobilnej w IVR i w innych kanałach np www • Zwracanie uwagi nie tylko na współczynnik FAR (odpowiada za bezpieczeństwo) ale również na FRR, który odpowiada za wygodę użytkowania • Spójny System raportowania biznesowego i bezpieczeństwa dla wszystkich kanałów: aplikacja mobilna, IVR, www • Odporność na ataki z użyciem odtwarzania sklejonych nagrań lub sztuczne wytwarzanie odpowiedniej barwy głosu
Bankowość korporacyjna	• Cena urządzenia umożliwiająca masowe zastosowanie przy zachowaniu wysokiej jakości • Mały rozmiar czytnika • Zapewnienie bezpiecznego przechowywania danych biometrycznych przez użytkownika • Możliwość integracji rozwiązania z wdrożoną w banku infrastrukturą klucza publicznego (PKI) • Bezpieczna komunikacja z systemami banku, odporność na ataki • Możliwość zastosowania z technologiami typu Sign What You See • Wysoka akceptowalność społeczna • Wsparcie na najpopularniejszych przeglądarek (IE, Mozilla, Chrome) i systemów operacyjnych (Windows, MacOS, Linux)
Mobilny doradca	• Możliwość zastosowania z urządzeniami przenośnymi • Możliwość bezpiecznej komunikacji przez sieć otwartą

6. ODPORNOŚĆ NA FAŁSZERSTWA, ZABEZPIECZENIA, ZAGROŻENIA, WYKLUCZENIA

Podstawowymi cechami stosowania systemów biometrycznych jest łatwość stosowania oraz ich wysoki stopień odporności na fałszerstwa związane z uwierzytelnianiem. Każda z technik biometrycznych jest oceniana według wielu parametrów. Wśród nich są dwa podstawowe parametry techniczne:

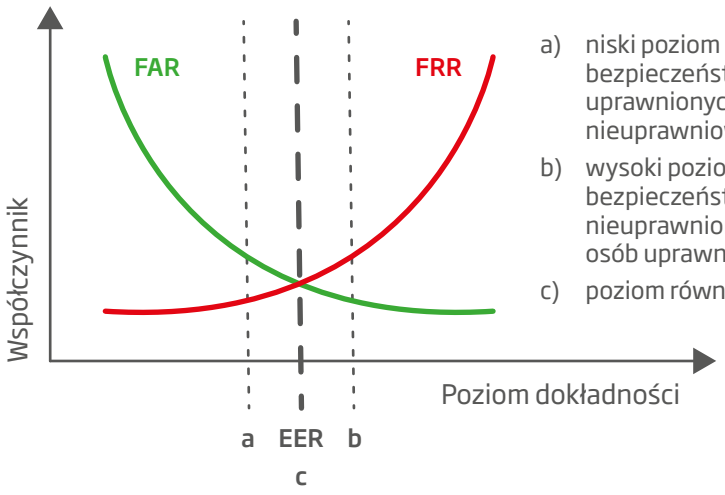
- współczynnik fałszywej akceptacji (FAR), który mówi o prawdopodobieństwie uwierzytelnienia osoby nieuprawnionej
- współczynnik fałszywego odrzucenia (FRR), który mówi o prawdopodobieństwie braku uwierzytelnienia osoby uprawnionej

Współczynniki te są sobie przeciwstawne – im wyższy FAR tym większa wiarygodność, ale i większa podatność na fałszywe odrzucenia. Wyższy współczynnik FRR powoduje mniejszą ilość odrzuceń (większą wygodę), ale kosztem wiarygodności. W praktyce przy rozsądnym wzajemnym ustawieniu parametrów (zwanym także punktem równowagi ERR) mało prawdopodobne jest by osoba nieuprawniona osiągnęła sukces przy zachowaniu należytej wygody w stosowaniu uwierzytelniania biometrycznego.

Tak jak każdy system informatyczny także uwierzytelnienie biometryczne może podlegać atakom. Mogą mieć one różnoraki charakter od fałszowania cech biometrycznych do podmiany wzorców biometrycznych, wyniku porównania lub ataku na system informatyczny.

