

BIOMETRIA W BANKOWOŚCI ELEKTRONICZNEJ – RYNEK, TECHNOLOGIA, KLIENT

SYGN. WIB PAB 8/2022

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

Warszawa, maj 2022

 PROGRAM
ANALITYCZNO
BADAWCZY

O Raporcie

Raport **Biometria w bankowości elektronicznej – RYNEK, TECHNOLOGIA, KLIENT** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy:

Raport przygotowany przez zespół w składzie:

Michał Olczak – nadzór nad opracowaniem raportu

– Partner Obserwatorium.biz. Współzałożyciel i członek zarządu Obserwatorium.biz. Posiada ponad 12-letnie doświadczenie w rozwoju bezpiecznych aplikacji, architekt bezpieczeństwa oraz organizator OWASP Poznań. Członek Forum Bezpieczeństwa Transakcji Elektronicznych ZBP z ponad 10-letnim doświadczeniem w tworzeniu systemów bankowości internetowej i mobilnej w banku BZWBK. Absolwent Politechniki Poznańskiej, kierunek informatyka. Promuje kulturę innowacji w połączeniu z cyberodpowiedzialnością.

dr Miłosz Brakoniecki

– Partner Obserwatorium.biz sp. z o.o. Współzałożyciel i członek zarządu Obserwatorium.biz. Doktor nauk humanistycznych UAM w Poznaniu (specjalność socjologia), skończył studia podyplomowe ze strategii i planowania biznesu na Akademii Ekonomicznej w Poznaniu. W latach 2006–2014 dyrektor bankowości elektronicznej w Banku Zachodnim WBK, gdzie odpowiadał za rozwój biznesowy bankowości elektronicznej, sprzedaż przez kanały elektroniczne oraz płatności elektroniczne. W latach 2012–2014 członek Prezydium Rady Bankowości Elektronicznej Związku Banków Polskich. Współtwórca największego w Polsce serwisu crowdfundingowego Siepomaga.pl, Fundacji Siepomaga.pl oraz FinTechów Rachuneo i Compay. W latach 2016–2018 Co-lider Zespołu Cyfrowej Tożsamości Programu Paperless/Cashless przy Ministerstwie Cyfryzacji, w latach 2016–2020 Członek Rady Nadzorczej Diners Club Polska Sp. z o.o. Prelegent w kilkudziesięciu konferencjach branżowych w kraju i za granicą, autor licznych publikacji dot. gospodarki cyfrowej i bankowości.

Marcin Wolski

– Ekspert i doradca Zarządu Obserwatorium.biz. Od 2014 roku pracuje jako Specjalista ds. Bezpieczeństwa Informacji. Posiada kompetencje w zakresie następujących obszarów: usługi zaufania oraz identyfikacji elektronicznej, system zarządzania bezpieczeństwem informacji, zarządzanie ryzykiem, analiza procesów biznesowych, RODO. Uczestniczył w licznych opracowaniach analitycznych związanych z usługami zaufania, identyfikacją elektroniczną oraz rozwiązaniami usług mobilnych, jak również opracowywał dokumentację związaną z infrastrukturą klucza publicznego. Absolwent Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej w Warszawie. Audytor wiodący ISO 27001.

Maciej Krzyżański

– Ekspert i doradca Zarządu Obserwatorium.biz. Absolwent Akademii Ekonomicznej w Poznaniu (specjalność bankowość). Posiada wieloletnie doświadczenie w zakresie sprzedaży i obsługi klienta przez telefon i w innych kanałach zdalnych. W latach 1999–2017 związany zawodowo z WBK SA/BZWBK SA, w tym przez 11 lat z bankowym *contact center*, gdzie jako menedżer, a następnie dyrektor ds. sprzedaży tworzył od podstaw procesy sprzedaży produktów bankowych i obsługi klienta przez telefon i Internet, rozwijał i budował nowe lokalizacje i zespoły oraz realizował cele banku w zakresie sprzedaży produktów finansowych, obsługi posprzedażowej, aktywizacji i utrzymania klienta. Ma także doświadczenie w zakresie rozwoju oferty i sprzedaży produktów kredytowych i kartowych. Odpowiadał za tworzenie i realizację multikanalowych kampanii CRM, wspierających sprzedaż oferty banku. W Obserwatorium.biz odpowiada za rozwój projektów związanych z cyfrowymi kanałami komunikacji, sprzedaży i obsługi klienta, w tym z wykorzystaniem technologii biometrycznych – dla sektora finansowego i administracji publicznej.

Dominika Rzęsa

– Ekspert Obserwatorium.biz. Absolwentka Wydziału Nauk Społecznych Uniwersytetu im. Adama Mickiewicza w Poznaniu. W Obserwatorium.biz zajmuje się przygotowaniem procesów badawczych, analizą i budowaniem procesów biznesowych, analizą usług zaufania, analizą zgromadzonych danych oraz przeprowadzaniem wywiadów i badań. Posiada doświadczenie w testowaniu serwisów internetowych i aplikacji na urządzenia mobilne (m.in. badania użyteczności serwisów transakcyjnych banków (Złoty Bankier) oraz aplikacji mInstitucja), prowadzeniu wywiadów FGI oraz IDI. Uczestniczyła w licznych opracowaniach analitycznych bazujących na danych jakościowych i ilościowych związanych m.in. z usługami zaufania, identyfikacją elektroniczną.



O Programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie analizy zjawisk, tworzenia opracowań i porządkowania wiedzy w obszarach cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania ich wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz kreowania wartości dla klientów bankowości. PAB WIB kładzie duży nacisk na rozwój współpracy ze środowiskami akademickimi i eksperckimi, poszukując synergii w zakresie zainteresowań badawczych autorów oraz potrzeb rozwojowych sektora bankowego.

W ramach programu realizowane są analizy i badania w następujących obszarach:

-  **Nowe technologie i cyberbezpieczeństwo**
-  **Zdolność banków do finansowania gospodarki**
-  **Bankowość spółdzielcza**
-  **Rynek nieruchomości**
-  **Zielony ład i finansowanie energetyki odnawialnej**
-  **Finansowanie projektów innowacyjnych**

Więcej na temat działalności programu na stronie www.pab.wib.org.pl

Kontakt:

dr Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@wib.org.pl

Jacek Gieorgica
m: 603 626 254
e: jgieorgica@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Tomasz Pawlonka
m: 505 917 778
e: tpawlonka@wib.org.pl



Spis treści

○	Wstęp	5
	Podsumowanie	5
	Cele raportu	6
	Metodologia	6
	Zawartość raportu	6
○	ROZDZIAŁ I. Biometria – wykorzystywane mechanizmy i sposoby zastosowania	7
	1.1. Wskazanie głównych typów biometrii – podział na cechy podlegające pomiarowi (np. głos, odcisk palca) vs. funkcje (np. uwierzytelnienie, autoryzacja transakcji, identyfikacja)	8
	1.2. Analiza SWOT poszczególnych typów biometrii	9
	1.3. Klasyfikacja typów biometrii ze względu na rekomendowane zastosowania danego typu biometrii oraz wymagania techniczne	12
	1.4. Biometria „w urządzeniu” vs. „na serwerze”	13
	1.5. Standaryzacja i certyfikacja rozwiązań biometrycznych	14
	2.6. Czynniki sprzyjające wzrostowi popularności i przyswajania biometrii, a kwestie bezpieczeństwa	15
	2.7. Czynniki warunkujące wzrost odporności na ataki systemów opartych o biometrię	16
	2.8. Rozwój narzędzi technologicznych w biometrii a kwestie ochrony prywatności i bezpieczeństwa danych	18
	2.9. Biometria a elektroniczna identyfikacja i usługi zaufania	19
○	ROZDZIAŁ II. Biometria w polskiej bankowości elektronicznej. Benchmarking zastosowania biometrii na rynku bankowości elektronicznej	21
	2.1. Konteksty zastosowania biometrii w bankowości i płatnościach elektronicznych na rynku polskim	22
	2.2. Funkcje (logowanie, autoryzacja transakcji), urządzenia (mobile vs. desktop) i typy zbieranych wzorców (odcisk palca, twarz, styl pisanie)	24
	2.3. Wybrane przykłady zastosowania biometrii na polskim rynku finansowym – benchmarking polskiego rynku oraz najciekawsze przykłady z EU	27
○	ROZDZIAŁ III. Biometria w bankowości elektronicznej z perspektywy klienta. Badanie User Experience wdrożonych mechanizmów biometrycznych w polskich aplikacjach bankowych	29
	3.1. Cel i zakres badania	30
	3.2. Metodologia i wprowadzenie do badań	30
	3.3. Podsumowanie badań – wyniki	30
	3.4. Generalne wnioski	36
○	ROZDZIAŁ IV. Przyszłość metod biometrycznych i ich zastosowania w bankowości elektronicznej	37
	4.1. Ścieżki rozwoju metod biometrycznych z uwzględnieniem kwestii prywatności, ergonomii użycia, ogólnego postrzegania przez społeczeństwo, infrastruktury po stronie użytkownika i banków oraz bezpieczeństwa	38
	4.2. Potencjał biznesowy biometrii, w tym rozszerzenie zastosowań na rynku finansowym i poza nim	39
	4.3. Biometria a inne metody elektronicznej identyfikacji czy uwierzytelnienia – orkiestracja metod zabezpieczeń z perspektywy banku vs. oczekiwania klientów	41



Wstęp

Niniejszy raport zawiera diagnozę sytuacji w zakresie narzędzi biometrycznych wykorzystywanych aktualnie przez polski sektor finansowy, szczególnie bankowy. Raport przedstawia podsumowanie informacji zawartych na stronach podmiotów bankowych, a także syntetyczne podsumowanie głosu użytkowników bankowości elektronicznej.

Podsumowanie

Prace nad niniejszym raportem pozwoliły wypracować następujące wnioski:

1. Biometria w procesach cyfrowych, w szczególności wykorzystywana jako wsparcie procesów zdalnego pozyskiwania klientów przez banki, odgrywa coraz większą rolę. Znaczna część banków, których działanie przeanalizowano w niniejszym raporcie, wykorzystuje zdalną identyfikację opartą o wideoidentyfikację wspieraną mechanizmami biometrycznymi. Zarówno sytuacja związana z pandemią SARS-CoV2, jak i coraz większy rozwój rynku e-commerce, w tym dostęp do usług online dla użytkowników Internetu, wskazują, że tradycyjne kanały pozyskiwania klientów są uznawane za coraz mniej wygodne. Z tego względu oczekujemy, że biometria w procesach pozyskiwania klientów w kanałach zdalnych, w kolejnych latach będzie coraz szerzej wykorzystywana jako element wspierający proces identyfikacji klientów.
2. Dotychczasowe doświadczenia z biometrią zwerifikowane badaniami przeprowadzonymi na użytkownikach bankowości elektronicznej potwierdzają, że poszczególne metody (zwłaszcza odcisk palca) są dobrze zakorzenione wśród użytkowników, a ich użycie na co dzień w operacjach takich jak logowanie do aplikacji mobilnych nie sprawia większego problemu. Co więcej, użytkownicy wskazują, że zastosowanie mechanizmów opartych o biometrię zwiększa ich poczucie bezpieczeństwa w procesach bankowych.
3. W naszej opinii metody biometryczne nie będą się znacząco rozwijać pod kątem poszerzenia wachlarza dostępnych metod. Jesteśmy zdania, że biometria, która oparta jest o odcisk palca czy wizerunek twarzy, to metody na tę chwilę wystarczająco wygodne dla użytkowników usług finansowych.
4. Dużą niewiadomą jest biometria behawioralna, dla której w sektorze bankowym nie odnotowaliśmy wielu wdrożeń, w szczególności jako metody wspierającej procesy uwierzytelnienia użytkowników. Wyjątkiem jest podpis biometryczny (który wchodzi w zakres biometrii behawioralnej), dla którego zaobserwowaliśmy znaczące wdrożenie w sektorze leasingowym i który stanowi istotną alternatywę dla procesu „papierowego” w klasycznym procesie leasingowym.
5. Oprócz zastosowania biometrii w procesach identyfikacji oraz logowania do usług takich jak aplikacje mobilne dostrzegamy potencjał do jej większego zastosowania w procesach autoryzacji transakcji (przelewów czy pożyczek). Autoryzacja oparta o mobilną autoryzację, wykorzystująca metody biometryczne, odnalazła się jako czynnik uwierzytelniający w procesach kartowych jako mechanizm 3D Secure. Zauważamy jednak, że duża część banków ostrożnie podchodzi do pełnego zastąpienia PIN-ów/hasła mobilnych potwierdzeniem biometrycznym, zwłaszcza w transakcjach zlecanych z poziomu aplikacji mobilnych, co jednak z czasem może ulec zmianie na korzyść wykorzystywania głównie metod biometrycznych.
6. Niezaprzeczalnie kluczową sprawą w kontekście biometrii jest bezpieczeństwo danych osobowych, zwłaszcza że dane biometryczne to dane szczególnych kategorii ze względu na ich wpływ na prywatność. Dostrzegamy coraz większe zainteresowanie obszarem danych osobowych organów takich jak Komisja Europejska (koncepcja europejskiego cyfrowego portfela tożsamości). Z pewnością rozwój metod, narzędzi oraz całego rynku dostawców biometrycznych będzie się rozwijać, jeśli nie wydarzą się poważne incydenty związane np. z wyciekiem baz danych biometrycznych czy z nadmiernym profilowaniem użytkowników.

Cele raportu

Celem raportu było określenie „krajobrazu” narzędzi biometrycznych w bankowości elektronicznej stosowanych aktualnie, uzupełnienie go o perspektywę użytkowników – klientów polskich banków, a równocześnie wskazanie kierunków rozwoju samych narzędzi i sposobów ich wykorzystania. Zależało nam również na przedstawieniu pełnego obrazu zastosowań narzędzi biometrycznych w aplikacjach bankowych na podstawie benchmarkingu rynku oraz badań klienckich.

Metodologia

Raport został opracowany w oparciu o następujące metody:

- badanie jakościowe na użytkownikach bankowości elektronicznej,
- analizę materiałów dostępnych publicznie na stronach internetowych banków,
- metodę ekspercką, polegającą na zaproszeniu do raportu ekspertów z rynku dostawców technologii i rozwiązań biometrycznych,
- benchmarking rozwiązań dostępnych na rynku polskim oraz europejskim.

Zawartość raportu

Oprócz bieżącego wstępu podsumowującego, na raport składają się:

- rozdział pierwszy, zawierający opis wykorzystywanych mechanizmów biometrycznych i sposobów ich zastosowania, klasyfikację typów biometrii oraz analizę SWOT poszczególnych metod; obejmuje on także informacje na temat czynników sprzyjających wzrostowi popularności biometrii, uwzględniając jednocześnie kwestie bezpieczeństwa i prywatności;
- rozdział drugi stanowiący podsumowanie zastosowania oraz funkcji biometrii w polskiej bankowości elektronicznej na podstawie przeprowadzonej analizy 15 banków;
- rozdział trzeci, który zawiera podsumowanie wyników badań User Experience mechanizmów biometrycznych wdrożonych w polskich aplikacjach bankowych;
- rozdział czwarty, przedstawiający prognozy dotyczące przyszłości metod biometrycznych i ich zastosowania w bankowości elektronicznej, w szczególności poprzez wskazanie ścieżek rozwoju oraz potencjału zastosowania biometrii poza rynkiem finansowym.



Biometria – wykorzystywane mechanizmy i sposoby zastosowania



1.1. Wskazanie głównych typów biometrii – podział na cechy podlegające pomiarowi (np. głos, odcisk palca) vs. funkcje (np. uwierzytelnienie, autoryzacja transakcji, identyfikacja)

Biometria [z gr. *bíos* – „życie”, *metréō* – „mierzę”] to – jak definiuje Encyklopedia PWN – dziedzina nauk biologicznych zajmująca się zastosowaniem metod statystyki matematycznej w naukach przyrodniczych, przede wszystkim do analizy danych liczbowych oraz do testowania modeli matematycznych i hipotez teoretycznych dotyczących zmienności organizmów. Jedną z tych nauk przyrodniczych jest antropometria, koncentrująca się na zbieraniu danych o mierzalnych cechach ludzi. Z niej zdaje się wywodzić dzisiejsze powszechne rozumienie biometrii, zdefiniowane nieco wężiej, wskazujące jednocześnie możliwości jej praktycznego zastosowania: biometria to dziedzina nauki wykorzystująca dobrodziejstwa technologii komputerowych do identyfikacji i weryfikacji osób na podstawie cech fizycznych lub behawioralnych.

W pomiarach biometrycznych najczęściej wykorzystywane są następujące cechy fizyczne:

- odciski palców dłoni;
- wizerunek twarzy;
- wzór tęczówki oka;
- układ żył w palcach i siatkówce oka;

oraz cechy behawioralne:

- głos;
- pismo odręczne;
- sposób korzystania z urządzeń, takich jak klawiatura komputerowa czy smartfon.

