



RAPORT BIOMETRYCZNY 2.0

„Bankowość biometryczna”

Grupa FTB ds. Biometrii

Warszawa, 2013

Praca zbiorowa pod redakcją Tadeusza Woszczyńskiego

Redakcja:

Tadeusz Woszczyński (redaktor prowadzący), Zbigniew Marcinkowski, Mariusz Sudoł

Współautorzy:

K. Arciszewski, B. Bińkowska-Artowicz, S. Cekała, M. Czechowski, W. Częścik, Ł. Hoppe, P. Izbicki, W. Kujawa, J. Kurczych, L. Modzelewski, S. Myśliński, M. Olszewski, D. Pawęda, R. Poznański, L. Szczęciński, M. Waluś, F. Wołowski, J. Wójtowicz.

0. Wstęp	3
0. Recenzje	4
1. O Raporcie	6
1.1. Cel dokumentu.....	6
1.2. Adresaci.....	6
1.3. Rozpowszechnianie i odpowiedzialność za rekommendacje...6	
2. Definicje	7
3. Technologie biometryczne w bankowości	9
3.1. Rodzaje technologii biometrycznych.....	9
3.2. Porównanie technologii biometrycznych.....	9
3.3. Kryteria doboru technologii biometrycznych na przykładzie sektora bankowego.....	10
3.4. Technologie biometryczne zastosowane w sektorze bankowym	11
3.4.1. Biometria odcisku palca (linii papilarnych palca) ...11	
3.4.2. Biometria naczyń krwionośnych palca	13
3.4.3. Biometria głosowa	14
3.4.4. Biometria podpisu odręcznego.....	15
3.4.5. Biometria przyszłości	18
4. Bezpieczeństwo w biometrii.....	21
4.1. Współczynniki bezpieczeństwa i pracy technologii biometrycznych	21
4.2. Bezpieczeństwo systemów biometrycznych	22
4.2.1. Sposoby przechowywania i porównywania danych biometrycznych	23
4.2.2. Zabezpieczenia czytników biometrycznych.....	24
4.3. Przykłady procedur bezpieczeństwa w systemach biometrycznych	25
4.3.1. Biometria w oddziale bankowych.....	25
4.3.2. Biometria w Contact Center	27
5. Norma ISO 19092	28
6. Zastosowania biometrii.....	30
6.1. Bankomaty.....	32
6.2. Oddział bankowy	34
6.3. Bankowość internetowa	36
6.4. Kanał zdalny (Infolinia, IVR, Help desk, bankowość mobilna)	37
6.5. Płatności	38
6.6. Fizyczna i logiczna kontrola dostępu	38
6.7. Skrytki depozytowe	39
6.8. Podpis biometryczny.....	42
6.9. Systemu obiegu dokumentów z biometrią podpisu odręcznego	43
6.10. Dystrybucja gotówki.....	45
6.11. Rejestracja czasu pracy	45
7. Zastosowania biometrii w usługach na linii bank - administracja publiczna	46
7.1. Rejestracja działalności gospodarczej w okienku banku ... 46	
7.2. Biometryczne wypłaty świadczeń społecznych	47
8. Wybrane studia przypadków wdrożeń biometrii w bankowości	49
8.1. Wdrożenia biometrii w Polsce	49
8.1.1. Podkarpacki Bank Spółdzielczy.....	50
8.1.2. Bank Polskiej Spółdzielczości S.A. (BPS)	51
8.1.3. Bank Spółdzielczy w Kielcach	52
8.1.4. Powiślański Bank Spółdzielczy w Kwidzynie.....	55
8.1.5. Bank BPH S.A.	56
8.1.6. Getin Bank	58
8.1.7. Asekuracja.....	59
8.2. Wdrożenia zagraniczne	59
8.2.1. Turcja - IS Bankası	59
8.2.2. Turcja - Ziraat Bankası.....	60
8.2.3. Turcja - Vakif Bank	61
8.2.4. Japonia - największy projekt biometryczny świata	61
8.2.5. Japonia - Resona Bank.....	63
8.2.6. Brazylia - Banco de Bradesco	64
8.2.7. Nigeria	64
8.2.8. Słowacja - Tatra Banka	65
8.2.9. Rumunia - ING Bank.....	65
8.2.10. Wielka Brytania - Barclays	65
8.2.11. Indonezja - Bank Negara Indonesia (Persero) Tbk.	66
8.2.12. Izrael	66
9. Wybrane studia przypadków wdrożeń biometrii w innych sektorach	67
9.1. Polska - T-Mobile	67
9.2. Węgry - T-Mobile	67
9.3. Turcja - Global Bilgi	67
9.4. Turcja - SGK	67
9.5. Europa - Biometria w systemach informacyjnych Unii Europejskiej.....	68
10. Aspekty prawne biometrii.....	75
10.1. Biometria w bankowości	75
10.2. Biometria a ochrona danych osobowych.....	76
10.3. Biometria a prawo pracy.....	79
10.4. Podpis biometryczny.....	83
10.5. Biometria a prawo podatkowe	84
11. Autorzy raportu	87
11.1. Redakcja.....	87
11.2. Współautorzy	87
11.3. Koordynacja ze strony Związku Banków Polskich	87

Jeszcze 5 lat temu bankowość biometryczna wydawała się terminem dalekim od rzeczywistości. Dzisiaj banki w związku ze zwiększającą się liczbą fraudów w oddziałach, bankomatach bądź bankowości internetowej, poszukują nowej, wiarygodnej metody uwierzytelniania klienta banku. Coraz większa liczba kart w naszym portfelu, zwiększająca się liczba kodów PIN, haseł dostępowych i loginów sprawia, że korzystanie z usług bankowych staje się coraz mniej komfortowe. Coraz bardziej obciążający jest koszt papierowego obiegu dokumentów, a szczególnie ich archiwizacji i przechowywania. Należ również zwrócić uwagę na dużą grupę osób wykluczonych cyfrowo i finansowo. Banki poszukują technologii, które pozwolą im zaoszczędzić koszty, lecz równocześnie umożliwiają otwarcie nowych usług i produktów.

„Biometria jest obecnie najmocniejszą metodą uwierzytelniania.”

Odpowiedzią na powyższe potrzeby jest biometria. Biometria jest obecnie najmocniejszą metodą uwierzytelniania. Ponieważ wykorzystuje ona unikalne cechy naszego ciała lub zachowania, nie wymaga ona posiadania dodatkowych identyfikatorów. Jest ona uniwersalna, można ją stosować w wielu usługach bankowych. Przez ostatnie lata, technologie biometryczne dojrzały. Na rynku są dostępne technologie stworzone dla potrzeb bankowości, zapewniające zachowanie prywatności użytkowników i zapewniające odpowiednie bezpieczeństwo urządzeń.

Polska, jako pierwszy kraj w Europie wdrożyła biometrię w sektorze bankowym. W 2010 rozpoczęto wdrożenie pierwszych w Europie bankomatów biometrycznych, a w 2012 utworzono pierwszy w Europie system oddziałów biometrycznych. Największym rynkiem europejskim stosującym biometrię w bankowości jest Turcja, gdzie czołowe banki wdrożyły biometrię w bankomatach. Macierzą bankowości biometrycznej jest

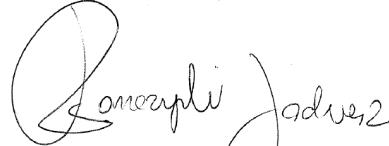
jednak Japonia gdzie uwierzytelnianie biometryczne w bankach funkcjonuje od 2005 roku i korzysta z niej ponad 40 mln osób.

W 2007 roku z inicjatywy sp. Prof. Remigiusza Kaszubskiego powstała w ramach Forum Technologii Bankowych (FTB) przy Związku Banków Polskich (ZBP) - Grupa ds. Biometrii, która miała na celu popularyzację zastosowania biometrii w polskiej bankowości. Grupa ds. Biometrii zrzesza zarówno reprezentantów banków, dostawców technologii biometrycznych, integratorów systemowych, dostawców rozwiązań kartowych, oraz niezależnych ekspertów ze środowisk bankowych jak i reprezentantów świata nauki. Grupa ds. Biometrii jest organizatorem jedynej w Europie konferencji poświęconej w 100% bankowości biometrycznej - Spring Biometric Summit. W 2009 Grupa wydała pierwszy w Polsce raport biometryczny pt. „Biometria w bankowości i administracji publicznej” oraz opinię prawną pt. „Prawne aspekty biometrii”, które stanowiły podstawę dla banków zainteresowanych biometrią.

Niniejsze opracowanie jest odpowiedzią na zmieniający się sektor bankowy oraz świat biometryczny. Znajdują w nim Państwo informacje na temat technologii biometrycznych, kluczowych aspektów bezpieczeństwa, zastosowania, studia przypadku, jak i aspekty prawne biometrii w Polsce.

Raport ten jest dedykowany pamięci Prof. Remigiusza Kaszubskiego, jednego z najwybitniejszych reformatorów polskiego sektora bankowego, wybitnego eksperta prawa bankowego i promotora biometrii w Polsce.

W imieniu Grupy ds. Biometrii zapraszam do lektury.



Tadeusz Woszczyński
Współzałożyciel
i Przewodniczący Grupy ds. Biometrii

Biometria jest nowoczesną i bezpieczną metodą uwierzytelniania tożsamości, która wg. badań może być przyszłością światowej bankowości. Z jednej strony biometria zapewnia praktycznie 100% gwarancję poprawnego uwierzytelniania oraz wygodę użytkownika (brak kart i kodów PIN), lecz z drugiej strony pozostaje pytanie o akceptowalność społeczną takiego rozwiązania. W bankowości wprowadzane są najnowsze technologie, w tym również biometryczne (np. biometria naczyń krwionośnych palca, biometria głosowa), które niwelują lęk związany z biometrią odcisku palca, ponieważ gwarantują dużo wyższy poziom ochrony prywatności użytkowników. Polska była pierwszym krajem w Europie, w którym wprowadzono biometrię w usługach bankowych. Banki komercyjne zastosowały ją do uwierzytelnienia tożsamości klientów w swoich placówkach, a banki spółdzielcze wykorzystują ją do uwierzytelniania tożsamości klientów dokonujących wypłat w bankomatach. Interesujące wydaje się też zastosowanie biometrii w automatycznych oddziałach bankowych.

Raport biometryczny 2.0 „Bankowość biometryczna” jest bardzo rzetelnym kompendium wiedzy na temat zastosowania biometrii w bankowości. Mimo coraz częściej pojawiającego się w Polsce tematu biometrii, dla wielu banków w Polsce nadal istnieje potrzeba dostarczenia merytorycznych opracowań dotyczących tego zagadnienia. Raport napisany przez ekspertów Forum Technologii Bankowych Związku Banków Polskich rozjaśnia wiele obszarów, począwszy od dostępnych technologii, aspektów prawnych, po prezentację konkretnych zastosowań. Kluczowym elementem raportu jest opis wdrożeń w polskim sektorze bankowym jak również zagranicą, które powinny pozwolić zrozumieć bankom, rozważającym zastosowanie biometrii, jaki był w danym przypadku konkretny business case dla wdrożenia tej innowacyjnej technologii. Jako Przewodniczący Rady Bankowości Elektronicznej ZBP potwierdzam

wysoką wartość merytoryczną Raportu. Dla Banku PKO BP S.A., w którym mam przyjemność piastować stanowisko Wiceprezesa Zarządu Banku, materiał ten będzie również ważnym źródłem wiedzy o biometrii.

„ Biometria coraz mocniej wkracza w polski rynek bankowy

Należy stwierdzić, że biometria coraz mocniej wkracza w polski rynek bankowy. Nie należy jednak pozycjonować jej jako konkurencji dla kart płatniczych, czy też coraz mocniej rozwijających się płatności mobilnych, ale jako uzupełnienie dla tych rozwiązań. Motorem napędowym dla rozwoju biometrii w Polsce, byłyby zapewne utworzenie ogólnodostępnej sieci bankomatów biometrycznych, jak i ogólnopolska sieć płatności. Należy zatem bacznie obserwować rynek bankowości biometrycznej, zarówno pod względem sukcesu obecnych projektów, jak i nowych rozwiązań w najbliższej przyszłości.

Dzięki wieloletniej pracy Związku Banków Polskich i funkcjonującym w nim Forum Technologii Bankowych zostały położone fundamenty pod wdrożenia biometrii w naszym kraju, a polski rynek bankowy może stanowić wzór dla innych krajów zainteresowanych wdrożeniami biometrii.

Piotr Alicki

*Przewodniczący Rady Bankowości Elektronicznej ZBP,
Wiceprezес Zarządu PKO Bank Polski S.A.*

Z dużym zainteresowaniem przeczytałem „Raport Biometryczny 2.0 - Bankowość Biometryczna” stworzony przez Grupę Roboczą do spraw Biometrii przy Forum Technologii Bankowych Związku Banków Polskich. Jest to już druga wersja raportu przygotowana przez tą Grupę. Członkowie zespołu, propagując wiedzę, umożliwiли polskim instytucjom finansowym wdrożenie unikalnych i nowoczesnych rozwiązań biometrycznych. Znaczące jest także to, że w tym obszarze, polska bankowość jest promotorem tych technologii na skalę europejską.

„Pierwsze tak kompleksowe i rzetelne opracowanie na temat biometrii, które zostało wydane na rynku polskim

Autorzy raportu zaprezentowali temat biometrii bardzo szeroko, wzbogacając dodatkowo o praktyczne zastosowania uwierzytelnienia biometrycznego. Bezpieczeństwo transakcji biometrycznej jest bardzo istotnym elementem prezentowanego Raportu. Znaczący wkład w Raporcie mają także liczne przykłady wdrożeń. Biometria w polskiej bankowości nie jest obecnie nowością, ale jedną ze standardowych usług oferowanych Klientom. Oprócz opisu polskich wdrożeń w sektorze bankowym, Raport zawiera także przykłady międzynarodowe, w odniesieniu do innych dziedzin gospodarki – telekomunikacji oraz administracji państwej. Aspekty prawne stosowania biometrii są istotnym elementem przedstawionego Raportu.

Praca zbiorowa „Raport Biometryczny 2.0 - Bankowość Biometryczna” pod redakcją Tadeusza Woszczyńskiego, jest pierwszym tak kompleksowym i rzetelnym opracowaniem na temat biometrii, który został wydany na rynku polskim. Z dumą należy podkreślić, że liczne wdrożenia w polskim sektorze bankowym są potwierdzeniem celowości takich publikacji.

Andrzej Kawiński
*Ekspert Forum Technologii Bankowych ZBP
Prezes Instytutu Analiz i Prognoz Rynkowych*

1. O Raporcie

1.1. Cel dokumentu

Niniejszy „Raport Biometryczny 2.0” powstał w celu upowszechnienia aktualnego stanu wiedzy z zakresu biometrii i jej wykorzystania w sektorze finansowym i administracji publicznej. Ilość haseł, którymi zmuszeni są zarządzać dziś użytkownicy rośnie w bardzo szybkim tempie. W podobnym tempie rosną też nadużycia związane z kradzieżami tożsamości. W dokumencie tym prezentujemy realną alternatywę wykorzystania rozwiązań biometrycznych w Polskim sektorze finansowym jak i na styku bank - administracja publiczna.

Dziś już kilka banków w Polsce wykorzystuje rozwiązania biometryczne do weryfikacji swoich klientów, jak i pracowników. Jesteśmy jednak wciąż na etapie bardzo wczesnego rozwoju rozwiązań biometrycznych w Polsce, stąd potrzeba usystematyzowania wiedzy oraz obalenia wielu mitów.

1.2. Adresaci

Dołożyliśmy wszelkich starań, aby zebrana wiedza została przedstawiona w sposób przystępny i niewymagający wiedzy specjalistycznej. Dokument z pewnością będzie pomocny Członkom Zarządów Banków i menedżerom odpowiedzialnym za budowanie rozwiązań dla swoich klientów z wykorzystaniem rozwiązań biometrycznych. Połączliśmy w raporcie wielowymiarową wiedzę z zakresów: prawa, bezpieczeństwa rozwiązań biometrycznych oraz zastosowań biometrii. Dużą uwagę w raporcie poświęciliśmy przykładom już wykorzystywanych i sprawdzonych rozwiązań biometrycznych w Polsce i na świecie.

Raport przydatny będzie też każdemu, kto będzie chciał poszerzyć swoją wiedzę z zakresu wykorzystania biometrii w sektorze finansowym.

1.3. Rozpowszechnianie i odpowiedzialność za rekomendacje

Zaprośnieni przez ZBP do pracy nad raportem eksperci, dołożyli staranności, aby na miarę ich wiedzy, obowiązujących przepisów oraz dostępnych norm i standardów zapewnić wysoki poziom niniejszego dokumentu.

Raport może być rozpowszechniany w całości lub we fragmentach pod następującymi warunkami:

- każdorazowo należy podawać źródło i cytaty, jak również opisać je w następujący sposób: Woszczyński T.A., Marcinkowski Z., Sudoł M. et. all: Raport Forum Technologii Bankowych przy Związku Banków Polskich - Raport Biometryczny 2.0, Warszawa 2013: XXX (wydawnictwo);
- należy podawać wszystkich autorów raportu;
- bez odrębnej zgody FTB ZBP oraz Redaktorów merytorycznych nie można pobierać wynagrodzenia za rozpowszechnianie raportu ani wykorzystywać go w celach komercyjnych.

2. Definicje

Niniejszy rozdział zawiera podstawowe pojęcia wykorzystywane w dalszej części opracowania. Źródłem definicji są w większości przypadków normy oraz słownik biometryczny ISO/IEC.

- **Biometria:** dział informatyki zajmujący się automatycznym rozpoznawaniem tożsamości człowieka poprzez analizę cech fizycznych (t.j. odcisk palca, układ naczyń krwionośnych palca lub dłoni) bądź behawioralnych (np. sposób chodu, dynamika pisania na klawiaturze, intonacja głosu).
- **Dane biometryczne:** dane na dowolnym etapie przetwarzania będące wynikiem pomiaru biometrycznego (np. dane surowe/źródłowe, czyli próbki biometryczne, cechy biometryczne, wzorce biometryczne).
- **Cechy biometryczne (wektor cech):** liczby lub etykiety (np. minucje odcisku palca, bity kodu żył krwionośnych palca lub dłoni, średnia prędkość składania podpisu odręcznego) wyznaczone na podstawie próbki biometrycznej i używane w porównywaniu biometrycznym.
- **Wzorzec biometryczny:** zbiór cech biometrycznych wykorzystywany w bezpośrednim porównywaniu z cechami badanej próbki biometrycznej.
- **Biometryczne dane referencyjne:** dane biometryczne (np. próbki lub cechy) przypisane do tożsamości i zachowane w systemie w celu późniejszego rozpoznawania tożsamości.
- **System Zarządzania Tożsamością:** system składający się z jednej lub więcej aplikacji, które zarządzają uwierzytelnianiem tożsamości.
- **Tożsamość:** zbiór cech fizycznych i behawioralnych, które czynią osobę jednoznacznie rozpoznawalną.
- **Uwierzytelnienie:** proces, który ustala i/lub weryfikuje tożsamość osoby.
- **Weryfikacja tożsamości:** proces potwierdzania lub zaprzeczania prawdziwości zgłoszonej (zadeklarowanej) tożsamości poprzez porównywanie danych referencyjnych (np. hasła, klucza, wzorca biometrycznego) osoby ubiegającej się o dostęp z referencjami uprzednio sprawdzonymi i zapamiętanymi w Systemie Zarządzania Tożsamością.
- **Biometryczna weryfikacja tożsamości:** proces porównania typu „1 do 1” (1:1) badanego wzorca biometrycznego odpowiadającego deklarowanej tożsamości (np. nr PESEL, nr klienta, nr karty kredytowej, nr telefonu, nr konta) z biometrycznymi danymi referencyjnymi zapisanymi w centralnej bazie danych lub na karcie elektronicznej. System biometryczny weryfikuje i potwierdza tożsamość i najczęściej (głównie ze względów bezpieczeństwa) prezentuje swoją decyzję w formie binarnej (Tak/Nie).
- **Identyfikacja tożsamości:** proces ustalania rzeczywistej Tożsamości danej osoby.
- **Biometryczna identyfikacja tożsamości:** proces porównania typu „1 do wielu” (1:N) badanego wzorca biometrycznego ze wszystkimi danymi referencyjnymi (lub danymi referencyjnymi zawartej grupy) zapisanymi w bazie danych. System biometryczny w najprostszym przypadku potwierdza tożsamość osoby (dane istnieją w bazie) lub informację o braku danych potwierdzających tożsamość w bazie danych. W innych, bardziej rozbudowanych systemach rezultatem może być lista rankingowa zawierająca dane dotyczące tożsamości, dla których dane referencyjne były najbliższe badanemu wzorcowi biometrycznemu.
- **Rejestrowanie tożsamości:** proces tworzenia i zapisywania danych (np. biometrycznych) podmiotów w bazach danych. Proces ten ma na celu reprezentację tożsamości osoby w Systemie Zarządzania Tożsamością poprzez utworzenie unikalnego identyfikatora związanego z rejestrowaną tożsamością.
- **Rejestracja biometryczna:** kluczowy proces w systemach wykorzystujących biometrię. W tym procesie po raz pierwszy pobierane są próbki biometryczne i generowane są wzorce biometryczne, stanowiące biometryczne wzorce referencyjne w systemie. W procesie tym należy zwrócić szczególną uwagę na mechanizmy i procedury w zakresie:
 - a) zapewnienia, iż osoba rejestrująca (przeprowadzająca proces akwizycji wzorców) osobę rejestrowaną jest do tego uprawniona,
 - b) zapewnienia, iż osoba rejestrująca dokona weryfikacji tożsamości osoby rejestrowanej przed pobraniem próbki biometrycznej (np. poprzez okazanie odpowiednich dokumentów tożsamości),
 - c) zapewnienia pozyskania najwyższej jakości próbki biometrycznych, z których powstaje biometryczny wzorzec referencyjny podczas rejestracji.

W procesie uwierzytelnienia biometria może być wykorzystana do Identyfikacji Tożsamości oraz do Weryfikacji Tożsamości. W zastosowaniach praktycznych biometrię wykorzystuje się najczęściej do **Weryfikacji Tożsamości**. Wiąże się z tym stosowanie innej niż w przypadku systemów identyfikacji biometrycznej polityki przechowy-

wania danych oraz ich transferu. Każdy system biometryczny stosuje inne metody wyznaczania cech biometrycznych, budowania na ich podstawie wzorców i ich późniejszego zabezpieczania, nawet dla tej samej modalności biometrycznej (np. rozpoznawania odcisku palca). Z tych względów każda realizacja rozwiązania biometrycznego musi być oceniana niezależnie, w zakresie samej technologii, jak i realizacji **Systemu Zarządzania Tożsamością**.

- **Podpis biometryczny** – podpis cyfrowy typu serwerowego, w którym dostęp do klucza prywatnego jest uwierzytelniany/wyzwalany biometrycznie. Przez podpis serwerowy rozumie się podpis realizowany z wykorzystaniem serwera, zamiast karty kryptograficznej mającej zastosowanie w tradycyjnym modelu podpisu elektronicznego.

3. Technologie biometryczne w bankowości

3.1. Rodzaje technologii biometrycznych

Biometria to technika pomiaru istot żywych w celu automatycznego rozpoznawania osób. Metody biometryczne dzielą się na dwie podgrupy:

- Badające cechy fizyczne
- Badające cechy zachowania (behavioralne)

Biometria kojarzona jest przede wszystkim z metodami badającymi cechy fizyczne. Do metod tych zaliczamy biometrię linii papilarnych (odcisków palców), tęczówki oka, siatkówki oka, wzoru naczyń krwionośnych palca i dłoni, kształtu (geometrii) twarzy bądź dloni.

Rzadziej wykorzystywanymi technikami są metody biometryczne badające nasze zachowanie, mimo że towarzyszą nam w codziennym życiu. Do metod tych zaliczyć można biometrię sposobu intonacji głosu, biometrię podpisu odręcznego (badającą m.in. dynamikę podpisu), a także biometrię badającą fale mózgowe (reakcja mózgu na falę P300) czy sposoby poruszania się.

Poniższa tabela przedstawia zestawienie najpopularniejszych metod biometrycznych na rynku.

Metoda biometryczna	Opis metody	Wybrani producenci urządzeń/rozwiązań
Odcisk palca	Bazuje na układzie punktów charakterystycznych (minucji) linii papilarnych	NEC, Morpho, Precise, Crossmatch
Tęczówka oka	Bazuje na cechach charakterystycznych tęczówki oka	Panasonic, LG, IrisGuard
Naczynia krwionośne palca	Bazuje na unikalnym wzorze układu naczyń krwionośnych wewnętrz palca	Hitachi (Hitachi Ltd., Hitachi Omron Terminal Solutions), NEC, Sony
Naczynia krwionośne dloni	Bazuje na unikalnym wzorze układu naczyń krwionośnych wewnętrz ludzkiej dłoni	Fujitsu
Rozpoznawanie twarzy	Bazuje na analizie obrazu 2D/3D twarzy	Aurora, NEC
Geometria dloni	Bazuje na cechach charakterystycznych dloni	HandPunch
Głos	Bazuje na analizie charakterystyki głosu	Nuance, EasyVoice
Podpis odręczny	Bazuje na charakterystyce wizualnej podpisu (dwuwymiarowy obraz), ale także na sposobie, w jaki podpis został złożony, tj. dynamice pióra	Xyzmo, Wacom

Tabela 1: Najpopularniejsze technologie biometryczne i ich producenci

3.2. Porównanie technologii biometrycznych

Porównanie możliwości biometrycznych, a przede wszystkich bazujących na nich technologii biometrycznych i urządzeń jest zadaniem bardzo trudnym. Porównując bowiem np. „biometrię odcisku palca” należy wziąć pod uwagę istnienie na rynku wielu rodzajów skannerów linii papilarnych różniących się sposobem pomiaru (optyczne, pojemnościowe, ultradźwiękowe, dokładnością, a co za tym idzie również bezpieczeństwem). Ta sama sytuacja zachodzi w przypadku innych technologii (biometria naczyniowa, biometria tęczówki itd.).