> „Ważnym parametrem przy wyborze techniki biometrycznej jest jej akceptowalność społeczna

Prostą metodą fałszowania jest zamiana oryginalnej cechy biometrycznej na jej fotografię. W systemach rozpoznawania twarzy lub tęczówki oka taka metoda jest wskazywana jako najczęściej stosowana. Popularne jest również wykonanie żelowej kopii linii papilarnych palca, a w systemach głosowych wykorzystanie na-



a) niski poziom dokładności – niższy stopień bezpieczeństwa, mniej odrzuconych osób uprawnionych, ale i mniej odrzuconych osób nieuprawniownych
b) wysoki poziom dokładności – wyższy stopień bezpieczeństwa, więcej odrzuconych osób nieuprawnionych, ale i więcej odrzuconych osób uprawnionych
c) poziom równowagi

Rys. Poglądowe wykresy współczynników FRR i FAR w funkcji poziomu dokładności

grań. Ataki na takie biometrie są związane z dostępnością cechy biometrycznej – wykonanie zdjęcia twarzy lub pozyskanie obrazu linii papilarnych nie nastręcza większych kłopotów fałszerzowi. Trudniejsze do pozyskania i podrobienia są cechy ukryte np. naczynia krwionośne lub cechy behawioralne np. podpis odręczny. Oczywiście producenci urządzeń biometrycznych zdają sobie sprawę z takich niebezpieczeństw i starają się wyeliminować tego typu fałszerstwa poprzez stosowanie testów żywotności – czyli kontroli, czy pozyskana próbka należy do żywej osoby. Prymitywne fałszerstwa, jak wyżej wymienione, są łatwe do wyeliminowania, a dobre (ale droższe) urządzenia posiadają bardzo wyrafinowane testy żywotności, co, niestety, wydłuża czas uwierzytelniania.

Atak może zostać przeprowadzony również na infrastrukturę informatyczną podczas przetwarzania, przesyłania lub przechowywania wzorców. Należy zatem stosować zabezpieczenia gwarantujące niedostępność i nienaruszalność wzorców, poprawność ich porównania stosując metody kryptograficzne, wzajemne uwierzytelnianie urządzeń i serwerów, certyfikaty, podpisy.

Ważnym parametrem przy wyborze techniki biometrycznej jest jej akceptowalność społeczna. Rozpoznawanie linii papilarnych ma wciąż posmak „metod policyjnych", choć z systemami policyjnymi typu AFIS – omawiane tutaj systemy oprócz palca nie mają nic wspólnego. Podobnie rozpoznawanie siatkówki oka rodzi sprzeciw – oko należy poddać badaniu poprzez zbliżenie go do okularu. Wysoką akceptowalność mają techniki rozpoznawania twarzy, tęczówki, naczyń krwionośnych, podpisu odręcznego, głosu – nie mają one złych konotacji, nie budzą negatywnych emocji i są łatwe w użyciu.

Jeszcze innym parametrem, który należy uwzględnić przy wyborze techniki biometrycznej jest poziom wykluczenia grupy osób. Jednym z podstawowych czynników, który stanowi o wygodzie stosowania technik biometrycznych jest cecha powszechnego jej posiadania. Powszechność nie jest jednak absolutna. Każda technika biometryczna ma ograniczenia, które należy wziąć pod uwagę. Od około 4% populacji nie można pobrać wzorców linii papilarnych ze względu na różne zmiany chorobowe skóry (inne niż skaleczenia czy otarcia). U osób starszych można zauważyć tendencję do opuszczania powiek – co utrudnia stosowanie techniki rozpoznawania tęczówki oka. Wiele osób cierpi na dysgrafię lub parkinsonizm, co uniemożliwia złożenie zbieżnego ze wzorcem podpisu odręcznego. Sporo jest osób z upośledzeniem fizycznym, mowy, chorobami oczu lub naczyń krwionośnych – wszystkie one ograniczają im stosowanie określonych technik biometrycznych. Umożliwienie wyboru jednej z kilku udostępnionych technik biometrycznych jest prostym rozwiązaniem problemu wykluczenia osób z deficytami w jakimś zakresie.