Początki biometrii sięgają XIX wieku i wywodzą się z kryminalistyki. Identyfikacja osób długo możliwa była tylko w oparciu o ich dane osobowe oraz opisy wyglądu. Rozwijające się dopiero od połowy XIX wieku techniki fotograficzne umożliwiły utrwalanie wizerunku osób, jednak i to w wielu przypadkach było niewystarczające. Dopiero zastosowanie technik antropometrycznych¹ zdecydowanie rozszerzy-

ło możliwości identyfikacji przestępców. Za pioniera badań w tym zakresie uważa się francuskiego policjanta Alphonse’a Bertillona, który wprowadził system identyfikacji osób w oparciu o pomiary ciała, m.in. wzrostu, wymiarów głowy, długości małego palca czy długości przedramienia. System opierał się na odkryciu, że wymiary te pozostają niezmiennie podczas całego dorosłego życia człowieka. Umożliwiał względnie szybkie odnajdowanie dokumentów w archiwach kryminalnych, w których zastosowano oznaczenia i sortowanie według podlegających pomiarom cech, a w połączeniu z fotografiami – szybką identyfikację podejrzanych. W 1893 roku Bertillon opublikował wyniki swoich badań nad zastosowaniem tych metod biometrycznych do identyfikacji przestępców w podręczniku pt. *Identification anthropométrique*.

Metoda Bertillona była niedoskonała i wkrótce ustąpiła miejsca daktyloskopii. Badania nad odciskami palców były prowadzone już w XVI wieku, jednak dopiero w XIX odkryto, że układ linii na opuszkach palców jest unikalny dla każdego człowieka. Badania nad nimi prowadzone były przez naukowców w różnych częściach świata. W 1823 roku czeski antropolog Jan Evangelista Purkyně zidentyfikował i opisał dziewięć powtarzalnych układów linii papilarnych, których kombinacje i wariacje tworzą unikalne wzory. Od 1858 roku Sir William James Herschel, brytyjski oficer w Indiach, stosował odciski palców i dłoni jako podpisy pod umowami, uznając je za trwałe i niepowtarzalny element identyfikacyjny osoby. W 1880 roku szkocki lekarz i misjonarz Henry Faulds zaproponował utrwalanie odcisków palców za pomocą atramentu i wykorzystanie ich do identyfikacji osób w kryminalistyce. Przebywając z misją w Japonii, zainteresował się odciskami palców po tym, jak towarzysząc przyjacielowi w wykopaliskach archeologicznych, zauważył, że w starożytnych fragmentach gliny można dostrzec delikatne odciski pozostawione przez rzemieślników. Badania, które później prowadził, znalazły wkrótce praktyczne zastosowanie – Faulds przekonał lokalną policję o niewinności człowieka podejrzanego o włamanie do szpitala, w którym pracował, dzięki porównaniu jego linii papilarnych z odciskami palców pozostawionymi przez sprawcę. Jego rekomendacje nie zostały jednak przyjęte przez Scotland Yard.

Autorstwo metody identyfikacji za pomocą odcisków palców przypisuje się także Sir Francisowi Galtonowi, angielskiemu naukowcowi, który w trzech książkach poświęconych tej materii wydanych pod koniec XIX wieku oszacował prawdopodobieństwo posiadania takich samych układów linii papilarnych przez dwie osoby i opracował obowiązujący do dziś system klasyfikacji odcisków palców. Do praktyki krymina-

¹ Antropometria – dział antropologii, zajmujący się metodami zbierania danych o budowie ludzkiego ciała z wykorzystaniem pomiarów odległości między tzw. punktami antropometrycznymi, czyli określonymi miejscami na ciele lub szkielecie człowieka.



listycznej identyfikację przez odciski palców wprowadził pod koniec wieku Sir Edward Richard Henry, ówczesny szef policji w Bengalu. Henry, opierając się na pracach Galtona, opracował system klasyfikacji odcisków palców umożliwiającą stosunkowo łatwe tworzenie i przeszukiwanie baz danych kryminalnych. Wydana przez niego w 1897 roku monografia *Classification and Uses of Fingerprints* została uznana przez inne jednostki policyjne Imperium Brytyjskiego, a Henry'ego wezwano do Londynu, gdzie utworzył biuro ds. odcisków palców i zaadaptował swoją metodę do praktyki Scotland Yardu.

Kolejnym kamieniem milowym w historii rozwoju biometrii był artykuł Mitchella Trauringa *Automatic Comparison of Finger-Ridge Patterns*, opublikowany w 1963 roku w amerykańskim magazynie *Nature*. Badacz zaprezentował w nim i udowodnił możliwość użycia metody automatycznego porównywania minucji we wzorach linii papilarnych do szybkiej, zautomatyzowanej weryfikacji tożsamości. Od tego momentu zaczął się rozwój automatycznych systemów rozpoznawania i weryfikacji linii papilarnych, a także innych cech biometrycznych.

Za prekursora biometrii twarzy uważany jest amerykański matematyk Woodrow Bledsoe. W latach 60. XX wieku opracował on metodę klasyfikacji zdjęć z użyciem tzw. tabletu RAND – urządzenia, za pomocą którego można było wprowadzić do bazy danych współrzędne cech twarzy (położenia oczu, nosa, linii włosów i ust) na siatce za pomocą rysika emitującego impulsy elektromagnetyczne. Dzięki temu możliwe stało się wyszukiwanie osoby w takiej bazie danych poprzez odfiltrowanie kandydatów o zbliżonych współrzędnych danych cech. W latach 70 zwiększono dokładność ręcznego systemu rozpoznawania twarzy. Amerykańscy naukowcy A. Jay Goldstein, Leon D. Harmon i Ann Lesk opracowali i wykorzystali do tego celu 21 dodatkowych cech twarzy (tzw. markerów), takich jak grubość warg i kolor włosów. Do rozwoju biometrii twarzy przyczynił się bez wątpienia amerykański rządowy program *The Facial Recognition Technology* (FERET), którego celem było stworzenie automatycznego systemu rozpoznawania twarzy.

Historia biometrii tęczówki oka jest stosunkowo młoda. Co prawda już w 1936 roku okulista Frank Burch zidentyfikował różnice we wzorach ludzkich tęczówek i zaproponował metodę rozpoznawania osób w oparciu o te wzory. Jednak dopiero w 1987 lekarze Leonard Flam i Aran Safir opatentowali koncepcję identyfikacji tęczówki opartą na unikalności jej układu, a technologie oparte na tych koncepcjach zaczęły się szerzej rozwijać i komercjalizować dopiero w XXI wieku.

Naukowe podwaliny dla biometrii głosu położył Szwed Carl Gunnar Fant, który w 1960 roku opublikował model opisujący fizjologiczne komponenty akustycznej produkcji mowy. Jego odkrycia posłużyły do lepszego zrozumienia biologicznych składników mowy, co ma kluczowe znaczenie dla rozpoznawania mówcy. Pierwszy funkcjonujący system biometrii głosu zdolny do dokładnego zarejestrowania i rozpoznawania próbek ludzkiego głosu opracowała w 1976 roku amerykańska firma Texas Instruments.

Koncepcja biometrii behawioralnej obsługi urządzeń sięga swymi korzeniami XIX wieku i wiąże się z wynalezieniem telegrafu. Operatorzy stawali się rozpoznawalni dzięki sposobowi, w jaki nadawali sygnały kodowane alfabetem Morse'a. W czasie II wojny światowej stosowano weryfikację autentyczności przekazywanych komunikatów na podstawie charakterystycznych dla znanych nadawców sposobów posługiwania się telegrafem.

Funkcje biometrii

Technologie biometryczne znajdują zastosowanie wszędzie tam, gdzie istotna jest tożsamość osoby. Mogą pełnić dwie funkcje:

1. identyfikacji – czyli rozpoznania osoby poprzez porównanie pobranej od niej próbki biometrycznej (lub kilku próbek) z posiadanymi wzorcami biometrycznymi uprzednio zidentyfikowanych i zweryfikowanych osób [porównanie 1:N (lub M:N), odpowiedź na pytanie „Kim jest?”];
2. weryfikacji tożsamości – czyli stwierdzenia, czy dana osoba jest tym, za kogo się podaje, poprzez porównanie pobranej od niej próbki biometrycznej z posiadanym wzorcem biometrycznym [porównanie 1:1, odpowiedź na pytanie „Czy jest tym, za kogo się podaje?”].

1.2. Analiza SWOT poszczególnych typów biometrii

W tym rozdziale przedstawiono charakterystykę poszczególnych metod biometrycznych z wykorzystaniem elementów metodologii SWOT (z ang.: *strengths* – silne strony, *weaknesses* – słabe strony, *opportunities* – szanse, *threats* – zagrożenia). Takie ujęcie pozwala wstępnie ocenić i porównać poszczególne typy biometrii, biorąc pod uwagę podstawowe aspekty: efektywność działania, dostępność i przyswajanie przez społeczeństwo, bezpieczeństwo, wymagania w zakresie implementacji w procesach biznesowych (w tym koszty).



LINIE PAPILARNE

MOCNE STRONY	SŁABE STRONY
- Unikalność układów linii papilarnych daje wysoką skuteczność - Szybkość weryfikacji dzięki małemu rozmiarowi wzorca - Duża dostępność	- Uszkodzenia, wiek – mogą obniżać skuteczność - Wymagany czytnik w urządzeniu mobilnym / dedykowane urządzenie
SZANSE	ZAGROŻENIA
- Powszechna i znana metoda - Możliwość wykorzystania kamer w urządzeniach mobilnych jako czytników	- Relatywnie łatwy do pozyskania / podrobienia wzorzec - W przypadku kompromitacji wzorca – trudny do zastąpienia

TWARZ

MOCNE STRONY	SŁABE STRONY
- Wygoda użycia - Duża dostępność kompatybilnych urządzeń mobilnych	- Mniej skuteczna od innych metod - Czynniki obniżające dokładność rozpoznania (zarost, okulary, maski, warunki oświetleniowe) - Zastrzeżenia dotyczące utraty prywatności
SZANSE	ZAGROŻENIA
- Powszechna i znana metoda - Możliwość wykorzystania kamer w urządzeniach mobilnych jako czytników	- Deep fakes² - W przypadku kompromitacji wzorca – niemożliwy do zastąpienia

2

UKŁAD ŻYŁ (PALEC, DŁOŃ, SIATKÓWKA OKA)

MOCNE STRONY	SŁABE STRONY
Wysoka skuteczność w dobrych warunkach	- Niska temperatura otoczenia wpływa na wyniki (palec, dłoń) - Wymagane dedykowane urządzenia - Mało popularna metoda
SZANSE	ZAGROŻENIA
Możliwość wykorzystania kamer i oświetlenia w urządzeniach mobilnych jako czytników żył w palcach	W przypadku kompromitacji wzorca – niemożliwy do zastąpienia

² Technika obróbki obrazu polegająca na łączeniu obrazów twarzy ludzkich przy użyciu technik sztucznej inteligencji (Wikipedia 18.02.2022)



TĘCZÓWKA

MOCNE STRONY	SŁABE STRONY
• Organ rzadko ulegający uszkodzeniu • Wysoka skuteczność dzięki wysokiej unikalności wzorów • Szybkość przetwarzania dzięki małemu rozmiarowi wzorca	• Stosunkowo młoda technologia • Konieczność stosowania specjalistycznych urządzeń i warunków
SZANSE	ZAGROŻENIA
• Możliwość wykorzystania kamer w urządzeniach mobilnych jako czytników	• W przypadku kompromitacji wzorca – niemożliwy do zastąpienia

GŁOS

MOCNE STRONY	SŁABE STRONY
• Wysoka skuteczność w dobrych warunkach • Trudny do podrobienia wzorec • Wygoda użycia	• Dźwięki otoczenia, choroby aparatu głosu obniżają skuteczność • Możliwość wykorzystania nagrania głosu
SZANSE	ZAGROŻENIA
• Naturalnie przeznaczona do wsparcia procesów obsługi klienta przez telefon	• Obawy użytkowników o bezpieczeństwo danych / prywatność • Rozwój voice deep fakes

SPOSÓB KORZYSTANIA Z URZĄDZEŃ (PROFIL BEHAWIORALNY)

MOCNE STRONY	SŁABE STRONY
• Łatwość użytkowania • Pasywna – nie wymaga świadomych akcji ze strony użytkownika	• Wymagany proces „uczenia się” / pobrania dużej liczby próbek do zbudowania wzorca • Niska dokładność ze względu na zmienność sposobu korzystania z urządzenia w różnych warunkach / sytuacjach
SZANSE	ZAGROŻENIA
• Umożliwia ciągle monitorowanie użytkownika	• Obawy użytkowników o bezpieczeństwo danych / prywatność



Zestawienie cech metod biometrycznych pokazuje, że te szeroko dostępne i popularne oraz relatywnie szybkie i tanie w implementacji typy biometrii (odciski palców, twarz) są jednocześnie mniej skuteczne i mniej bezpieczne. Mało popularne metody, choć często bardziej dokładne i bezpieczne (układ żył), utrzymują swój status ze względu na wysoki koszt wdrożenia, wąski zakres zastosowań czy funkcjonujące w odbiorze społecznym zastrzeżenia. Biorąc jednak pod uwagę, że spośród wymienionych typów biometrii dominujące pod względem popularności są biometria twarzy i odciski palców, można wywnioskować, że najistotniejszymi dla przeciętnego konsumenta wartościami są łatwość użycia i wygoda, jakie dają te metody zabezpieczeń.

1.3. Klasyfikacja typów biometrii ze względu na rekomendowane zastosowania danego typu biometrii oraz wymagania techniczne

Typy biometrii można klasyfikować w kilku ujęciach. Ze względu na rodzaj przeprowadzanej analizy możemy pogrupować metody biometryczne następująco:

1. Analiza wizualna
 - a. odciski palców dłoni
 - b. wizerunek twarzy
 - c. wzór tęczy oka
 - d. układ żył w palcach i siatkówce oka
 - e. geometria dłoni
 - f. budowa ucha
2. Analiza audialna
 - a. emitowany głos
3. Analiza behawioralna
 - a. pismo odręczne
 - b. sposób korzystania z urządzeń, takich jak klawiatura komputerowa czy smartfon
 - c. chód
4. Analiza chemiczna
 - a. DNA

Najbardziej powszechne typy biometrii można też przedstawić w podziale ze względu na rekomendowane zastosowania:

	ODCISKI PALCÓW	TWARZ	OKO	DŁOŃ	GŁOS	PISMO	Sposób KORZYSTANIA Z KOMPUTERA / SMARTFONA
EWIDENCJA OBYWATELI							
– wsparcie systemów ewidencyjnych danymi biometrycznymi (np. system Aadhaar w Indiach)	✓	✓	✓				
TRANSPORT/KONTROLA GRANIC							
– przyspieszenie odpraw	✓	✓	✓				
– kontrola podróży							
BEZPIECZEŃSTWO PUBLICZNE							
– wsparcie działań organów ścigania	✓	✓	✓				
– monitoring tłumów / zgromadzeń							
SŁUŻBA ZDROWIA							
– kontrola uprawnień do świadczeń	✓	✓	✓				
KONTROLA DOSTĘPU							
– do pomieszczeń i urządzeń	✓	✓	✓	✓	✓		
– do systemów / sieci							
BANKOWOŚĆ							
– onboarding KYC							
– logowanie / kontrola dostępu	✓	✓	✓	✓	✓	✓	✓
– autoryzacja operacji /transakcji							
– płatności							



Najbardziej powszechne typy biometrii – wymagania techniczne po stronie użytkownika i instytucji:

	ODCISKI PALCÓW	TWARZ	OKO	DŁOŃ	GŁOS	PISMO	Sposób KORZYSTANIA Z KOMPUTERA / SMARTFONA
UŻYTKOWNIK	Onsite: brak wymagań	Onsite: brak wymagań	Onsite: brak wymagań	Onsite: brak wymagań	Onsite: brak wymagań	Onsite: brak wymagań	Onsite: nie dotyczy
	Online: – smartfon z czytnikiem linii papilarnych – smartfon z kamerą o odpowied- niej rozdziel- czości	Online: smartfon z kamerą o odpow- iedniej rozdziel- czości	Online: smartfon z kamerą o odpowied- niej rozdziel- czości		Online: telefon	Online: – skaner – smartfon z kamerą	Online: komputer / smartfon
INSTYTUCJA	Onsite: czytniki linii papilarnych, dedykowane oprogramo- wanie	Onsite: kamery, de- dykowane oprogramo- wanie	Onsite: kamery, dedykowane oprogramo- wanie	Onsite: czytniki dłoni, dedy- kowane oprogra- mowanie	Onsite: mikrofon, dedy- kowane oprogra- mowanie	Onsite: skanery, dedykowa- ne oprogra- mowanie	Onsite: nie dotyczy
	Online: zapew- nienie opro- gramowania dla użytkow- nika	Online: za- pewnienie oprogramo- wania dla użytkow- nika	Online: za- pewnienie oprogramo- wania dla użytkownika			Online: za- pewnienie oprogra- mowania dla użyt- kownika	Online: dedykowane oprogramo- wanie

1.4. Biometria „w urządzeniu” vs. „na serwerze”

Przy wdrażaniu rozwiązań biometrycznych warto pamiętać o dwóch głównych modelach implementacji opartych na zbieraniu danych i weryfikacji wzorca: z wykorzystaniem urządzenia oraz modelu „na serwerze”. Pierwszy z nich charakteryzuje się wykorzystaniem czytników biometrycznych do rejestracji oraz weryfikacji biometrycznej za pomocą oprogramowania zainstalowanego w urządzeniu. W modelu „na serwerze” pobranie wzorców biometrycznych odbywa się za pomocą czytników urządzenia, jednak ich przetwarzanie (rejestracja i weryfikacja) następuje po przekazaniu do centralnego systemu biometrycznego. Dzięki temu mamy możliwość skorzystania z dodatkowej weryfikacji po stronie serwera oraz szansę na zbudowanie centralnej bazy wzorców biometrycznych, co daje większe możliwości, jeśli chodzi o moc obliczeniową, wykorzystanie danych

do nauki dla algorytmów sztucznej inteligencji oraz powiązanie różnych czynników w silniku uwierzytelniania i identyfikacji użytkowników. Wadą modelu „na serwerze” jest większe skomplikowanie i często rozmiar oraz wrażliwość przesyłanych i przechowywanych danych.