Istnieją organizacje międzynarodowe (np. *International Biometric Group* w USA), które podejmują się porównania konkretnych technologii biometrycznych i konkretnych urządzeń, bazując na określonym planie i wskazanym celu testu (np. pomiar współczynników bezpieczeństwa, dla 1000 osób, które zostaną przedstawione w dalszej części raportu/opracowania). Jest również wiele organizacji, które dokonują badań i publikują raporty bezpieczeństwa dla technologii biometrycznych. Do takich organizacji należy m.in. *Fraunhofer FOKUS* w Niemczech, *Naukowa Akademicka Sieć Komputerowa (NASK)* czy *Instytut Maszyn Matematycznych (IMM)* w Polsce.

Poniżej przedstawiono porównanie metod biometrycznych, które analizuje kluczowe aspekty technologii w tym bezpieczeństwo, praktyczność, rozmiar urządzeń, akceptowalność.

Metoda biometryczna	Bezpieczeństwo metody	Unikalność wzorca	Koszt urządzeń	Wielkość urządzeń	Akceptowalność społeczna
Odcisk palca	Średnie	Wysoka	Niski-Średni	Mały / Średni	Niska
Tęczówka oka	Wysokie	Wysoka	Wysoki	Duży	Niska
Naczynia krwionośne palca	Wysokie	Wysoka	Średni	Mały / Średni	Wysoka
Naczynia krwionośne dloni	Wysokie	Wysoka	Średni	Średni / Duży	Średnia
Geometria twarzy	Niskie	Niska	Średni	Średni / Duży	Średnia
Geometria dloni	Niskie	Niska	Średni	Duży	Średnia
Głos	Średnie	Średnia	n/d*	n/d*	Wysoka
Podpis odręczny	Niskie	Niska	Średni**	Średni-Duży**	Wysoka

Tabela 2: Porównanie metod biometrycznych

* Urządzeniem wykorzystanym w biometrii głosowej jest np. telefon komórkowy

** Urządzeniem wykorzystywanym w biometrii podpisu odręcznego jest tablet

3.3. Kryteria doboru technologii biometrycznych na przykładzie sektora bankowego

Aby system biometryczny w banku odniósł oczekiwany sukces, należy odpowiednio dobrać technologię biometryczną. Poniżej przedstawiono wybrane kryteria, na które trzeba zwrócić uwagę przy doborze technologii.

- **Zastosowanie** – najważniejsze jest sprecyzowanie usługi, w której bank chce wprowadzić uwierzytelnianie biometryczne. Dopiero do wybranej usługi można dobrać odpowiednią technologię biometryczną. Przykładowo biometria głosowa jest naturalnym wyborem dla uwierzytelniania operacji w Contact Center, natomiast nie nadaje się np. do wdrożenia w bankomatach.
- **Bezpieczeństwo** – kolejnym kluczowym kryterium doboru technologii i konkretnego rozwiązania biometrycznego, niezależnie od zastosowania w banku jest bezpieczeństwo. Należy brać uwagę zarówno zabezpieczenia samego czytnika biometrycznego (np. blokady antywłamaniowe, szyfrowanie wzorców biometrycznych, testy żywotności), bezpieczeństwo rozwiązania (np. szyfrowanie transmisji, szyfrowanie bazy danych) jak i bezpieczeństwo samej modalności (unikalność danej biometrycznej, współczynniki bezpieczeństwa, odporność na oszustwa). Dobrym wyznacznikiem bezpieczeństwa biometrycznych rozwiązań bankowych jest norma ISO 19092 (Rozdział 5).
- **Akceptowalność** – aby odnieść sukces wdrożenia biometrii, szczególnie w zastosowaniach w bankowości detalicznej, dana biometryka musi być akceptowalna przez klientów. Dlatego też rekomenduje się przeprowadzenie badań marketingowych („focusy”, ilościowe), które potwierdzą czy z wybranej biometrii będą chcieli korzystać klienci. Dotychczas największe problemy z akceptowalnością społeczną można było spotkać we wdrożeniach biometrii odcisku palca, szczególnie w Europie, Turcji i w Japonii.
- **Uniwersalność** - przed wdrożeniem biometrii należy ustalić czy będzie ona używana tylko w jednym czy kilku obszarach. W przypadku wielu zastosowań należy wybrać technologię gwarantującą największą uniwersalność.
- **Rozmiar urządzenia biometrycznego** - rozmiar czytnika biometrycznego jest ważny w kontekście zastosowań. Przykładowo: czytniki biometryczne dedykowane do bankomatów powinny dawać możliwość implementacji na wszystkich dostępnych typach bankomatów bez konieczności znaczących zmian na urządzeniu, przy jednoczesnym zapewnieniu ergonomiczności i bezpieczeństwa. Czytniki do bankowości internetowej powinny być małe i poręczne.
- **Referencje w bankowości** - jest wiele dobrych technologii biometrycznych zapewniających najwyższy poziom bezpieczeństwa, które nigdy nie przyjęły się w sektorze bankowym (np. biometria tęczówki oka). Dlatego bank przy doborze technologii biometrycznej powinien kierować się referencjami w sektorze bankowym.

Poniżej przedstawiono zestawienie technologii biometrycznych w kontekście ich zastosowań w bankowości:

Metoda biometryczna	Bankomat	Oddział	Bankowość internetowa / korporacyjna	Infolinia /IVR	Płatności	Kontrola dostępu / Skrytki depozytowe
Odcisk palca	TAK	TAK	TAK	NIE	TAK	TAK
Tęczówka oka	NIE	NIE	NIE	NIE	NIE	TAK
Naczynia krwionośne palca	TAK	TAK	TAK	NIE	TAK	TAK
Naczynia krwionośne dloni	TAK*	TAK	TAK	NIE	TAK	TAK
Geometria twarzy	NIE	NIE	NIE	NIE	NIE	TAK
Geometria dloni	NIE	NIE	NIE	NIE	NIE	TAK
Głos	NIE	TAK**	TAK	TAK	NIE	TAK
Podpis odręczny	NIE	TAK	NIE	NIE	TAK	NIE

Tabela 3: Podział technologii biometrycznych wg zastosowań

* W zależności od modelu bankomatu

** W celu rejestracji klientów/pracowników

3.4. Technologie biometryczne zastosowane w sektorze bankowym

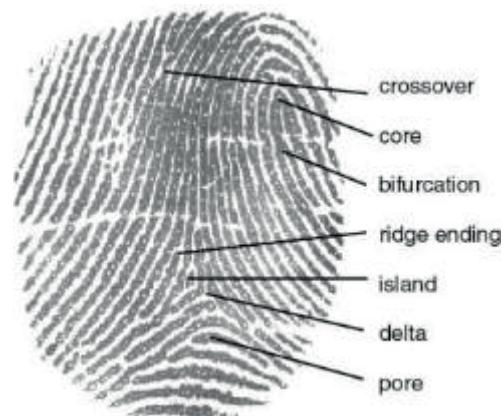
Niniejszy rozdział zawiera szczegółowy opis czterech wybranych technologii biometrycznych mających największą wdrożenie w sektorze finansowym.

3.4.1. Biometria odcisku palca (linii papilarnych palca)

Biometria linii papilarnych jest jedną z najwcześniej wykorzystywanych cech anatomicznych w weryfikacji tożsamości. Grzbiety i brudzy występujące na opuszkach palców uważa się za unikalne dla danej osoby. Odciski palców są unikalne dla każdego palca tej samej ręki. Są unikalne również w przypadku bliźniat jednojajowych. Biometria odcisku palca może być stosowana zarówno w celu weryfikowania tożsamości, jak i identyfikowania osób.

Przez ponad sto lat, urzędy stojące na straży prawa klasyfikowały obrazy odcisków palców przypisując je do jednego z kilku głównych typów i podtypów Henry'ego (tj. pętli, spiral i łuków) oraz ustalały tożsamość dopasowując punkty kluczowe zakończeń grzbietów i rozdwojeń. Z kolei F. Galton, wprowadził pojęcie detali (określone również mianem minucji) oraz opublikował prace poświęcone unikalności oraz niezmienności odcisków palców. Klasyfikacja oraz porównywanie odcisków palców bazuje na porównaniu detali wyróżnionych w obrazach linii papilarnych. Przykłady detali, to: zakończenie (ridge ending), rozdwojenie (bifurcation), ogrodzenie (enclosure) oraz wyspa (island). W 1918 r. E. Locard opracował zasadę, iż 12 identycznych detali pozwala wnioskować o identyczności dwóch odcisków palców. Pomiar cechy biometrycznej może być realizowany z wykorzystaniem czytnika linii papilarnych - najczęściej optycznego, pojemnościowego lub ultradźwiękowego.

Najnowsze techniki dopasowywania odcisku palca koncentrują się na unikalnych punktach obrazu palca - minucjach. Algorytmy obrazowania wyodrębniają minucje i tworzą własne wzorce z zakodowanymi minucjami. Minuce wykorzystuje około 80% algorytmów zaimplementowanych w dostępnych na rynku urządzeniach biometrycznych. Systemy mogą również analizować malutkie pory potowe palca lub liczbę grzbietów między dwoma punktami kluczowymi (takimi jak jądro i delty).



Rys.1: Obraz odcisku palca

Źródło: pagesperso@orange.fr

Wady technologii biometrycznej opartej na wzorze linii papilarnych związane są z charakterystyką biometryczną, bowiem na wynik pomiaru silny wpływ ma stan powierzchni palca. Do czynników mogących wpływać na jakość pobieranych odcisków palców od różnych osób i ograniczenie jakości pobieranego obrazu zalicza się brud, tłuszcz (na przykład smary i oleje), wysuszenie lub pękanie odcisków. Uważa się, że również wiek, płeć i rozmiary ciała mogą mieć wpływ na jakość obrazów palca, podobnie jak położenie (obrócenie, przesunięcie i nacisk) palca na skanerze. Międzynarodowa Organizacja Lotnictwa Cywilnego (International Civil Aviation Organization ICAO) ONZ wymaga, by informacja biometryczna (obraz twarzy, odciski palca, obraz tęczówki) na dokumentach podróży czytanych maszynowo spełniała wymagania standardu ISO/IEC JTC1 19794.

Wczesne systemy były dosyć wrażliwe na oszustwa realizowane dosyć prymitywnymi acz skutecznymi metodami. Nowoczesne systemy linii papilarnych palca wyposaża się dodatkowo w podsystemy „identyfikacji życia”. W tych podsystemach stosowana jest technologia bazująca na rozpoznawaniu struktury skóry. Skóra ma budowę warstwową i wykazuje złożoną interakcję ze światłem. Światło, przechodząc przez skórę, ulega rozproszeniu i absorpcji. Te optyczne różnice zapewniają poprawność weryfikacji, czy próbka badana przez czytnik jest częścią żywego człowieka.



Rys.2: Czytnik linii papilarnych

Źródło: www.precisebiometrics.com

w celu uwierzytelnienia oszusta. Z tego powodu konieczne jest stosowanie dodatkowych zabezpieczeń danych biometrycznych. Zabezpieczeniem najczęściej wykorzystanym dla ochrony wrażliwych danych biometrycznych są typowe techniki kryptograficzne. Odciski palców zostały uznane w UE za wrażliwe dane biometryczne.

Choć pobieranie odcisków palców jest uważane za nieinwazyjne, społeczeństwo może je negatywnie postrzegać z powodu historycznego wykorzystywania przez urzędy stojące na straży prawa. Ponieważ odciski palców są uważane za dane wrażliwe, ich zastosowanie wzbudza szereg wątpliwości, szczególnie pod względem interpretacji prawnej.

Powysze kontrowersje spowodowały iż biometria odcisku palca nie jest powszechna w rozwiązaniach bankowych, szczególnie w Europie i dalekiej Azji. Jednakże istnieją rynki w których biometria linii papilarnych została wdrożona w bankowości i ma bardzo silną pozycję. Takim przykładem może być przede wszystkim Brazylia, gdzie bankomaty biometryczne z czytnikiem linii papilarnych wykorzystywane są m.in. przez CAIXA (ok. 12 000 bankomatów), a także Indie (np. Canara Bank) oraz kraje afrykańskie. W Polsce w systemie bankowości korporacyjnej wykorzystuje biometrię odcisku Bank PEKAO S.A.

Godnymi uwagi zaletami metod biometrycznych opartych o badanie (czytanie) linii papilarnych są: powszechna akceptacja użytkowników (metoda jest uważana w sondażach za jedną z najmniej inwazyjnych metod biometrycznych), wygoda (niewielkie rozmiary czytników, prosta procedura skanowania linii papilarnych) i stosunkowo duża niezawodność (elektroniczne skanowanie linii pozwala na zarejestrowanie wystarczającej liczby szczegółów i zapewnia sporą dokładność; błędy mogą być rzędu 1:100 000).

Koszty skanerów linii papilarnych także są niewielkie i będą jeszcze spadać w miarę rozwoju technologii i wzrostu popytu. Można już spotkać skanery zintegrowane z „myszką” komputerową lub z klawiaturą komputera. Najbardziej znany producentami biometrycznych czytników biometrycznych są m.in.: NEC, Precise Biometrics czy Morpho.

Źródłowe dane biometryczne (obrazy odcisków palca), przetworzone cechy biometryczne, wzorce biometryczne, a nawet wyniki weryfikacji mogą zostać zamienione lub skradzione i wykorzystane ponownie



Rys.3: Bankomaty biometryczne wyposażone w czytnik linii papilarnych (Brazylia)

Źródło: www.lumidigm.com

3.4.2. Biometria naczyń krwionośnych palca

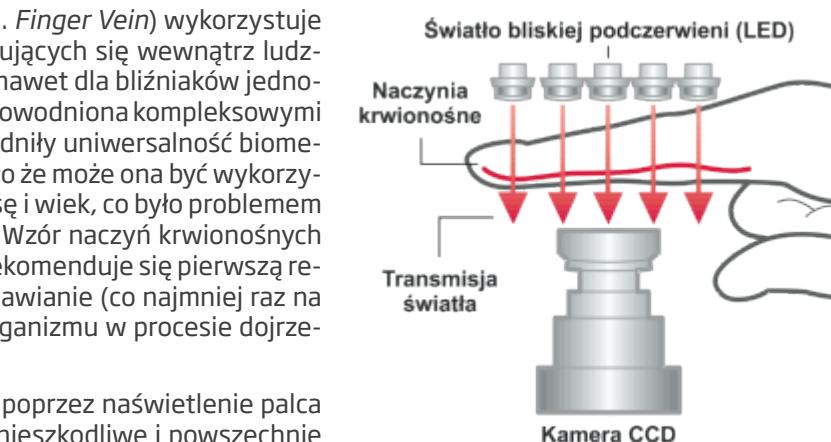
Biometria naczyń krwionośnych palca (ang. *Finger Vein*) wykorzystuje unikalny wzór naczyń krwionośnych znajdujących się wewnętrz ludzkiego palca. Wzór ten jest niepowtarzalny nawet dla bliźniaków jednojajowych. Unikalność technologii została udowodniona kompleksowymi badaniami medycznymi. Badania te udowodniły uniwersalność biometrii naczyń krwionośnych palca, co oznaczało że może ona być wykorzystana przez wszystkich, bez względu na rasę i wiek, co było problemem wśród innych technologii biometrycznych. Wzór naczyń krwionośnych nie zmienia się przez całe życie, jednakże rekommenduje się pierwszą rejestrację w wieku 15 lat i okresowe jej ponawianie (co najmniej raz na 5 lat) ze względu na intensywny wzrost organizmu w procesie dojrzewania.

Wzór naczyń krwionośnych jest pobierany poprzez naświetlenie palca światłem bliskiej podczerwieni, które jest nieszkodliwe i powszechnie stosowane w medycynie. Ze względu na różnice w absorbcji promieniowania widma bliskiej podczerwieni przez hemoglobinę natlenioną i odtnienioną znajdująca się w żyłach i tętnicach oraz inne tkanki palca, możliwe jest uzyskanie dobrej jakości obrazu układu naczyń krwionośnych w postaci ciemniejszych obszarów występujących w obrazie rejestrowanym przez matrycę kamery. Obraz naczyń krwionośnych jest następnie analizowany, w wyniku czego podczas rejestracji powstaje unikalny, referencyjny wzorzec biometryczny. Wzorzec biometryczny powstaje w sposób jednokierunkowy (nie da się odtworzyć struktury naczyń krwionośnych na jego bazie) i nie zawiera żadnych danych wrażliwych. Podczas weryfikacji biometrycznej, żywego palec jest porównywany w czasie rzeczywistym z zapisanym wcześniej wzorcem referencyjnym.



Rys.5: Czytnik UBreader

Źródło: Hitachi Omron TS



Rys.4: Sposób naświetlania palca w czytniku biometrycznym

Źródło: Hitachi

Dzięki temu że dana biometria znajduje się wewnętrz ludzkiego ciała, technologia ta zapewnia ochronę prywatności użytkowników. Fakt ten został potwierdzony przez CNIL (francuska organizacja ochrony danych osobowych), który stwierdził że biometria *Finger Vein* nie stanowi żadnego zagrożenia dla prywatności użytkowników.

Technologia *Finger Vein* powstała pod koniec lat 90-tych w Japonii. Została ona stworzona i opatentowana przez japońską firmę Hitachi. Głównym celem tej technologii było stworzenie alternatywy dla biometrii odcisku palca, która ze względu na wiele wad i kontrowersji z nią związanych nie przyjęła się w społeczeństwie japońskim.

Flagowym produktem biometrii naczyniowej są czytniki z serii Ubreader firmy Hitachi Omron Terminal Solutions (HOTS), które są powszechnie stosowane w bankowości japońskiej. Czytniki te są de facto zaawansowanymi czytnikami kryptograficznymi zawierającymi ogromną liczbę zabezpieczeń zapewniających bezpieczeństwo transakcji. Coraz więcej firm, w tym między innymi Sony, NEC czy Morpho (czytnik multimodalny) opracowuje swoje rozwiązania biometrii naczyń krwionośnych palca, jednakże dotychczas nie odniosły one komercyjnego sukcesu.

Zalety technologii *Finger Vein*:

- wygodna dla użytkownika (brak konieczności posiadania karty, pamiętania kodu PIN oraz posiadania dowodu osobistego, skrócony czas obsługi),
- w pełni realizuje postulat przeciwdziałania wykluczeniu cyfrowemu,
- zapewnia oszczędności dla banku (lokalne wypłaty z bankomatów, brak konieczności wydawania klientom lokalnym kart płatniczych, redukcja papierowego obiegu dokumentów),
- bezpieczna i dokładna ($FAR < 0,0001\%$), posiada najlepsze parametry bezpieczeństwa i pracy wśród dostępnych technologii biometrycznych,
- chroni prywatność użytkowników (posiada akredytacje organizacji ochrony danych osobowych),
- charakteryzuje się wysoką akceptowalnością społeczną (potwierdzona badaniami),
- bezpieczna dla zdrowia.

Biometria naczyń krwionośnych palca została wykorzystana w największych projektach bankowych na świecie. Liderem jest rynek japoński, gdzie biometria *Finger Vein* jest wykorzystana w 293 bankach (m.in. Mizuho Bank, SMBC, Japan Post Bank, CITI, HSBC itd.) i wdrożona w ponad 76 tysiącach bankomatów. W 2010 roku IS Bankasi wdrożył największy projekt biometryczny w regionie EMEA właśnie w oparciu o technologię *Finger Vein* (3000 bankomatów). Od 2009 roku technologia ta funkcjonuje również w polskim sektorze spółdzielczym (m.in. Podkarpacki Bank Spółdzielczy, Bank BPS, BS Kielce itd.) oraz komercyjnym (BPH SA, Getin Bank), zarówno w bankomatach (ponad 200 urządzeń) i oddziałach (ponad 500 oddziałów).



Rys.5a

Źródło: Michał Walus

Podobną technologią do technologii *Finger Vein* jest technologia naczyń krwionośnych dloni (ang. *Palm Vein*) opracowana przez firmę Fujitsu. Bazuje ona na unikalnym układzie naczyń krwionośnych w całej dłoni. Technologia ta również miała swoje zastosowania w bankach w Japonii (np. Bank of Tokyo Mitsubishi), jednakże w dużo mniejszym stopniu niż *Finger Vein*. Została ona także wdrożona w jednym z banków w Brazylii (Banco de Bradesco) i Turcji (Ziraat Bank). Jednakże ze względu na duży rozmiar całego czytnika (łącznie z podstawą unieruchamiającą dłoń) i znaczącą liczbą odrzuceń (związaną z dużym obszarem skanowania) technologia nie zyskuje na popularności w europejskiej bankowości mimo intensywnych kampanii promujących.

3.4.3. Biometria głosowa

Najczęściej komunikujemy się za pomocą głosu. Potrafimy jednocześnie rozpoznawać naszego rozmówcę po głosie, zanim ten się przedstawi, o ile osobę tę znamy z wcześniejszych kontaktów. Naukowcy badają możliwości weryfikacji ludzkiego głosu przez maszyny już od ponad 40 lat, lecz dopiero w dobie rozwoju telefonii komórkowej, biometria głosowa rozwinęła się komercyjnie i z powodzeniem zdobywa społeczne zaufanie.

Na głos ludzki składają się dwa czynniki:

1. Fizyczna budowa kanału głosowego (długość kanału głosowego, płuca, tchawica, głośnia, kanał gardłowy, język, kanał nosowy, kanał ustny, usta etc.)
2. Cechy behawioralne (sposób wypowiadania się charakterystyczny dla danej osoby)

Biometria głosowa jest jedną z najbezpieczniejszych i najłatwiejszych w masowych zastosowaniach metodą weryfikacji tożsamości na odległość. Biorąc pod uwagę powszechnie użycie telefonów za pośrednictwem których użytkownik może korzystać z różnych usług, praktycznie nie istnieje potrzeba inwestycji w dodatkowy specjalistyczny sprzęt po stronie użytkownika - wystarczy zwykły telefon komórkowy lub stacjonarny. Dzięki biometrii głosowej, użytkownik zyskuje bezpieczny dostęp do usług zdalnych przez telefon gdzie zabezpieczeniem jest jego własny głos.

Biometria głosowa może służyć do weryfikacji klientów w Contact Center, urządzeniach mobilnych (smarfony i tablety z dedykowaną aplikacją), stronach internetowych czyli wszędzie tam gdzie dana osoba musi być uwierzytelniona na odległość. Biometria głosowa skutecznie wspiera zapewnienie wysokich standardów bezpieczeństwa, np. w obszarze zarządzania ryzykiem czy zapobiegania oszustwom i kradzieżom tożsamości.

Kategorie zastosowań:

- **Systemy zależne od treści:** Treść hasła jest z góry ustalona i każda osoba ma takie samo hasło np. „W moim banku mój głos jest moim hasłem”
- **Systemy niezależne od treści:** Kategoria ta pozwala na transparentne uwierzytelnienie osoby podczas zwykłej rozmowy telefonicznej. Niezależnie od tego co mówimy, system weryfikuje tożsamość rozmówcy na bieżąco. Operator ma pewność, że podczas całej rozmowy telefonicznej rozmawia cały czas z tą samą osobą.
- **Systemy konwersacyjne:** Oparte są o metodę zależną od treści. Podczas rejestracji wypowiadamy kilka, kilkanaście różnych treści głosowych np. Datę urodzenia, numer telefonu, tajne hasło ustalone podczas rejestracji etc. Podczas uwierzytelnienia system używa losowo wybrane frazy i prosi o ich wypowiedzenie. Systemy te rekommendowane są np. do uwierzytelnienia transakcji finansowych w systemach IVR (ang. Interactive Voice Response).

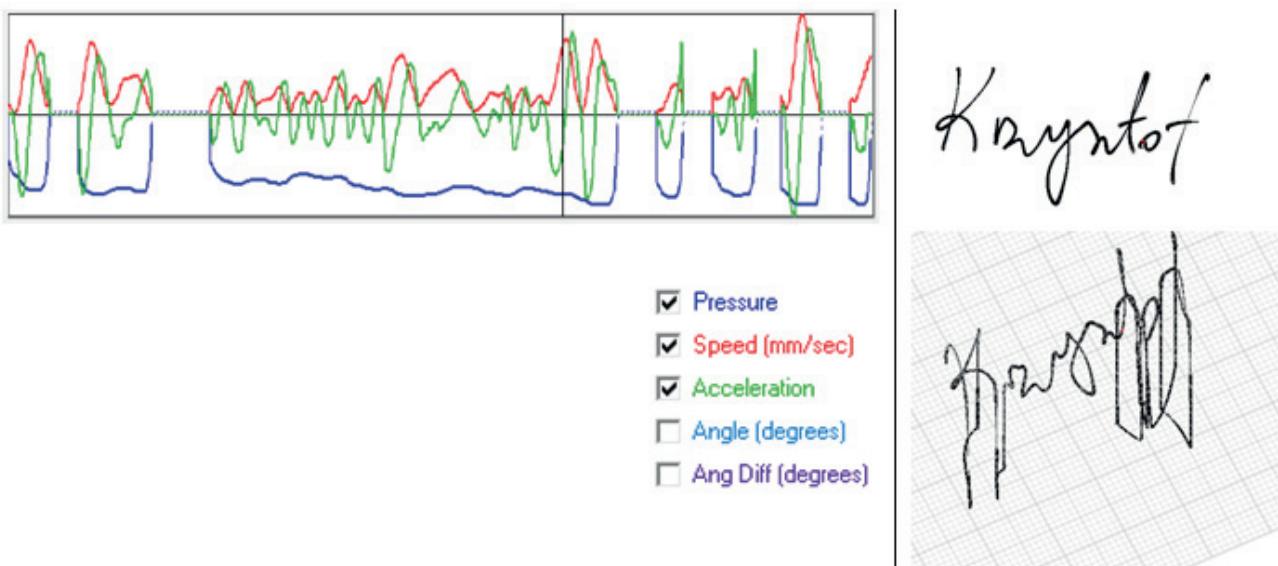
Na dzień publikacji raportu ilość osób, które w różnych systemach na świecie zarejestrowała swój głos wynosi ponad 30 milionów.