> Każda technika biometryczna ma ograniczenia, które należy wziąć pod uwagę

7. KORZYŚCI

Poniżej przedstawione zostały podstawowe korzyści wynikające z wykorzystania biometrii w bankowości:

1. Zwiększenie bezpieczeństwa:
- Eliminacja ryzyka błędnej weryfikacji tożsamości lub identyfikacji Klienta,
- Eliminacja ryzyka związanego z nieuprawnionym dostępem do rachunków,
- Redukcja fraudów wewnętrznych, dokonywanych przez pracowników banku,
- Redukcja fraudów zewnętrznych np. dokonywanych przez osobę identyfikującą się fałszywym dokumentem tożsamości,

2. Zwiększenie wygody:
- Klienci nie muszą nosić przy sobie karty płatniczej, dowodu osobistego, pamiętać kodu PIN ani żadnego innego dokumentu przy dokonywaniu wszelkich operacji,
- Klienci nie muszą pamiętać wzoru podpisu złożonego na bankowej Karcie Wzorów Podpisu,
- Klienci nie musza pamiętać odpowiedzi na pytania bezpieczeństwa w kanale call center,
- Możliwość otwarcia banku na klientów niekorzystających z kart płatniczych

3. Optymalizacja kosztów:
- Redukcję kosztów papierowego obiegu dokumentów - koszt papieru, wydruków, archiwizacji itd.
- Przyśpieszenie procesów poprzez wykorzystanie technologii cyfrowej zamiast dokumentów papierowych
- Zmniejszenie kosztów obsługi klienta – zniesienie konieczności wydania klientowi karty bankomatowej
- Ograniczenie kosztów wypłat na bankomatach (realizowanie operacji bez użycia karty)
- Budowanie biznesu na wypłatach świadczeń (prowizja od wypłaty) przy jednoczesnym odciążeniu oddziałów
- Redukcja kosztów związana z utrzymywaniem stanowisk audytujących stanowiska kasowe
- Zmniejszenie nakładów czasowych na obsługę – odciążenie personelu
- Możliwość uruchomienia nowego kanału akwizycji klientów – bez użycia „wet signature"
- Ograniczenie kosztów związanych z utrzymaniem call center

4. Zmiana wizerunkowa
- Innowacyjna i bezpieczna instytucja

Oprócz powyższych zalet, każda instytucja wdrażająca lub planująca wdrożenie technologii biometrycznej, podczas analizy swoich procesów, z całą pewnością jest w stanie znaleźć szereg dodatkowych, które nie zostały wymienione.

8. BIOMETRIA A PODPIS ELEKTRONICZNY

Coraz częściej spotykaną formą składania podpisów odręcznych jest zastosowanie specjalizowanych tabletów i rysików. Podpis odręczny składany w ten sposób jest rejestrowany i przechowywany w postaci zdigitalizowanej. Mimo że ma on postać cyfrową, nie można go w żaden sposób określić mianem podpisu elektronicznego w rozumieniu technologii klucza publicznego (PKI) - nie jest funkcją dokumentu, nie chroni integralności dokumentu, może być łatwo przeniesiony pomiędzy dokumentami.

Wykorzystanie danych biometrycznych w funkcji podpisu pod dokumentem elektronicznym (na wzór podpisu odręcznego pod dokumentem papierowym) napotyka na istotne bariery bezpieczeństwa oraz nie jest uregulowane prawnie. Realizacja podpisu pod dokumentem elektronicznym polegająca na prostym dodaniu do treści dokumentu wartości cechy biometrycznej (np. graficznego obrazu podpisu odręcznego wraz z danymi o dynamice podpisu), w aspekcie bezpieczeństwa skutkuje zsumowaniem się ujemnych cech obu rozwiązań. Podpis, który nie jest funkcją dokumentu nie chroni jego integralności, a możliwość skopiowania danych biometrycznych z jednego dokumentu do drugiego umożliwia fałszerstwa. Jakakolwiek próba zmiany tego stanu rzeczy musi wiązać się z rozszerzeniem tego schematu o sekret znajdujący się w posiadaniu osoby podpisującej, ale wtedy z kolei włączanie danych biometrycznych do podpisu traci sens, bo do złożenia podpisu wystarczyłby sam sekret.