Głos klientów pokazuje bieżący poziom świadomości użytkowników bankowości internetowej i mobilnej, który jest wypadkową dotychczasowych doświadczeń z rozwiązaniami stosowanymi w bankach, własnej potrzeby bezpieczeństwa oraz potrzeby kontroli i wygody stosowanych rozwiązań. Nie da się zaprzeczyć, że poprzez promocję i utrzymanie pewnych konkretnych rozwiązań, takich jak choćby kody sms, oraz brak w masowej skali i świadomości incydentów podkopujących zaufanie do nich, wciąż są one niekwestionowanym standardem wykorzystywanym przez klientów. Rozwiązania mające na celu zwiększenie bezpieczeństwa, związane z wymaganiami silnego

uwierzalniania klienta w ramach PSD2, ewidentnie zwiększają czas potrzebny na przejście danego procesu i są często negatywnie odbierane przez klientów, również w kontekście percepcji ich bezpieczeństwa (na przykład konieczność zapisywania hasła, aby móc je poprawnie wpisać do systemu). Zastąpienie kodów SMS lub wykorzystanie dodatkowo metod biometrycznych wydaje się naturalnym krokiem w rozwoju metod uwierzalniania w zgodzie z wymogami regulacyjnymi oraz oczekiwaniami klientów, coraz częściej korzystającymi z rozwiązań mobilnych.

Coraz więcej banków stosuje lub testuje stosowanie biometrii przy logowaniu i autoryzacji transakcji, czego przykładem jest logowanie do aplikacji mobilnej z wykorzystaniem odcisków palca czy rozpoznawanie biometrii twarzy w co najmniej kilkunastu działających komercyjnie w naszym kraju bankach. Według dostępnych badań Polacy są otwarci na rozwiązania biometryczne, wskazując na ich wygodę i wierząc w ich bezpieczeństwo. W 2016 roku dwa banki, natomiast obecnie 13 banków wykorzystuje biometrię w różnych kontekstach użycia, od identyfikacji przez uwierzalnianie czy autoryzację w kanałach zdalnych.

Ponieważ projektując rozwiązania identyfikacji, uwierzalniania i autoryzacji, poruszamy się w trójkącie „bezpieczeństwo – wynik finansowy – ergonomia”, warto szukać rozwiązań, które przyniosłyby poprawę jednego z tych aspektów, pozostawiając pozostałe na podobnym, wysokim poziomie. Dlatego należałoby szukać optymalizacji zwiększających użyteczność w stosowanych już rozwiązaniach, ale równocześnie trzeba też dostrzegać potencjał w usługach, które od strony bezpieczeństwa i użyteczności są tak samo optymalne jak dotychczasowe, ale mogą przynieść znaczne oszczędności kosztowe.

1.5. Standaryzacja i certyfikacja rozwiązań biometrycznych

Jednym ze sposobów adresowania wyzwań związanych z nowymi zagrożeniami oraz ciągłą pogonią za bezpiecznymi rozwiązaniami na przyszłość jest tworzenie przez zaufane podmioty norm, reguł i zaleceń dotyczących proceduralnych oraz technicznych zasad tworzenia narzędzi identyfikacji i uwierzalniania, między innymi poprzez stworzenie ram „zawężających”, dostępnych tylko dla takiej specyficznej branży, jaką jest sektor finansowy.

Przykładem tego typu inicjatywy realizowanej przez sektor prywatny jest konsorcjum przemysłowe FIDO („Fast Identity Online”), stworzone przez ponad dwieście firm amerykańskich, głównie z sektora finansowego i technologicznego (na przykład PayPal, Bank

of America, Google, MasterCard, Visa, Qualcomm, RSA, Samsung czy Lenovo).

FIDO jest szerokim standardem, obejmującym zarówno dojrzałe, aktualnie powstające i będące w formie „załążkowej”, jak i mogące dopiero powstać narzędzia. Na pewno ma obejmować narzędzia biometryczne, na przykład bazujące na odcisku palca, naczyń krwionośnych, na identyfikacji głosu czy twarzy, a także na zabezpieczeniu techniczno-sprzętowym, a więc tokenach (w tym tokenach – USB), kartach mikroprocesorowych, modułach NFC oraz wbudowanych bezpiecznych elementach („embedded secure element”). FIDO docelowo ma umożliwiać integrację z dwoma wypracowywanymi standardami „dwustopniowego uwierzalniania” – Universal 2nd Factor (U2F) oraz Universal Authentication Framework (UAF). Pierwszy z nich, pierwotnie wypracowywany przez Google, a aktualnie otwarty, specjalizuje się w wykorzystywaniu narzędzi typu pamięci USB lub nośników NFC jako narzędzi uwierzalniania.

Innym przykładem jest 3D Secure 2.0, który jest zaktualizowaną w 2016 roku wersją standardu 3D Secure, uwzględniającą wymagania PSD2 w zakresie silnego uwierzalniania klienta poprzez wykorzystanie biometrii odcisku palca, głosu czy skanu twarzy. Standard ten uwzględnia przesunięcie w kierunku rozwiązań mobilnych oraz stanowi próbę budowy bezpiecznego ekosystemu dla płatności z wykorzystaniem mobilnych portfeli.

Wypowiedź eksperta

Standaryzacja i certyfikacja to fundamentalne procesy zapewniające szeroko rozumianą jakość i bezpieczeństwo. To samo dotyczy systemów IT, a w szczególności rozwiązań biometrycznych. Niestety, jak pokazuje dotychczasowa praktyka, obszar biometrycznych rozwiązań, pomimo istnienia szeregu standardów (np. ISO/IEC) dotyczących m.in. jakości obrazowania, parametrów wydajnościowych czy odporności na ataki podstawieniowe, opierał się procedurom certyfikacji. Z uwagi na brak powszechnej certyfikacji odbiorcy nie mają możliwości prostej weryfikacji parametrów rozwiązań (muszą skorzystać z badań laboratoryjnych pod kątem spełnienia kryteriów np. ISO czy NIST) i przez to są narażeni na niskiej jakości produkty. Na szczęście z pomocą w tej sytuacji przyszło międzynarodowe stowarzyszenie FIDO Alliance, zajmujące się standaryzacją usług uwierzalniania – będące autorem specyfikacji Universal Second Factor (U2F) oraz Universal Authentication Framework (UAF).

FIDO zaproponowało pierwszy na szeroką skalę program certyfikacji dla rozwiązań rozpoznawania biometrycznego – Biometric Component Certification.



W ramach certyfikacji weryfikowane są parametry wydajnościowe systemu biometrycznego (estymatory błędów częstości fałszywej akceptacji i fałszywego odrzucenia: False Acceptance Rate [FAR] i False Rejection Rate [FRR]) oraz odporność rozwiązań na ataki prezentacyjne (Presentation Attack Detection [PAD]) – estymator błędu akceptacji nieautentycznej próbki obcej: Impostor Attack Presentation Accept Rate (IAPAR).

W proces badania rozwiązań biometrycznych włączone są akredytowane laboratoria (lista znajduje się na stronie FIDO), które wykonują testy według obowiązujących w środowisku standardów dotyczących rozpoznawania biometrycznego, tj. norm ISO/IEC-19795 oraz ISO/IEC-30107. FIDO przyjmuje w swojej testowej metodyce, że badane rozwiązania powinny spełniać następujące wymagania: współczynnik FRR na poziomie nie większym niż 5% (5/100) dla zadeklarowanego FAR, zaś współczynnik FAR powinien być nie większy niż 0,01% (1/10000). Wartość współczynnika IAPAR powinna być nie większa niż 7% (7/100). Producent rozwiązania może zadeklarować niższe wartości współczynników niż wymagane przez FIDO i przedstawić opcjonalnie również dane z badań własnych (ang. self-attestation).

Wojciech Wodo, Kierownik B+R Payeye

1.6. Czynniki sprzyjające wzrostowi popularności i przyswajania biometrii, a kwestie bezpieczeństwa

Jak wskazaliśmy w poprzednich rozdziałach, wzrost popularności rozwiązań biometrycznych wiąże się z masową akceptacją przez użytkowników oraz poszukiwaniem coraz wygodniejszych, a zarazem bezpiecznych rozwiązań, które zastąpią rozwiązania oparte o hasła oraz kody SMS. Te znane i popularne metody autoryzacji stają się już dziś niewystarczające, a zarazem – ze wzrostem dostępności nowych metod biometrycznych – pojawia się szansa na powiązanie ich w celu budowy spójnego ekosystemu bankowości, która w sposób wygodny wykorzystuje metody biometryczne do zapewnienia odpowiedniego poziomu bezpieczeństwa połączonego z wygodą wykorzystania rozwiązań mobilnych.

Coraz częściej widzimy rozwiązania biometryczne, które w sposób niemal niezauważony są uruchamiane w celu zwiększenia bezpieczeństwa krytycznych procesów związanych z uwierzytelnianiem użytkownika. Przykładem może tutaj być FaceID lub biometria behawioralna na etapie logowania do aplikacji mobilnej bankowości.

Oczywiście wygoda rozwiązania jest wysoce pożądaną cechą rozwiązań biometrycznych, jednak w pierw-

szej fazie wdrożeń często potrzebna była faza bardziej widocznych weryfikacji biometrycznych z uwagi na zbudowanie świadomości bezpieczeństwa rozwiązania. Jednak z czasem przyzwyczajenie i „normalne” korzystanie staje się z perspektywy użytkownika ważniejsze niż obawa przed nieautoryzowanym dostępem. Z drugiej strony pozwala to na jeszcze wygodniejszą implementację procesów płatności czy identyfikacji użytkownika, czego przykładem mogą być rozwiązania wykorzystujące mobilne portfele czy autoryzację w bankowości do innych procesów identyfikacji czy usług zaufania w administracji publicznej lub innych usługach komercyjnych, które wymagają wysokiego poziomu bezpieczeństwa oraz wygody użytkownika.

Wypowiedź eksperta

Niewątpliwie na wzrost popularności rozwiązań biometrycznych wpłynął sam fakt oswojenia się z nimi poprzez silną ekspozycję, m.in. dzięki producentom smartfonów – najpierw rozwiązania oparte o odcisk palca (Touch ID), a potem o biometrię twarzy (Face ID). Użytkownicy zweryfikowali swoje lęki i uprzedzenia w praktyce, mając okazję doświadczyć wygody i łatwości wykorzystania tych rozwiązań do odblokowywania swojego telefonu. Później dołączyły do nich kolejne użycia – aplikacje bankowe czy narzędzia służące do zarządzania tożsamością (mObywatel). W tych przypadkach rolę odgrywał autorytet instytucji, które wprowadzały takie rozwiązania – np. środowiska bankowego.

Olbrzymi wpływ na wzrost świadomości i zaufania do rozwiązań biometrycznych miało również wprowadzenie dyrektywy UE PSD2, która na szeroką skalę wymusiła użycie tzw. silnego uwierzytelniania (SCA – Strong Customer Authentication) i zobligowała środowisko bankowe do wdrożenia rozwiązań technicznych w tym zakresie.

Obecnie nie trzeba już nikogo przekonywać, że biometria działa i jest wygodna. Pozostaje pytanie, na ile jest bezpieczna? W tym przypadku należy jak zawsze zwrócić uwagę na kilka aspektów: przede wszystkim na higienę użycia biometrii oraz świadomość użytkowników, jakość implementacji rozwiązań biometrycznych oraz dbałość dostawców rozwiązań o ochronę danych biometrycznych.

Na część wymienionych wyzwań odpowiedź stanowią wspomniane już wcześniej w rozdziale 1.5 standaryzacja i certyfikacja, zaś edukacja rynku i klienta jest procesem cyklicznym i ciągłym. Okazuje się, że bezpieczeństwo i wygoda nie zawsze muszą być ze sobą sprzeczne; wydaje się, że dobrze przygotowane i wdrożone rozwiązanie biometryczne stanowi tego doskonały przykład.

Wojciech Wodo, Kierownik B+R Payeye

1.7. Czynniki warunkujące wzrost odporności na ataki systemów opartych o biometrię

Technologie biometryczne służą do rozpoznawania osób na podstawie cech biologicznych i behawioralnych, w związku z czym są często wykorzystywane jako element systemów bezpieczeństwa. System bezpieczeństwa wspomagany technologią biometryczną ma na celu rozpoznawanie osób, które są identyfikowane jako „przyjaciele” lub „wrogowie”, lub może próbować rozpoznać osoby, które nie są znane systemowi jako jedno z nich. Od początku istnienia technologii opartych o biometrię powszechnie uznawano możliwość podważenia rozpoznawania przez przeciwników biometrii, podobnie jak potrzebę zastosowania środków bezpieczeństwa w celu wykrywania i pokonania prób podważenia rozpoznawania lub ataków prezentacyjnych.

Atak na biometrię lub próba podważenia wyniku weryfikacji biometrycznej mogą mieć miejsce w dowolnym punkcie systemu bezpieczeństwa i być podejmowane przez dowolnego uczestnika, czy to osobę wewnątrz systemu, czy też z zewnątrz. System oparty o biometrię służy do kontroli ryzyka, w szczególności

takiego, że niewłaściwa osoba uzyska dostęp lub zostanie błędnie zidentyfikowana. Dostępne są międzynarodowe standardy, jak ISO/IEC 30107-1:2016 *Information technology – Biometric presentation attack detection – Part 1: Framework*, które określają techniki automatycznego wykrywania ataków na prezentację, zwane *Presentation Attack Detection – PAD*³). Standard jest skierowany do dostawców systemów biometrycznych i laboratoriów testowych.

Standard ISO 30107 rozróżnia trzy poziomy ryzyka⁴:

- Poziom A, który nie wymaga dużego nakładu finansowego i czasu do przeprowadzania ataku oraz umiejętności atakującego
- Poziom B, który wymaga umiarkowanych umiejętności oraz kilku dni przygotowań do przeprowadzenia ataku
- Poziom C, który wymaga większych nakładów finansowych, dużych umiejętności oraz kilkunastu dni przygotowań do przeprowadzenia ataku.

Poniżej zaprezentowano tabelę zawierającą mapowanie poziomów na dany typ biometrii oraz atrybut ataku:

	ODCISK PALCA	TWARZ	TĘCZÓWKA	GŁOS
Poziom A	wydruk papierowy, bezpośrednie wykorzystanie ukrytego wydruku na skanerze	wydruk papierowy wizerunek twarzy, wyświetlacz telefonu komórkowego ze zdjęciem twarzy	Wydruk papierowy, wyświetlacz telefonu komórkowego ze zdjęciem tęczówki	powtórka nagrania audio
Poziom B	Poziom A, Odcisk palca wykonany ze sztucznego materiału, jak żelatyna, silikon, masa plastyczna	Poziom A, maska papierowa, wyświetlacz wideo z twarzą (z ruchem i mruganiem)	Poziom A, wyświetlacz wideo z tęczówką (z ruchem i mruganiem)	Poziom A, powtórka nagrania audio z określoną frazą, naśladowanie głosu
Poziom C	Poziom A&B, wydruk 3D	Poziom A&B, maski silikonowe, maski teatralne	Poziom A&B, soczewki kontaktowe z określonym wzorem	Poziom A&B, syntezytor mowy

Źródło: https://www.nist.gov/system/files/documents/2020/09/03/10_ibpc-prez-fido-ssanden-v5.pdf

³ (PAD) Wykrywanie ataku prezentacyjnego. Podgrupa metod określania ataku prezentacyjnego, zwana wykrywaniem obecności, obejmuje pomiar i analizę cech anatomicznych lub mimowolnych bądź dobrowolnych reakcji w celu ustalenia, czy próbka biometryczna jest pobierana od żywego podmiotu obecnego w punkcie pobrania. https://csrc.nist.gov/glossary/term/presentation_attack_detection.