3.4.4. Biometria podpisu odręcznego

Technologia biometrii podpisu odręcznego służy weryfikowaniu tożsamości osoby na podstawie jej podpisu odręcznego. Tak jak w przypadku innych technologii biometrycznych, weryfikacja dokonywana jest przez system komputerowy przez porównanie wzorców biometrycznych: wzorca bazowego skonstruowanego uprzednio i utrzymywane go przez system i wzorca konstruowanego przez system w czasie weryfikacji.

Wzorzec podpisu odręcznego konstruowany jest przez system komputerowy w sposób jednoznaczny na podstawie cech podpisu i czynników występujących w czasie podpisywania. Wzorzec zatem wynika z szeregu cech i czynników, a nie tylko z samego graficznego kształtu podpisu. Cechami i czynnikami wpływającymi na kształt (wartość) wzorca mogą być:

- ruchy jakie osoba wykonuje pisakiem w czasie podpisywania - istotne są tu: szybkość i jej zmienność (przyspieszenie), przy czym cechy te dotyczą ruchu przy zetknięciu pisaka z powierzchnią na której podpis jest składany, jak i ruchu nad tą powierzchnią (chwilowo odrywając pisak od powierzchni w czasie podpisywania),
- położenie pisaka względem płaszczyzny na której składany jest podpis - mowa tu o kącie nachylenia pisaka i o zmianach tego kąta w czasie,
- nacisk wywierany pisakiem na powierzchnię podpisywania - jego zmienność w czasie,
- kształt graficzny podpisu.



Źródło: IBM

Można stwierdzić iż dla systemu komputerowego określającego zgodność (pasowanie, czy też podobieństwo) biometrycznych wzorców podpisu odręcznego sam ostateczny, graficzny kształt podpisu jest najmniej istotny, gdyż wynika on (można go odtworzyć) z zarejestrowanych ruchów pisaka.

Dobra (komercyjnie stosowana) technologia podpisu odręcznego powinna wykorzystywać wszystkie powyższe cechy podpisu odręcznego. Jakość w jakiej te cechy są określone zależy jednakże od zastosowanej technologii „zbierania” samego podpisu. To „zbieranie” podpisu musi odbywać się z użyciem specjalizowanego urządzenia rodzaju „tablet” (dalej zwanego urządzeniem do składania podpisu), na płaszczyźnie którego osoba weryfikowana składa podpis specjalnym, przeznaczonym do tego celu pisakiem.

Urządzenia:

Obecnie na rynku dostępny jest cały szereg urządzeń do składania podpisu. Praktycznie wszystkie ich rodzaje umożliwiają połączenie do komputera osobistego za pośrednictwem złącza USB. Dla niektórych z nich powierzchnia na której składany jest podpis jest jednocześnie wyświetlaczem na którym można wyświetlać w tle fragmenty dokumentów, czy też formularzy wobec których (na których) składany jest podpis (podpis złożony na takim dokumencie/formularzu elektronicznym, w swojej formie graficznej zwykle później pozostaje dokładnie w tym samym miejscu i formie). Niektóre z nich zabezpieczają dane (szyfrują) przed przekazaniem ich do stacji roboczej za pośrednictwem kabla USB. Są także takie, które jednocześnie są urządzeniami przeznaczonymi do bezpośrednich, konkretnych zastosowań, np. są terminalami POS (ang. *point-of-sale*).



Rys.7: Przykładowe tablety do składania podpisu odręcznego

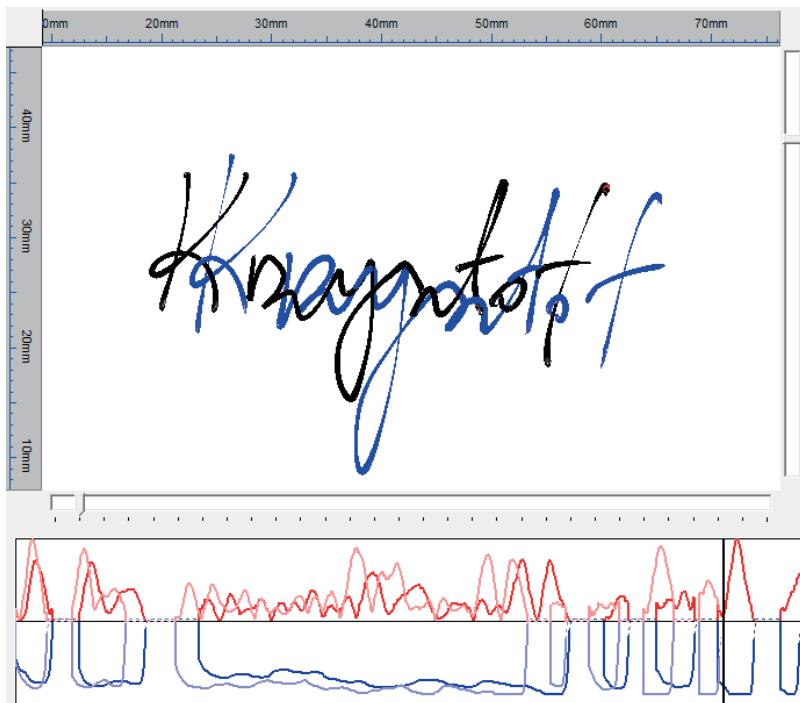
Źródło: IBM

łóżenie pisaka) kształtowane w czasie podpisywania nie będą w każdej chwili w tym czasie jednakowe. Takie dwa „jednakowe” podpisy winny mieć „zblizony rozkład wartości tych cech w czasie” (lub inaczej: „górnki i dolki występujące winny w analogicznej kolejności i wielkości, jednakże być może w nieco różnych odległościach od siebie”). Sztuką jest określenie wiarygodnego i możliwie doskonałego algorytmu porównywania dwóch wzorców. W konstrukcji algorytmów zastosowanie mają techniki i modele matematyczne takie jak ukryte modele Markowa, czy dynamiczne marszczenie czasu (ang. *Dynamic Time Warping*).

Należy zaznaczyć, iż samo urządzenie do składania podpisu jest istotnym elementem stosowanej technologii biometrycznej podpisu odręcznego, jednak nie jedynym równie istotnym. Innym elementem, który ma kluczowe znaczenie dla jakości technologii jest sposób porównywania biometrycznych wzorców podpisu odręcznego.

Algorytmy do weryfikacji podpisów:

Podobnie jak w przypadku innych technologii biometrycznych, sposób porównywania wzorców nie musi być odebrany za prosty w swojej formie, to znaczy nie polega na prostym porównaniu dwóch przedstawionych wartości. Wynika to bezpośrednio z niepowtarzalności (jaką należy założyć) dwóch podpisów złożonych przez tę samą osobę. Oczywiście nadal będą to dwa „jednakowe” podpisy, co może być stwierdzone przez specjalistę-grafologa, jednak cechy podpisu (ruch i po-



Rys.8: Porównanie dwóch „jednakowych” podpisów

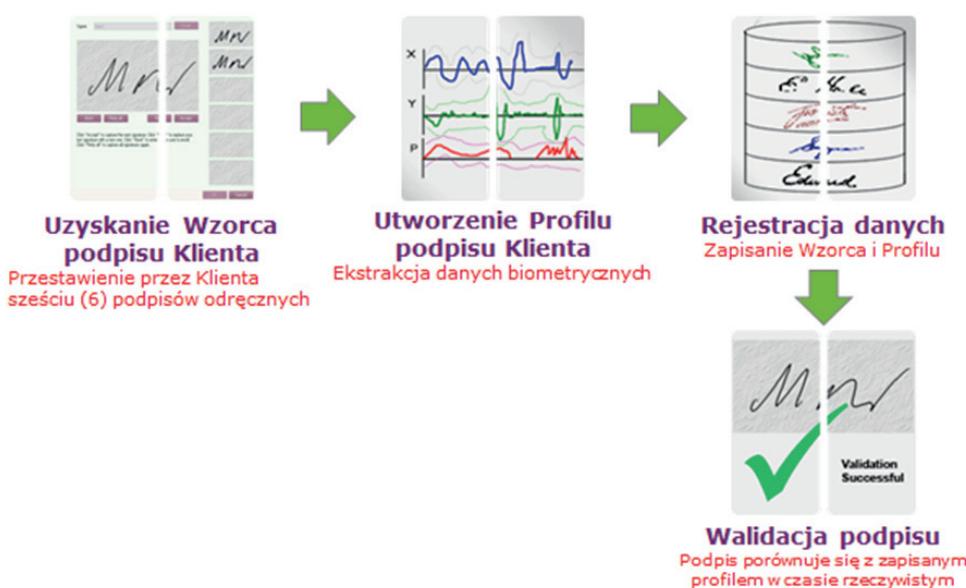
Źródło: IBM

Decyzja o dopasowaniu do siebie wzorców, podejmowana przez system komputerowy jest jednoznaczna, natomiast, tak jak w innych technologiach biometrycznych, sposób porównywania wzorców dokonywany jest w sposób przybliżony i dopuszcza pewien poziom, którego uwzględnienie decyduje o fałszywym odrzuceniu poprawnego podpisu, i o fałszywym przyjęciu niepoprawnego podpisu.

Obecnie najlepsze realizacje opisywanej technologii osiągają dwu-procentowy (2%) poziom błędów zrównoważonych (ang. ERR - Equal Error Rate), określający w technologiach biometrycznych częstość fałszywych akceptacji i fałszywych odrzuceń. Należy przy tym pamiętać, iż prócz porównywanych systemowo wzorców biometrycznych, technologia uwzględnia utrzymywanie wzoru graficznego podpisu wraz ze źródłowymi cechami podpisu (i procesu podpisywania), co nadal daje możliwość tradycyjnej (grafologicznej) analizy podpisów, a tym samym i tradycyjnej weryfikacji tożsamości, post factum.

Zastosowanie:

Niezależnie od sposobu zastosowania opisywanej tu technologii, pierwszym elementem scenariusza działania zawsze jest skonstruowanie biometrycznego wzorca podpisu odręcznego. Odbywa się to przez kilkukrotne złożenie takiego samego podpisu, przy czym system komputerowy weryfikuje tę zgodność i sam decyduje o ilości wymaganych do złożenia podpisów – zwykle jest to pięć podpisów. Po zweryfikowanym złożeniu wystarczającej ilości pasujących do siebie podpisów system wylicza wzorzec biometryczny i umieszcza go w swojej bazie wzorców biometrycznych. Każdy kolejny przypadek weryfikacji zgodności podpisów dokonywany jest właśnie wobec przechowywanego tam wzorca.



Rys.9: Scenariusz konstruowania i wykorzystywania wzorca biometrycznego

Źródło: IBM

Dla biometrii podpisu odręcznego najbardziej popularne są następujące zastosowania:

- Weryfikacja tożsamości klienta w oddziale
- Uwierzytelnianie operacji klienta w oddziale
- Podpisywanie dokumentów (w elektronicznych systemach obiegu dokumentów)
- Płatności

Ze względu na wciąż wysoki poziom fałszywej akceptacji, biometria podpisu odręcznego nie jest nigdy główną metodą uwierzytelniania. Jednakże niektóre banki w Europie wdrożyły ją w swoich oddziałach, np. Bank GE Money Bank w Czechach. W Polsce biometrię podpisu odręcznego testował m.in. Bank Millennium. Alior Bank S.A., który w każdym ze swoich oddziałów posiada tablęty do składania podpisu odręcznego nie zastosował w nich biometrii.

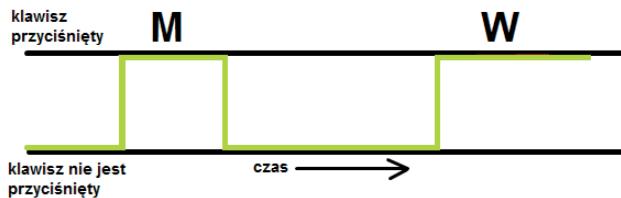
Opisywana tu technologia jest obecnie standaryzowana przez organizację ISO (International Organization for Standardization): ISO/IEC 19794-7:2007 (*Information technology - Biometric data interchange formats - Part 7: Signature/sign time series data*).¹

3.4.5. Biometria przyszłości

Spośród wielu rodzajów biometryk, do najczęściej obecnie wykorzystywanych w sektorze finansowym należy zaliczyć opisane powyżej: biometrię wzoru naczyń krwionośnych, podpis odręczny, biometrię głosową jak i biometrię siatkówki oraz tęczówki oka (głównie w krajach arabskich). Z punktu widzenia klienta jest to środek jego uwierzytelnienia przy dostępie do usług znajdujących się w ofercie banku. Z perspektywy banku i jego pracowników jest to narzędzie pracy, system kontroli dostępu do zasobów infrastruktury.

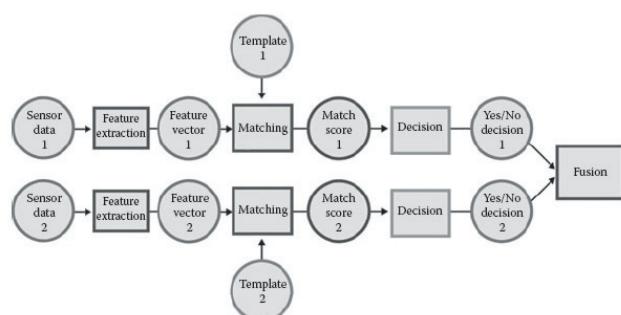
Pracownicy poprzez uwierzytelnianie biometryczne (odcisk palca, układ naczyniowy żyły) logują się do swoich stacji roboczych. Natychmiast po zalogowaniu mają oni dostęp do aplikacji i funkcji, które zostały im nadane przez administratorów systemów zgodnie z obowiązującymi matrycami ról. W tym obszarze możliwe jest wdrożenie dodatkowych mechanizmów oceny czy osoba znajdująca się przed ekranem monitora jest osobą upoważnioną do jego obsługi, czy nie (np. pracownik oddalił się od komputera, zapominając o zablokowaniu ekranu i ktoś nieupoważniony korzysta z jego stacji). Biometria dynamiki pisania na klawiaturze (ang. *keystroke dynamic*) jest cechą behawioralną, która poprzez analizę odstępów czasowych między kliknięciem poszczególnych klawiszy i czasu gdy klawisze są wcisnięte, ocenia prawdopodobieństwo umożliwiając stwierdzenie czy przed komputerem cały czas znajduje się właściwa osoba. Potencjalnie wprowadzenie tego typu zabezpieczenia przy stosunkowo niskim nakładzie

finansowym, pozwoliłoby przeciwdziałać nieupoważnionemu dostępowi do zasobów infrastruktury.



Rys.10: Schemat analizy dynamiki pisma na klawiaturze

Od początku lat 90-tych obserwowane jest coraz to większe zainteresowanie technikami multibiometrycznymi. W systemach tego typu w procesie uwierzytelniania stosuje się analizę więcej niż jednej cechy biometrycznej. Uzasadnieniem takiego działania jest chęć poprawy parametrów bezpieczeństwa takich jak FAR czy FRR.



Rys.11: Schemat działania systemu multibiometrycznego
Źródło: CRC Press²

FAR (False Acceptance Rate) to współczynnik niesłusznej akceptacji, przyznanie dostępu nieuprawnionej osobie. FRR (False Rejection Rate) jest natomiast współczynnikiem niesłusznego odrzucenia, świadczy o odmowie dostępu osoby uprawnionej. W przypadku analizy większej ilości biometryk trudniejszym staje się 'oszukanie' systemu i dostęp osoby nieuprawnionej. Dodatkowym atutem jest zwiększenie niezawodności oferowanych urządzeń, gdyż w momencie nieprawidłowego działania jednego z sensorów odpowiedzialnych za odczyt danych biometrycznych, istnieje możliwość autentykacji innymi. Eliminuje to przypadki odmowy dostępu osób upoważnionych.

Zgodnie z przyjętą taksonomią³ istnieją następujące rodzaje systemów multibiometrycznych: multisensoryczne - wykorzystujące wiele sensorów do akwizycji wzorca jednej cechy biometrycznej, multiekstrakcyjne - bazujące na zastosowaniu różnych algorytmów

2 Chuck Wilson: Vein pattern recognition: a privacy-enhancing biometric. CRC Press, 2011

3 Arun Ross: An Introduction to Multibiometrics, Proc. of the 15th European Signal Processing Conference (EUSIPCO), Poznań, 09.2007.

1 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38751

do wyodrębnienia cech charakterystycznych, wie-loinstancyjne – przetworzeniu i analizie poddawana jest sekwencja wzorców (następujące po sobie klatki z nagrania kamery), multimodalne – gdzie rozpoznanie osoby następuje w oparciu o różne cechy biometryczne (np. geometria i układ naczyniowy palca) oraz systemy hybrydowe. Z pewnością tworzenie tego typu systemów wiąże się z szeregiem wyzwań technologicznych i konstrukcyjnych dla ich twórców, jednak ich wdrożenie będzie wiązało się ze zwiększeniem użyteczności a co za tym idzie jakości obsługi. Przykładami miejsc gdzie stosowanie systemów multibiometrycznych miałyby sens, mógłby być: dostęp do ścisłe chronionych zasobów i pomieszczeń przez pracowników oraz autoryzacja wysokokwotowych transakcji przez klientów.

Ze względu na standaryzację protokołów transmisji danych, w perspektywie kilku najbliższych lat możemy się spodziewać utworzenia ogólnego bankowego hosta autoryzacyjnego transakcji biometrycznych o zasięgu krajowym lub międzynarodowym. Będą to kanały wymiany informacji potrzebnych do uwierzytelnienia płatności między instytucjami finansowymi. Umożliwi to realizację wypłat na podstawie uwierzytelnienia biometrycznego w bankomatach należących do innych banków bez konieczności deponowania w nich naszych cech osobniczych.

Do ciekawych projektów prowadzonych obecnie w polskich ośrodkach badawczych (np. Politechnika Śląska, Akademia Górnictwo-Hutnicza) należy zaliczyć: wykrywanie i rozpoznawanie mikro ekspresji twarzy oraz analiza ruchu gałek ocznych podczas mrugnięcia. Wstępne wyniki wskazują możliwość wykrywania takich cech jak zainteresowanie rozmówcy tematem prowadzonej rozmowy bądź wykrywanie irytacji i kłamstwa. Choć wykorzystanie tych biometryk w bankowości jest obecnie mało prawdopodobne, być może w przyszłości w placówkach bezobsługowych znajdą one swoje zastosowania. Niewątpliwie wprowadzanie tego typu rozwiązań jest korzystne dla banków ze względu na kilkukrotnie niższe koszty związane z uruchomieniem i działaniem tego typu placówek w porównaniu do tradycyjnych oddziałów. Alternatywnie wykorzystanie omawianych biometryk może znaleźć zastosowanie w urządzeniach VTM (Virtual Teller Machine), które oprócz realizacji transakcji wpłat i wypłat gotówkowych jak dzisiejsze urządzenia dualne z funkcją bankomatu i wpłatomatu, umożliwiają wirtualny kontakt z konsultantem banku. Urządzenia VTM z powodzeniem funkcjonują już w Chinach, RPA, Japonii i Hong Kongu. W 2013 zostanie uruchomiona pierwsza sieć urządzeń VTM w Polsce.



Rys.12: Różne urządzenia VTM z uwierzytelnianiem biometrycznym

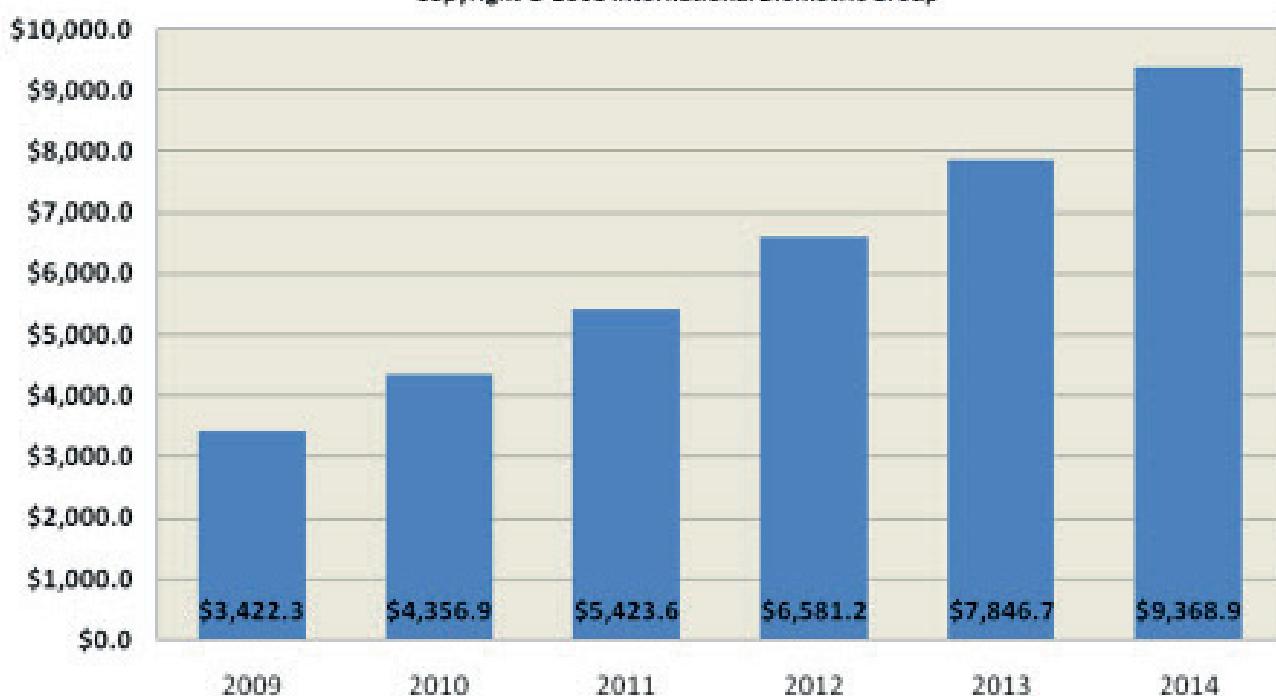
Źródło: Huawei, Wincor Nixdorf, Hitachi

Swoistą ciekawostką jest prowadzenie prac nad wykorzystaniem ludzkiego DNA w procesach identyfikacji i weryfikacji osobniczej. Niestety, ze względu na skomplikowanie procesu jego analizy, wykorzystanie tej cechy w systemach komercyjnych jak na razie pozostaje w sferze science-fiction.

Polska jest jednym z najszybciej rozwijających się dostawców systemów biometrycznych na świecie. Według prognoz Biometrics Market and Industry Report 2009 - 2014 w 2014 roku całkowite dochody ze sprzedaży oraz licencjonowania produktów i usług biometrycznych znacznie przekroczą 9 mld USD. W biometrii niewątpliwie tkwi duży potencjał, tylko od nas zależy jaką innowacyjność zaoferujemy naszym klientom. Biometrię czeka w najbliższych latach rozwit, popularyzacja i upowszechnienie na masową skalę. Na szczęście wdrażane technologie zdecydowanie odbiegają od literackich i filmowych wizji gdzie biometria jest narzędziem inwigilacji a nie sposobem na zwiększenie użyteczności i funkcjonalności znanych nam urządzeń.

Annual Biometric Industry Revenues, 2009-2014 (\$m USD)

Copyright © 2008 International Biometric Group



Rys.13: Wzrost wartości rynku biometrycznego w latach 2009 - 2014

Źródło: International Biometric Group

4. Bezpieczeństwo w biometrii

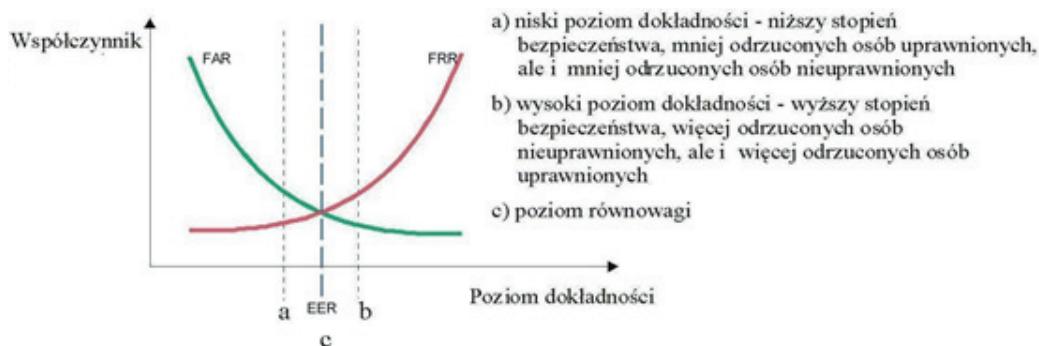
4.1. Współczynniki bezpieczeństwa i pracy technologii biometrycznych

Naturalną cechą systemów uwierzytelniania biometrycznego jest porównywanie dwóch (lub więcej) wzorców cech biometrycznych pobranych w różnym czasie. Pierwszy z nich jest pobierany podczas rejestracji użytkownika w systemie, zaś drugi, na bieżąco, w momencie uwierzytelnienia. Choć twierdzenie o niezmienności cech biometrycznych jest prawdziwe, to wzorce tych samych cech biometrycznych pobierane w różnym czasie są różne. Można stwierdzić, że jeżeli porównywane są dwa identyczne wzorce, to mamy do czynienia z próbą nieuprawnionego uwierzytelnienia (oszustwa). Tak więc w procesie uwierzytelnienia następuje ocena podobieństwa dwóch wzorców. Zazwyczaj wynikiem porównania jest punktacja lub wyrażona w procentach zgodność wzorców. Przyjęcie odpowiedniego progu (w punktach lub procentach) kwalifikuje uwierzytelnienie jako pozytywne bądź negatywne. Wiele urządzeń biometrycznych pozwala na płynną regulację takiego progu, a tym samym istotnie wpływa na wiarygodność uwierzytelnienia.