Dane biometryczne mogą być za to wykorzystane do uwierzytelnienia dostępu do kluczy kryptograficznych, przy pomocy których składany jest klasyczny podpis elektroniczny, w tym podpis kwalifikowany. Technologia ta określana jest jako Bio PKI. W modelu tym klucz prywatny użytkownika przechowywany może być na karcie krypto procesorowej (wariant najbardziej zbliżony do klasycznego podpisu elektronicznego) albo w centralnym module HSM banku lub instytucji zaufanej trzeciej strony. Dane biometryczne pobierane w momencie składania podpisu uwierzytelniają dostęp do klucza.

Wariant z zastosowaniem karty krypto procesorowej, w której zamiast PIN-u wykorzystywane jest uwierzytelnienie biometryczne, w niewielkim tylko stopniu wykorzystuje siłę biometrii, gdyż zmusza użytkownika do posiadania karty i czytnika. Stąd pod względem kosztów, ergonomii i wygody użytkownika lepszym rozwiązaniem jest przechowywanie klucza w centralnym module HSM.

> W Polsce z rozwiązania BioPKI łączącego biometrię i PKI korzysta już kilka banków w Polsce

W takim modelu, użytkownik za pomocą metod biometrycznych uwierzytelnia się przed serwerem Banku, który wykorzystując klucz prywatny użytkownika zdeponowany w module HSM, wykonuje w jego imieniu podpis elektroniczny. Tak podpisany dokument może zostać następnie oznaczony czasem oraz podpisany przez pracownika w imieniu Banku. Bezpieczeństwo schematu oparte jest na zaufaniu do strony, której powierzone zostają klucze. Rozwiązanie to łączy zalety biometrii i podpisu elektronicznego, eliminując w dużym stopniu wady obu technologii.

W Polsce z rozwiązania BioPKI łączącego biometrię i PKI korzysta już kilka banków w Polsce (m.in. Getin Bank).

9. ZAKOŃCZENIE

Intensywny rozwój i pozytywny odbiór technologii biometrycznych znajdują dla nich szerokie możliwości zastosowania w sektorze bankowym na wielu różnych płaszczyznach. Wymierne korzyści występują w obszarach bankowości korporacyjnej, detalicznej, mobilnej, zarówno w oddziałach, obsłudze zdalnej czy w bankomatach.

Zakres potencjalnych innowacji stale się rozszerza. Najważniejszym jest patrzenie na technologie biometryczne nowoczesnym okiem z perspektywy XXI wieku, co pozwala dostrzec w nich zupełnie nowy wymiar świadczenia usług bankowych.

Żeby być nowoczesnymi, banki potrzebują dotrzymywać kroku postępowi technologicznemu. Pożytek dla banków jest tu podwójny, ponieważ przede wszystkim biometria unowocześnia infrastrukturę i zwiększa bezpieczeństwo banków, wznosząc je na nowy poziom. Jednocześnie implementacja rozwiązań biometrycznych podnosi atrakcyjność banków wobec klientów, zwiększając ich komfort, efektywność ich obsługi oraz świadomość tych benefitów.

Biometria przynosi nowe szanse i wyzwania, które dzisiaj są niezwykle przydatne, a jutro będą pożądane, a pojutrze niezbędne.

> „Żeby być nowoczesnymi, banki potrzebują dotrzymywać kroku postępowi technologicznemu

10. AUTORZY

10.1. REDAKCJA

- **Tadeusz Woszczyński** - Przewodniczący Grupy ds. Biometrii, Członek Prezydium Forum Technologii Bankowych ZBP, Dyrektor Regionalny CEE i CIS, Grupa Systemów Informatycznych, Hitachi Europe Ltd. - redaktor prowadzący i merytoryczny, współautor

10.2. WSPÓŁAUTORZY

- **Michał Czechowski** – Członek Zarządu, Noa Tech Sp. z o.o.
- **Łukasz Hnatkowski** – Sekretarz Forum Technologii Bankowych, Związek Banków Polskich
- **Artur Krystosik** – Dyrektor, Enigma SOI
- **Zbigniew Marcinkowski** – Wiceprzewodniczący Grupy ds. Biometrii, Członek Prezydium Forum Technologii Bankowych, Wiceprezes Zarządu Algotech Polska
- **Mariusz Sudoł** – ekspert Forum Technologii Bankowych
- **Jarosław Wójtowicz** – Instytut Maszyn Matematycznych

09.2015