⁴ https://www.nist.gov/system/files/documents/2020/09/03/10_ibpc-prez-fido-ssanden-v5.pdf (styczeń 2022)



Celem standardu ISO/IEC 31007-1:2016 jest zapewnienie podstaw (ang. *framework*) dla wykrywania ataków na prezentację, zdefiniowanie terminów i ustanowienie ram, za pomocą których da się określić i wykryć ataki prezentacyjne, aby można je było kategoryzować, uszczegóławiać i komunikować w celu późniejszego podejmowania decyzji w systemie biometrycznym oraz działań związanych z oceną wyników. Standaryzacja obszaru wykorzystania systemów biometrycznych oraz identyfikacja podstawowych mechanizmów ataku jest zasadniczym czynnikiem warunkującym budowanie odporności systemów bezpieczeństwa wszystkich dostawców technologii opartych o biometrię.

Kolejnym standardem, tym razem technicznym, jest ETSI TS 119 461 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects*, który definiuje wymagania dla dostawców komponentów wspierających proces potwierdzania tożsamości na rzecz dostawców usług zaufania (m.in. proces zdalnego potwierdzania tożsamości oparty o techniki biometryczne). Jest to nowy standard, zatwierdzony w roku 2021, który stanowi odpowiedź na potrzeby rynkowe w zakresie zdefiniowania wymagań dla dostawców technologii wspierających procesy elektronicznej identyfikacji, również wykorzystujących biometrię w ramach zdalnej identyfikacji.

Kolejnym czynnikiem warunkującym w sposób pośredni wzrost odporności systemów są prowadzone przez certyfikowane laboratoria niezależne badania, których celem jest przeprowadzenie ataków PAD w celu weryfikacji odporności danego rozwiązania biometrycznego. Jednym z takich laboratoriów jest firma iBeta, która posiada akredytację NIST NVLAP jako niezależne laboratorium testowe, a norma ISO 30107-3 jest objęta zakresem akredytacji. Firma iBeta przeprowadza ocenę na poziomie 1 oraz 2. Listę wybranych wyników ocen firmy iBeta można prześledzić na stronie laboratorium⁵.

Ostatnim i znaczącym czynnikiem warunkującym wzrost odporności są prowadzone cyklicznie, od wielu lat badania National Institute of Standards and Technology (NIST). NIST to amerykańska agencja rządowa, której misją jest opracowywanie i ustanawianie standardów, mających zastosowanie w wielu różnych branżach – w tym standardów technologii

informatycznych, cyberbezpieczeństwa, a także biometrii. NIST prowadzi również programy testowe, w ramach których wykonywana jest szeroka ewaluacja rozwiązań biometrycznych dostawców, którzy wyrażą wolę przystąpienia do badania i poddania się ocenie.

Face Recognition Vendor Test (FRTV) został przeprowadzony po raz pierwszy w 2000 roku, w odpowiedzi na zapotrzebowanie amerykańskich instytucji rządowych. Jego celem była techniczna ocena możliwości dostępnych na rynku systemów rozpoznawania twarzy. W teście wzięło udział pięciu dostawców. W latach 2002-2013 NIST przeprowadził jeszcze cztery edycje tego programu testowego, a od 2017 roku FRTV prowadzony jest nieprzerwanie, z raportami publikowanymi w przybliżeniu co miesiąc. Program FRTV obejmuje badanie technologii biometrycznych w kilku zakresach, m.in. w zakresie weryfikacji tożsamości 1:1 i identyfikacji 1:N, zdolności wykrywania przekształconych fotografii twarzy (*face morph*) czy wpływu jakości analizowanych fotografii twarzy na skuteczność algorytmów biometrycznych.

Badania prowadzone przez podmioty takie jak NIST – niezależne od dostawców technologii biometrycznych, a jednocześnie kojarzone jako wysoce kompetentne – i publikowane przez nie raporty są czynnikiem zdecydowanie pobudzającym rozwój biometrii. W FRTV 1:1 można zaobserwować rosnące liczby uczestniczących w testach dostawców rozwiązań biometrycznych. Pierwszy raport (2000) obejmował testy technologii zgłoszonych przez zaledwie pięć firm. W prowadzonym aktualnie ciągłym badaniu liczba uczestników wzrosła pięciokrotnie – od 31 w 2017 roku i do 156 w 2021. **Ma to związek zarówno ze wzrostem liczby nowych podmiotów na rynku technologii biometrycznych, jak i z ich dążeniem do stałej poprawy swoich produktów.** Dobre pozycje w rankingach badań takich jak prowadzone przez NIST stanowią bowiem cenne argumenty w negocjacjach z potencjalnymi nabywcami czy inwestorami.

Porównanie wyników z zaledwie pięciu lat badania ciągłego FRTV 1:1 pokazuje progres, jaki poczyniły technologie biometryczne. W niektórych pomiarach można zaobserwować wzrost skuteczności o blisko dwa rzędy wielkości – tabela na kolejnej stronie pokazuje wyniki liderów zestawień pomiędzy pierwszym a najnowszym badaniem danej kategorii:

⁵ <https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/>

	Zdjęcia paszportowe (visa images)	Zdjęcia policyjne (mugshot images)	Zdjęcia amatorskie („wild” images)
Najlepszy wynik w:	(FNMR @ FMR = 0,00001)	(FNMR @ FMR = 0,00001)	(FNMR @ FMR = 0,00001)
pierwszym badaniu (03–06.2017)	0,05	0,05	0,4
najnowszym badaniu (11.2021)	0,0006	0,0022	0,028
zmiana	+ 8333%	+ 2273%	+ 1429%

FNMR – false non-match rate; udział pasujących par błędnie uznanych za niepasujące (błędnie odrzuconych)

FMR – false match rate; udział niepasujących par błędnie uznanych za pasujące (błędnie zaakceptowanych)

1.8. Rozwój narzędzi technologicznych w biometrii a kwestie ochrony prywatności i bezpieczeństwa danych

Rozwój narzędzi technologicznych w biometrii nieustannie niesie ze sobą konieczność implementowania mechanizmów bezpieczeństwa chroniących dane biometryczne oraz prywatność osoby fizycznej. Implementacja zabezpieczeń wynika przede wszystkim z obowiązujących regulacji prawnych. W Europie obowiązuje ogólne rozporządzenie o ochronie danych (RODO), które wprost oznacza dane biometryczne jako takie, które wymagają szczególnego traktowania i ochrony. Zgodnie z definicją dane biometryczne oznaczają *dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne*. Utrata kontroli nad danymi biometrycznymi może nieść poważne ryzyko dla podstawowych praw i wolności jednostki. Co istotne, zgodnie z artykułem 9 RODO, przetwarzanie danych biometrycznych traktuje się jako przetwarzanie szczególnych kategorii danych osobowych i jest ono domyślnie zabronione. Najważniejszą przesłanką, która dopuszcza przetwarzanie tego rodzaju danych, jest spełnienie warunku pozyskania wyraźnej zgody od osoby, której dane dotyczą. Istnieją także inne przesłanki, które są wskazywane w opiniach prawnych jako dopuszczalne. Na przykład wskazuje się, że dopuszczalne jest przetwarzanie danych szczególnych kategorii, jeżeli jest ono niezbędne ze względów związanych z ważnym interesem publicznym. W opinii prawnej kancelarii Osborne Clarke przesłanka ta może być zastosowana w sektorze bankowym w celach ochrony klientów banku czy zabezpieczenia transakcji elektronicznych. Przetwarzanie w związku z ważnym interesem pu-

blicznym jest już stosowane w praktyce w bankach w Europie, które zapewniają zgodność z przepisami RODO. Odniesienia do tych przesłanek są zwykle spotykane, gdy są one zgodne z mandatem do powiadamiania swoich klientów w ich publicznych warunkach użytkowania. Powiadomienia te często odnoszą się do prawa do przetwarzania wrażliwych danych osobowych na podstawie prawnej z RODO (lub innej regulacji), gdy chodzi o interes publiczny, bezpieczeństwo lub roszczenia prawne, i powołują się na potencjalną obserwację „działań użytkownika» w aplikacjach, formularzach, stronach internetowych, aplikacjach mobilnych i innych formach korzystania z usług⁶.

W celu spełnienia wymagań prawnych dostawcy oraz prawni administratorzy narzędzi biometrycznych (np. banki) muszą uwzględnić stosowanie silnych zabezpieczeń. Analizując dostępne rozwiązania oparte o biometrię, obserwuje się stosowanie różnych warstw ochrony. W przypadku danych pobranych z odcisków palca czy głosu są to najczęściej rozwiązania bazujące na architekturze urządzenia użytkownika. Wzorzec biometryczny jest przechowywany wyłącznie na urządzeniu. Jest to najczęściej spotykane w smartfonach, które używają czujników linii papilarnych Touch ID, takich jak „Secure Enclave” firmy Apple. Pamięć na urządzeniu może służyć do przechowywania danych biometrycznych za pośrednictwem chipa, który przechowuje dane oddzielnie w sieci urządzenia. Przechowując dane na samym urządzeniu, organizacja wdrażająca proces weryfikacji biometrycznej nie ma nad nimi kontroli. Ten rodzaj przechowywania danych biometrycznych jest szczególnie bezpieczny, ponieważ nie przechowuje się żadnych wrażliwych danych na serwerach baz danych.

⁶ Report 2021 Global Data Privacy Regulation of Physical & Behavioral Biometrics, s. 18



W przypadku danych behawioralnych (biometria behawioralna) mamy do czynienia z zabezpieczeniami stosowanymi wyłącznie po stronie przetwarzającego dane, np. banku. Oto główne stosowane mechanizmy:

- Tworzony jest unikatowy profil behawioralny, przechowywany w formie zbioru danych niezawierającego informacji, takich jak imię, nazwisko czy numer konta bankowego. W zbiorze danych zapisywane są wyłącznie informacje o sposobie używania urządzeń, np. klawiatury, myszki czy ekranu telefonu.
- Profil behawioralny oraz dane w nim zawarte chronione są za pomocą kryptografii symetrycznej oraz jednokierunkowej funkcji skrótu. Dzięki tym zabezpieczeniom można zawsze porównać zachowanie osoby do danego profilu, ale nie można na podstawie profilu odtworzyć zachowania osoby.
- Surowe dane, które są generowane i zbierane od powracających klientów, dodatkowo poprawiają profil i jego dokładność, a następnie są natychmiast usuwane.

W rozdziale 1.2, dotyczącym analizy silnych i słabych stron poszczególnych typów biometrii, wskazywano, że w przypadku kompromitacji wzorca może wystąpić brak możliwości ponownego użycia danego typu biometrii przez użytkownika (np. twarz). Dlatego z punktu widzenia bezpieczeństwa tak istotne jest przeprowadzanie przez banki i innych dostawców usług cyklicznego procesu analizy ryzyka w celu dopasowania odpowiedniej technologii i narzędzi biometrycznych w procesach identyfikacji, uwierzytelnienia i autoryzacji w oferowanych rozwiązaniach.

1.9. Biometria a elektroniczna identyfikacja i usługi zaufania

Rozwój narzędzi biometrycznych możemy zaobserwować w obszarze elektronicznej identyfikacji (eID) i usług zaufania, w szczególności jako komponentu wspierającego procesy rejestracji użytkowników, uwierzytelnienia do usług online i autoryzacji operacji (złożenie oświadczenia woli w przypadku podpisu elektronicznego). W celu pełnego zrozumienia i umiejscowienia biometrii w obszarze elektronicznej identyfikacji i usług zaufania należy zdefiniować obydwa terminy.

Zgodnie z definicją z rozporządzenia eIDAS, „identyfikacja elektroniczna oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną lub

osobę fizyczną reprezentującą osobę prawną”⁷. Dane dotyczące biometrii stanowią pewien zbiór danych, który umożliwia przeprowadzenie identyfikacji osoby, jednak nie jest to jedyny komponent, który składa się na usługę identyfikacji elektronicznej. Aby w pełni wyjaśnić zagadnienie elektronicznej identyfikacji, należy przedstawić pojęcie, które doprecyzuje ten obszar. Jest to pojęcie środka identyfikacji elektronicznej, który zgodnie z eIDAS oznacza „materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online”⁸. Przykładami takich środków mogą być:

- profil zaufany,
- profil osobisty (zawarty w warstwie elektronicznej dowodu osobistego) lub
- login, hasło oraz jednorazowy kod/biometria.

Środek identyfikacji elektronicznej musi posiadać wcześniej zdefiniowany zestaw danych pozwalających na identyfikację lub uwierzytelnienie. W każdym z powyższych przykładów dane biometryczne mogą być wykorzystywane jako czynnik wspierający proces identyfikacji (zakładanie środka identyfikacji) lub proces uwierzytelnienia (jako dostarczenie informacji o tym, kim jesteśmy, np. odcisk palca).

W rozporządzeniu eIDAS zostały zdefiniowane także usługi zaufania⁹, które oznaczają usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:

- tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
- tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub
- konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

Zgodnie z tą definicją biometria nie jest usługą zaufania, natomiast może być wykorzystywana w procesach identyfikacji i uwierzytelnienia na rzecz świadczenia konkretnej usługi zaufania.

Na rynku usług zaufania w Europie jest wielu dostawców, którzy oferują usługi zdalnej identyfikacji klienta na

⁷ Art. 3, pkt. 1 Rozporządzenie eIDAS.

⁸ Art. 3, pkt. 2 Rozporządzenia eIDAS.

⁹ art. 3 pkt 16 rozporządzenia eIDAS.

rzecz procesu wydawania certyfikatów podpisu elektronicznego. W szczególności okres pandemii przyniósł konieczność rozwoju tego typu usług. Usługi zdalnej (wideo)identyfikacji, które wykorzystują narzędzia biometryczne, są dostarczane w dwóch modelach:

- usługa identyfikacji z operatorem, który jest odpowiedzialny za przeprowadzenie weryfikacji tożsamości - narzędzia biometryczne są tutaj narzędziem wspierającym operatora w procesie ustalenia tożsamości czy zweryfikowania autentyczności dokumentu tożsamości;
- usługa wideoidentyfikacji bez operatora (automatyczna identyfikacja), która polega m.in. na wykorzystywaniu algorytmów biometrycznych w celu ustalenia, czy prezentowana twarz osoby identyfikowanej przed ekranem kamery urządzenia jest identyczna z wizerunkiem prezentowanym na zdjęciu twarzy na dokumencie tożsamości.

Mechanizmy biometryczne są wykorzystywane również w procesach autoryzacji w momencie składania kwalifikowanego podpisu elektronicznego. Posiadacz podpisu kwalifikowanego za pomocą aplikacji mobilnej służącej do składania podpisu jest w stanie autoryzować, np. za pomocą odcisku palca, dyspozycję oświadczenia woli.

Zastosowanie biometrii w kontekście identyfikacji ma miejsce przy potwierdzaniu tożsamości w oparciu o informacje zapisane w dokumentach tożsamości (dowody osobiste, paszporty). Konieczność podążania dokumentu za postępem technologicznym, a także rosnące zagrożenia międzynarodowe, wymogły opracowanie międzynarodowych norm, których celem było ujednolicenie dokumentów podróży i wprowadzenie w nich identyfikatorów biometrycznych, przy uwzględnieniu ujednoliconego podejścia do bezpieczeństwa danych. Pierwszym polskim dokumentem biometrycznym zawierającym elektroniczny nośnik informacji, a w nim zapisany cyfrowy wizerunek twarzy posiadacza, był paszport. W Polsce każdy obywatel wnioskujący o wydanie paszportu i uprawniony do jego posiadania od 2006 roku mógł otrzymać paszport biometryczny. Od czerwca 2009 roku jest on dodatkowo zabezpieczony drugą cechą biometryczną, zapisaną w mikroprocesorze (odcisk palca)¹⁰. Z kolei w dowodach osobistych dane biometryczne (zdjęcie biometryczne) są umieszczane od marca 2019 roku, natomiast od listopada 2021 są już wydawane dokumenty z drugą cechą (odciskiem palca).

Ciekawym zastosowaniem biometrii jest technologia podpisu biometrycznego, która może stanowić alternatywę dla klasycznych podpisów opartych o Infrastrukturę Klucza Publicznego. Jest to podpis elektroniczny, którego ideą jest odwzorowanie podpisu odręcznego w formacie elektronicznym, który zachowa wszystkie jego dotychczasowe biometryczno-grafologiczne cechy, natomiast zostanie wzbogacony o takie cechy, jak czas złożenia podpisu, przyspieszenie/tempo składanego podpisu oraz nacisk używanego piórka na matrycę. Podpis składany jest na urządzeniach ze specjalnym oprogramowaniem, wyposażonych w dotykowe ekrany; w zależności od ich typów, zapisywany jest szereg parametrów wykorzystywanych w analizie autentyczności¹¹. Dane biometryczne podpisu, unikalne dla każdego człowieka, przechowywane są w dokumencie w postaci zaszyfrowanej, lecz możliwej do odczytania w przypadku konieczności analizy autentyczności złożonego podpisu. Wykorzystanie danych biometrycznych zbieranych z podpisu odręcznego oraz mechanizmy szyfrowania użyte w samym oprogramowaniu zwiększają wielokrotnie poziom bezpieczeństwa podpisywania dokumentów w porównaniu z tradycyjnym, papierowym procesem. Bezpieczeństwo całego procesu może zostać wzmocnione za pomocą usług zaufania, takich jak kwalifikowana pieczęć elektroniczna (zapewnienie integralności dokumentu) czy znacznika czasu w celu określenia czasu powstania dokumentu elektronicznego.