Wiarygodność uwierzytelniania w technikach biometrycznych jest charakteryzowana przez następujące współczynniki:

- fałszywej akceptacji nieuprawnionej osoby (FAR - False Acceptance Rate)
- fałszywego odrzucenia uprawnionej osoby (FRR - False Rejection Rate)
- równowagi (EER - Equal Error Rate)

Fałszywa akceptacja nieuprawnionej osoby zachodzi wtedy, gdy pozytywne uwierzytelnienie jest przyznane osobie nieuprawnionej. Fałszywe odrzucenie uprawnionej osoby następuje przy odmowie dostępu osobie uprawnionej. Należy pamiętać, że im lepszy FAR tym gorszy FRR i mniejsza wygoda użytkowania - jest więcej fałszywych odrzuceń. I na odwrót - im lepszy FRR, a więc wygoda użytkowania, tym gorszy jest parametr FAR - czyli wiarygodność uwierzytelnienia. Jest jednak pewien poziom równowagi pomiędzy parametrami (EER)



Rys.14: Poglądowe wykresy współczynników FRR i FAR

Źródło: Instytut Maszyn Matematycznych

Poniższa tabela przedstawia wyniki badań przeprowadzonych w 2006 roku przez International Biometric Group (IBG) z USA, które porównują współczynniki bezpieczeństwa i pracy dla wybranych technologii biometrycznych:

Biometria	Naczynia krwionośne palca	Naczynia krwionośne dloni	Tęczówka
Producent	Hitachi	Fujitsu	IrisGuard
Urządzenie	UBReader	PalmSecure	H100
FTE, dwie próby	0,55%	1,63%	7,01%
FRR	1,26%	4,23%	1,76%
FAR	0,01%	0,0118%	0,01%
Czas rozpoznania [s]	1,23	2,13	4,22
Czas rejestracji [s]	33,3	61,7	44,5

Tabela 4: Wyniki porównania technologii przeprowadzonego przez IBG (2006 rok)

Biometria głosowa: Najbardziej skuteczne silniki biometrii głosowej są dziś na poziomie FAR 0,01% i FRR poniżej 5%.

4.2. Bezpieczeństwo systemów biometrycznych

Coraz powszechniejsze wykorzystanie biometrii w życiu codziennym stawia przed nami priorytet odpowiedniego zabezpieczenia tożsamości użytkowników w szeroko rozwiniętym społeczeństwie informacyjnym.

Dane biometryczne mogą być przetwarzane po ich pobraniu (np. obraz odcisku palca, obraz tęczówki, obrazu układu naczyń krwionośnych itp.), a wzorzec biometryczny, który jest zbiorem cech biometrycznych, przedstawiany jest przeważnie w formie cyfrowej i przechowywany w bazie danych.

Dane biometryczne są obecnie przetwarzane zarówno w sektorze prywatnym i publicznym i są wykorzystywane do automatycznej weryfikacji (pozwalającej sprawdzić autentyczność osoby) lub identyfikacji tożsamości użytkowników (pozwala sprawdzić, czy cecha biometryczna jest w centralnej bazie danych i do kogo należy). Dane biometryczne są wykorzystywane również w celu zapewnienia bezpiecznego dostępu do chronionych obszarów fizycznych (stref zastrzeżonych, miejsc pracy itp.) lub informacyjnych (do elektronicznych systemów lub aplikacji).

Tak szerokie zastosowanie biometrii w środowiskach informatycznych narzuca konieczność odpowiedniego zabezpieczenia przetwarzanych danych biometrycznych. By zwiększyć bezpieczeństwo systemów informatycznych przetwarzających dane biometryczne, można zastosować różne metody. Można przechowywać wzorzec na karcie mikroprocesorowej, służącej do uwierzytelniania tożsamości użytkownika, w centralnej bazie danych lub na plastikowych, optycznych lub elektronicznych kartach. Można także, po dokonaniu ekstrakcji unikatowej cechy charakterystycznej tożsamości, tzw. wzoru biometrycznego, wybrać niezbędną liczbę charakterystycznych punktów (tzw. szablon/wektor cech) takiego wzoru i uzyskać tym samym wartość binarną (identyfikator - w zasadzie funkcjonalnie tożsamy np. z PIN) przechowywaną w czytniku. Takie przechowywanie danych biometrycznych w postaci zaszyfrowanego kodu jest teoretycznie i praktycznie niewystarczalne do odtworzenia wzorca biometrycznego. Wszędzie poza środowiskiem, w którym działa czytnik biometryczny, wiedza o tym identyfikatorze jest tylko nic nieznaczącą wartością binarną, dzięki czemu na jej podstawie nie można zidentyfikować tożsamości osoby.

Podczas przetwarzania danych biometrycznych kluczowym elementem jest zabezpieczenie wzorców biometrycznych przed ich nielegalnym ponownym użyciem, kradzieżą lub przetworzeniem. Zbiór wymagań którym powinien podlegać system informatyczny przetwarzający dane biometryczne został opracowany w ramach normy ISO 19092:2008 (norma omawiana jest w rozdziale 5), poświęconej bezpieczeństwu systemów biometrycznych. Wymagania te dotyczą:

- zabezpieczenia wzorca biometrycznego (przechowywanie, transmisja),
- fizycznego i logicznego zabezpieczenia czytnika biometrycznego, zabezpieczenia systemu informatycznego połączanego z systemem biometrycznym,
- przygotowania odpowiednich procedur i zasad dotyczących korzystania z systemu biometrycznego
- edukowania personelu pobierającego dane biometryczne, jak i edukowania użytkowników.

Kluczowym elementem jest zabezpieczenie wzorców biometrycznych, tak aby zminimalizować ryzyko odtworzenia informacji wrażliwych na podstawie nielegalnie pozyskanych danych biometrycznych lub uniemożliwić ponowne, nielegalne, wykorzystanie wzorców w procesie weryfikacji. Podstawowym zabezpieczeniem jest szyfrowanie wzorców i stosowanie znanych, bezpiecznych protokołów transmisji danych biometrycznych. Dodatkowo można zastosować połączenie biometrii z infrastrukturą klucza publicznego (PKI), dzięki czemu uzyskuje się dodatkowy poziom zabezpieczeń. Biometria stanowi w tym przypadku zabezpieczenie dostępu do klucza prywatnego w systemie PKI. Ma to zastosowanie przede wszystkim w systemach bankowych.

Przechowywanie wzorca biometrycznego może mieć miejsce w centralnej bazie danych lub na karcie mikroprocesorowej. W przypadku centralnej bazy danych jej administrator uzyskuje dostęp do danych w niej gromadzonych. Umieszczenie wzorca na karcie oraz jego porównanie na karcie oznacza, że jedynym dysponentem wzorca biometrycznego jest posiadacz karty, jednocześnie „właściciel” wzorca biometrycznego. Jedno i drugie zastosowanie ma swoje plusy i minusy. Skutki ewentualnego ataku na system centralny i system karty będą znacząco różne. Można pokusić się o stwierdzenie, że zagrożenie dla danych biometrycznych zgromadzonych na karcie będzie mniejsze niż dla systemów centralnych gdyż np. utrata karty z danymi biometrycznymi nie musi skutkować utratą tożsamości po jej zastrzeżeniu, utrata danych przez jedną osobę nie podważa funkcjonowania systemu jako całości.

Dynamiczny rozwój technologii biometrycznych, możliwości jej stosowania w różnych dziedzinach przemysłu wymusza istnienie coraz dokładniejszych regulacji określających zasady prawidłowego przetwarzania danych. Istniejące już przepisy dotyczące przetwarzania danych dają możliwość wykorzystywania biometrii w systemach informatycznych. W przeważającej mierze dotyczą one ochrony danych osobowych jednakże poprzez analogie nakładają one obowiązki na systemy przetwarzające dane biometryczne.

4.2.1. Sposoby przechowywania i porównywania danych biometrycznych

Pytanie jak przechowywać dane biometryczne jest kluczowym zagadnieniem, które należy rozwiązać już na etapie przygotowywania wstępnych założeń systemu korzystającego z biometrii. Wybór konkretnej metody ma istotny wpływ zarówno na potrzebną infrastrukturę i wprowadza konieczność zastosowania odpowiednich procedur organizacyjnych. Co więcej, wybór miejsca przechowywania danych biometrycznych ma wpływ nie tylko na ich bezpieczeństwo, ale także przenosi kontrolę nad nimi pomiędzy użytkownikiem a instytucją świadczącą usługę. Można wskazać trzy metody prze-

chowywania: w centralnej bazie danych, bezpośrednio w czytniku biometrycznym oraz na karcie kryptograficznej.

- **Centralna baza danych**

Wydaje się, że najbardziej naturalnym podejściem do przechowywania danych biometrycznych jest składowanie ich w centralnej bazie danych. Zastosowanie tego rozwiązania sprawia, że zarządzanie przechowywanymi wzorcami sprawia najmniej problemów. Mając pod kontrolą całą bazę danych, nie trzeba synchronizować każdego czytnika z osobna ani obawiać się, że użytkownik zgubi kartę kryptograficzną. Podejście takie najlepiej sprawdzi się w dużych organizacjach (np. w bankach) przy przechowywaniu dużej liczby wzorców. Dodatkowo, baza danych chroniona jest przed dostępem fizycznym w ramach struktury organizacyjnej instytucji, na podobnych zasadach jak chronione są bazy danych zwierające dane osobowe. Zaszyfrowanie informacji zabezpiecza je przed ewentualnym odczytem i umożliwia weryfikację integralności.

Główna zaleta tego rozwiązania może w niektórych sytuacjach okazać się największą wadą. Ze względu na to, iż wszystkie dane przechowywane są w jednym miejscu, skuteczny atak mógłby teoretycznie skompromitować cały system. Drugim wrażliwym punktem tego rozwiązania jest moment przekazania danych biometrycznych pomiędzy czytnikiem a bazą danych, gdzie następuje weryfikacja. Napastnik może próbować przechwycić transmisję i ją odpowiednio modyfikować, podając wzorce lub od razu generując pozytywną odpowiedź na weryfikację. Aby się przed tym zabezpieczyć cała transmisja pomiędzy czytnikami a serwerami powinna być odpowiednio zabezpieczona metodami kryptograficznymi. Należy jednak podkreślić, że przy zastosowaniu odpowiednich środków bezpieczeństwa i przestrzeganiu procedur bezpieczeństwa prawdopodobieństwo kompromitacji systemu zarówno poprzez atak na bazę danych jak i na czytnik lub transmisję jest bardzo niskie. Przechowywanie wzorców w centralnych bazach jest podstawowym rozwiązaniem w sektorze bankowym.

- **Czytniki biometryczne**

Rozwiązaniem stojącym w opozycji do centralnego przechowywania wzorców biometrycznych jest składowanie ich bezpośrednio w czytniku. Takie podejście sprawdza się szczególnie korzystnie w przypadku tworzenia systemów rozproszonych np. kontroli dostępu do pomieszczeń. W przypadku gdy wzorce nie są replikowane pomiędzy czytnikami kompromitacja jednego z nich nie zagrozi kompromitacji całego systemu lub zagrozi tylko jego niewielkiej części. Dodatkową zaletą jest fakt, iż dane przetwarzane są bezpośrednio w czytniku i wzorce nigdy go nie opuszczają. Czytniki mogą zostać także skonfiguro-

wane w taki sposób, że na wypadek kradzieży lub próby uszkodzenia dane w nich zawarte zostaną skasowane uniemożliwiając ich odtworzenie i ponowne użycie. Przechowywanie wzorców na czytnikach nie jest stosowane w bankowości.

• Karty kryptograficzne

W dzisiejszych czasach karty kryptograficzne (lub inaczej karty inteligentne, ang. *smart cards*) są po-wszechnie używane w wielu dziedzinach życia. Miniaturyzacja i wzrost mocy obliczeniowej pozwalają na coraz szersze zastosowanie, także w sytuacjach gdzie wymagany jest najwyższy poziom bezpieczeństwa. Karty inteligentne obsługują asymetryczne algorytmy kryptograficzne takie jak Diffie-Hellman i RSA. Wspierają także kryptografię symetryczną, algorytmy DES, 3DES, AES oraz funkcje skrótu z rodziną SHA i SHA-2. Dodatkowym zabezpieczeniem jest możliwa certyfikacja na zgodność z normami EMV, Common Criteria, FIPS-PUB 140-2 czy ITSEC v1.2. Możliwy jest także udział producentów w konsercjach takich jak MULTOS i organizacjach tj. Global Platform. Zarówno udział w różnych organizacjach jak i zgodność z normami wymuszą tworzenie odpowiedniego poziomu ochrony nie tylko przed odczytem danych z karty poprzez bezpośredni do niej dostęp, ale także poprzez ulot elektromagnetyczny. Ponadto, jak pokazują systemy PayPass i PayWave coraz popularniejsza oraz bezpieczniejsza jest również technologia bezstykowej komunikacji z kartą. Nie jest to co prawda nowość w tej dziedzinie, gdyż bezstykowe karty używane są od wielu lat choćby w transporcie miejskim czy jako elektroniczne legitymacje studenckie. Ponadto, dzisiejsza technologia pozwala na projektowanie wieloaplikacyjnych kart mających mnogość zastosowań i integrujących różne funkcjonalności. Na rynku istnieją dwie główne technologie kart kryptograficznych, MULTOS oraz Java Card.

Nie ma jedynego słusznego rozwiązania. Każde z nich ma swoje wady jak i zalety. Decydując się na wykorzystanie konkretnej metody niezbędne jest sporządzenie analizy ryzyka oraz oszacowanie kosztów implementacji każdego z nich.

4.2.2. Zabezpieczenia czytników biometrycznych

Czytniki biometryczne stanowią kluczowy element infrastruktury systemu biometrycznego w banku. Ponieważ na system biometryczny przeniesiona jest „odpowiedzialność” za poprawne uwierzytelnianie klienta, czytnik biometryczny musi być odpowiednio bezpieczny. Na rynku dostępnych jest wiele różnych czytników biometrycznych bazujących na różnych modalnościach biometrycznych, jednakże ich poziom bezpieczeństwa daje wiele do życzenia (np. wiele prostych czytników linii papilarnych, stosunkowo łatwych do podrobienia).

O kluczowym znaczeniu czytników biometrycznych oraz ich bezpieczeństwa mówi norma ISO 19092. Załącznik D normy ISO 19092⁴ określa wymagania bezpieczeństwa wobec urządzeń biometrycznych chroniących dostęp do informacji wrażliwych. Norma określa 3 poziomy bezpieczeństwa dla urządzeń biometrycznych i wymagania w każdym z nich:

Poziom 1:

- Urządzenia muszą być zbudowane z solidnych i odpornych komponentów.
- Obudowa (powłoka ochronna, uszczelniająca) ma chronić układy elektroniczne urządzenia przed warkami środowiskowymi i uszkodzeniami fizycznymi.
- Podczas wykonywania czynności serwisowych (utrzymywanych) wszystkie informacje prywatne (np. wzorce biometryczne) i inne krytyczne parametry bezpieczeństwa powinny zostać wyzerowane (proceduralnie lub automatycznie).

Poziom 2:

- Wymagania Poziomu 1
- Urządzenia biometryczne powinny zapewniać dowody włamania, kiedy zachodzi próba fizycznej interwencji w urządzenie (specjalne pokrycie, obudowa, dowody logiczne...)

Poziom 3:

- Wymagania Poziomu 1 i Poziomu 2
- Urządzenie powinno zawierać reakcję na włamanie – wszystkie informacje prywatne i parametry bezpieczeństwa powinny być zerowane po otwarciu obudowy, dostępu do interfejsu serwisowego itd.
- Jeśli urządzenie zawiera otwory wentylacyjne to powinny być one skonstruowane w ten sposób aby zapobiec dostępowi fizycznemu do urządzenia
- Urządzenia powinny mieć obudowy odporne na vandalizm i umożliwiające udowodnienie włamania lub też w przypadku zdjęcia obudowy powodowały jego uszkodzenie (tj. urządzenie nie będzie funkcjonować)

Wyżej wymienione wymagania, w tym przede wszystkim wymagania Poziomu 3 są kluczowe szczególnie wobec urządzeń które znajdują się w miejscowościach, gdzie nie jest zapewniona asysta pracownika banku (np. bankomaty pozaoddziały). Powyższe wymagania powinny być weryfikowane przez bank jako minimalne, rozważając produkty różnych dostawców.

Urządzenie biometryczne wykorzystane do uwierzytelniania operacji finansowych powinno być de facto bezpiecznym urządzeniem kryptograficznym. Oprócz wyżej wymienionych zabezpieczeń należy zweryfiko-

⁴ ISO 19092:2008(E): Financial services - Biometrics - Security framework

wać wyposażanie ich w następujące mechanizmy bezpieczeństwa:

- Testowanie żywotności - urządzenie powinno zapobiegać możliwości weryfikacji podrobionych obiektów. Oznosi się to szczególnie to biometrii odcisku palca bądź tęczówki oka, gdzie takie fraude miały miejsce.
- Wykrywanie obcych przedmiotów - urządzenie powinno wykryć umieszczenie przedmiotu obcego na czytniku. Np. przedmiotem obcym może być guma do żucia bądź moneta (wtedy informacja jest potrzebna ze względów serwisowych), jednakże może oznaczać teżingerencję w czytniki („skimmer biometryczny”)
- Szyfrowanie wzorców biometrycznych - wzorce biometryczne jako wrażliwa dana w systemie biometrycznym powinna być zabezpieczona mechanizmami kryptograficznymi
- Szyfrowanie transmisji między czytnikiem a systemem - transmisja między czytnikiem a systemem biometrycznym/informatycznym banku powinno być zabezpieczone mechanizmami kryptograficznymi, aby uniemożliwić ataki
- Parowanie urządzenia - urządzenie powinno być sparowane z komputerem bądź z systemem do którego jest podłączone, lub z danym użytkownikiem. Zapobiegnie to nieautoryzowanemu użyciu czytnika (po podłączeniu do niebezpiecznego urządzenia)
- Podpiswanie odpowiedzi czytnika - każda odpowiedź czytnika powinna być podpisywana elektronicznie przez czytnik aby być pewnym na jakim czytniku i przez kogo dana operacja została uwierzytelniona
- Zapobieganie nieautoryzowanej aktualizacji firmware czytnika - czytnik biometryczny powinien blokować możliwość zmiany firmware przez osoby nieuprawnione

4.3. Przykłady procedur bezpieczeństwa w systemach biometrycznych

4.3.1. Biometria w oddziale bankowych

Poniżej przedstawiono przykłady procedur i zasad, które należy wdrożyć wprowadzając uwierzytelnianie biometryczne w oddziałach bankowych.

Rejestracja pracownika:

W procesach biometrycznej technologii uwierzytelniania *Finger Vein* założono iż transakcje w oddziale będą uwierzytelniane zarówno przez klientów jak i doradców, dlatego też wraz z wdrożeniem technologii FV w Banku wymagane będzie:

1. Wszyscy pracownicy oddziałów Banku powinni zostać zarejestrowani w systemie biometrycznym
2. Kontynuacja rejestracji biometrycznej doradców w przypadku przyjmowania nowych pracowników
3. Archiwizacja wzorców *Finger Vein* doradców w celach kontrolnych/audytowych (nawet w przypadku odejścia pracownika). Proces powinien odbywać się z zachowaniem komisyjności (dwóch pracowników banku)
4. Rejestracja wzorców nowych pracowników powinna odbywać się komisjnie w asyście dwóch uprawnionych do tego pracowników banku

Przypisanie czytnika z pracownikiem oddziału/proces logowania do systemu:

1. Codziennie rano pracownik oddziału przed rozpoczęciem operacji weryfikuje swoją tożsamość (porównanie z wzorami wszystkich pracowników danego oddziału). Powoduje to przypisanie danego urządzenia biometrycznego do pracownika oddziału.
2. Podczas logowania doradcy do systemu banku musi nastąpić sprawdzenie czy dla danego identyfikatora istnieją wzorce biometryczne. W przypadku wykrycia przez system iż Pracownik nie jest zarejestrowany, musi nastąpić rejestracja Pracownika.

Rejestracja klienta:

1. Klient rejestruje swoje dane biometryczne (np. w przypadku biometrii naczyń krwionośnych palca min. 2 palce z jednej ręki). Podczas rejestracji klient przedstawia min. 2 dokumenty tożsamości ze zdjęciem (tj. dowód os., prawo jazdy lub paszport). Podobna procedura jest wykorzystana w bezpiecznych środowiskach, jak np. procedura wyrabiania podpisu kwalifikowanego
2. Rejestracja wzorców biometrycznych klienta banku zostaje potwierdzona/uwierzytelniona biometrycznie przez pracownika banku przeprowadzającego rejestrację. Dana rejestracja zostaje przypisana do danego pracownika banku.
3. Opcjonalnie dla podniesienia poziomu bezpieczeństwa: rejestracja może być komisjna, uwierzytelniona przez 2 uprawnionych pracowników banku (np. kasjer i dyrektor oddziału).

Zmiana danych klienta:

Zmiana danych w systemie biometrycznym, w tym przede wszystkim zmiana wzorców biometrycznych klienta jest operacją wrażliwą i niesie za sobą konieczność wdrożenia następujących wymagań/procedur:

1. Komisjonalność potwierdzenia zmiany danych, tj. uwierzytelnienie biometryczne przez dwóch pracowników oddziału (np. kasjer i dyrektor oddziału).
2. System biometryczny powinien wymagać opisu argumentującego zmianę danych. Opis ten powinien być przechowywany na serwerze banku.
3. System biometryczny powinien generować raporty okresowe na temat nowych rejestracji wzorów bądź zmiany danych jako krytycznego elementu systemu zawierające np.: datę i czas operacji, nr ID kasjera, nr czytnika, nr operacji itd. Dane te będą podpisane elektronicznie.

Uwierzytelnianie operacji w oddziale:

1. Klient Banku powinien zostać zweryfikowany biometrycznie przed rozpoczęciem jakichkolwiek operacji w oddziale (identyfikator + biometria). W przypadku braku wzorca w systemie biometrycznym system będzie wymagał rejestracji biometrycznej klienta, a w przypadku braku zgody klienta uruchomienia ścieżki alternatywnej.
2. Każda operacja finansowa (wpłata, wypłata, przelew) lub operacji związana z ryzykiem, powinna zostać potwierdzona biometrycznie przez klienta.
3. Pracownik oddziału będący klientem banku nie może uwierzytelnić transakcji ani innych czynności w kontekście swojego numeru klienta.
4. System biometryczny uniemożliwi przypisanie wzorca palca doradcy pod numer klienta inny niż nr doradcy.
5. Wielokrotna (liczba X - ustalana przez departament bezpieczeństwa banku) błędna weryfikacja poprawności wzorca palca doradcy banku powinna powodować zablokowanie możliwości uwierzytelniania poprzez wzorzec przypisany do danego numeru klienta. Zdjęcie blokady będzie możliwe przez osobę/osoby posiadającą określone uprawnienia.
6. X-krotna błędna weryfikacja wzorca Klienta musi wymuszać wykorzystanie innej danej biometrycznej przypisanej do danego klienta, np. przyłożenie drugiego palca Klienta. Jeżeli X-krotne porównanie tego wzorca kończy się efektem negatywnym to musi to oznaczać, że zachodzi wysokie prawdopodobieństwo, iż jest to próba wyłudzenia środków. Każde zablokowanie operacji doradcy jak i klienta powinno być raportowane przez system biometryczny w trybie dziennym lub w czasie rzeczywistym (event generowany do departamentu bezpieczeństwa).

Rezygnacja klienta zarejestrowanego biometrycznie z korzystania z usługi biometrycznej w oddziale Banku

Rezygnacja klienta z korzystania z usługi biometrycznej

niesie ze sobą konieczność przeprowadzenia następujących czynności:

1. Biometryczne potwierdzenie rezygnacji (komisjonalne - dokonane przez dwóch pracowników oddziału).
2. Biometryczne potwierdzenie rezygnacji przez klienta.
3. Archiwizacja wzorca/wzorców biometrycznych klienta.
4. Wygenerowanie raportu dotyczącego rezygnacji klienta potwierzonego podpisem odrečnym klienta, zgodnym ze wzorem podpisu.

Rezygnacja klienta niezarejestrowanego biometrycznie z korzystania z usługi biometrycznej w oddziale Banku:

Rezygnacja klienta z korzystania z usługi biometrycznej niesie ze sobą konieczność przeprowadzenia następujących czynności:

1. Biometryczne potwierdzenie rezygnacji (komisjonalne - dokonane przez dwóch pracowników oddziału).
2. Wygenerowanie raportu dotyczącego rezygnacji klienta potwierzonego podpisem odrečnym klienta, zgodnym ze wzorem podpisu.