Podpis biometryczny odnalazł zastosowanie w następujących sektorach:

- Sprzedaż – zawieranie umów ubezpieczeniowych, wynajem samochodów, obrót nieruchomościami, umowy leasingowe;
- Zdrowie – wyrażanie zgód przez pacjentów;
- HR – dokumentacja pracownicza;
- Logistyka – obsługa zamówień, protokoły;
- Compliance – umowy o zachowaniu poufności we współpracy między firmami (NDA), kontrakty biznesowe;
- Operatorzy pocztowi – potwierdzenie odbioru.

¹⁰ <https://www.cpd.gov.pl/technologia/biometria-w-dokumentach/>

¹¹ Informacje marketingowe <https://www.monolit-it.pl/pl/oferta/dla-it/E-podpis-SIGNATURIX>



Biometria w polskiej bankowości elektronicznej. Benchmarking zastosowania biometrii na rynku bankowości elektronicznej



2.1. Konteksty zastosowania biometrii w bankowości i płatnościach elektronicznych na rynku polskim

Niniejszy rozdział zawiera podsumowanie wybranych zastosowań biometrii w bankowości i płatnościach elektronicznych w ujęciu 15 analizowanych, największych polskich banków.

Identyfikacja użytkowników na potrzeby procesu rejestracji jako nowych użytkowników bankowości elektronicznej na przestrzeni ostatnich kilku lat znacząco ewaluowała. Obecnie 12 na 15 analizowanych banków oferuje zakładanie rachunku zdalnie przy wykorzystaniu metod biometrycznych i stanowi istotną alternatywę dla tradycyjnych kanałów pozyskiwania nowych klientów (oddział, kurier). W tym kontekście istotne jest jeszcze, iż konta uruchamiane zdalnie mają ograniczoną funkcjonalność, na przykład nie pozwalają na aktywację Profilu Zaufanego, czyli środka identyfikacji elektronicznej w celu korzystania z publicznych usług cyfrowych. Porównując te dane z danymi z raportu **Obserwatorium.biz Bezpieczeństwo bankowości elektronicznej**¹² z roku 2016, należy stwierdzić, że nastąpił istotny wzrost popularyzacji tej metody. W ówczesnym raporcie nie odnotowano takiego procesu u żadnego z banków.

Poza procesem rejestracji biometria znajduje coraz szersze zastosowanie w procesach uwierzytelnienia oraz autoryzacji operacji:

1. W roku 2016 na 10 badanych banków, tylko 4 zapewniały możliwość logowania do bankowości mobilnej przy wykorzystaniu biometrii. Obecnie

(stan na styczeń 2021), wszystkie 15 analizowanych banków umożliwia logowanie za pomocą biometrii.

2. W 2016 roku żaden bank nie stosował mobilnej autoryzacji. Wówczas metodami autoryzacji były kody sms, hasła mobilne czy tokeny sprzętowe lub mobilne. Obecnie dostrzegalny jest wzrost popularności mobilnej autoryzacji, do której powoli podłączane są metody biometrii:

- uwierzytelnienie do bankowości internetowej oparte o biometryczną autoryzację stosują 4 na 15 banków;
- autoryzacja przelewów za pomocą biometrii zleconych w bankowości zarówno internetowej, jak i mobilnej dopuszcza 6 z 15 banków;
- autoryzacja pożyczek zleconych w bankowości mobilnej i internetowej jest na tym samym poziomie – umożliwiają takie rozwiązanie 2 z 15 banków;
- autoryzację płatności kartą w Internecie (3D Secure) za pomocą biometrii umożliwia 10 z 15 banków.

Wszędzie tam, gdzie bank dopuścił autoryzację transakcji za pomocą biometrii, jest przewidziany alternatywny (zapasowy) kanał autoryzacji (wcześniej zdefiniowany PIN/hasło mobilne), na wypadek, gdyby wystąpił problem z jej użyciem.

Poniżej zaprezentowano tabelę podsumowującą zastosowania biometrii według stanu na styczeń 2022.

¹² <https://obserwatorium.biz/bezpieczenstwo-bankowosci-elektronicznej-01-2016.html>

**Tabela 1.** Podsumowanie zastosowania biometrii na rynku bankowości elektronicznej – stan styczeń 2022

Konteksty zastosowania biometrii	Alior	BNP Paribas	Bank Pekao	PKO BP	mBank	Millenium	Bank Handlowy	BOŚ	Bank Pocztowy	Credit Agricole	ING Bank	Nest bank	Getin Bank	Santander	SGB	Zestawienie
Zakładanie rachunku za pomocą technologii biometrycznych	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Nie	Nie	Tak	Tak	Nie ¹³	Tak	Tak	Tak	12/15
Uzyskanie kredytu za pomocą technologii biometrycznych	Tak (firmy)	Nie	Nie	Nie	Nie	Nie	Tak (karta kredytowa)	Nie	Tak	Nie	Nie	Nie	Tak	Nie	Nie	4/15
Logowanie do aplikacji mobilnej	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	15/15
Uwierzytelnienie do bankowości internetowej oparte o biometryczną autoryzację	Nie	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	Tak	Nie	Tak	Tak	Nie	4/15
Autoryzacja przelewów zleconych w bankowości internetowej	Nie	Nie	Nie	Tak	Tak	Tak	Nie	Nie	Nie	Nie	Tak	Nie	Tak	Tak	Nie	6/15
Autoryzacja przelewów zleconych w bankowości mobilnej	Tak	Nie	Tak	Tak	Tak	Tak	Nie	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Nie	6/15
Autoryzacja pożyczki zleconej w bankowości mobilnej	Nie	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Nie	Tak ¹⁴	Nie	Nie	2/15
Autoryzacja pożyczki zleconej w bankowości internetowej	Nie	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Nie	Tak ¹⁵	Nie	Nie	2/15
Autoryzacja płatności kartą w Internecie	Tak	Tak	Nie	Nie	Nie	Tak	Nie	Nie	Tak	Tak	Tak	Tak	Tak	Tak	Tak	10/15

Źródło: Opracowanie własne

¹³ Nest Bank umożliwia założenie rachunku za pomocą wideoidentyfikacji z operatorem, natomiast w toku prac nad niniejszym raportem nie potwierdzono, czy w ramach procesu są wykorzystywane mechanizmy biometrii.

¹⁴ Weryfikacja tożsamości odbywa się za pomocą weryfikacji selfie

¹⁵ J.w.

2.2. Funkcje (logowanie, autoryzacja transakcji), urządzenia (mobile vs. desktop) i typy zbieranych wzorców (odcisk palca, twarz, styl pisania)

Na użytek niniejszego raportu przeprowadzono analizę i weryfikację funkcji biometrycznych w kontekście danego rodzaju bankowości elektronicznej. Weryfikacji podlegały zastosowane wzorce biometryczne, takie jak odcisk palca, twarz, styl pisania w odniesieniu do możliwości ich zastosowania w bankowości mobilnej (telefon) oraz bankowości internetowej (desktop). Jako przykład funkcji wybrano następujące czynności:

- logowanie do usługi;
- autoryzacja przelewu;
- autoryzacja transakcji kartą w Internecie (mechanizm 3D Secure).

Na podstawie przeprowadzonych badań można stwierdzić, że biometria w **bankowości mobilnej** jest już mocno zakorzeniona. Potwierdza to wynik, który wskazuje, że wszystkie badane banki (15) w pewnym stopniu umożliwiają wykonywanie czynności w oparciu o biometrię. Podsumowanie wyników prezentuje się następująco:

1. Logowanie do aplikacji mobilnej

- Wszystkie banki umożliwiają logowanie do aplikacji mobilnej za pomocą odcisku palca;¹⁶

- 13 z 15 banków umożliwia logowanie za pomocą twarzy;
- Cztery z nich umożliwiają logowanie za pomocą tęczówki oka.

Logowanie twarzą może być uwarunkowane systemem operacyjnym (iOS, Android) po stronie urządzenia klienckiego. Zdarzają się sytuacje, kiedy logowanie twarzą dostępne jest tylko z poziomu konkretnego systemu operacyjnego (np. iOS w Banku Millenium czy Citi Handlowy).

2. Autoryzacja przelewu zleconego w bankowości mobilnej

- Autoryzację za pomocą odcisku palca i twarzy dopuszcza 5 z 15 banków,
- Dwa banki umożliwiają autoryzację za pomocą tęczówki oka.

W większości przypadków autoryzacja przelewów jest ograniczona do określonych progów kwotowych (np. Pekao SA do kwoty 120 zł).

Poniższa tabela prezentuje podsumowanie funkcji biometrycznych na urządzeniu typu mobile, co oznacza różne zastosowania w kontekście zleceń realizowanych za pomocą bankowości mobilnej (według stanu na 2022).

Tabela 2. Podsumowanie funkcji biometrycznych na urządzeniu typu mobile – stan styczeń 2022

Funkcje biometryczne na urządzeniu typu mobile (bankowość mobilna)	Alor	BNP Paribas	Bank Pekao	PKO BP	mBank	Millenium	Bank Handlowy	BOŚ	Bank Pocztowy	Credit Agricole	ING Bank	Nest bank	Getin Bank	Santander	SGB	Zestawienie
Logowanie do bankowości za pomocą odcisku palca	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	15/15
Logowanie do bankowości za pomocą twarzy	Nie	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Nie	Tak	Tak	13/15
Logowanie do bankowości za pomocą tęczówki oka ¹⁶	Nie	Tak	Tak	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	4/15

¹⁶ Na wybranych telefonach z systemem Android można używać rozpoznawania tęczówki.



Tabela 2. cd.

Funkcje biometryczne na urządzeniu typu mobile (bankowość mobilna)	Allor	BNP Paribas	Bank Pekao	PKO BP	mBank	Millenium	Bank Handlowy	BOŚ	Bank Pocztowy	Credit Agricole	ING Bank	Nest bank	Getin Bank	Santander	SGB	Zestawienie
Autoryzacja przelewu za pomocą odcisku palca	Tak	Nie	Tak	Tak	Tak	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Nie	5/15
Autoryzacja przelewu za pomocą twarzy	Tak	Nie	Tak	Tak	Tak	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Nie	5/15
Autoryzacja przelewu za pomocą tęczy oka	Nie	Nie	Tak	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	2/15

Źródło: Opracowanie własne

Biometria w **bankowości internetowej** spełnia nieco inną rolę. Żaden ze wzorców biometrycznych nie jest wykorzystywany do operacji logowania do bankowości internetowej. Pierwsze zastosowanie możemy zidentyfikować w przypadku autoryzacji operacji przelewów zleconych w bankowości internetowej (mobilna autoryzacja przy wykorzystaniu aplikacji bankowej). Szczegółowe wyniki są następujące:

- Autoryzację za pomocą odcisku palca dopuszcza 7 z 15 banków;
- Autoryzację za pomocą twarzy dopuszcza 7 z 15 banków;
- Autoryzację za pomocą tęczy oka dopuszczają 2 z 15 banków.

W tym miejscu warto też wskazać, że dwa banki (mBank oraz ING Bank Śląski) oferują możliwość uruchomienia biometrii behawioralnej, która wspiera proces weryfikacji przelewu po stronie banku. Ostatnią weryfikowaną funkcją była autoryzacja płatności kartą w Internecie. Wyniki prezentują się następująco:

- Autoryzację płatności kartą za pomocą odcisku palca dopuszcza 11 z 15 banków;
- Autoryzację płatności kartą za pomocą twarzy dopuszcza 11 z 15 banków;
- Autoryzację płatności kartą za pomocą tęczy oka dopuszczają 2 z 15 banków.

Użycie konkretnej metody biometrycznej w operacji logowania jest w dużej mierze uwarunkowane urządzeniem (telefonem z konkretnym systemem operacyjnym oraz wspierającą technologią), które dopuszcza stosowanie konkretnej metody. Natomiast w przypadku autoryzacji przelewów za pomocą mobilnej autoryzacji widać wyraźnie działające mechanizmy oceny ryzyka, gdyż duża część banków w niskim stopniu wdrożyła funkcje biometrii do zatwierdzania operacji lub jeśli ją wdrożyła, to są to operacje niskiego ryzyka.

Poniższa tabela prezentuje podsumowanie funkcji biometrycznych na urządzeniu typu desktop, co oznacza różne zastosowania w kontekście zleceń realizowanych za pomocą bankowości internetowej (według stanu na styczeń 2022).

**Tabela 3.** Podsumowanie funkcji biometrycznych na urządzeniu typu desktop – stan styczeń 2022.

Funkcje biometryczne na urządzeniu typu desktop (bankowość internetowa)	Alior	BNP Paribas	Bank Pekao	PKO BP	mBank	Millenium	Bank Handlowy	BOŚ	Bank Pocztowy	Credit Agricole	ING Bank	Nest bank	Getin Bank	Santander	SGB	Zestawienie
Logowanie do bankowości za pomocą odcisku palca	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	0/15
Logowanie do bankowości za pomocą twarzy	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	0/15
Logowanie do bankowości za pomocą tęczówki oka	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	0/15
Autoryzacja przelewu ¹⁷ za pomocą odcisku palca	Tak	Nie	Nie	Tak	Tak	Tak	Nie	Nie	Nie	Nie	Tak	Nie	Tak	Tak	Nie	7/15
Autoryzacja przelewu ¹⁸ za pomocą twarzy	Tak	Nie	Nie	Tak	Tak	Tak	Nie	Nie	Nie	Nie	Tak	Nie	Tak	Tak	Nie	7/15
Autoryzacja przelewu ¹⁹ za pomocą tęczówki oka	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	2/15
Autoryzacja przelewu za pomocą profilu behawioralnego	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	2/15
Autoryzacja płatności kartą za pomocą odcisku palca	Tak	Tak	Nie	Nie	Nie	Tak	Nie	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	11/15
Autoryzacja płatności kartą za pomocą twarzy	Tak	Tak	Nie	Nie	Nie	Tak	Nie	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	11/15
Autoryzacja płatności kartą za pomocą tęczówki oka	Nie	Tak	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Nie	Tak	Nie	Nie	Nie	Nie	2/15

Źródło: Opracowanie własne

¹⁷ Mobilna autoryzacja.¹⁸ Mobilna autoryzacja.¹⁹ Mobilna autoryzacja.



2.3. Wybrane przykłady zastosowania biometrii na polskim rynku finansowym – benchmarking polskiego rynku oraz najciekawsze przykłady z EU

Jednym z najbardziej dostrzegalnych zastosowań biometrii na polskim rynku finansowym jest zdalne zakładanie rachunków bankowych za pomocą wideoweryfikacji (w sposób samodzielny przez użytkownika przy użyciu selfie). Okres pandemii SARS-CoV-2 z całą pewnością przyspieszył proces wdrożenia przez sektor finansowy modelu pozyskiwania nowych klientów za pomocą zdalnej identyfikacji. W rozdziale 2.1 mogliśmy zauważyć, że na 15 analizowanych banków aż 13 umożliwia założenie rachunku bankowego w sposób zdalny, bez wychodzenia z domu.

Rozwiązania z zastosowaniem zdalnej identyfikacji znajdziemy również w innych krajach Unii Europejskiej. Rynek dostawców identyfikacji automatycznej (tzw. selfID) oraz identyfikacji z operatorem (tzw. wideoID) rozwija się, a wdrożenia w sektorze finansowym możemy znaleźć w takich krajach, jak Hiszpania, Włochy, Austria, Bułgaria, Grecja, a także w Wielkiej Brytanii (od niedawna poza Unią Europejską).

Innym ciekawym zastosowaniem jest biometryczna karta płatnicza, którą w grudniu 2021 roku do swojej oferty wprowadził Bank Pocztowy. Jest to karta wydawana w systemie MasterCard, która posiada zintegrowany czytnik linii papilarnych. Biometria stanowi zabezpieczenie transakcji – jest wymagana przy płatnościach zbliżeniowych i zastępuje kod PIN. Wykonanie płatności kartą jest możliwe tylko po pozytywnym uwierzytelnieniu biometrycznym. Wzorzec biometryczny musi zostać najpierw zapisany na karcie – do tego przeznaczony jest specjalny czytnik dołączany do karty przez bank. Wzorzec jest zaszyfrowany i po zapisaniu na karcie służy do weryfikacji odcisku palca podczas wykonywania transakcji. Cała operacja odbywa się w układzie elektronicznym karty – ani wzorzec, ani pobrana próbka nie są transmitowane do systemów banku.

Kolejnym zastosowaniem biometrii, które było już sygnalizowane w rozdziale 2.1, jest autoryzacja biometryczna w transakcjach kartowych w internecie. Autoryzacja biometryczna zyskuje na znaczeniu w związku z obowiązkiem stosowania silnego uwierzytelniania (ang. strong customer authentication, SCA) przy płatnościach kartą od początku 2021 i jest częścią 3D Secure. W UE spotkamy się także z przypadkami stosowania biometrii w procesach pożyczkowych. Sofinco, działająca na rynku hiszpańskim firma pożyczkowa (zależna od Crédit Agricole Consumer Finance), wprowadziła możliwość wniosko-

wania online o pożyczki gotówkowe przy wsparciu biometrycznego rozpoznawania twarzy. Cały proces udzielenia pożyczki przebiega bez konieczności wizyty klienta w placówce stacjonarnej: identyfikacja i weryfikacja tożsamości odbywają się w oparciu o selfie i zdjęcie dowodu tożsamości, dodatkowo wymagane dokumenty można załączyć również w formie zdjęcia lub skanu, a do podpisania umowy służy hasło SMS.

Biometria znajduje swoje naturalne zastosowanie w środowisku usług finansowych oferowanych całkowicie zdalnie. Jednym z przykładów tak działających podmiotów jest brytyjska firma Monese, która operuje na rynku europejskim od 2015 roku jako Instytucja Pieniądza Elektronicznego. Monese oferuje tzw. natychmiastowe konta – rachunki płatnicze, które można otworzyć tylko online (firma nie prowadzi działalności stacjonarnej). Otwarcie rachunku odbywa się poprzez aplikację mobilną i wykorzystuje mechanizm skanowania tzw. OCR dokumentu oraz wideoweryfikację do potwierdzenia tożsamości wnioskodawcy. Obsługa rachunku i wydanej do niego karty płatniczej – fizycznej i wirtualnej – odbywa się również przez aplikację mobilną, do której dostęp można uzyskać także dzięki metodom identyfikacji biometrycznej dostępnym w smartfonach, czyli biometrii twarzy lub palca. Monese – FinTech, który w 2016 roku zdobył tytuł „Best Challenger Bank” podczas European Fintech Awards – odniósł sukces rynkowy i skutecznie konkuruje z tradycyjnymi bankami, oferując szybki i wygodny proces z minimalnymi warunkami wstępnymi w porównaniu do ich oferty. Aktualnie firma działa w ponad trzydziestu krajach i szczeni się pozyskaniem 2 mln klientów w 2020 roku. To osiągnięcie nie byłoby możliwe bez zastosowania biometrycznej metody identyfikacji i weryfikacji tożsamości, która zastąpiła tradycyjne procesy KYC i pozwoliła na skuteczne wykorzystanie przewag, jakie dają regulacje dotyczące działania Instytucji Pieniądza Elektronicznego wobec banków.

Ostatnią metodą, która nie jest jeszcze popularna, ale na pewno ma mocno innowacyjny charakter, są „płatności okiem”. Firma PayEye jako pierwsza na świecie wprowadziła komercyjnie możliwość płatności w ten sposób. Udostępniony został cały autorski ekosystem, na który składają się własne urządzenia płatnicze eyePOS, aplikacja dla użytkowników, system zawierający specjalne algorytmy oraz mocno rozbudowany proces, dzięki któremu czynność, jaką jest spojrzenie, może być w bezpieczny sposób „zamieniona w pieniądze”. Odpowiedzią na potrzebę zmiany w systemach płatności w dobie globalnego dynamicznego rozwoju jest technologia biometryczna, ponieważ otworzyła ona kolejne możliwości, nad którymi pracuje coraz więcej firm. Jednym z pionierów tego nowego kierunku jest właśnie PayEye –



który postanowił efektywnie wykorzystać ogromny potencjał biometrii. Decydując się na wykorzystanie tęczy oka, skoncentrowano się przede wszystkim na tym, aby to innowacyjne rozwiązanie i usługa były jeszcze bardziej bezpieczne, precyzyjne, skalowalne oraz globalne. Dalszym krokiem jest fuzja biometrii z wykorzystaniem zarówno tęczy, jak i twarzy.

Autorska identyfikacja daje szerokie możliwości i pozwala myśleć bardzo przyszłościowo i perspektywnie. W ramach stałego progresu PayEye rozwija się również w e-commerce. Zastosowań rozwiązania jest wiele – to, miejmy nadzieję, niebawem również imprezy masowe, identyfikacja na lotniskach czy paczkomaty.

Wypowiedź eksperta

Biometria, czyli mierzenie naszych indywidualnych cech fizycznych i behawioralnych w celu potwierdzania tożsamości, nie jest niczym nowym. Odcisk dłoni w jaskini pozostawiony przez prehistorycznego człowieka to właśnie jeden z pierwszych przykładów jej zastosowania. W dzisiejszych czasach, dzięki nowoczesnej technologii, możemy ją rozwijać i dostosowywać do potrzeb. Pod koniec zeszłego roku w Polsce pojawiła się pierwsza biometryczna karta płatnicza wyposażona w czytnik linii papilarnych, zwiększający bezpieczeństwo płatności. Biometria behawioralna, która zapamiętuje indywidualne zachowania użytkowników, to kolejny krok w stronę digitalizowania usług.

Jako Xtension szukaliśmy rozwiązania, które pomoże zoptymalizować sytuacje biznesowe face-to-face przy jednoczesnym zagwarantowaniu maksymalnego bezpieczeństwa zawieranych transakcji. Nasz produkt

– elektroniczny podpis biometryczny signaturIX – zachowuje zaawansowane parametry biometryczne podpisu, takie jak pozycja, prędkość, przyspieszenie ruchu rysika czy jego nacisk na matrycę w zaszyfrowanej postaci wewnątrz dokumentu. Co więcej, narzędzie zintegrowane jest z unikalną usługą Zaufanej Strony Trzeciej, świadczoną przez kwalifikowanego dostawcę Usług Zaufania, który gwarantuje poufność danych biometrycznych. Autentyczność i integralność podpisu zapewnia kwalifikowana pieczęć elektroniczna. Zebrane dane stanowią wartość dowodową i mogą być wykorzystywane przy ewentualnej weryfikacji podpisu przez uprawnionego biegłego sądowego. Właśnie dlatego signaturIX jest idealnym rozwiązaniem w sytuacjach wymagających oświadczenia woli wyrażonej podpisem, w formie pisemnej.

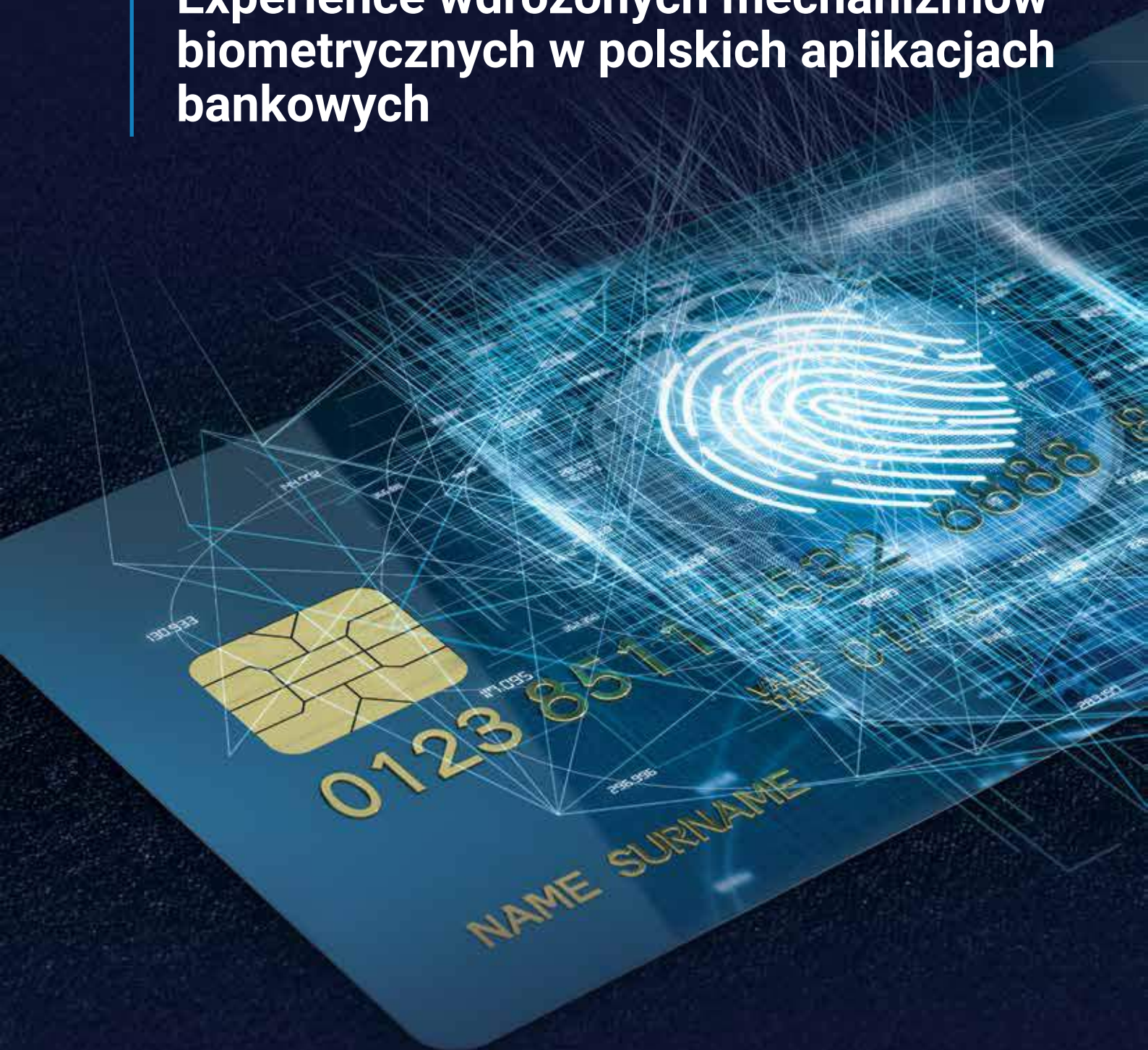
Najlepszym przykładem jego zastosowania są biura obsługi klientów. Użytkownik w wygodny i bezpieczny sposób podpisuje zgody, umowy, ankiety czy regulaminy. Jedyne, czego potrzebuje, to tablet i rysik. Firmy oszczędzają czas i przede wszystkim pieniądze dzięki redukcji kosztów związanych z obsługą papieru. Nie są już konieczne drukowanie oraz archiwizacja dokumentów. To kluczowe w kontekście wspierania procesów paperless.

Rynek finansowy, a także wiele innych obszarów gospodarki, jak nieruchomości, telekomunikacja czy ubezpieczenia, mierzy się z wieloma wyzwaniami związanymi z szeroko pojętym obiegiem dokumentów oraz bezpiecznym gromadzeniem i przechowywaniem danych. Wierzę, że metody podpisywania dokumentów oparte na biometrii behawioralnej rozwiążą większość z nich i zapewnią nową jakość świadczonych usług.

Tomasz Ostaszewski, CEO Xtension sp. z o.o.



Biometria w bankowości elektronicznej z perspektywy klienta. Badanie User Experience wdrożonych mechanizmów biometrycznych w polskich aplikacjach bankowych



3.1. Cel i zakres badania

W ramach realizacji raportu przeprowadzono jakościowe badanie użyteczności rozwiązań biometrycznych w bankowości mobilnej z perspektywy klientów wybranych sześciu polskich banków.

Celem badania było:

- zbadanie opinii klientów na temat rozwiązań w zakresie biometrii wprowadzonych do bankowości elektronicznej;
- sprawdzenie wiedzy użytkowników na temat biometrii;
- poznanie odczuć respondentów po sprawdzeniu możliwości zaimplementowanych funkcjonalności;
- sprawdzenie wiedzy klientów na temat promowania biometrii w bankowości elektronicznej.

3.2. Metodologia i wprowadzenie do badań

Badanie zostało zrealizowane w okresie od 1.12.2021 do 31.01.2022 roku na próbie 60 respondentów. Respondenci otrzymali bezpośredni dostęp do bankowości elektronicznej sześciu banków. Badaniem zostały objęte następujące banki: PKO Bank Polski, Bank Millennium, Bank Pekao SA, ING Bank Śląski, Santander Bank Polska, mBank. W badaniu udział wzięły kobiety oraz mężczyźni w wieku 25-60 lat. Na każdy z banków przypadało 10 respondentów, którzy podczas badania skorzystali z aplikacji danej instytucji. Badanie odbyło się w formule stacjonarnej. Użytkownicy korzystali z systemu operacyjnego Android na wersjach aplikacji z grudnia 2021 roku. W ramach badania zrealizowane zostały również wywiady pogłębione, w których respondenci podzielili się swoimi spostrzeżeniami, uwagami czy pomysłami związanymi z funkcjonalnościami, jakie mieli okazję testować.

W badaniu wykorzystane zostały dwie techniki: dyferencjał semantyczny oraz ustrukturyzowany wywiad pogłębiony. Dyferencjał semantyczny pozwala ocenić stosunek respondenta do przedstawionego obiektu lub koncepcji za pomocą zestawu przeciwstawnych określeń (np. łatwe/trudne). Respondent ocenia za pomocą kilkustopniowej skali, z którym z określeń bardziej się zgadza. W badaniu dla tej techniki zastosowanie znalazł kwestionariusz, którego celem było zebranie danych na temat satysfakcji z procesu wykonywania danego zadania. Druga technika (wywiad bezpośredni) miała na celu wzbogacenie pozyskanej od badanego wiedzy, dopełnie-

nie jej o opinię użytkowników względem testowanych rozwiązań.

W ramach dostępów, pod okiem badacza, respondenci przeszli kilka scenariuszy w celu oceny użyteczności, wygody i wartości zastosowania mechanizmów biometrycznych. Zostały zbadane następujące scenariusze:

1. Onboarding mobile – zebranie wzorca biometrycznego i aktywacja biometrii w bankowości mobilnej:
 1. Dodanie odcisku palca;
 2. Dodanie skanu twarzy;
3. Uruchomienie aplikacji mobilnej banku w celu aktywacji biometrii;
4. Pierwsze logowanie do aplikacji mobilnej w celu weryfikacji aktywacji metody biometrycznej.
2. Wykorzystanie metod biometrycznych do zalogowania i autoryzacji transakcji:
 1. Uruchomienie aplikacji mobilnej banku;
 2. Odnalezienie opcji dodania metody biometrycznej w aplikacji mobilnej jako metody potwierdzenia transakcji;
 3. Wykonanie przelewu z poziomu bankowości internetowej;
 4. Przywrócenie aplikacji do ustawień fabrycznych / usunięcie ustawionych przed chwilą metod biometrycznych.

3.3. Podsumowanie badań – wyniki

W niniejszym rozdziale zawarto podsumowanie obejmujące wyniki przeprowadzenia obu scenariuszy oraz wywiadów pogłębionych.

Pierwszy ze scenariuszy zakładał zebranie wzorca biometrycznego i aktywację biometrii w bankowości mobilnej dla metod odcisku palca oraz skanu twarzy, a zebrane z tych czynności użytkowników wnioski były następujące:

1. Dodanie odcisku palca

Dodanie odcisku palca było prostym zadaniem, nawet dla respondenta, który nigdy nie korzystał z danego systemu operacyjnego (Android) czy urządzenia o podobnym rozmieszczeniu opcji w „Ustawieniach” tele-



fonu. Kluczem do sukcesu były instrukcje wyświetlane na ekranie telefonu. Respondenci, którzy wykonali to zadanie, robili to intuicyjnie i szybko. Respondenci, dla których stanowiło to problem, mogli stosować się do instrukcji, które widniały na ekranie telefonu.

Poniżej przedstawione zostało zagregowane podsumowanie skuteczności realizacji zadania „Znalezienie w Ustawieniach telefonu i dodanie odcisku palca”. Dane zostały zagregowane, aby możliwe było podjęcie próby oceny rynku jako całości.

Tabela 4. Podsumowanie skuteczności realizacji zadania „Znalezienie w Ustawieniach telefonu i dodanie odcisku palca”

Liczba respondentów	Odnalezienie funkcjonalności	Realizacja procesu
46	Samodzielnie znalazło funkcjonalność	Samodzielnie rozpoczęło i zakończyło zadanie
0	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
0	Nie było w stanie znaleźć funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
14	Samodzielnie znalazło funkcjonalność	Potrzebowało wsparcia w realizacji zadania
0	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Nie udało się zrealizować zadania

Źródło: Opracowanie własne

2. Dodanie skanu twarzy

Dodanie skanu twarzy nie należało to trudnych zadań. Jasne instrukcje w telefonie oraz szybkie skanowanie wizerunku twarzy przyczyniły się do braku problemów przy tym zadaniu.

Poniżej przedstawione zostało zagregowane podsumowanie skuteczności realizacji zadania „Znalezienie w Ustawieniach telefonu i dodanie skanu twarzy”. Dane zostały zagregowane, aby możliwe było podjęcie próby oceny rynku jako całości.