Uwierzytelnianie transakcji metodą inną niż biometria Finger Vein:

W przypadku braku możliwości potwierdzenia transakcji metodą biometryczną wynikającej z przyczyn losowych takich jak: obcięcie palca lub ręki, złamania ręki, choroby itp., lub braku zgody klienta na korzystanie z metody biometrycznej, musi istnieć mechanizm uwierzytelniania bez konieczności korzystania z biometrii, tzw. ścieżka alternatywna autoryzacji. Jednakże proces ten musi spełniać następujące zasady:

1. Zapis dokładnych informacji o transakcji zawierający m.in.: datę, godzinę, kod transakcji, nr pracownika/pracowników, nr klienta oraz podanie powodu braku możliwości wykorzystania uwierzytelniania biometrycznego. Transakcja uwierzytelniana metodą inną niż biometria musi zostać zarejestrowana w kontekście danego klienta, doradcy i oddziału.
2. Raportowanie o przeprowadzeniu transakcji w systemie bez użycia biometrii w trybie dziennym lub w czasie rzeczywistym (rekommendowane).
3. Opcjonalnie: Komisjonalność przeprowadzenia takiej transakcji przez dwóch pracowników Oddziału

Powyższe rekommendacje wynikają z doświadczeń przy wdrożeniach biometrii w oddziale. Kompleksowe wytyczne dotyczące procedur bezpieczeństwa i procesów biznesowych można znaleźć w normie ISO 19092.

4.3.2. Biometria w Contact Center

Norma ISO 19092 jest dobrym drogowskazem do budowania procedur bezpieczeństwa również dla biometrii głosowej. Norma ta uwzględnia tę biometrię w zastosowaniach bankowych i doskonale nadaje się do stosowania nie tylko w sektorze bankowym.

Projektując system biometrii głosowej należy pamiętać o:

- Wyborze odpowiednio silnego hasła głosowego w przypadku stosowania metody zależnej od treści. Hasło powinno być jednocześnie łatwe do zapamiętania. Może być to np. wybrane w ramach konkursu dla klientów hasło reklamowe – wspólne hasło dla wszystkich klientów i/lub numer telefonu komórkowego lub data urodzenia – będą to jednocześnie hasła inne dla każdego klienta.
- Projektując strategię weryfikacji, należy uwzględnić czas niezbędny do rejestracji. Mimo, że posiadanie szeregu różnych wzorców głosu i fraz kodujących dla każdego klienta może być korzystne w sensie bezpieczeństwa, to istotnym jest, aby nie wymagało to wydłużenia czasu rejestracji, bo prowadzi to do wysokiej liczby odrzuceń i niskiej akceptacji przez klientów.
- Warto system wypróbować na mniejszej liczbie klientów – w ten sposób klienci i zespół danej instytucji nabiera doświadczenia, w jaki sposób stosować biometrię głosową. Dobrym przykładem jest nabieranie doświadczenia poprzez wykorzystanie biometrii głosowej do procesu resetu hasła.
- Tworzenie ścieżek awaryjnych w przypadku kilku-krotnego odrzucenia próbki głosowej. Scenariusze te będą bardzo przydatne w celu utrzymania wysokiej jakości obsługi klienta. Należy tworzyć je z dbałością o bezpieczeństwo i wygodę nawigacji po menu. Pozytywne doświadczenie klienta gra tu kluczową rolę, ale nie możemy zapominać o bezpieczeństwie. W przypadku gdy uwierzytelnieni głosem nie jest możliwe, zawsze możemy zastosować metody obecnie stosowane – uwierzytelnieni bezpośrednio u konsultanta. Każdy taki przypadek powinien być zbadany indywidualnie.

5. Norma ISO 19092

W 2008 roku ISO opublikowało standard dedykowany dla sektora finansowego. W istocie było to już drugie wydanie tej normy uwzględniające znacznie więcej zagadnień biometrii. Pierwsza wersja normy 19092 została opublikowana już w 2006r. Głównym celem tej normy jest zwiększenia bezpieczeństwa transakcji finansowych i ustanowienie ogólnych norm i zasad wdrożeń systemów biometrycznych w instytucjach finansowych.

Jedną z najważniejszych cech tej normy jest usystematyzowanie terminologii używanej w biometrii. Tłumaczenie terminów z jednego języka na drugi zawsze pozostawia pole do swobodnej interpretacji tłumaczy. W normie tej znajdziemy klarowne zestawienie terminologii i tłumaczenia z języka angielskiego na język polski takich choćby skrótów jak: FAR, FRR, ERR itp.

Norma podkreśla, iż biometria dojrzała już na tyle, że wiarygodność systemów biometrycznych oraz ich koszt są na takim poziomie, że z powodzeniem mogą być wykorzystywane w branży finansowej.

W Normie opisano środki i procedury umożliwiające zastosowanie biometrii jako mechanizmu uwierzytelniania na potrzeby bezpiecznego, zdalnego dostępu lub lokalnego dostępu fizycznego.

Wyszczególniono następujące techniki biometryczne:

- Biometria odcisku palca
- Biometria głosu
- Biometria tęczówki
- Biometria siatkówki
- Biometria twarzy
- Biometria geometrii dłoni
- Biometria podpisu
- Biometria żyły

Bardzo ciekawą i zarazem praktyczną wskazówką jest punkt 7.5 Oceny osiągów – zawarte w tym punkcie wskazówki na co zwrócić uwagę podczas testowania danego systemu biometrycznego są niezwykle cenne podczas wykonywania testów każdego systemu biometrycznego.

W punkcie 8 opisano podstawowe idee architektury systemów biometrycznych, szczegółowo opisując z jakich podsystemów składa się system biometryczny.

Norma kładzie duży nacisk na zbieranie wzorców biometrycznych - najważniejszym procesie w całym systemie biometrycznym. Opisuje jakie zabezpieczenia należy stosować podczas pobierania pierwszego wzorca biometrycznego - tu należy zwrócić szczególną uwagę na proces weryfikacji nie tylko osoby rejestrowanej ale i rejestrującej. Bezpieczeństwo systemów biometrycznych jest zagadnieniem niezwykle istotnym w branży

finansowej, stąd cały rozdział 10 Normy poświęcony jest właśnie Infrastrukturze bezpieczeństwa.

Ponadto Norma opisuje takie zagadnienia jak:

- Przeglądy okresowe i audyty
- Polityka bezpieczeństwa
- Bezpieczeństwo personelu
- Zarządzanie operacyjne
- Zarządzanie dostępem do systemu biometrycznego
- Dziennik zdarzeń
- Cykl życia informacji biometrycznej (cykl życia wzorca)

Norma ISO 19092: 2008 zawiera w skrócie:

- Podstawy bezpieczeństwa dotyczące stosowania biometrii w celu uwierzytelniania osób korzystających z usług finansowych
- Przedstawia definicje 57 terminów związanych z biometrią
- Wskazuje i opisuje różne rodzaje technologii biometrycznych w tym kwestie związane z ich stosowaniem, wady, zalety
- Opisuje ogólną architekturę systemów
- Określa minimalne wymagania niezbędne do skutecznego zarządzania systemem biometrycznym
- Przedstawia cele kontroli i zalecenia przydatne dla specjalistów
- Określa obowiązkowe zabezpieczenia

„ Biometria dojrzała już na tyle, że wiarygodność systemów biometrycznych oraz ich koszt są na takim poziomie, że z powodzeniem mogą być wykorzystywane w branży finansowej

Pełny tekst normy dostępny jest do nabycia na stronie: www.iso.org. W maju 2010r Polski Komitet Normalizacyjny opublikował polską wersję normy ISO 19092:2008 o symbolu PN-ISO 19092:2010 Usługi finansowe -- Biometria -- Podstawy bezpieczeństwa. Pełny tekst normy dostępny jest do nabycia na stronie <http://sklep.pkn.pl/pn-iso-19092-2010p.html>. Jest to tłumaczenie na język polski normy ISO 19092:2008. W opisie normy znajdziemy podstawowe opisy obejmujące:

- Wykorzystanie biometrii do uwierzytelniania pracowników i klientów korzystających z usług finansowych poprzez weryfikację lub identyfikację tożsamości
- Walidacja danych przedstawionych podczas rejestracji
- Zarządzanie informacją biometryczną w całym cyklu jej życia
- Bezpieczeństwo informacji biometrycznej w całym jej cyklu życia
- Zastosowanie biometrii do logicznej i fizycznej kontroli dostępu
- Nadzór w celu ochrony instytucji finansowych
- Bezpieczeństwo fizyczne sprzętu wykorzystywanego w systemie biometrycznym

Norma ISO 19092 mimo, iż jest dedykowana dla sektora finansowego, może być dobrym wyznacznikiem wdrożeń biometrycznych w każdym sektorze gospodarki.

6. Zastosowania biometrii

Wraz z wkraczaniem komputeryzacji do coraz to nowych obszarów życia, wzrasta poziom ryzyka wykorzystania stosowanych technologii do prowadzenia działań o charakterze przestępczym. Firmy sektora finansowego są bez wątpienia „liderem”, który ciągle musi odpierać różnego rodzaju dedykowane, coraz bardziej innowacyjne ataki mające na celu pozyskanie w sposób nielegalny jak najbardziej realnych pieniędzy.

Rozpoznawanie osób, ich identyfikacja i weryfikacja na podstawie charakterystycznych dla każdego człowieka cech biometrycznych, cieszy się coraz większym zainteresowaniem. W ostatnim czasie bardzo aktualnymi problemami stały się wycieki danych z systemów informatycznych wielu firm i korporacji, ataki na strony internetowe, kradzieże pieniędzy z kont bankowych, jak również kopiowanie kart na urządzeniach bankomatowych. Wielu naukowców pracuje nad stworzeniem technik zapewniających szeroko rozumiane bezpieczeństwo dostępu do różnego rodzaju zasobów infrastruktur IT w połączeniu z wygodą i prostotą ich użytkowania. Dotychczasowe doświadczenia wykazały, iż systemy wykorzystujące techniki biometryczne doskonale nadają się do tego celu. Czy biometria i wykorzystanie technik biometrycznych w procesach bankowych jest właściwą odpowiedzią na pytanie, w jaki sposób możemy chronić klientów banków i zapewnić im maksymalne bezpieczeństwo korzystania z oferowanych przez naszą instytucję produktów i usług? Patrząc na wdrożenia biometrii w bankach, odpowiedź na to pytanie jest twierdząca.

W pierwszej połowie lat 60-tych XX wieku, niezależnie od siebie, Luther G. Simjiana oraz John Shepherd-Baron opracowali prototypy urządzeń dokonujących całkowicie zautomatyzowanych wypłat pieniędzy. Pierwsze maszyny tego typu przyjmowały papierowe karty, kupowane uprzednio w banku, które po przeprowadzeniu transakcji zatrzymywane były w jego wnętrzu. Idea działania bankomatów nie zmieniła się. Wykorzystano osiągnięcia z wielu dziedzin, które w znacznym stopniu uprościły proces autoryzacji transakcji, jednocześnie zwiększając stopień bezpieczeństwa, eliminując możliwości nadużyć. W odróżnieniu od prototypu stosowane karty papierowe zostały w nowych urządzeniach(bankomatach) zastąpione plastиковymi. Oprócz numeru karty, daty ważności i danych jej posiadacza, na ich odwrocie pojawił się pasek magnetyczny. Standardem jest również mikroprocesor na awersie karty. Do realizacji transakcji konieczne jest dwuelementowe uwierzytelnienie, poprzez włożenie karty do bankomatu (coś, co klient posiada) oraz podanie znanego tylko posiadaczowi karty kodu identyfikacyjnego (coś, co klient zna). Po poprawnej weryfikacji następuje realizacja transakcji. Opisany schemat transakcji, stosowany powszechnie we wszystkich krajach, na wszystkich kontynentach,

choć wygodny dla użytkownika, nie zapewnia skutecznej ochrony przed pozyskaniem danych karty i realizacji nieupoważnionych transakcji przez zorganizowane grupy przestępce specjalizujące się w tzw. skimmingu bankomatowym. Proceder przestępczy polega na zamontowaniu na bankomacie nakładki kopiącej zawartość paska magnetycznego, a także kamery lub specjalnej nakładki na klawiaturze do pozyskania kodu PIN. Dane te umożliwiają wykonanie kopii karty, za pomocą której możliwe jest pobranie gotówki z konta klienta banku za pośrednictwem bankomatów. Innym typem przestępstwa kartowego jest skimming w placówkach handlowych, polegający na wykonaniu kopii karty przez sprzedawcę lub inną osobę, która weszła w jej chwilowe posiadanie. Większość kart oferowanych obecnie na rynku umożliwia, oprócz realizacji transakcji bankomatowych, również dokonywanie płatności internetowych bez fizycznego udziału karty, jedynie poprzez podanie kompletu danych na niej zawartych. Dotyczy to zarówno kart kredytowych, jak i debetowych. Pozyskanie danych karty przez osobę nieupoważnioną może skutkować bardzo nieprzyjemnymi konsekwencjami (finansowymi i prawnymi) dla jej posiadacza oraz dla banku.

Nie tylko skimming bądź pozyskanie danych karty płatniczej do realizacji nieuprawnionych transakcji internetowych są realnymi zagrożeniami dla klientów banków. Z roku na rok wzrasta ilość ataków phishingowych na Klientów bankowości internetowej. Wykorzystując złośliwe oprogramowanie oraz proste metody socjotechniczne, przestępcy bez większego wysiłku są w stanie pozyskać, od nieświadomych zagrożenia osób, dane potrzebne do zalogowania się i realizacji nieupoważnionych płatności z poziomu usług bankowości elektronicznej i mobilnej. Innym, również bardzo niebezpiecznym procederem, jest fałszowanie dokumentacji bankowej, mającej na celu wyłudzanie kredytów. Znane są przypadki, gdy oszust, posługując się skradzionymi dokumentami klienta, otwiera konto w banku a następnie przy użyciu sfałszowanej historii rachunku z innej instytucji finansowej wyłudza kredyt.

Należy tu postawić pytanie: jakie mamy możliwości zapobiegania wyżej przedstawionym scenariuszom przestępczym? Istnieje już szereg urządzeń uniemożliwiających bądź utrudniających pozyskanie danych wrażliwych. Złamanie każdego zabezpieczenia, czy to sprzętowego czy softwarowego, jest tylko kwestią czasu. Postaram się wykazać, iż najskuteczniejszym rozwiązaniem, możliwym obecnie do wdrożenia w tej dziedzinie, jest wykorzystanie technik biometrycznych.

Metody biometryczne możemy przyporządkować do jednej z trzech klas: do klasy metod ogólnie uznanych (inaczej: tradycyjnych, dojrzałych), metod rozwijających się oraz tzw. metod alternatywnych, nad których wykorzystaniem trwają od niedawna prace, mające na celu stwierdzenie czy rozpatrywana cecha biometryczna spełnia założenia tzw. stabilności biometrycznej.

Aby daną cechę biometryczną uznać za stabilną, musi ona spełniać szereg właściwości. Zostały one opisane przez Rogera Clarke'a. Są to między innymi: uniwersalność - każda osoba powinna posiadać daną cechę biometryczną, jednoznaczność - żadne dwie osoby nie powinny posiadać takiej samej cechy biometrycznej, trwałość - niezmienność w czasie, mierzalność - możliwość pomiaru za pomocą (praktycznego) urządzenia pomiarowego, akceptowalność - brak obiekcji użytkowników przed pomiarem danej biometryki. Oczywiście wykorzystanie technik biometrycznych w sektorze finansowym, ze względu na swoją specyfikę, wymaga przeprowadzenia bardzo obszernych badań i testów, które muszą wykazać możliwość zastosowania danej cechy w systemach komercyjnych.

„Wprowadzenie możliwości uwierzytelniania transakcji cechą biometryczną, zdecydowanie ogranicza prawdopodobieństwo realizacji transakcji przestępczych

Joseph Rice jest niewątpliwie jednym z inicjatorów wykorzystania technik biometrycznych w sektorze finansowym. W 1984 roku nieznany sprawca, posługując się skradzionymi dokumentami, dokonał nieuprawnionej operacji na jego koncie bankowym. Spowodowało to rozpoczęcie przez niego prac nad technikami zabezpieczeń bazującymi na analizie cech biometrycznych. Ponad połtorarocznymi badaniami stworzył on prototyp urządzenia do akwizycji próbek biometrycznych wzorca układu naczyń podskórnego palca dłoni. Rozpoznanie wzorca układu naczyń jest nieinwazyjną, miarodajną techniką identyfikacji i weryfikacji osobniczej. W porównaniu do innych cech biometrycznych, pozyskanie próbki układu naczyń palca wiąże się z powszechną akceptacją społeczną. Biometryka ta nie jest wykorzystywana przez organy śledcze (takie jak policja czy prokuratura) i nie posiada pejoratywnego wydawniku, jakim niewątpliwie nacechowane jest wykorzystanie linii papilarnych. Akwizycja wzorca jest szybkim procesem, możliwym do przeprowadzenia bez fizycznego kontaktu dłoni z urządzeniem. Jednym z głównych atutów, w porównaniu do innych cech bio-

metrycznych, przemawiających na rzecz tej techniki jest niewrażliwość na czynniki zewnętrzne. Wzorzec żył i tężnic podskórnych dloni w zakresie światła widzialnego jest u większości osób niewidoczny. Pozyskanie go przez osoby nieupoważnione i wykorzystanie w systemie biometrycznym jest praktycznie niewykonalne bez akceptacji i współdziałania ze strony jego posiadacza. Należy tutaj uściślić, iż jest to cecha anatomiczno-fizjologiczna. Pozyskanie próbki biometrycznej wzorca układu naczyń palca umożliwia różnicę w absorpcji promieniowania światła podczerwonego między krew natlenioną, a innymi tkankami palca. Precyzując, eliminuje to możliwość pobrania wzorca z amputowanego palca lub od osoby zmarłej. Omawiana cecha spełnia wszystkie wymogi opisanej wcześniej stabilności biometrycznej.

Innymi uznanymi i z powodzeniem stosowanymi w sektorze finansowym technikami biometrycznymi są: biometria odcisku palca (przy logowaniu pracowników do stacji roboczych), biometria tęczówki oka (dostęp do obszarów chronionych tj. serwerownie, centra danych) czy biometria głosu (uwierzytelnienie klienta podczas rozmowy telefonicznej z pracownikami Contact Centre). Należy tutaj wspomnieć, iż w Polsce wszystkie dotychczasowe projekty bankowe dotyczące wdrożeń technologii biometrycznych otrzymały pozytywną opinię Generalnego Inspektora Ochrony Danych Osobowych.

Poprzez zastosowanie czytników biometrycznych na urządzeniach bankomatowych, możliwe jest zdecydowane zmniejszenie ilości incydentów skimmingowych. Wprowadzenie możliwości uwierzytelniania transakcji cechą biometryczną, zamiast czterocyfrowym kodem PIN, zdecydowanie ogranicza prawdopodobieństwo realizacji transakcji przestępczych. W odróżnieniu od możliwości pozyskania kodu identyfikacyjnego przez osoby nieupoważnione, nie jest możliwe pozyskanie cechy biometrycznej, jako wymaganego środka uwierzytelniającego do autoryzacji transakcji. Sygnatura biometryczna jest również zabezpieczeniem przed możliwością dokonania tzw. 'family fraud' - czyli posłużeniem się kartą klienta przez osobę znajdującą się w bliskim jego otoczeniu.

Identyfikacja biometryczna jest dodatkowym elementem dowodzącym, iż płatność została autoryzowana przez klienta. Zastosowanie terminali biometrycznych w środkach komunikacji miejskiej, gdzie obecne terminalne (notabene ze względów bezpieczeństwa) zostały pozbawione pin padów do wprowadzania kodu PIN, pozwoliłyby wyeliminować problem realizacji transakcji skradzionymi (jeszcze niezastrzeżonymi) kartami. W przypadku postępowań sądowych bank dysponowałby niezaprzecjalnymi dowodami, że transakcje zostały wykonane przez prawowitego posiadacza karty. To samo dotyczy weryfikacji tożsamości posiadacza usług bankowości elektronicznej.

Przyjrzyjmy się obsłudze klienta w placówkach banku. Obecnie, w większości instytucji finansowych, stosowane procedury weryfikacji tożsamości są nieefektywne. Identyfikacja klientów przez pracowników na podstawie porównania podpisu z kartą wzoru podpisów bądź zgodności zdjęcia w dokumencie tożsamości z obecnym wyglądem jest subiektywna i w dużej mierze nie daje pewności, że faktycznie obsługujemy tę osobę, za którą ona się podaje. Brak wystarczających mechanizmów kontrolnych wiąże się z ryzykiem powstawania fraudów zarówno zewnętrznych, jak i pracowniczych.

Wprowadzenie certyfikacji biometrycznej i stosowanie sygnatur biometrycznych jest środkiem pozwalającym skutecznie zmniejszyć koszty papierowego obiegu i archiwizacji dokumentów. W świetle prawa dopuszczone jest wykorzystanie cyfrowego podpisu dokumentów w wersji elektronicznej, bez konieczności archiwizacji dokumentów w tradycyjnej formie. Zastosowanie omawianych technik wpływa na szybkość i efektywność obsługi klienta, co przekłada się bezpośrednio na jego zadowolenie, a tym samym pozytywny wizerunek banku.

Bezpieczeństwo każdej nowej technologii jest bardzo ważnym aspektem branym pod uwagę przy projektowaniu nowoczesnych systemów informatycznych. Każdy z elementów zaawansowanego systemu musi spełniać określone standardy, gdyż bezpieczeństwo systemu jako całości zależy od bezpieczeństwa najsłabiej zabezpieczonego jego elementu.

Zgodnie z regulacjami wprowadzonymi przez ustawę o ochronie danych osobowych, dane biometryczne muszą być przechowywane w sposób uniemożliwiający ich przetwarzanie w sposób nieautoryzowany. Mając powyższe na uwadze, w obecnych wdrożeniach systemów biometrycznych, możemy spotkać się z trzema architekturami topologicznymi: lokalne repozytoria, centralna baza danych, a także rozwiązania polegające na przechowywaniu oraz dopasowaniu wzorców biometrycznych na kartach inteligentnych (technologia match-on-card).

Ze względu na popularyzację biometrii i biometrycznych systemów uwierzytelniania, coraz częściej poruszany jest temat bezpieczeństwa tego typu systemów. Ochrona baz danych tego typu powinna być więc realizowana w identyczny sposób, jak w przypadku baz zawierających dane osobowe. Najnowszym trendem jest wprowadzanie dodatkowych mechanizmów zabezpieczeń, polegających na implementacji metod nieodwracalnych transformacji znieksztalcających dane biometryczne.

Biometria, jest jednym z najbardziej dynamicznie rozwijających się działów informatyki. Wykorzystanie technik biometrycznych do autoryzacji płatności lub weryfikacji tożsamości wydaje się być obecnie jedynym sposobem, mogącym sprostać bardzo restrykcyjnym wymaganiom stawianym przy konstrukcji nowoczesnych systemów

kontroli dostępu. Biometria nie jest już elementem fikcji w filmach science-fiction, to standard bezpieczeństwa, który wkrótce powinien znaleźć powszechnie zastosowanie, nie tylko w bankowości.

6.1. Bankomaty

Bankowość biometryczna na świecie rozpoczęła się właśnie od zastosowania biometrii w bankomatach. W latach 2004-2005 ruszył największy projekt biometryczny na świecie w Japonii, gdzie do dzisiaj zaimplementowano ponad 80 000 tysięcy bankomatów wyposażonych w biometrię naczyniową (*Finger Vein* lub *Palm Vein*). W 2002 roku BanCafe, jeden z największych banków w Kolumbii, wdrożył 400 bankomatów biometrycznych wykorzystujących odcisk palca. Biometria jest bardzo popularną metodą uwierzytelniania w bankomatach w Brazylii. Banco de Bradesco wdrożył ponad 30 000 bankomatów biometrycznych (*Palm Vein*). Bankomaty biometryczne wdrożono także w Banco de Brasil (*Finger Print*) i CAIXA (*Finger Vein*, *Finger Print*). W Europie pion wiedzie Turcja, w której biometrię w bankomatach wykorzystują dwa największe banki - IS Bankası (*Finger Vein*) czy Ziraat Bankası (*Palm Vein*). Polska była pierwszym krajem w Europie, w którym wdrożono bankomaty biometryczne (*Finger Vein*) - w 2010 roku bankomaty biometryczne wdrożyły Podkarpacki Bank Spółdzielczy. Polska jest też pierwszym krajem, w którym funkcjonuje biometryczny host umożliwiający hosting danych biometrycznych oraz biometryczne transakcje międzybankowe - IT Card S.A. (*Finger Vein*).