Tabela 5. Podsumowanie skuteczności realizacji zadania „Znalezienie w Ustawieniach telefonu i dodanie skanu twarzy”

Liczba respondentów	Odnalezienie funkcjonalności	Realizacja procesu
20	Samodzielnie znalazło funkcjonalność	Samodzielnie rozpoczęło i zakończyło zadanie
0	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
0	Nie było w stanie znaleźć funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
0	Samodzielnie znalazło funkcjonalność	Potrzebowało wsparcia w realizacji zadania
0	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Nie udało się zrealizować zadania

Źródło: Opracowanie własne

3. Zmiana metody logowania w aplikacji mobilnej na metodę biometryczną

W przypadku tego scenariusza banki mocno różniły się poziomem użyteczności wdrożonych rozwiązań. Zazwyczaj inicjacji procesu zmiany metody można było dokonać w zakładkach Biometria/Logowanie/Zabezpieczenia. Opisy funkcji i poszczególnych kroków do wykonania były zazwyczaj przyjazne i zrozumiałe dla respondentów. Zwykle ten proces wymagał:

1. Logowania do aplikacji mobilnej;
2. Wybrania zakładki Ustawienia;

3. Wybrania zakładki w zależności od banku: „Bezpieczeństwo”; „Logowanie”; „metody logowania”;

4. Zaznaczenia opcji logowania jako metody biometrycznej.

Scenariusz nr 2 zakładał logowanie do bankowości mobilnej oraz potwierdzanie transakcji za pomocą metod biometrycznych.

Poniżej przedstawione zostało zagregowane podsumowanie skuteczności realizacji zadania „Znalezienie i zmiana metody logowania w aplikacji bankowej na metodę biometryczną”. Dane zostały zagregowane, aby możliwe było podjęcie próby oceny rynku jako całości.

Tabela 6. Podsumowanie skuteczności realizacji zadania „Znalezienie i zmiana metody logowania w aplikacji bankowej na metodę biometryczną”

Liczba respondentów	Odnalezienie funkcjonalności	Realizacja procesu
57	Samodzielnie znalazło funkcjonalność	Samodzielnie rozpoczęło i zakończyło zadanie
0	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
2	Nie było w stanie znaleźć funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
0	Samodzielnie znalazło funkcjonalność	Potrzebowało wsparcia w realizacji zadania
1	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Nie udało się zrealizować zadania

Źródło: Opracowanie własne

1. Logowanie za pomocą biometrii

Technika biometryczna, która jest wykorzystywana do logowania się do usług bankowych (najczęściej jest to odcisk palca), jest znana użytkownikom ze względu na jej wykorzystanie jako zabezpieczenia blokady wyświetlacza telefonu. Proces polegający na logowaniu do usług bankowych jest intuicyjny, podobnie jak odblokowanie telefonu w przypadku zastosowania metody odcisku palca. Natomiast logowanie twarzą nie powiodło się żadnemu respon-

dentowi – problem był zgłaszany do poszczególnych banków za pomocą aplikacji, infolinii oraz oddziału, nie udało się go jednak rozwiązać w żadnym przypadku w taki sposób, aby zakończyć logowanie respondenta sukcesem.

Poniżej przedstawione zostało zagregowane podsumowanie skuteczności realizacji zadania „Logowanie do aplikacji bankowej za pomocą biometrii”. Dane zostały zagregowane, aby możliwe było podjęcie próby oceny rynku jako całości.

**Tabela 7.** Podsumowanie skuteczności realizacji zadania „Logowanie do aplikacji bankowej za pomocą biometrii”

Liczba respondentów	Odnalezienie funkcjonalności	Realizacja procesu
50	Samodzielnie znalazło funkcjonalność	Samodzielnie rozpoczęło i zakończyło zadanie
0	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
0	Nie było w stanie znaleźć funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
0	Samodzielnie znalazło funkcjonalność	Potrzebowało wsparcia w realizacji zadania
0	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Potrzebowało wsparcia w realizacji zadania
10	Nie było w stanie znaleźć funkcjonalności	Nie udało się zrealizować zadania

Źródło: Opracowanie własne

2. Potwierdzanie transakcji biometrią (autoryzacja mobilna)

Banki, które posiadają to rozwiązanie, stosują dwa sposoby włączenia tej metody – pierwszy to włączenie biometrii jako metody logowania do aplikacji mobilnej i mobilną autoryzację jednocześnie oraz drugi – oddzielnie jako nową funkcjonalność w ramach funkcjonalności mobilnej autoryzacji. W ramach każdego rozwiązania klient jest informowany,

który sposób jest uruchomiany. Badanie wykazało, że większość respondentów nie miała problemów z włączeniem tej metody, o ile była ona dostępna w danym banku.

Poniżej przedstawione zostało zagregowane podsumowanie skuteczności realizacji zadania „Potwierdzenie wykonania transakcji metodą biometryczną”. Dane zostały zagregowane, aby możliwe było podjęcie próby oceny rynku jako całości.

Tabela 8. Podsumowanie skuteczności realizacji zadania „Potwierdzenie wykonania transakcji metodą biometryczną”

Liczba respondentów	Odnalezienie funkcjonalności	Realizacja procesu
17	Samodzielnie znalazło funkcjonalność	Samodzielnie rozpoczęło i zakończyło zadanie
2	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
0	Nie było w stanie znaleźć funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
0	Samodzielnie znalazło funkcjonalność	Potrzebowało wsparcia w realizacji zadania
1	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Potrzebowało wsparcia w realizacji zadania
10	Nie było w stanie znaleźć funkcjonalności	Nie udało się zrealizować zadania

Źródło: Opracowanie własne

3. Usunięcie metod biometrycznych

Usuwanie metody biometrycznej z ustawień telefonu, automatycznie usuwa się możliwość aktywacji biometrii jako narzędzia autoryzującego w aplikacjach bankowych – nie wszyscy zdają sobie sprawę z tego rozwiązania (tylko kilku respondentów wykonało tak zadanie, w większości robiąc to nieświadomie). Pro-

ces usunięcia metody biometrycznej z telefonu nie był już tak intuicyjny jak wcześniej realizowane scenariusze.

Poniżej przedstawione zostało zagregowane podsumowanie skuteczności realizacji zadania „Usunięcie metod biometrycznych”. Dane zostały zagregowane, aby możliwe było podjęcie próby oceny rynku jako całości.

Tabela 9. Podsumowanie skuteczności realizacji zadania „Usunięcie metod biometrycznych”

Liczba respondentów	Odnalezienie funkcjonalności	Realizacja procesu
36	Samodzielnie znalazło funkcjonalność	Samodzielnie rozpoczęło i zakończyło zadanie
0	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
1	Nie było w stanie znaleźć funkcjonalności	Samodzielnie rozpoczęło i zakończyło zadanie
22	Samodzielnie znalazło funkcjonalność	Potrzebowało wsparcia w realizacji zadania
1	Potrzebowało wskazówki badacza do znalezienia funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Potrzebowało wsparcia w realizacji zadania
0	Nie było w stanie znaleźć funkcjonalności	Nie udało się zrealizować zadania

Źródło: Opracowanie własne

Podsumowanie wywiadów pogłębionych

Następstwem wykonania opisanych scenariuszy było przeprowadzenie wywiadu pogłębionego z każdym z respondentów uczestniczącym w badaniu. Główne wnioski z tej części badania opisano poniżej:

1. Respondenci dostrzegają zarówno zalety, i jak i wady używania biometrii. Jako podstawowe zalety zostały wskazane:

- szybkość procesu;
- oszczędność czasu;
- brak konieczności zapamiętywania haseł;
- wygoda;
- bezpieczeństwo.

Jako podstawowe wady zostały wskazane:

- zależność od warunków pogodowych;

- zawodność czytników;
 - mniejsze bezpieczeństwo niż przy używaniu PINu;
 - zależność od sprzętu, problemy z logowaniem w przypadku uszkodzenia palca;
 - mniejsza anonimowość.
2. Respondenci ze wszystkich badanych banków oczekują szerszego zakresu edukacji na temat zalet stosowania biometrii oraz nabycia ogólnej wiedzy na jej temat (bezpieczeństwo stosowania). Porady w tym zakresie oczekiwane są od banku w różnej formie, w szczególności:
- za pomocą infolinii;
 - bezpośrednio u doradcy klienta;
 - w systemie bankowości elektronicznej, a w szczególności aplikacji mobilnej.

Warto rozważyć więc wypracowanie kodeksu dobrych praktyk w zakresie posługiwania się narzędziami bio-



metrycznymi w aplikacjach bankowych. W pierwszej kolejności taki kodeks powinien zostać rozpowszechniony wśród klientów bankowości elektronicznej poszczególnych banków.

3. Tylko 25 z 60 respondentów korzystało wcześniej (przed przeprowadzonym badaniem) z logowania do aplikacji bankowych przy pomocy biometrii.

4. Respondenci dostrzegają zagrożenia związane z utratą danych biometrycznych oraz ryzyka związane z prywatnością. Z pewnością zwiększona obawa użytkowników o wykorzystanie ich danych może doprowadzić do wstrzymania przyswajania tych metod w przypadku wystąpienia poważnych incydentów.

5. Większość respondentów wskazała, że bank nie przedstawił korzyści wynikających ze stosowania biometrii.

6. W trakcie realizacji zadań respondenci napotykali na różne problemy. Związane one były w szczególności z:

- a. dodaniem odcisku palca, które trwało zbyt długo;
- b. potwierdzeniem przelewu za pomocą odcisku palca lub skanu twarzy;
- c. znalezieniem opcji usunięcia odcisku palca z telefonu.

7. Respondenci, pytani „Czy i gdzie dostrzega Pan/Pani zastosowanie technologii opartych o np. odcisk palca/skan twarzy/tęczęwki oka”, bardzo często wskazywali takie jakie miejsca, jak:

- bankowość internetowa,
- poczta email,
- logowanie się do portali społecznościowych,
- lotniska.

Poniżej przedstawione zostało zagregowane podsumowanie wywiadu pogłębionego dotyczące percepcji bezpieczeństwa bankowości elektronicznej

Tabela. 10. Podsumowanie wywiadu pogłębionego dotyczącego percepcji bezpieczeństwa bankowości elektronicznej

Metody zabezpieczenia bankowości elektronicznej	Znajomość metod przez respondenta	Metody aktywnie promowane przez bank	Najbardziej bezpieczna i wygodna metoda z doświadczenia respondenta
Biometria – skan tęczęwki oka	–	1	1
Biometria – odcisk palca	–	15	20
Biometria – skan twarzy	–	6	4
Zarządzanie limitami transakcji w bankowości internetowej	57	33	20
Zarządzanie limitami transakcji w aplikacji mobilnej	54	29	21
Rejestracja bezpiecznego urządzenia	50	40	15
Kod SMS przesyłany na telefon komórkowy potwierdzający transakcje na koncie	60	45	41
Powiadomienia PUSH w aplikacji mobilnej	58	42	23

Źródło: Opracowanie własne

3.4. Generalne wnioski

1. Wyniki przeprowadzonych badań wskazują, że z perspektywy użytkowników bankowości elektronicznej stosowanie biometrii jest bardzo wygodne, szybkie oraz proste. Natomiast należy pamiętać, że nie może to być jedyna metoda logowania czy autoryzacji ze względu na potencjalną zawodność metod biometrycznych (np. uszkodzony czytnik, uszkodzony palec).
2. W przypadku zmiany metody logowania w aplikacji na metodę biometryczną banki mocno różniły się między sobą, jednak w żadnym z nich proces nie wydawał się dla respondentów trudny w zrealizowaniu.
3. Zadanie polegające na usunięciu metod biometrycznych okazało się niezrozumiałe dla wielu respondentów. Nie wszyscy byli świadomi, że usuwając metodę logowania biometrycznego z ustawień telefonu automatycznie usuwa się możliwość aktywacji biometrii jako narzędzia autoryzacji w aplikacji bankowej.
4. Respondenci są świadomi zagrożeń związanych z utratą kontroli lub wyciekiem danych biometrycznych. W tym zakresie niezbędne jest edukowanie klientów zarówno o zaletach stosowania biometrii, jak i o bezpiecznym stosowaniu poszczególnych metod.
5. Pozytywna percepcja biometrii oraz jej przyswojenie jest w dużym stopniu zależne od narzędzi, na których jest ona dostępna, zwłaszcza gdy główną metodą biometryczną są odciski palca, których niezawodność w dużym stopniu zależy od czytnika telefonu.
6. Użytkownicy są zaznajomieni z technikami biometrycznymi. Proces logowania się do usług bankowych za pomocą odcisku palca był dla nich intuicyjny. Logowanie za pomocą skanu twarzy wywołało wiele problemów technicznych i mimo zgłaszania problemu, nie udało się pozytywnie zakończyć tego procesu.
7. Z pewnością poziom stosowania biometrii wśród użytkowników bankowości elektronicznej ma jeszcze duży potencjał do wzrostu, nawet z uwzględnieniem aktualnie dostępnych metod i wspomnianych powyżej ograniczeń. Przeprowadzone badanie pokazało, że spora część klientów pierwszy raz miała styczność z biometrią w relacji z bankiem.



Przyszłość metod biometrycznych i ich zastosowania w bankowości elektronicznej



4.1. Ścieżki rozwoju metod biometrycznych z uwzględnieniem kwestii prywatności, ergonomii użycia, ogólnego postrzegania przez społeczeństwo, infrastruktury po stronie użytkownika i banków oraz bezpieczeństwa

W niniejszym raporcie najczęściej mowa jest o trzech metodach biometrycznych: rozpoznawaniu twarzy, odcisków palca, a także tej wykorzystującej czynniki behawioralne. Jeżeli chodzi o rozwój całego ekosystemu biometrii, autorzy raportu dostrzegają potencjał rozwoju w wymienionych metodach.

Rozpoznawanie twarzy w procesach identyfikacji i weryfikacji klienta znajdować się będzie na fali wzrostowej

Rozpoznawanie twarzy powinno umocnić swoją pozycję w procesach rejestracji oraz identyfikacji klientów w ramach procesów „Know Your Customer” (tzw. KYC). Wynika to bezpośrednio z wyzwań związanych z pandemią, ale również z zauważalnych trendów w rozwoju rynku e-commerce, przyzwyczajęń oraz nawyków społeczeństwa, zmierzających ku procesom w pełni zdalnym. W czasie prac nad niniejszym raportem (grudzień 2021 - luty 2022), większość banków dostępnych na polskim rynku oferowała automatyczne zakładanie rachunku przez selfie ID. Jest mało prawdopodobne, aby sytuacja znacząco zmieniła się na niekorzyść rozwiązań biometrycznych, tym bardziej w obliczu informacji o likwidacji przez banki placówek fizycznych²⁰. Natomiast istotnym aspektem, który ma wpływ na rozwój metod identyfikacji w pełni automatycznych (selfieID) opartych o biometrię w stosunku do zdalnej identyfikacji z operatorem (półautomatyczna weryfikacja klienta), jest przede wszystkim nieustanne doskonalenie mechanizmów wykrywania fraudów, co pozwoli bankom oraz całemu sektorowi finansowemu na pełną akceptację tego typu rozwiązań. Dodatkowo biometria może być używana również w procesach stacjonarnych, dla zwiększenia bezpieczeństwa procesów identyfikacji i weryfikacji klienta w oddziałach instytucji finansowych.

Zagrożeniem dla rozwoju metod biometrycznych opartych na rozpoznawaniu obrazów, w tym zwłaszcza na rozpoznawaniu twarzy, są obawy o profilowanie oraz prywatność użytkowników. Z uwagi na coraz częstsze przypadki nadużywania tego typu danych przez podmioty komercyjne oczekujemy wypracowania kodeksu dobrych praktyk, który będzie stosowany podobnie jak wytyczne w zakresie danych osobowych - w przeciwnym wypadku wzrastać będą obawy użyt-

kowników o wykorzystywanie ich danych i przyswajanie tych metod może zostać wstrzymane.

Większy rozwój mobilnej autoryzacji

Kilka lat temu autoryzacja operacji bankowych była oparta o kody jednorazowe, następnie kody SMS, aż po komunikaty PUSH w aplikacjach mobilnych. Obecnie do katalogu metod autoryzacji możemy zaliczyć biometrię, która jednocześnie zapewnia większe bezpieczeństwo (brak konieczności pamiętania PIN-ów), wygodę i ogranicza koszty po stronie banków w zakresie obsługi bramek SMS. Aktualnie mobilna autoryzacja nie znajduje jeszcze dużego zastosowania, jeżeli chodzi o cały sektor bankowy, jest ona używana przy zatwierdzaniu przelewów zleczanych w bankowości internetowej oraz mobilnej, natomiast można wysunąć tezę, iż w nadchodzących latach mobilna autoryzacja zupełnie wyeliminuje kody SMS, które są podatne na popularne ostatnio ataki phishingowe. W tym zakresie rolą banków jest cykliczna edukacja klientów na temat zalet mobilnej autoryzacji.