Rys.15: Czytnik biometryczny *Finger Vein* zaimplementowany na bankomacie

Źródło: PBS

Zapotrzebowanie na bankomaty biometryczne jest związane z szeregiem problemów i wyzwań, które trapecią sieci bankomatów:

- Rosnąca ilość przestępstw kartowych (w tym skimming);

- Rosnąca frustracja klientów związana z coraz większą ilością kodów PIN i kart;
- Coraz mniejsza opłacalność posiadania sieci bankomatowej i konieczność poszukiwania nowych usług;
- Brak popularności kart lokalnych (nie przyjęły się);
- Brak bezpiecznej alternatywy dla wypłaty kartowej (wypłaty telefonem nie sprawdzają się);
- Brak odpowiedniego narzędzia dla osób nieposiadających, bądź niepotrafiących korzystać z kart płatniczych;

Biometria w bankomacie może mieć następujące zastosowania:

- Dodatkowe zabezpieczenie do tradycyjnej wypłaty EMV (karta + PIN + biometria). Takie zastosowanie miało miejsce w Japonii, gdzie w wyniku przepisów nakazano 3 stopniowe uwierzytelnianie dla transakcji powyżej określonej kwoty (ok. 100 USD). W Europie takie zastosowanie biometrii nie sprawdza się (dąży się do uproszczenia procesu);
- Biometryczna wypłata lokalna, - czyli wypłata bezpośrednia z konta klienta banku, który posiada sieć bankomatów biometrycznych. Wprowadzając biometryczną wypłatę lokalną bank nie ponosi kosztu wypłaty ON-US dla transakcji kartowych. Usługa biometrycznej wypłaty lokalnej może być wprowadzona w różny sposób np.:
 - poprzez wprowadzenie unikalnego identyfikatora (np. PESEL, nr telefonu kom.) + biometria (np. palec, dłoń)
 - poprzez kartę (część nr karty jako identyfikator) + biometria
 - telefon z NFC + biometria
- Biometryczna wypłata świadczeń - biometria sprawdza się bardzo dobrze wśród klientów, którzy nie korzystają z kart. Dlatego też jest idealnym narzędziem do wprowadzenia wypłat świadczeń społecznych (np. zasiłków). Bank nie musi w tym przypadku ponosić kosztu wydania karty lub założenia rachunku. Lista świadczeń jest ładowana do systemu biometrycznego, na podstawie której wypłacana jest kwota zasiłku. Przeważnie wprowadzenie takiej usługi wiąże się również z doposażeniem bankomatu w dyspenser monet. Biometryczna wypłata świadczeń mogłaby być idealnym narzędziem do wypłat rent i emerytur dla osób, które mają problemy z korzystaniem z kart płatniczych (temat jest szerzej opisany w rozdziale 7 niniejszej publikacji);
- Biometryczna wypłata kredytu - część banków konsumenckich, nieposiadających stanowisk kasjerów w swoich oddziałach, bądź działających tylko w internecie mogłyby wykorzystać biometrię do wypłaty kredytu. W tym przypadku bank nie musiałby wydawać drogiej karty płatniczej, która byłaby wyko-

- rzystana tylko jeden raz do wypłaty kredytu;
- Biometryczne wypłaty międzybankowe - biometria jest idealnym narzędziem do stworzenia nowego systemu wypłat międzybankowych w bankomatach. Tworzenie się hostów biometrycznych w kraju, w których biometria staje się popularna umożliwia klientom wypłatę w bankomatach biometrycznych różnych banków. Pozwala to również na uzgodnienie prowizji od wypłaty tylko między bankami bądź firmami posiadającymi sieć bankomatów niezależnych bez narzucania stawek przez organizacje płatnicze.

Wykorzystanie biometrii w bankomatach umożliwia wiele zastosowań w tym przede wszystkim:

- Uwierzytelnianie wypłat lokalnych dla klientów banku bez konieczności wykorzystania karty i kodu PIN;
- Dodatkowe zabezpieczenie do transakcji kartowych, w tym transakcji EMV (karta+PIN+biometria);
- Uwierzytelnianie jednorazowych wypłat świadczeń społecznych takich jak zasiłki, renty i emerytury (temat jest szerzej opisany w rozdziale 7 niniejszej publikacji);
- Uwierzytelnianie usług dodatkowych.

Budując business case dla wdrożenia biometrii w sieci bankomatów należy wziąć pod uwagę następujące korzyści biznesowe:

- Redukcję fraudów na bankomatach
- Ograniczenie kosztów wypłat lokalnych (opłaty za transakcje ON-US)
- Otwarcie banku na klientów niekorzystających z kart płatniczych
- Możliwość zarobku na wypłatach świadczeń (prowizja od wypłaty) przy jednoczesnym odciążeniu oddziałów
- Możliwość ustalenia prowizji za wypłaty międzybankowe

Wśród technologii biometrycznych tylko 3 technologie wiodą prym wśród zastosowań bankomatowych: *Finger Vein* (biometria naczyń krwionośnych palca), *Finger Print* (biometria linii papilarnych) i *Palm Vein* (biometria naczyń krwionośnych dloni). W Polsce absolutnym liderem jest biometria *Finger Vein*, która została wdrożona w kilkunastu bankach spółdzielczych. Istnieje również host biometryczny umożliwiający przełączanie transakcji biometrycznych między bankami. Są tworzone niezależne sieci bankomatów biometrycznych na bazie *Finger Vein*. Kilka mniejszych banków rozpoczęło też testy technologii *Palm Vein*.

Dobierając technologię biometryczną do bankomatów należy zwrócić uwagę na dwie kluczowe cechy:

- Możliwość pracy w warunkach zewnętrznych (temperatura, światło, wilgoć)
- Możliwość implementacji na wszystkich bankomatach bez konieczności ich wymiany (rozmiar czytnika, możliwość integracji z bankomatomami różnych producentów)



Rys.16: Biometryczna transakcja na bankomacie

Źródło: PBS

Większość bankomatów w Polsce może zostać doposażona poprzez montaż dedykowanego czytnika biometrycznego, instalację odpowiedniego oprogramowania oraz drobne modyfikacje aplikacji bankomatowej.

Poniżej opisano przykładową transakcję biometrycznej wypłaty lokalnej w bankomacie bez użycia karty:

- Wybór w menu bankomatu opcji „Wypłata biometryczna”;
- Wprowadzenie na klawiaturze bankomatu identyfikatora (np. PESEL);
- Użytkownik przykładą palec do czytnika FV;
- Użytkownik wybiera kwotę wypłaty;
- Bankomat dokonuje wypłaty.

Jak widać z powyższego opisu biometryczna transakcja bankomatowa jest szybka i łatwa.

6.2. Oddział bankowy

Biometryczny oddział bankowy to zastosowanie biometrii, na którym można zbudować konkretny business case. Obok bankomatów to podstawowe wykorzystanie biometrii w bankowości. Jednakże po raz pierwszy w Europie biometryczny oddział bankowy na dużą skalę został wdrożony w Polsce. W 2012 roku Bank BPH zaimplementował biometrię *Finger Vein* w całej sieci swoich oddziałów własnych. Niedługo potem swoje placówki z uwierzytelnianiem biometrycznym operacji oddziałowych uruchomił Getin Bank, Podkarpacki Bank Spółdzielczy oraz Bank of Kyoto (Japonia). Wcześniej biometryczne oddziały bankowe wdrożyły m.in. Resona Bank w Japonii.

Obecnie oddziały bankowe borykają się z szeregiem problemów. Do kluczowych z nich należą: dłuża i niebezpieczna weryfikacja tożsamości (dowód osobisty, podpis, karta identyfikacyjna), brak odpowiednich zabezpieczeń umożliwiających dokonywanie fraudów wewnętrznych przez pracowników oddziałów, ogólna ilość papierowej dokumentacji (umowy), która generuje znaczące koszty itd. Na powyżej wymienione problemy rozwiążaniem może być zastosowanie odpowiedniej technologii uwierzytelniania biometrycznego.

Poniżej przedstawiono krótką analizę trzech podstawowych metod uwierzytelniania klienta w oddziale bankowym w Polsce:

Dowód osobisty

Dowód osobisty jest podstawowym identyfikatorem klienta, na podstawie którego uwierzytelniane są operacje w oddziale. Niewątpliwym plusem tego dokumentu jest komplet informacji umożliwiających jego weryfikację (PESEL, data ur., imię i nazwisko, adres zameldowania itd.). Większość klientów bankowych posiada go w portfelu podczas wizyty w oddziale, co jest niewątpliwą przewagą. Problem zaczyna się jednak, gdy go zapomnimy...

Brak posiadania przy sobie dowodu praktycznie uniemożliwia klientowi dokonanie jakiejkolwiek operacji w oddziale (od wpłaty do wzięcia kredytu) w większości banków w Polsce. Należy również wziąć pod uwagę, że weryfikacja dowodu osobistego przez pracowników banku jest przeważnie dokonywana pobieżnie (np. weryfikacja zdjęcia), czego następstwem są występujące fraudy (np. pobranie kredytu gotówkowego na dowód innej osoby lub dowód podrobiony).

Dużym problem dla administracji jak i w konsekwencji dla banków był upadek projektu PL.ID. Nowy, elektroniczny, bezpieczny dowód osobisty zawierający podpis elektroniczny miał zunifikować sposób uwierzytelniania w Polsce. Móglby on być również dobrym

narzędziem do uwierzytelniania w oddziałów bankowych. Na ten moment jednak projekt został wstrzymany. Co ciekawe podobne projekty w innych krajach, np. w Turcji również zostały zatrzymane. Co więcej wg. najnowszych wytycznych Unii Europejskiej, nowe dowody osobiste nie będą zawierać wzoru podpisu. Może to stanowić ogromny problem dla większości banków w Polsce, w których dowód osobisty i wzór podpisu stanowiły podstawowe narzędzie do weryfikacji tożsamości klienta.

Podpis odręczny

Podpis odręczny to podstawowa metoda autoryzacji operacji oddziałowych. Bank przechowują własne bazy wzorów podpisu bądź opierają się na wzorze podpisu zapisanym na dowodzie osobistym. Metoda jest nie-wątpliwie najbardziej naturalną metodą autoryzacji (każdy z nas ma swój podpis), jednakże zawiera ogólną ilość wad.



Rys.17: Urządzenie do składania podpisu odręcznego w oddziale Alior Bank

Źródło: Alior Bank (www.alior.pl)

Kontrowersje wzbudza przede wszystkim subiektywny sposób weryfikacji podpisu. Pracownik banku praktycznie nie ma możliwości, aby jednoznacznie stwierdzić czy podpis jest właściwy, a mimo to musi podjąć decyzję (często błędą). Podpis odręczny zmienia się z wiekiem, co może powodować ogromne problemy podczas dokonywania czynności w oddziale. W przypadku, kiedy zapomnimy wzór podpisu złożony w banku, bądź też w międzyczasie zmienimy podpis nie zmieniając go w bazie banku, grozi to uniemożliwieniem dokonania jakichkolwiek operacji. Kolejnym problemem jest fakt, że podpis odręczny jest łatwy do podrobienia, co otwiera pole na dokonanie fraudów.

Niektóre banki w Polsce wprowadziły do swoich oddziałów tablety umożliwiające elektroniczne pobranie wzoru podpisu odręcznego. W przeciwieństwie do wszechobecnych opinii, banki te nie wprowadziły mechanizmów biometrycznej weryfikacji podpisu odręcz-

nego (np. dynamiki podpisu). Na ten moment jest to wyłącznie skan podpisu.

Karta identyfikacyjna

Niektóre banki w Polsce wydają osobną kartę identyfikacyjną do uwierzytelnienia operacji w oddziałach bankowych. W ten sposób Bank wydaje klientowi swoje własne, zaufane narzędzie do uwierzytelniania.

Jednakże takie rozwiązanie staje się coraz bardziej archaiczne i posiada szereg drastycznych wad. Po pierwsze wydawnictwo osobnych kart wiąże się z dużymi kosztami (zakup i wydawnictwo kart, zakup i utrzymanie PIN PAD-ów itd.). Wykorzystanie kart identyfikacyjnych (przeważnie magnetycznych) nie daje jakiegokolwiek bezpieczeństwa. Gdyby była to jedyna metoda uwierzytelniania w oddziale to przestępca będący w posiadaniu karty i PINu mógłby dokonać znaczących fraudów. W niektórych bankach kartę identyfikacyjną stosuje się do identyfikacji, a następnie jest żądane okazanie dowodu osobistego. Nasuwa się zatem pytanie, po co ten kosztowny gadżet? Należy dodać fakt, że karty są unikalne dla danego banku, a więc nie mogą być wykorzystane w innych bankach, jako uniwersalne narzędzie do identyfikacji. Niektóre banki umożliwiają uwierzytelnianie przy pomocy karty debetowej. Niestety nie zmienia to faktu, że nie jesteśmy w stanie być 100% pewni czy osoba korzystająca przy danej operacji oddziałowej z karty jest osobą uprawnioną.

Biometria jest naturalną alternatywą dla w/w tradycyjnych metod uwierzytelniania. Wprowadzoną do oddziału bankowego biometrię można zastosować do:

- Weryfikacji tożsamości klienta w oddziale (np. zamiast dowodu osobistego, karty ID)
- Uwierzytelniania operacji/dyspozycji klienta w oddziale, np. wpłat, wypłat, przelewów itd. (zamiast dowodu i podpisu odręcznego)
- Podpisywania umów na linii klient - bank (np. założenie rachunku) - przy połączeniu biometrii z podpisem elektronicznym
- Biometryczne uwierzytelnianie wszelkich operacji w oddziale przez pracownika banku
- Dzięki powyższym zastosowaniom, bank może uzyskać następujące korzyści:
 - Zwiększenie bezpieczeństwa transakcji, a co za tym idzie redukcja fraudów wewnętrznych (dokonywanych przez pracownika banku) jak i zewnętrznych (np. przez osobę identyfikującą się fałszywym dokumentem tożsamości)
 - Redukcję kosztów związana z utrzymywaniem departamentu audytującego stanowiska kasowe
 - Redukcję kosztów papierowego obiegu dokumentów (koszt papieru, wydruków, archiwizacji itd.) - przy zastosowaniu podpisu biometrycznego

- Szybszą i efektywniejszą obsługę klienta w oddziale
- Zmianę wizerunkową banku - innowacyjny i bezpieczny bank



Rys.18: Czytnik biometryczny w oddziale BPH

Źródło: BPH S.A.

Wśród technologii biometrycznych zastosowanych w oddziałach bankowych największy sukces odniosły biometrie naczyniowe (biometria naczyń krwionośnych palca - *Finger Vein* lub dłoni - *Palm Vein*) oraz biometria podpisu odręcznego. Oczywiście pod względem technologicznym biometria odcisku palca (*Finger Print*) również nadaje się do zastosowania w oddziale, jednakże ze względów prawnych jest ona praktycznie niestosowana. W Polsce absolutnym liderem jest biometria *Finger Vein*, która została m.in. w oddziałach Banku BPH S.A., Getin Bank czy też Podkarpackim Banku Spółdzielczym. Projekt w banku BPH był pierwszym projektem wdrożenia biometrii w oddziałach w Europie. Getin Bank, jako pierwszy bank w Europie wdrożył rozwiązywanie biometrycznego podpisu elektronicznego (w oparciu o biometrię *Finger Vein*). W przyszłym roku kilka czołowych banków w Polsce planuje wdrożenia biometrii w swoich oddziałach. Biometria podpisu odręcznego została wdrożona między innymi w bankach w Czechach (GE Money Bank) czy też w we Włoszech. Jednakże ze względu na bezpieczeństwo nie jest jedną metodą uwierzytelniania.

6.3. Bankowość internetowa

Bankowość internetowa jest na ten moment najmniej zagospodarowanym kanałem sprzedaży, w którym wykorzystuje się biometrię. Na ten moment uwierzytelnianie w kanale internetowym zdominowane jest przez hasła sms-owe, hasła zdrapki czy też tokeny kryptograficzne. Dla klientów korporacyjnych popularną metodą są karty intelligentne z PKI. Na niską popularność biometrii w bankowości internetowej nie ma wpływu jej użyteczność, a wciąż wysoka cena urządzeń, która uniemożliwia jej stosowanie na dużą skalę. Biometria jest jednak idealnym narzędziem do:

- Logowania do platformy internetowej
- Uwierzytelniania operacji na platformie internetowej
- Resetowania haseł dostępowych

W bankowości internetowej idealnym jest połączenie biometrii w systemem PKI. Dzięki temu biometria umożliwiałaby również składanie oświadczeń woli (w tym podpisywanie umów) w kanale internetowym.

Najbardziej naturalnym wyborem w tym kanale dostępu wydaje się być biometria odcisku palca. Czytniki linii papilarnych są wbudowywane w laptopy, co zwiększa popularność tego typu biometrii. Niestety zastosowane w nich czytniki są bardzo słabej jakości i są bardziej gadżetem niż narzędziem do uwierzytelniania, dlatego żaden bank nie wykorzystał ich do uwierzytelniania. Można znaleźć na rynku czytniki linii papilarnych dobrej jakości, które mogłyby być zastosowane w kanale internetowym. Na ten moment czytniki linii papilarnych są najtańszą propozycją. Na rynek wprowadzane są również nieco droższe czytniki naczyń krwionośnych palca lub dłoni, które zapewniają dużo większe bezpieczeństwo i prywatność.

W bankowości internetowej możemy również wykorzystać biometrię głosową np. do potwierdzania transakcji przez telefon swoim głosem jako alternatywę do SMSów. Częstym problemem w bankowości internetowej jest też zapominanie haseł dostępu. Użytkownik musi się wtedy skontaktować z bankiem w celu resetowania hasła. W tym celu najczęściej dzwoni na infolinię, łączy się z konsultantem i po uwierzytelnieniu otrzymuje tymczasowe hasło. Proces ten można automatyzować poprzez użycie biometrii głosowej i sprawić, aby cały proces resetu hasła dla bankowości internetowej był w pełni automatyczny. Bank może ułatwić w ten sposób resetowanie hasła i jednocześnie zwiększyć bezpieczeństwo.



Rys.19: Karta biometryczna dla klientów biznesowych w PEAKO S.A.

Źródło: PEAKO S.A.

Pierwszym bankiem w Europie, który zastosował biometrię w bankowości internetowej był Bank PEKAO S.A. w Polsce. Bank wprowadził w 2010 roku do oferty rozwiązania biometryczne dla klientów korporacyjnych. Użytkownicy internetowej platformy transakcyjnej PekaoBIZNES24 mogą na podstawie odcisków palców logować się do systemu i autoryzować zlecenia. Dotychczas wydano ok. 3000 specjalnych kart mikroprocesorowych „Pekao BIOeSignature”, które służą do przechowywania podpisu elektronicznego wraz z odciskiem biometrycznym linii papilarnych palca. Taki sposób identyfikacji klientów daje gwarancję, że do systemu ma dostęp właściwy użytkownik, a nie inną osobą, która weszła w nieuprawniony sposób w posiadanie jego kodu PIN lub karty.

Na 2014 rok przewidywane jest największe wdrożenie biometrii w kanale internetowym. Jeden z największych banków w Wielkiej Brytanii planuje wdrożyć ponad 20 000 czytników opartych na biometrii naczyń krwionośnych palca (*Finger Vein*) i PKI (karty SIM).

6.4. Kanał zdalny (Infolinia, IVR, Help desk, bankowość mobilna)

Najbardziej rozpowszechnioną biometryczną metodą uwierzytelnienia w kanale zdalnym jest dziś biometria głosowa. Korzysta z niej ponad 30 milionów osób na całym świecie.

Bieżące zabezpieczenia w postaci PIN-ów, haseł i udzielania odpowiedzi zawierających osobiste informacje nie gwarantują bezpieczeństwa – można je łatwo utracić lub zapomnieć, a ponadto należy je często zmieniać. Praktyka pokazuje, że klienci bardzo rzadko zmieniają raz ustawione hasło, o ile nie jest wymuszana systemowa zmiana hasła. Biometria głosowa stanowi stosunkowo łatwe i opłacalne rozwiązanie tych problemów w kanale zdalnym.



Rys.20: Zastosowania biometrii głosowej

Źródło: Algotech

Biometria głosowa używana jest najczęściej przez centra obsługi klienta (Call Center/Infolinie) podczas rozmów telefonicznych, kiedy rozmówcy chcą uzyskać

dostęp do chronionych danych lub usług i transakcji. Biometria głosowa stosowana jest zazwyczaj celem uwierzytelnienia osoby przed uzyskaniem dostępu do usług chronionych, takich jak np. konto bankowe lub do uwierzytelniania transakcji lub czynności takich jak np. wykonanie przelewu lub zmiana hasła.

Biometria głosowa stosowana jest w bankach w następujących obszarach:

- Weryfikacja w systemach IVR - zastąpienie klasycznej metody identyfikatora i telepinu hasłem głosowym - Systemy konwersacyjne
- Weryfikacja transakcji wysokiego ryzyka - uwierzytelnienie osoby podczas zwykłej rozmowy z konsultantem w Contact Center - Systemy niezależne od treści i stale monitorujące obecność danej osoby od początku do końca rozmowy
- Weryfikacja osoby w kanale mobilnym - Systemy konwersacyjne lub Systemy zależne od treści
- Reset hasła dostępowego

Biometria głosowa ze względu na swoją naturę, jest biometrią, która rozwija się najszybciej ze wszystkich biometrii na świecie pod względem dynamiki przyrostu ilości użytkowników.

Na dzień publikacji niniejszego raportu największy system biometrii głosowej pracuje w Turcji w firmie Global Bilgi obsługując ponad 10 milionów klientów największego tureckiego operatora telefonii komórkowej Turkcell.

Bankowość mobilna:

Smartfony dostępne już od kilku lat na rynku zyskały szerokie grono wielbicieli. Smartfony i tablety zostały dostrzeżone również przez banki i urządzenia te są dziś synonimem nowoczesnej bankowości - bankowości mobilnej - to dla tych urządzeń napisano dziesiątki dedykowanych aplikacji za pomocą których „bankujemy” na co dzień. Wciąż nierozwiązanym problemem

jest intuicyjny i jednocześnie bezpieczny sposób uwierzytelnienia użytkownika mobilnego. W zdecydowanej większości, metody uwierzytelnienia w aplikacjach mo-

bilnych nie różnią się zupełnie od sposobu uwierzytelnienia na stronie www, czyli za pomocą loginu i hasła.

Smartfony poprzez wbudowane mikrofony czynią je urządzeniami, które w łatwy sposób możemy zamienić na czytnik biometryczny rejestrujący głos w celu uwierzytelnienia. Warto dodać, że jeśli dana instytucja stosuje uwierzytelnienie głosowe w IVR (biometria głosowa zależna od treści), wówczas możemy tę samą metodę uwierzytelnienia zastosować w aplikacji mobilnej na smartfon lub tablet z wbudowanym mikrofonem.

Uczyni to urządzenia mobilne przyjaźniejsze dla użytkownika jak również zyskamy na poziomie bezpieczeństwa dostępu do usług w aplikacjach mobilnych.

6.5. Płatności

Płatności to naturalny rozwój bankowości biometrycznej. Banki wdrażając biometrię w bankomatach bądź w oddziałach zbierają znaczącą bazę „klientów biometrycznych”, która mogłyby stanowić podstawę dla nowego, niezależnego schematu płatności.

Obecnie rynek płatności regulowany jest przez organizacje płatnicze (np. VISA, Master Card), w którym podstawowym narzędziem płatniczym jest karta, uwierzytelniana kodem PIN. Posługiwanie się kartą z paskiem magnetycznym i kodem PIN było jednak mało bezpieczne i wygodne. Bezpieczeństwo podniesiono poprzez wprowadzenie płatności EMV. Problem z wygodą pozostał szczególnie dla drobnych płatności. W ostatnich latach rynek poszukiwał narzędzi do wygodnych mikropłatności. Testowano wiele technologii, jednakże zwycięstwo odniósły ponownie organizacje płatnicze wprowadzając szybkie płatności bezstykowe. Banki dalej poszukują alternatyw wprowadzając np. szereg różnych płatności mobilnych. Mimo że komórka jest narzędziem powszechnym to do głównych problemów płatności mobilnych zaliczyć można: brak standaryzacji, powolność oraz niskie bezpieczeństwo. Wymienione wady wskazują, że należy szukać dalej alternatywy lub uzupełnienia dla płatności kartowych.

Jednym z ciekawych wyborów są płatności biometryczne. Biometria gwarantuje najwyższy poziom bezpieczeństwa, co umożliwia realizację płatności bez limitu kwot (jak w przypadku płatności zbliżeniowych). Jednakże biometria w bankowości jest technologią uwierzytelniania, a nie identyfikacji (szczególnie przy tak dużych populacjach). Należy więc się zastanowić, jaki powinien być sposób identyfikacji klienta w płatnościach biometrycznych aby transakcja była szybka i wygodna. Poniżej przedstawiono przykłady możliwych identyfikatorów w płatnościach biometrycznych:

- Karta płatnicza + biometria (zamiast PIN)
- Karta zbliżeniowa + biometria (bez ograniczeń kwoty)

- Identyfikator (np. numer telefonu) + biometria
- Telefon z NFC + biometria
- Karta plastikowa z kodem paskowym + biometria
- Karta plastikowa z wzorcem biometrycznym w QR code + biometria
- Karta bezstykowa dalekiego zasięgu (WPAN) + biometria

W ostatnich latach szereg Banków w Europie rozpoczęła projekty pilotażowe płatności biometrycznych. W 2011 roku ruszył pilotaż w Banku IS Bankasi A.S. w Turcji, który wcześniej uruchomił sieć bankomatów biometrycznych. Zintegrowano tradycyjny terminal POS z czytnikiem



Rys.21: Rozwiązywanie biometrycznych płatności w Auchan
 Źródło: <http://secureidnews.com>

biometrycznym *Finger Vein*. Klient miał możliwość zapłaty w tradycyjny sposób bądź przy pomocy karty (jako identyfikator) i biometrii. Pierwsze biometryczne terminale płatnicze zainstalowano m.in. w sieci kin należących do Banku. W 2012 roku Banque Accord we Francji uruchomił pilotaż w sieci supermarketów Auchan. W rozwiązyaniu wykorzystano kartę MasterCard dalekiego zasięgu (WPAN) oraz dwie technologie biometryczne do wyboru: biometrię odcisku palca (*Finger Print*) i biometrię naczyń krwionośnych palca (*Finger Vein*). Dzięki takiemu połączeniu klient nie musiał wyciągać karty płatniczej z kieszeni, a za wszelkie zakupy płacił palcem. W grudniu 2012 roku UniCredit przedstawił terminal Papilon (POS) z możliwością identyfikacji przy pomocy biometrii naczyń krwionośnych dłoni (*Palm Vein*). Urządzenie zostało opracowane przez departament R&D banku. Zaimplementowano urządzenie testowo z jednym z merchantów.