W niniejszym raporcie uwzględniono także inne metody, które są mniej popularne i obecnie nie mają większego zastosowania w sektorze bankowym. Jednak badania firmy PayEye, pioniera w zakresie wykorzystania tęczówki oka do płatności pokazały, że: „75% respondentów ufa biometrii oka, na której unikatowości, oprócz biometrii twarzy, system PayEye opiera swe funkcjonowanie. Znakomita większość, bo aż ponad 80% respondentów, uważa, iż płatności i zabezpieczenia biometryczne są przyszłością sektora finansowego”²¹. W tym miejscu należy odnotować, iż zauważalne trendy w zakresie tej metody wymagają dalszego monitorowania.

Biometria behawioralna jako niezauważalny czynnik wspierający bezpieczeństwo transakcji

Według danych w publicznie dostępnych kanałach tylko dwa banki w Polsce na 15 oferują możliwość włączenia przez klientów zabezpieczeń opartych o biometrię behawioralną (w kontekście bezpieczeństwa transakcji typu przelew czy logowania do serwisów). Wciąż nie jest to znaczący rezultat. Wierzymy jednak, że trend wzrostowy tej metody nadejdzie, ponieważ dostrzegamy związane z nią znaczące korzyści zarówno dla klienta, jak i dla banku, zwłaszcza dla zapewnienia bezpieczeństwa transakcji. Biometria behawioralna może z powodzeniem stanowić dodatkowy czynnik analizy ryzyka zachowań klienta i wspierać mechanizmy antyfraudowe. Jednak tutaj kluczowym aspektem przyswojenia tej metody jest edukacja klientów, która wyjaśni wszelkie wątpliwo-

²⁰ <https://www.bankier.pl/wiadomosc/Rzez-placowek-bankowych-jest-ich-najmniej-w-historii-Topnieje-rowniez-zatrudnienie-8242790.html> (luty 2022).

²¹ Wypowiedź dr hab. Barbary Mróz-Gorgoń, prof. UEW- CMO PayEye



ści związane z jej stosowaniem. Od strony jej wdrożenia bardzo ważne jest wykorzystanie odpowiednio dobranych źródeł danych oraz algorytmów z uwagi na wydajność tworzenia wzorca (profilu) behawioralnego oraz jego skuteczności przy weryfikacji. Wzorce muszą być też odporne na zmiany zachowania klientów w zależności od wykorzystywanych przez nich urządzeń. Poprawne wdrożenie powinno charakteryzować się możliwie sprawnym tworzeniem profili (1–3 miesiące dla 95% użytkowników), które można wykorzystywać do weryfikacji użytkownika w trakcie logowania oraz wiarygodności sesji podczas wypełniania formularzy czy połączeń wideo.

Drugim kierunkiem zastosowania biometrii behawioralnej są podpisy biometryczne, o których już kilkakrotnie wspominaliśmy w niniejszym raporcie. Wydają się one powrotem do procesu stacjonarnego, jednak stanowią alternatywę w procesach klasycznych, stacjonarnych, gdzie istnieje potrzeba zapewnienia bezpiecznego, a przede wszystkim elektronicznego obiegu dokumentu przy zachowaniu formy pisemnej w świecie fizycznym.

Jakie podstawowe czynniki mogą wpływać na rozwój oraz upowszechnienie poszczególnych metod biometrycznych? Poniżej zawarliśmy próbę odpowiedzi na to pytanie, w krótkim podsumowaniu:

1. Nadrzędnym czynnikiem dla wszystkich metod opartych o cechy fizyczne jest zapewnienie niezawodności działania oraz odporności na błędy urządzenia, np. czytnika. Za ten czynnik w dużej mierze odpowiedzialni są dostawcy technologii, np. smartfonów czy rozwiązań do identyfikacji klientów (dostawcy aplikacji selfID).
2. Rozwój technologii smartfonów ułatwia i przyspiesza implementację najprostszych metod – odcisk palca / wizerunek twarzy. Metod tych używamy na co dzień przy odblokowaniu telefonu, więc obawy podczas włączania mechanizmów biometrycznych do kolejnych usług, np. w aplikacji bankowych, są mniejsze.
3. Technologie biometryczne, które są oparte na przechowywaniu wzorca biometrycznego na urządzeniu klienckim zapewniają łatwiejszą kontrolę wzorca, a co za tym idzie, większe bezpieczeństwo po stronie użytkownika niż przekazywanie danych do centralnej bazy. Ponadto taki model eliminuje ryzyko kompromitacji bazy wzorców po stronie administratora danych, a także zmniejsza nakłady operacyjne związane z utrzymaniem dużych baz danych z danymi szczególnych kategorii. Z kolei takie podejście jest mniej skalowalne, jeśli chodzi o wykorzystanie wzorca na innych urządzeniach

czy w innych kanałach, co może być barierą w przyszłym rozwoju rozwiązania lub gdy kontrola nad wzorcem jest wymagana po stronie centralnej, chociażby dla potrzeb dowodowych.

4. Czynnikiem niebezpośrednim, lecz równie istotnym jest standaryzacja rynku dostawców tożsamości oraz rozwiązań biometrycznych. Jak już wspominaliśmy w rozdziale 1.8, prowadzone są zarówno niezależne testy rozwiązań biometrycznych, jak i certyfikacja rozwiązań oraz dostawców, które pozwalają np. bankom efektywniej wybrać dostawcę biometrii do swoich procesów. Aktualnie rynek dostawców tej technologii jest mocno rozproszony, dlatego warto obserwować tych dostawców, którzy zamierzają poddać niezależnemu audytowi swoje rozwiązania techniczne oraz organizacyjne. Z punktu widzenia banków bardziej zaufanym oraz prostszym do zweryfikowania i wyboru jest dostawca, który posiada certyfikację zarówno swojego rozwiązania, jak i organizacji.

4.2. Potencjał biznesowy biometrii, w tym rozszerzenie zastosowań na rynku finansowym i poza nim

Pierwsze spojrzenie na polski rynek bankowy może dać wrażenie, że biometria jest w nim dobrze zadowolona. Jak wykazano w niniejszym raporcie, aż 12 z 15 analizowanych banków działających w Polsce umożliwia otwarcie konta w procesach wykorzystujących technologie biometryczne. Oferty te skierowane są głównie do ludzi wchodzących w dorosłe życie i rozpoczynających korzystanie z usług bankowych. Jednak w innych obszarach działalności bankowej biometria nie jest równie powszechna. Niewiele banków oferuje inne możliwości zakupu innych produktów bankowych w ścieżkach wykorzystujących identyfikację i uwierzytelnienie biometryczne. Nie stwierdzono również powszechnego wykorzystania biometrii w procesach obsługi posprzedażowej klienta. Większość banków umożliwia dostęp do bankowości elektronicznej z wykorzystaniem biometrycznego logowania, ale już tylko kilka z nich daje możliwość autoryzowania operacji zlecanych w tych serwisach.

Można zatem zadać pytanie: czy banki we właściwy sposób konstruują i realizują strategię budowania i utrzymywania relacji z klientami? Czy stosowanie biometrii tylko do nawiązywania relacji z klientami i zapewniania dostępu do konta może mieć konsekwencje w postaci niskich poziomów satysfakcji czy ostatecznie – wysokich wskaźników odejść? Do zagospodarowania pozostają jeszcze takie obszary jak:

- sprzedaż produktów kredytowych i leasingowych dla nowych klientów, w której można zastosować wideoweryfikację wspieraną technologią biometryczną,
- potwierdzanie operacji składanych w różnych kanałach,
- inne procesy posprzedażowe, wymagające stosowania procedur KYC (np. aneksowanie umów).

Wydaje się to niezmiernie istotne, gdy uwzględnimy obserwowany trend redukcji placówek bankowych i przenoszenia sprzedaży produktów finansowych i obsługi klienta do internetu. Dopóki wiele niestandardowych, specyficznych procesów bankowych będzie wymagać fizycznej obecności klienta w placówce, dopóty trudno będzie planować i realizować strategię pełnej cyfryzacji obsługi. Technologie biometryczne mogą w tym przypadku znacząco ułatwić transformację.

Można przyjąć, że banki stale upraszczają procesy operacyjne i rozszerzają wachlarz czynności, które klienci mogą zlecić lub wykonać zdalnie. Wciąż jednak należy zakładać, że w przypadku niepowodzenia spowodowanego czy brakiem wiedzy, czy umiejętności posługiwania się narzędziami udostępnianymi przez banki klienci mogą rezygnować z usług banku lub przenosić załatwienie sprawy do oddziałów stacjonarnych lub też szukać wsparcia w obsłudze zdalnej. Koncepcja wirtualnego oddziału bankowego zakłada rozszerzenie zarówno komunikacji klienta z pracownikiem banku (nie tylko rozmowy głosowe czy czat, ale i rozmowy wideo z udostępnianiem zawartości ekranów), jak i zakresu czynności i spraw, które można załatwić, w stosunku do standardowej obsługi zdalnej. Biometria może w tym przypadku być niezbędnym narzędziem, zapewniającym właściwe uwierzytelnienie użytkownika i bezpieczeństwo procesów realizowanych w ramach takich kontaktów.

Charakterystyczne jest w zasadzie wyłączenie przypisania wsparcia technologiami biometrycznymi do smartfonów i innych urządzeń mobilnych – z powodu udostępniania przez ich producentów odpowiednich narzędzi i czytników. Tymczasem komputery osobiste, czyli urządzenia, które współcześni klienci banków powszechnie wykorzystują do pracy, nauki czy rozrywki, również posiadają podzespoły umożliwiające uruchamianie metod biometrycznych – kamery i czytniki linii papilarnych, a systemy operacyjne – odpowiednie oprogramowanie (Windows Hello, Touch Id, Face Id). W toku badań przeprowadzonych na potrzeby niniejszego raportu w żadnym z banków nie stwierdzono rozwiązań, które dawałyby możliwość dostępu do internetowych serwisów bankowych i wykonywania w nich operacji za pomocą weryfikacji bio-

metrycznej. W tym obszarze należy dostrzec potencjał do rozwoju.

Biometria ma duży potencjał biznesowy, co potwierdzają dotychczasowe przypadki jej użycia: pozwala pozyskiwać klienta całkowicie zdalnie – szybko i małym kosztem, ułatwia dostęp klienta do usług, eliminując kosztowną obsługę błędnych logowań, zmiany haseł itp., poprawia satysfakcję klienta. Znając te korzyści, banki powinny rozszerzać implementacje technologii biometrycznych na inne obszary swego działania.

Wypowiedź eksperta

Zabezpieczenia biometryczne cieszą się coraz wyższym zaufaniem użytkowników z uwagi na prostotę użycia i bezpieczeństwo. Coraz częściej w życiu codziennym korzystamy z nich, aby odblokować telefon czy komputer, czy też potwierdzić swoją tożsamość, zakładając konto w banku przez internet.

Nie oznacza to jednak, że potencjał biznesowy zawarty w rozwiązaniach opartych o biometrię został już wyczerpany. Nowe możliwości, które daje szybka i skuteczna analiza unikalnych cech danej osoby – wizerunku, odcisków palca czy tęczy oka – pozwalają oferować bardziej bezpieczne, a zarazem szybsze i wygodniejsze doświadczenia użytkownikom końcowym. Już dziś, zastępując podatne na przechwycenie hasła czy kody SMS zabezpieczeniami biometrycznymi, możemy w praktyce zminimalizować ryzyko dokonania przez niepowołaną osobę zakupu, przelewu czy odczytu poufnych danych.

Analiza cech biometrycznych w ramach procesów potwierdzania tożsamości – zwłaszcza zdalnych – pozwala na określenie, czy dany dokument tożsamości jest wykorzystywany przez jego właściciela. Najnowsze rozwiązania potrafią skutecznie porównać wizerunek osoby utrwalony na dokumencie (zarówno w warstwie wizualnej, jak i elektronicznej) z aktualnym zdjęciem osoby posługującej się nim, przy uwzględnieniu zmian cech twarzy zachodzących z wiekiem, zmiany zarostu, a nawet zmian wynikających z operacji plastycznych. Co więcej, taki wizerunek może być szybko i automatycznie porównany z anonimową bazą cech twarzy w celu określenia, czy dana osoba nie identyfikowała się wcześniej innymi danymi – przy braku konieczności przechowywania danych wrażliwych klientów. Połączenie metod opartych na biometrii z odczytem danych z okazanych dokumentów istotnie zwiększa bezpieczeństwo procesów potwierdzania tożsamości, znacznie redukując możliwość nadużyć.

Do wyzwań stojących przed zabezpieczeniami biometrycznymi należy rozwój technik związanych z szeroko



rozumianymi deep fakes. Najlepsze na rynku rozwiązania potrafią obecnie wykrywać zarówno manipulacje polegające na dopasowaniu twarzy oszusta do nagranej sylwetki innej osoby, jak i na „ożywieniu” zdjęcia innej osoby zgodnie z ruchami adversarza nagranych wcześniej, niwelując ryzyko powodzenia także tego typu ataków.

Paweł Narolski
Head of Research and Development
IDENTT

4.3. Biometria a inne metody elektronicznej identyfikacji czy uwierzytelnienia – orkiestracja metod zabezpieczeń z perspektywy banku vs. oczekiwania klientów

W niedługiej, choć bogatej historii bankowości elektronicznej w Polsce i na świecie można zauważyć ewolucję metod identyfikacji i weryfikacji tożsamości: od prostych zabezpieczeń typu login i hasło, które początkowo dawały pełny dostęp do serwisów bankowości elektronicznej, poprzez predefiniowane listy haseł jednorazowych do potwierdzania pojedynczych operacji, hasła generowane przez specjalne urządzenia (tzw. tokeny), powiadomienia *push* w aplikacjach bankowych na smartfonach, aż po weryfikację biometryczną odcisku palca i wizerunku twarzy, głównie udostępnianą przez dostawców urządzeń mobilnych. Dołączają do tego kolejne metody, w tym na polskim rynku – rozwiązania oparte o dokumenty tożsamości: dowód osobisty z warstwą elektroniczną w połączeniu z aplikacją mobilną, np. eDO App, czy udostępniana przez organy rządowe aplikacja mObywatel z danymi tożsamości pochodzącymi z rejestrów państwowych. W perspektywie kilku lat dołączy do nich Europejski Portfel Cyfrowej Tożsamości, do którego akceptacji będą zobowiązane m.in. instytucje finansowe.

Chociaż niektóre z tych metod identyfikacji i uwierzytelnienia „odchodzą do lamusa”, większość z nich jest wciąż wykorzystywana, często w kombinacjach, dla zapewnienia wyższego poziomu bezpieczeństwa

informacji i transakcji. Nie miały wpływu na utrzymanie prostych metod mają oczekiwania klientów banków, których przyzwyczajenia, niechęć do zmian i wygoda często przeważają nad racjonalnym podejściem do kwestii bezpieczeństwa. Współczesne implementacje biometrycznych metod identyfikacji i uwierzytelnienia w urządzeniach mobilnych pozwalają bankom na pogodzenie dwóch teoretycznie rozbieżnych celów: utrzymania względnie wysokiego poziomu bezpieczeństwa rozwiązań bankowości elektronicznej i dostarczenia klientom jak najlepszego *customer experience*. Badania klientów sześciu polskich banków, przeprowadzone na potrzeby niniejszego raportu, potwierdzają otwartość na stosowanie oraz generalnie dobrą przyswajalność metod biometrycznych (palec i twarz) jako sposobu dostępu do bankowości mobilnej.

Mnogość metod identyfikacji i uwierzytelnienia, które są pożądane przez klientów, może być dla podmiotów finansowych wyzwaniem w kwestiach implementacji, utrzymania i zarządzania. Ze względu na optymalizację nakładów i kosztów oraz potencjalną monetyzację wykorzystania tych narzędzi warto rozważyć stałe się skupienie odpowiedzialności za ich cały cykl życia w jednym miejscu w strukturze organizacyjnej: jednostka, która gromadzi wiedzę ekspercką na temat metod, słucha głosu klienta, planuje rozwój, organizuje dostawców oraz wdraża i optymalizuje narzędzia identyfikacji i uwierzytelnienia. Jednocześnie jest wewnętrznym dostawcą całej palety różnych metod dla różnych procesów biznesowych i operacyjnych, czyli odpowiada za ich propagowanie w organizacji, wsparcie w implementacji i obsłudze. Warto wziąć tutaj także pod uwagę orkiestrację, czyli zautomatyzowanie całego *workflow* identyfikacji i uwierzytelnienia, począwszy już od dynamicznego dostosowywania katalogu metod udostępnianych w danym procesie biznesowym. Dzięki takiemu podejściu, serwując metody identyfikacji i uwierzytelnienia w kanałach zdalnych, można zapewnić przede wszystkim spójność propozycji dla klientów w różnych procesach sprzedażowych i obsługowych, a także możliwość wyboru – co jest niezmiernie istotne dla ich odbioru i zadowolenia z obsługi.



Raport przygotowany na zlecenie Fundacji
Warszawski Instytut Bankowości



PROGRAM
ANALITYCZNO
BADAWCZY