6.6. Fizyczna i logiczna kontrola dostępu

Fizyczna kontrola dostępu to najstarsze zastosowanie biometrii na świecie. Celem systemu kontroli dostępu jest dopuszczenie uprawnionych osób do określonych

miejsc. Najbardziej popularnym rozwiązaniem jest wykorzystanie bezstykowych kart dostępowych (RFID) lub ewentualne kodów PIN. Jednakże system kontroli dostępu oparty na kartach RFID bardziej kontroluje dostęp kart niż samych użytkowników. Systemy używające numerów PIN pozwalają na wejście każdemu, kto zna dany numer, niezależnie od tego, czy jest to osoba uprawniona, czy też nie. Wykorzystanie biometrii w kontroli dostępu daje gwarancję wejścia na dany obszar tylko osobom uprawnionym. Jest to szczególnie ważne w bankach gdzie znajduje się szereg stref krytycznych takich jak:

- Skarbiec
- Centrum przetwarzania danych (Data Center)
- Centrum kart

W dużych organizacjach czytniki biometryczne mogą zlikwidować użycie kart. Mimo że czytniki biometryczne są droższe niż czytniki kart, to w perspektywie całkowitych kosztów, biometria bardziej się opłaca i daje oszczędności finansowe i administracyjne. Nie trzeba, bowiem wydawać karty dla każdego pracownika i nimi zarządzać. Zgubienie lub zniszczenie karty powoduje, bowiem konieczność wystawienia nowej.

Istnieją dwa rodzaje systemów biometrycznych do kontroli dostępu:

- Systemy standalone

W takim przypadku czytnik biometryczny funkcjonuje również jako pełny kontroler dla pojedynczych drzwi. Wzorce biometryczne rejestrowane i zapisywane są na czytniku. Podczas weryfikacji, urządzenie porównuje daną biometryczną z wzorcem przechowywanym w pamięci, i na tej podstawie decyduje o otwarciu lub nie otwarciu drzwi. Liczba użytkowników jest ograniczona przez pamięć urządzenia i różni się w zależności od producenta.

- Systemy sieciowe

W systemach sieciowych czytniki biometryczne są połączone z systemem centralnym poprzez sieć Ethernet. Główną zaletą takiego systemu jest możliwość centralnego zarządzania i monitorowania systemu oraz nadawania uprawnień i dystrybucji wzorców biometrycznych.

Istnieje wiele przypadków, kiedy biometryczne czytniki kontroli dostępu muszą zostać zintegrowane z istniejącą infrastrukturą kartową. Najczęściej stosowana jest metoda „emulacji czytnika kart”. W tym przypadku urządzenie biometryczne współpracuje z systemem w taki sposób jak czytnik kart.

Zależnie od potrzeb oraz zdefiniowanego poziomu bezpieczeństwa wzorce biometryczne służące do autoryzacji użytkowników w systemie KD mogą być przechowywane:

- na karcie bezstykowej (np. Mifare),
- na centralnym serwerze,
- bezpośrednio na czytniku biometrycznym.



Rys.22: Rozwiązanie biometrycznej kontroli dostępu

Źródło: <http://www.ego.uk.net>

Na rynku istnieje ogromna liczba urządzeń do kontroli dostępu opartych o technologie biometryczne. Najbardziej popularne są urządzenia oparte na biometrii odcisku palca oraz biometrii tęczówki oka. Wcześniej wykorzystywano inne technologie biometryczne takie jak biometria kształtu dłoni bądź kształtu twarzy. W ostatnich latach pojawiły się na rynku czytniki oparte o biometrię naczyń krwionośnych palca i dłoni, sprawdzone w rozwiązaniach bankowych. We Francji po akredytacji CNIL (odpowiednik polskiego GODO) umożliwiającej przechowywanie danych biometrycznych na serwerze, wdrożono kilkadziesiąt tysięcy czytników biometrycznych opartych o biometrię naczyń krwionośnych palca. W Polsce wiele banków stosuje biometryczną kontrolę dostępu do stref krytycznych. Np. Eurobank S.A. stosował biometrię tęczówki oka do kontroli dostępu na początku swojej działalności w Polsce.

6.7. Skrytki depozytowe

Tradycyjne skrytki depozytowe, umieszczone zwykle w pomieszczeniach skarbcowych zabezpieczone są zamkiem, którego otwarcie wymaga użycia dwóch kluczy. Jeden klucz, tzw. Master znajduje się w posiadaniu banku, drugi posiada klient. Tak skonstruowany zamek jest bezpieczny, gdy gospodarka kluczami jest zorganizowana prawidłowo. Oznacza to, że klucz Master musi być odpowiednio zabezpieczony i nie może ulec „skopiowaniu”. Klient także powinien odpowiednio zabezpieczyć swój klucz i w żadnym wypadku nie powinien wykonywać jego kopii, gdyż może się dostać w niepowołane ręce.

Rozwiążanie tradycyjne z wykorzystaniem zamka na dwa klucze wymusza wdrożenie odpowiednich procedur w banku. Do każdorazowego otwarcia skrytki, niezbędną jest asysta pracownika banku, który w pierwszej kolejności otworzy częściowo zamek swoim kluczem, a następnie umożliwi całkowite otwarcie klientowi przy pomocy jego klucza. Stwarza to znaczny problem, gdyż pracownik banku musi być do dyspozycji klientów praktycznie cały dzień w godzinach otwarcia placówki bankowej. Podczas każdej wizyty klienta, zobowiązany jest do potwierdzenia tożsamości klienta (przy pomocy dowodu osobistego) i odnotowania tego faktu w odpowiednim dokumencie. W niektórych bankach klient musi czekać aż pracownik oddziału będzie dostępny, aby mógł udać się z nim do pomieszczenia ze skrytkami depozytowymi. Żaden system niestety nie kontroluje tego, czy pracownik odpowiednio dokumentuje pobyt klienta w skarbcu ze skrytkami, ani tego czy klucze nie są kopiowane.

Podsumowując tradycyjne rozwiązanie skrytek depozytowych posiada następujące wady:

- niskie bezpieczeństwo
- wysokie koszty utrzymania
- czasochłonność obsługi
- brak dostępności poza godzinami pracy oddziału

Rozwiązaniem powyższych problemów może być właśnie biometria. Podstawowym rozwiązaniem jest biometryczna kontrola dostępu na wejściu do skarbcu ze skrytkami. Dzięki temu bank może zwiększyć bezpieczeństwo, dostępność usługi i czas obsługi (nie trzeba, bowiem weryfikować dokumentu tożsamości). Idealnym rozwiązaniem jest jednak rozwiązanie kompleksowe, oparte na elektronicznych zamkach z wykorzystaniem biometrycznej kontroli dostępu oraz systemie informatycznym nadzorującym skrytki, zapewniającym stabilność i najwyższy poziom bezpieczeństwa przechowywanych wartości. Rozwiązanie to pozwala na zmianę dotychczasowych procedur, zwiększenie bezpieczeństwa i wprowadzenie pełnego, automatycznego nadzoru nad działaniem skrytek.

Poniżej przedstawiono koncepcję działania biometrycznych skrytek depozytowych opartych o biometrię palca (biometria naczyń krwionośnych palca - *Finger Vein* lub linii papilarnych - *Finger Print*):

- 1.) Klient podpisuje umowę z bankiem na korzystanie ze skrytki depozytowej w oddziale Banku. Podczas podpisywania umowy:
 - otrzymuje numer skrytki
 - otrzymuje klucz mechaniczny
 - przykłada swój palec do czytnika w celu rejestracji danych biometrycznych. Po prawidłowej rejestracji biometrycznej, jego dane przesypane są na serwer banku

Rejestracja danych biometrycznych może odbyć się w dowolnym okienku obsługi klienta banku wyposażonym w czytniki biometryczny i przeglądarkę internetową (webowa konsola rejestracyjna).

2.) Klient udaje się do skarbcu w celu skorzystania ze swojej skrytki. Nie musi asystować mu pracownik banku. W celu otwarcia drzwi do skarbcu oraz skrytki, w pomieszczeniu przedskarbcowym musi otworzyć skrytkę elektronicznie. W tym celu na terminalu biometrycznym wpisuje swój numer skrytki i przykłada palec do czytnika w celu dokonania weryfikacji. System sprawdza, czy dane biometryczne wykorzystywane do otwarcia, zgadzają się z danymi pobranymi podczas rejestracji klienta. Jeżeli tak, otwierają się drzwi do skarbcu, a na skrytce klienta otwiera się zamek elektroniczny. Po tej operacji klient może udać się do skarbcu.

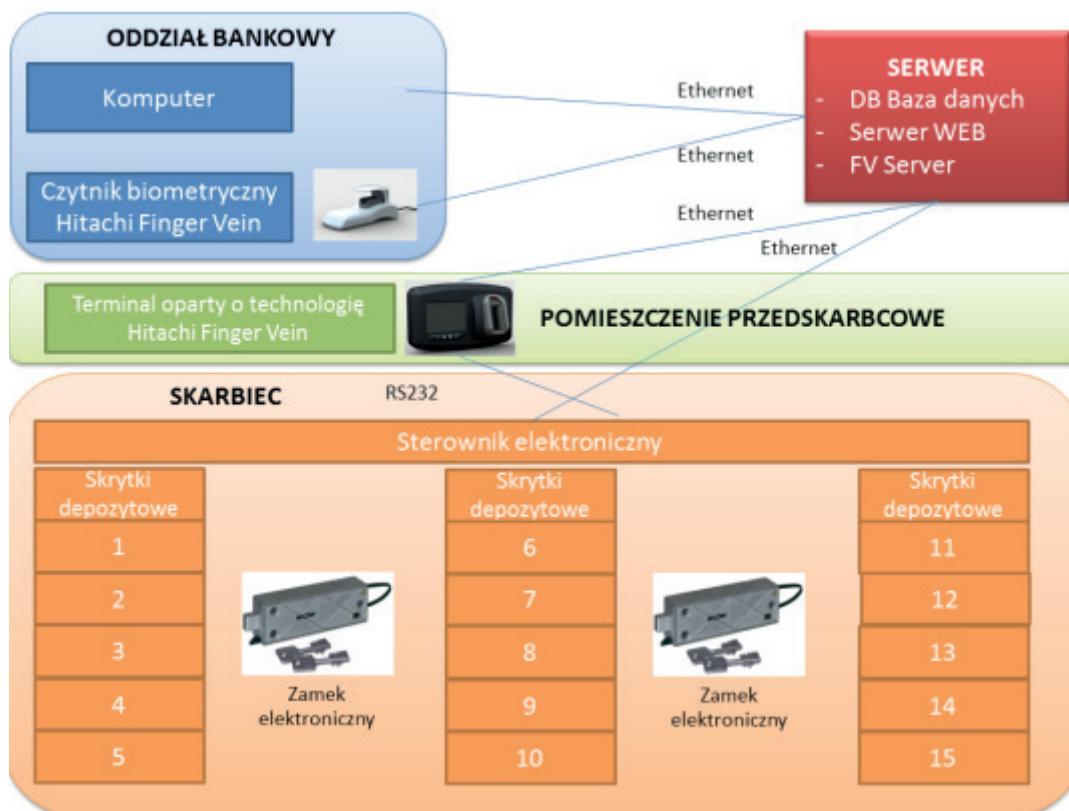
3.) Klient po wejściu do skarbcu przy pomocy klucza może otworzyć swoją skrytkę. Jeżeli przed użyciem klucza, klient nie dokonał prawidłowego uwierzytelniania na terminalu biometrycznym to po pierwsze nie może dostać się do pomieszczenia, jak również użycie klucza mechanicznego nie pozwoli na otwarcie skrytki. Po zakończeniu operacji, klient zamyka skrytkę. Ponowne użycie klucza, bez wcześniejszego uwierzytelniania na terminalu biometrycznym nie będzie możliwe. Opcjonalnie aby jeszcze lepiej uszczelnić proces, przed wyjściem z pomieszczenia klient ponownie powinien uwierzytelnić się biometrycznie.

Powyższy proces pozwala zapewnić najwyższe bezpieczeństwo i automatyzację obsługi skrytek depozytowych, przy jednoczesnej, znaczącej redukcji kosztów.

Poniżej przedstawiono przykładową architekturę rozwiązania opartego o *Finger Vein*:

W/w system bezpiecznych skrytek depozytowych składa się z czterech podstawowych elementów:

- Serwer



Rys.23: Przykładowa architektura systemu bezpiecznych skrytek depozytowych

Źródło: KŁOS NTB

- Przechowuje bazę danych użytkowników, dane biometryczne, historię zdarzeń
- Udostępnia stronę www, dzięki której pracownik banku może zarejestrować dane biometryczne nowego Klienta w placówce banku
- Weryfikuje tożsamość klienta po przyłożeniu palca do czytnika biometrycznego
- Oddział Bankowy
 - Poprzez stronę www zarządza listą klientów korzystających ze skrytek depozytowych oraz ich danymi biometrycznymi wymaganymi do otwarcia skrytki. Pracownik oddziału weryfikuje klienta podczas rejestracji w systemie - w tym celu wykorzystuje czytnik biometryczny

- Pomieszczenie przedskarbowe
 - Terminal biometryczny zainstalowany w pomieszczeniu przedskarbowym służy do weryfikacji tożsamości klienta, który ma zamiar skorzystać ze swojej skrytki depozytowej
- Skarbiec
 - Sterownik elektroniczny, do którego podłączone są wszystkie skrytki depozytowe umożliwia otwieranie zamków w części elektronicznej. Moduł ten także kontroluje czy rygiel zamka jest otwarty oraz czy drzwi skrytki są otwarte. Dzięki temu wykrywa on nieuprawnione otwarcie skrytek (otwarcie siłowe - bez identyfikacji biometrycznej)



Rys.24: Przykładowe rozwiązanie dedykowane dla skrytek depozytowych

Źródło: Hitachi Omron TS

Prawidłowo zaimplementowany system bezpiecznych skrytek depozytowych na bieżąco nadzoruje w tle każdą próbę weryfikacji tożsamości Klienta, uprawnionego i nieuprawnionego otwarcia skrytki, manipulowania itp. Wszelkie zdarzenia powinny być rejestrowane na serwerze i mogą posłużyć do generowania wszelkich raportów. Wystąpienie zagrożenia lub niebezpiecznego zdarzenia, powinien automatycznie wywoływać alarm.

W systemach bezpiecznych skrytek depozytowych stosowane są przede wszystkim: biometria naczyń krwionośnych palca (*Finger Vein*) lub biometria odcisku palca (*Finger Vein*). W systemach tych można stosować też technologie biometryczne typowe dla kontroli dostępu, takie jak biometria tęczówki oka. Pionierem w wykorzystaniu biometrycznych skrytek depozytowych jest Japonia, gdzie wykorzystanie ich staje się powszechnie. Jednym z czołowych banków wykorzystujących biometryczne skrytki depozytowe jest Resona Bank.

6.8. Podpis biometryczny

Podpis elektroniczny, szczególnie ten weryfikowany certyfikatem kwalifikowanym⁵ rozwiązuje wiele problemów w kontaktach B2B i B2G i pozwala na optymalizację kosztową i procesową obiegu informacji.

⁵ Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2001 r. Nr 130, poz. 1450 ze zm.)

Dostępne na rynku rozwiązania bazujące na kartach mikroprocesorowych nie są jednak powszechnie w segmencie klienta masowego. Prawdopodobnie wynika to z faktu, że stosowanie takiego podpisu elektronicznego wymaga posiadania umiejętności technicznych, wiedzy na temat samej technologii, a także poniesienia dodatkowego kosztu związanego z uzyskaniem certyfikatu kwalifikowanego.

W celu ominięcia wyżej opisanych niedogodności związanych z podpisem elektronicznym bazującym na kartach mikroprocesorowych, optymalne byłoby wprowadzenie podpisu serwerowego z silnym uwierzytelnianiem użytkowników. System taki, po poprawnym uwierzytelnieniu użytkownika, umożliwia uwolnienie przechowywanego w bezpiecznym środowisku serwerowym klucza prywatnego oraz dokonanie za jego pomocą podpisu dokumentu elektronicznego ze skutkiem prawnym. Takie podejście umożliwia rezygnację z konieczności posiadania przez użytkowników kart mikroprocesorowych.

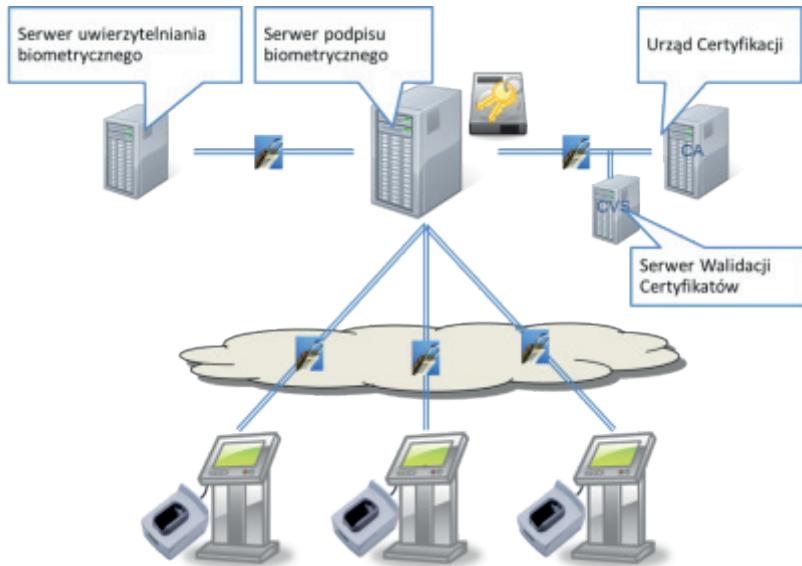
Podpis biometryczny, bazujący na zaawansowanej technologii naczyniowej, np. używanej w oddziałach banków, to system oparty na nakreślonych powyżej założeniach. Klucz prywatny użytkownika jest przechowywany w centralnym repozytorium, a dostęp do niego wymaga silnego uwierzytelnienia z wykorzystaniem unikalnej cechy biometrycznej. Kluczowe w zastosowaniu takiego rozwiązania są: zgodność przyjętych rozwiązań technicznych i formalnych z obowiązującym prawem oraz możliwość uzyskania podpisu ze skutkiem prawnym pod dokumentem elektronicznym. Spełnienie powyższych warunków umożliwi wprowadzenie tego typu rozwiązania w miejsce tradycyjnego podpisu odręcznego.

W analizie aspektów prawnych najistotniejsze wydają się zagadnienia zgodności rozwiązania z ustawą o ochronie danych osobowych (zagadnienie opisane szczegółowo w rozdziale 10.2 niniejszego raportu) oraz zapewnienie skuteczności czynności cywilno-prawnych (w tym przypadku podpisywanie dokumentów elektronicznych) wykonywanych przez klienta banku, o których mowa w rozdziale 10.4 niniejszego raportu.

Uruchomienie w banku podpisu biometrycznego na bazie biometrycznej infrastruktury oddziałowej niesie za sobą szereg zalet w warstwie procesowej i kosztowej. Wśród najważniejszych wymienić należy:

- optymalizację procesów związanych z obiegiem dokumentów podpisanych,
- redukcję kosztów obiegu podpisanych dokumentów papierowych (druk, transport, archiwizacja),
- ułatwione składowanie, weryfikacja, wyszukiwanie podpisanych dokumentów elektronicznych (w porównaniu zarówno do dokumentów papierowych jak i ich zeskanowanych wersji),

- eliminacja działań nieuprawnionych polegających na posługiwaniu się podrobionym lub skradzionym dokumentem tożsamości podczas podpisywania dokumentów.



Rys.25: Wysokopoziomowa architektura podpisu biometrycznego

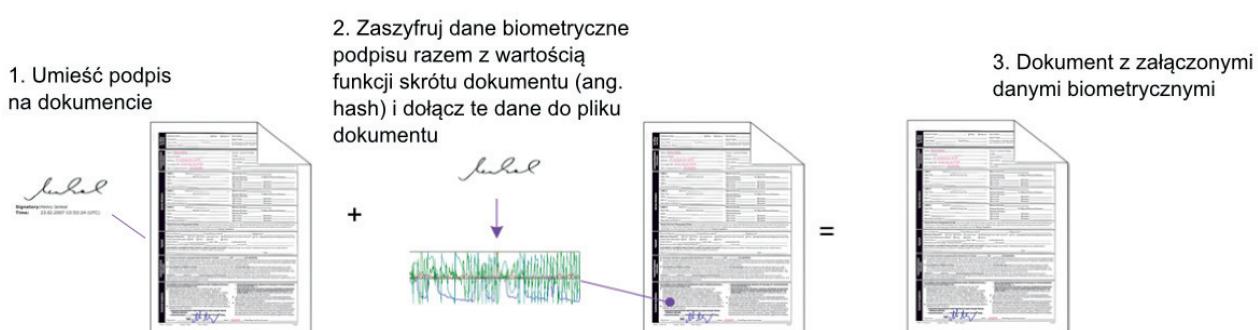
Źródło: Hitachi

Opisany powyżej system podpisu biometrycznego łączy zalety silnego uwierzytelnienia biometrycznego i podpisu elektronicznego dokumentów i może być z powodzeniem stosowany w bankach, czego konsekwencją jest m.in. redukcja kosztów obiegu podpisanych dokumentów papierowych oraz optymalizacja procesów związanych z ich obiegiem.

6.9. Systemu obiegu dokumentów z biometrią podpisu odręcznego

Powyżej przedstawiono koncepcję rozwiązania paper-less opartego o podpis biometryczny tj. połączenie silnego uwierzytelnienia biometrycznego (np. Finger Vein) z PKI. W niniejszym rozdziale przedstawiono koncepcję systemu opartego o biometrię podpisu odręcznego.

Poza zastosowaniem biometrii podpisu odręcznego wprost w procesie uwierzytelniania tożsamości, warto wspomnieć o innym komercyjnie uzasadnionym i sprawdzonym sposobie zastosowania opisywanej technologii biometrycznej – zastosowaniu w połączeniu z systemami obiegu dokumentów (ang. paper-less workflow). Sposobem na zredukowanie kosztów i usprawnienie obiegu dokumentów jest wprowadzenie mechanizmu sygnowania treści dokumentów elektronicznych biometrycznym podpisem odręcznym, będącym połączeniem (zespoleniem) zwyczajnej, graficznej reprezentacji podpisu i „niewidocznego” wzorca biometrycznego. Niewidoczna część wykorzystywana jest w weryfikowaniu tożsamości osoby podpisanej, post factum. Zespolenie takie jest jednoznaczne i niezaprzecjalne. Jednoznaczność oznacza tu brak możliwości skutecznego, prostego skopiowania wzorca i doklejenia go do innego dokumentu – technika zespalania umożliwia proste wykrycie niezgodności między dokumentem podpisowanym i wzorcem podpisującym. Zabezpieczenie i jednoznaczność zespolenia zwykle realizowane jest przy zastosowaniu mechanizmów szyfrowania (np. w oparciu o tradycyjny standard X.509 – szyfrowanie asymetryczne).

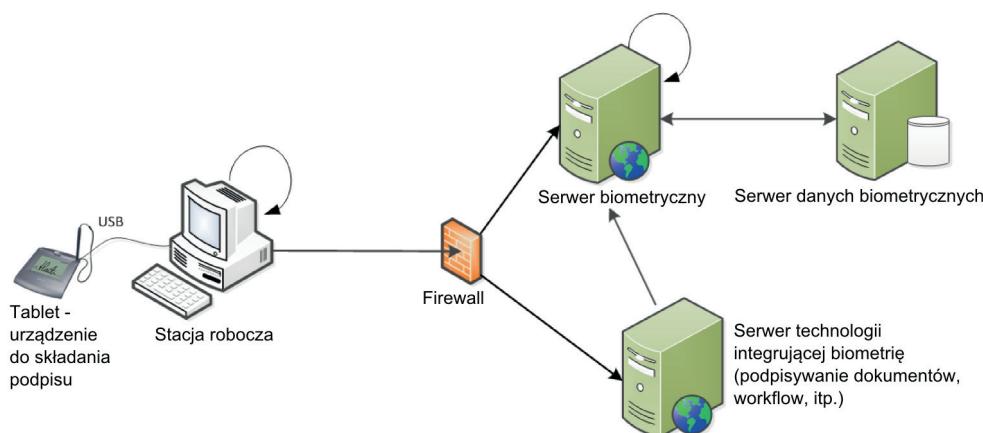


Rys.26: Konstrukcja dokumentu sygnowanego biometrycznym podpisem odręcznym

Źródło: IBM

Typowa architektura środowiska działania technologii biometrycznej uwzględnia topologię współpracujących między sobą szeregu urządzeń - są nimi:

- stacje robocze i tablety (urządzenia do składania),
- serwer biometryczny i baza danych biometrycznych, służące składowaniu wzorców biometrycznych i określaniu zgodności wzorców (w procesie weryfikacji tożsamości)
- ewentualny serwer przetwarzający dokumenty elektroniczne, podpisywane z użyciem opisywanej technologii biometrycznej, lub też służący innym celom współdziałania tej technologii z innymi technologiami zintegrowanymi (np. technologią obiegu dokumentów, czy też zarządzania procesami biznesowymi [ang. BPM - Business Process Management]).



Rys.27: Architektura środowiska działania systemu biometrii podpisu odręcznego

Źródło: IBM

Określając wartość i adekwatność zastosowania technologii biometrycznej na podstawie podpisu odręcznego warto wskazać podstawowy obecnie, jak się wydaje, czynnik decydujący o tym właśnie aspekcie, czyli o akceptowalności społecznej. Obecnie klienci banków wyrażają swoją akceptację przede wszystkim na piśmie, składając podpis odręczny. Stosowanie tej technologii pozwala utrzymanie tego zwyczaju i nie tworzy potrzeby akceptacji nowych, innych metod wyrażania akceptacji. Opisywana tu technologia umożliwia zorganizowanie elektronicznego obiegu dokumentów w skali nieograniczonej lokalizacjami (geograficznie), z względnie niższymi kosztami i z wysokimi wskaźnikami wydajności w procesach akceptacji, w których wymagane są podpisy (przemieszczenie dokumentów papierowych jest czasochłonne i generuje dodatkowe koszty).

Jednym z pierwszych banków który wprowadził rozwiązanie „Paperless” na bazie biometrii podpisu odręcznego był GE Money Bank w Czechach, gdzie zaimplementowano 1200 tabletów do składania podpisu odręcznego.

6.10. Dystrybucja gotówki

System dystrybucji gotówki składa się z wielu elementów takich jak: placówki bankowe, bank centralny, sortownie, punkty odbioru gotówki (sklepy, hurtownie). Każdy z tych punktów posiadać musi specjalne rozwiązania do przekazywania/przyjmowania i transportu gotówki. Są to między innymi: bankomaty, wpłatomaty, szafy transferowe, wrzutnie nocne, inteligentne sejfy, walizki do transportu wartości, koperty bezpieczne i wiele innych. Pomiędzy wszystkimi w/w punktami gotówka transportowana jest przez konwoje w specjalnie przystosowanych do tego bankowozach. Finalnie trafia ona do sortowni, gdzie następuje jej przeliczenie, po-sortowanie, pakowanie i przygotowanie do dalszego transportu. Na każdym etapie niezbędnego jest zadbanie o bezpieczeństwo.

Niestety gotówka jest bardzo „łakomym” łupem dla wielu złodziei, dlatego też wymyślają oni niezwykłe sposoby na jej kradzież. Jednej z bardziej zuchwałych kradzieży dokonano w 2010 roku, kiedy to złodzieje podając się za pracowników firmy konwojującej ukradli z jednej z sortowni 5 mln złotych.⁶

Kolejnym ciekawym przykładem ukazującym spryt złodziei jest powszechny skimming, czyli instalowanie specjalnych nakładek na bankomaty, umożliwiających odczyt numeru karty klienta, a następnie wykorzystanie tych danych do wypłaty pieniędzy na skopiowanych kartach.

Kilka lat temu w Polsce, we Wrocławiu złodzieje włamali się do wrzutni nocnej i ukradli z niej 3 mln złotych. Po-sługiwali się kodami, które bez problemów otworzyły zamki elektroniczne.⁷

Tak samo jak złodzieje posługują się coraz to nowymi pomysłami w celu dokonania kradzieży, tak samo departamenty bezpieczeństwa różnych instytucji powinny wykorzystywać nowoczesne technologie. Przykładem wykorzystania nowoczesnych technologii w celu podnoszenia bezpieczeństwa w systemach dystrybucji gotówki jest wykorzystanie technologii biometrycznej do uwierzytelniania konwojentów firm CIT.

W przypadku takiego systemu w sortowni gotówki zainstalowany jest system umożliwiający uwierzytelnienie konwojenta, który przyjedzie po odbiór gotówki. Odbywa się to w bardzo prosty sposób, poprzez wykorzystanie bezpiecznego czytnika biometrycznego do odczytu i weryfikacji jego danych biometrycznych. Następnie serwer dokonuje uwierzytelnienia konwojenta i zwraca informację o tym czy konwojent jest uprawniony do odbioru gotówki. Objęcie systemem wielu firm konwojujących daje pełną kontrolę nad przydzielonymi upraw-

nieniami i pozwala natychmiast je odebrać w przypadku zagrożenia. Dzięki temu mamy pewność, że w przypadku zwolnienia danego pracownika, nie pobierze on gotówki z sortowni, a także zapewniajemy 100% gwarancję, że pod danego pracownika nie podszyje się żaden inny. Cała operacja przekazania gotówki potwierdzana jest także odczytaniem danych biometrycznych osoby wydającej gotówkę z sortowni.

System ten znacznie zwiększa bezpieczeństwo podczas przekazywania gotówki. W przypadku implementacji takiego systemu w każdej sortowni, każdej placówce bankowej i w każdym punkcie/sklepie, który przekazuje gotówkę, wyeliminujemy całkowicie możliwość tego typu przestępstw.

Technologia ta wykorzystywana jest już w kilku sortowniach gotówki na rynku polskim i z powodzeniem odnosi sukces, zwiększa poziom bezpieczeństwa i chroni przed kradzieżą tożsamości. W 2012 roku pilotowy system wdrożyła i zaoferowała w Polsce firma KŁOS Nowoczesne Technologie Bankowe Sp. z o.o. w oparciu o centralny serwer przechowujący dane konwojentów oraz biometrię Finger Vein.

6.11. Rejestracja czasu pracy

Systemy rejestracji czasu pracy (RCP) działające w oparciu o techniki biometryczne są coraz częściej stosowane na świecie. Niewątpliwy wpływ na stosowanie takich systemów ma nieustannie obniżająca się ich cena przy wzroście współczynnika gwarantujących niepodważalność rejestracji pracowników oraz wygoda w użytkowaniu. Systemy biometryczne skutecznie rozbijają „spółdzielnie” pracowników, gdy jeden „dyżurny” pracownik uwierzytelnia obecność kilku innych za pomocą przekazanych mu kart zbliżeniowych (RFID) lub wprost fałszując podpis na liście obecności.

6 <http://www.rmf24.pl/fakty/polska/news-podal-sie-zakonwojenta-banku-i-zniknal-z-5-milionamizlotyc,n1d,242068>

7 <http://miasta.gazeta.pl/wroclaw/1,35751,5673009.html>

7. Zastosowania biometrii w usługach na linii bank - administracja publiczna

7.1. Rejestracja działalności gospodarczej w okienku banku

Z dniem 1 lipca 2011 r. rozpoczął działanie portal ceidg.gov.pl dający dostęp do Centralnej Ewidencji i Informacji o Działalności Gospodarczej⁸ (CEIDG). Celem wprowadzenia CEIDG było m.in. ograniczenie czasu oraz formalności związanych z rozpoczęciem działalności gospodarczej przez osobę fizyczną. Portal ceidg.gov.pl umożliwia założenie, zawieszenie, wznowienie i zakończenie działalności gospodarczej, zmodyfikowanie danych w istniejącym wpisie oraz łatwy dostęp do informacji o przedsiębiorcach.

Warunkiem skutecznego złożenia poprzez portal ceidg.gov.pl wniosku w formie elektronicznej o założenie (zawieszenie, wznowienie, zakończenie) działalności gospodarczej jest posiadanie przez wnioskodawcę możliwości złożenia podpisu pod wnioskiem w jeden z akceptowanych w CEIDG sposobów. Nowelizacja ustawy o swobodzie działalności gospodarczej⁹ z 13 maja 2011 r. wskazuje możliwe sposoby podpisu wniosku CEIDG-1 (zastępującego dotychczas używany wniosek EDG-1). Art. 27 ust. 7 wymienia kolejno:

- podpis elektroniczny weryfikowany za pomocą certyfikatu kwalifikowanego,
- podpis potwierdzony profilem zaufanym ePUAP,
- podpis osobisty, oraz
- podpis w inny sposób akceptowany przez system CEIDG umożliwiający jednoznaczną identyfikację osoby składającej wniosek i czas jego złożenia.

Poniżej przeanalizowano kolejno wyżej wymienione rodzaje podpisu wniosku.

Certyfikat kwalifikowany jest dostępny i ustawowo uregulowanym narzędziem¹⁰. Ponieważ weryfikowany przy jego pomocy podpis elektroniczny nie zyskał do tej pory szerokiego grona użytkowników w grupie osób fizycznych, jego zastosowanie do złożenia wniosku poprzez portal CEIDG wymaga najczęściej uprzedniej osobistej wizyty wnioskodawcy w punkcie partnerskim jednego z kwalifikowanych podmiotów świadczących

⁸ Centralna Ewidencja i Informacja o Działalności Gospodarczej została utworzona na bazie ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (tekst jednolity: Dz. U. 2010 Nr 220 poz. 1447 ze zm.)

⁹ Ustawa z dnia 13 maja 2011 r. o zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw (Dz. U. Nr 131, poz. 764)

¹⁰ Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2001 r. Nr 130, poz. 1450 ze zm.)

usługi certyfikacyjne (urzędów certyfikacji) w celu jego pozyskania.

Profil zaufany jest bezpłatną metodą potwierdzenia tożsamości obywateli w kontakcie z administracją publiczną. Uzyskanie profilu zaufanego wymaga wizyty w wyznaczonym punkcie celem potwierdzenia tożsamości osoby otrzymująccej taki profil.

Podpis osobisty, o którym mowa w przepisach o dowodach osobistych¹¹, jest narzędziem do składania podpisu osobistego przy użyciu dowodu osobistego nowego typu. Brak możliwości wykorzystania tej metody podpisu jest bezpośrednio związany z przesuwającym się terminem wprowadzenia nowych dokumentów tożsamości. Warto też dodać, że nawet po wprowadzeniu nowych dowodów osobistych przewidziany jest okres przejściowy, w którym stare dokumenty będą wymieniane (nowa metoda podpisu będzie więc dostępna w tym okresie tylko dla pewnej podgrupy obywateli).

Czwarty sposób podpisu wniosku, a więc „podpis w inny sposób akceptowany przez system CEIDG” to możliwość pozostawiona przez ustawodawcę na potrzeby wykorzystania w przyszłości innych sposobów podpisywania wniosków.

Z powyższego przeglądu metod podpisu wniosków dopuszczonych przez CEIDG wynika, że osoba fizyczna nieposiadająca ani certyfikatu kwalifikowanego, ani profilu zaufanego, nie będzie w stanie złożyć w formie elektronicznej wniosku o założenie działalności gospodarczej bez uzyskania wymienionych powyżej narzędzi służących do podpisu. Świadomy tego ustawodawca uwzględnił więc możliwość wypełnienia wniosku w urzędzie lub wizyty w urzędzie miasta lub gminy w celu własnoręcznego podpisania wniosku wypełnionego w formie elektronicznej.

W związku z opisaną powyżej sytuacją braku powszechnie używanej metody podpisu wniosków w wersji elektronicznej, pojawiła się możliwość uruchomienia przez banki dla klientów końcowych nowej usługi, polegającej na wsparciu procesu zakładania przez nich działalności gospodarczej. Wartością dodaną dla klienta jest możliwość uzyskania kompleksowej pomocy w procesie zakładania firmy, z uwzględnieniem wsparcia merytoryczno-prawnego udzielanego przez przeszkołonego pracownika banku oraz możliwości finalizacji wszystkich niezbędnych formalności w jednym miejscu (np. w placówce banku), a więc oprócz samego złożenia wniosku CEIDG-1 również np. założenie konta firmo-

¹¹ 11 Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2010 r. Nr 167, poz. 1131)

wego, podpisanie umowy na obsługę księgową, etc. z perspektywy banku uruchomienie takiego „jednego okienka” daje natomiast możliwość pozyskania nowych klientów z segmentu klienta biznesowego oraz generowanie przychodu poprzez zaoferowanie w pakiecie z usługą wsparcia zakładania działalności gospodarczej produktów i usług finansowych.

Usługa wsparcia w zakładaniu działalności gospodarczej jest obecnie świadczona przez niektóre instytucje finansowe. Jej świadczenie opiera się na wypełnieniu w formie papierowej wniosku o założenie działalności gospodarczej oraz o pełnomocnictwo udzielane przez klienta pracownikowi danej instytucji i późniejszym reprezentowaniu go przez tego pracownika w odpowiednich urzędach. W związku z pojawiением się CEIDG i możliwości elektronicznego składania wniosków CEIDG-1, pojawiła się możliwość optymalizacji dotychczas używanego sposobu świadczenia tej usługi.

Usługa wsparcia w zakładaniu działalności gospodarczej może być świadczona na kilka sposobów. Bank, jako agent urzędu certyfikacji, może wydawać klientom certyfikaty kwalifikowane, przy pomocy których weryfikowany będzie podpis składany pod wnioskiem CEIDG-1. Wiąże się to z kosztem certyfikatu, który musi ponieść osoba fizyczna oraz koniecznością spełnienia wszystkich wymogów formalno-prawnych narzuconych ustawą o podpisie elektronicznym. Zaletą tego rozwiązania jest natomiast standardowe wsparcie tego rodzaju podpisu przez systemy e-administracji (ePUAP, CEIDG, EUGO, etc.).

Inną możliwością jest wydawanie przez banki profilu zaufanego zgodnego z ePUAP. Do chwili obecnej żadna z instytucji finansowych nie zdecydowała się jednak na zaoferowanie takiej możliwości swoim klientom, co może wynikać zarówno ze względów formalnych, jak i niskiej popularności tej usługi.

Alternatywą dla powyższych metod jest zastosowanie opisanego w ustawie o swobodzie działalności gospodarczej czwartego sposobu składania podpisu, tj. wspomnianego wcześniej „podpisu w inny sposób akceptowanego przez system CEIDG umożliwiającego jednoznaczna identyfikację osoby składającej wniosek i czas jego złożenia”. Do tego celu służyć może jedna z technologii zapewniających uwierzytelnienie klienta banku, przy czym z uwagi na skutki prawne podpisu pod wnioskiem w CEIDG wybrać należy technologię zapewniającą silne uwierzytelnienie i wysoki poziom bezpieczeństwa. Świetsnym przykładem takiej technologii jest wykorzystywana przez bank oddziałowa infrastruktura biometryczna, używana np. do uwierzytelniania klientów w oddziałach i wypłat z bankomatów. Dodatkowymi zaletami są wysokie bezpieczeństwo, brak konieczności użycia kart mikroprocesorowych oraz możliwość dotarcia do klientów „wykluczonych cyfrowo”. Trzeba jednak podkreślić, że w przypadku stosowania tego podejścia, należy uzyskać akceptację Ministerstwa Gospodarki na

wykorzystanie w CEIDG konkretnego rozwiązania używanego przez bank.

„Usługa wsparcia w zakładaniu działalności gospodarczej jest obecnie świadczona przez niektóre instytucje finansowe”

Opisywany powyżej przykład wykorzystania infrastruktury biometrycznej banku do składania wniosków w CEIDG (lub innych systemach e-administracji) stanowi dobry przykład na możliwość rozszerzenia zakresu wykorzystania zalet zaawansowanej biometrii oddziałowej poza klasyczne czynności bankowe. W tym przypadku dostępność technologii silnego uwierzytelniania klientów w oddziałach pozwala zaoferować klientom końcowym nowe usługi na styku z administracją publiczną.

7.2. Biometryczne wypłaty świadczeń społecznych

Osoby uprawnione do odbioru świadczeń społecznych niejednokrotnie oczekują w długich kolejkach aby odebrać pieniądze w godzinach pracy urzędu. Bywa, że urzędy współpracują z bankami w zakresie dystrybucji środków. Te najczęściej jedynie zastępują okienko urzędu, okienkiem banku. Obsługa wypłat polega na przesłaniu przez urząd papierowej listy osób uprawnionych do wypłat. Pracownik banku każdorazowo weryfikuje tożsamość Klienta na podstawie dowodu tożsamości. Następnie Klient zobowiązany jest do złożenia odręcznego podpisu na liście wypłat. Wypłaty świadczeń możliwe są przeważnie tylko przez 3 kolejne dni w miesiącu dla uprawnionych osób. Po zakończeniu wypłat pracownik wykonywał ręcznie raport wypłaconych i niewypłaconych zasiłków tzw. zwrotów i przekazuje w wersji papierowej do właściwego urzędu. Taka procedura powoduje wielogodzinne kolejki w okienkach kasowych oraz czasochlonną obsługę wykonywaną przez pracowników. Osoby uprawnione do odbioru świadczeń mają jednocześnie utrudniony dostęp do bankowości elektronicznej. Taki sposób usług świadczeń społecznych funkcjonuje w większości miejsc w Polsce.

Dobrym rozwiązaniem, które sprawdziło się już w kilku miejscach w Polsce jest dystrybucja świadczeń w ban-

komatach biometrycznych dostępnych 24h na dobę. Wypłata środków z takich bankomatów możliwa jest bez posiadania przy sobie żadnych dokumentów ani nawet karty bankomatowej. Wystarczy jednorazowa rejestracja w placówce bankowej, zarejestrowanie wzorca biometrycznego, a później już tylko 24h dostęp do bankomatu. Środki można wypłacać w każdej chwili bez względu na godziny urzędowania placówki bankowej.

„Rozwiążanie z wykorzystaniem bankomatu wyposażonego w czytnik biometryczny Finger Vein znacznie skróciło czas potrzebny do obsługi wypłat świadczeń socjalnych

Kluczem powodzenia takiej właśnie dystrybucji gotówek jest wygoda użytkowania – środki można wypłacić nie posiadając przy sobie ani karty bankomatowej ani nawet dokumentu tożsamości. Wystarczy wpisać swoją datę urodzenia, ilość środków do wypłaty, zweryfikować się biometrycznie i środki są wypłacane w ciągu kliku sekund.

Rozwiążujemy w ten sposób szereg problemów, które mają dziś urzędy:

- Dostęp do potrzebnej gotówki 24h
- Wygoda osób uprawnionych do świadczeń
- Brak konieczności posiadania karty bankomatowej
- Zwiększenie bezpieczeństwa wypłat świadczeń społecznych

Przykładem wdrożenia biometrycznych wypłat świadczeń społecznych jest projekt w Podkarpackim Banku Spółdzielczym. Nowoczesne rozwiązanie z wykorzystaniem bankomatu wyposażonego w czytnik biometryczny *Finger Vein* znacznie skróciło czas potrzebny do obsługi wypłat świadczeń socjalnych. W nowej technologii dane klientów wraz z zeskanowanym wzorcem biometrycznym palca wprowadzane są jednorazowo do bazy danych systemu biometrycznego, a następnie wykorzystywane do uwierzytelniania klienta w bankomacie. Urząd przesyła do PBS plik z listą wypłat świad-

czeń drogą elektroniczną. Lista zawiera podstawowe niezbędne dane takie jak: imię, nazwisko, PESEL i kwotę wypłaty. Lista zacztywana jest przez pracownika w systemie biometrycznym. Trwa to niecałą minutę. Po zeczytaniu pliku system jest gotowy do realizowania wypłat. Klienci mogą pobierać swoje świadczenia z bankomatu o dowolnej porze dnia i nocy. Aby wypłacić pieniądze wystarczy przyłożyć palec w czytniku biometrycznym w bankomacie a po poprawnej weryfikacji następuje wypłata gotówki. Cały proces trwa kilka sekund. Po zakończonym procesie wypłat pracownik przekazuje drogą elektroniczną do urzędu raport z listą wypłacanych zasiłków. Nowe rozwiązanie biometryczne przyniosło wiele korzyści zarówno dla klientów jak i banku. Do najważniejszych można zaliczyć: znaczne zmniejszenie nakładów czasowych na obsługę, podniesienie poziomu bezpieczeństwa, zwiększenie jakości obsługi, wygodę dla klienta oraz promowanie wizerunku banku, jako nowoczesnej instytucji.

Z doświadczeń Podkarpackiego Banku Spółdzielczego korzystają inne banki spółdzielcze w Polsce. Biometryczne wypłaty świadczeń społecznych są wdrożone również w Baku Spółdzielczym w Pruszczu Gdańskim.

8. Wybrane studia przypadków wdrożeń biometrii w bankowości

Rozwój nowych technologii w bankowości oraz stale postępujący proces informatyzacji wymusza na uczestnikach rynku usług finansowych stałe podnoszenie jakości produktów oferowanych klientom z zachowaniem pełnego bezpieczeństwa w dostępie do środków pieniężnych. Biometria umożliwia zwiększenie efektywności i dostępności usług bankowych, zwiększając przy tym bezpieczeństwo. W niniejszym rozdziale przedstawiono wybrane studia przypadków wdrożeń biometrii w Polsce oraz zagranicą.

8.1. Wdrożenia biometrii w Polsce



Rys.28: Bankomat biometryczny w Banku Spółdzielczym w Pruszu Gdańskim (Grupa SGB)

Źródło: Wincor Nixdorf

Obecnie Polska jest absolutnym liderem we wdrażaniu biometrii w bankowości na skalę Europy. Polski sektor bankowy wdrażała biometrię w sposób bardzo usystematyzowany i może stanowić wzór dla innych krajów Unii Europejskiej.

Pierwsze działania związane z rozpowszechnianiem biometrii w bankowości rozpoczęły się w połowie 2007 r. w tym czasie świadomość sektora bankowego na temat biometrii była bardzo niska. Kluczową rolę w rozwoju biometrii w polskiej bankowości odegrał Związek Banków Polskich. Pod jego egidą w sierpniu 2007 r. powstała strategia popularyzacji biometrii w Polsce, a w następstwie Grupa ds. Biometrii przy Forum Technologii Bankowych Związku Banków Polskich, zrzesza-

jącą firmy technologiczne, integratorów systemowych oraz ośrodki naukowe. Inicjatorem działań związanych z popularyzacją biometrii w bankowości był sp. Prof. Remigiusz Kaszubski. Pierwszym krokiem milowym w rozwoju biometrii była oficjalna publikacja „Polskiego Raportu Biometrycznego”, która stała się kompendium wiedzy dla banków, sektora publicznego i rządowego. Kolejnym przełomowym wydarzeniem było wydanie w styczniu 2011 roku ekspertyzy prawnej „Biometria w bankowości i administracji publicznej” pod redakcją sp. Prof. Remigiusza Kaszubskiego. Ta publikacja zdefiniowała podstawy prawne dla biometrii w bankowości i przełamała stereotypy oraz niejasności związane z jej wdrożeniem w banku.

Od marca 2010 roku działają w Polsce pierwsze w Polsce i Europie biometryczne bankomaty. Pierwszy pilotowy bankomat Banku Polskiej Spółdzielczości S.A. (BPS) został zainstalowany w Warszawie przy ul. Płockiej. W ramach pilotu biometria Finger Vein wykorzystywana była do uwierzytelniania wypłat lokalnych (bez karty) oraz jako zabezpieczenie do kart EMV. Dzisiaj Bank BPS wdrożył już ponad 60 bankomatów biometrycznych i 90 stanowisk biometrycznych w swoich oddziałach w całej Polsce.

Na przełomie marca i kwietnia 2010 roku w Sanoku uruchomiony został pilotowo bankomat biometryczny w Podkarpackim Banku Spółdzielczym (PBS). PBS Sanok chciał wykorzystać bankomaty biometryczne do wypłat zasiłków społecznych. Rozwiążanie biometryczne Finger Vein miało na celu rozładowanie kolejek, które powstają w dniach realizacji wypłat. Generują je osoby uprawnione do otrzymania tego rodzaju świadczeń, które zjawiają się masowo w banku. To właśnie w banku PBS Sanok został uruchomiony pierwszy w Europie produkcyjny system biometryczny. Oprócz świadczeń klienci PBS mogą wypłacać pieniądze ze swojego konta bez korzystania z karty i kodu PIN. Oczywiście bankomat biometryczny może realizować jednocześnie tradycyjne transakcje z wykorzystaniem kart płatniczych, dzięki czemu jest użyteczny w całym okresie eksplatacji. Bank zyskuje dzięki temu dodatkowe, nieobecne do tej pory na polskim i europejskim rynku, bezobsługowe (dla banku) rozwiązanie, optymalizujące proces obsługi Klienta. Natomiast świadczeniobiorcy i klienci PBS mogą obsłużyć się sami a personel placówki koncentruje się na obsłudze bardziej wymagających klientów oraz na sprzedaży produktów. Obecnie PBS posiada sieć ok. 85 bankomatów biometrycznych.

W latach 2010 - 2013 do grona użytkowników bankomatów biometrycznych wykorzystujących biometrię Finger Vein dołączyły (pilotowo lub produkcyjnie) kolejne banki spółdzielcze między innymi Bałtycki Bank Spółdzielczy w Darłowie, BS Kielce, BS Koronowo, BS

Mosina, BS Pruszczański, Mazowiecki Bank Spółdzielczy w Łomiankach i Powiślański Bank Spółdzielczy w Kwidzynie. W 2013 roku projekt pilotażowy w 15 oddziałach i na 15 bankomatach rozpoczął największy, niezrzeszony bank spółdzielczy - Krakowski Bank Spółdzielczy (KBS). W sumie na terenie całego kraju działa w tej chwili ok. 250 bankomatów biometrycznych. Właśnie w Polsce powstał pierwszy w Europie host biometryczny w firmie IT Card S.A. (Grupa PBS). IT Card oferuje swoim klientom (bankom) usługę uwierzytelniania biometrycznego oraz hosting danych biometrycznych. Jest to szczególnie ważna oferta dla małych banków, których nie stać na zakup, wdrożenie i utrzymanie centralnego systemu biometrycznego. IT Card umożliwia przełączenie transakcji biometrycznych między bankami podłączonymi do ich systemu biometrycznego. Oznacza to, że klient Banku X będzie mógł wypłacić biometrycznie środki z bankomatu bez konieczności korzystania z karty. IT Card rozwija również swoją sieć bankomatów Planetcash Cash4You, która jeśli zostanie wyposażona w czytniki biometryczne, utworzy największą w Europie niezależną sieć bankomatów biometrycznych. Biorąc na informacjach rynkowych, mówi się, że Euronet - właściciel największej niezależnej sieci bankomatów, również rozważa implementację hosta biometrycznego.

8.1.1. Podkarpacki Bank Spółdzielczy



Rys.29: Bankomat biometryczny w Podkarpackim Banku Spółdzielczym
Źródło: PBS

Podkarpacki Bank Spółdzielczy to największy bank spółdzielczy w Polsce, zrzeszony w Grupie PBS. W 2011 roku obchodził 140-lecie swojego istnienia. Jest bankiem z bogatymi tradycjami, ale jednocześnie nowoczesnym, stale poszukującym innowacyjnych rozwiązań technologicznych, poprawiających wygodę i zadowolenie klientów.

Tak było w przypadku potrzeby usprawnienia wypłat świadczeń socjalnych dla osób, które nie posiadają konta bankowego. PBS poszukiwał nowego rozwiązania eliminującego długie oczekiwanie klientów w okienku bankowym dokonujących wypłat świadczeń socjalnych. Kilkugodzinne oczekивание w kolejce, kłopotliwa weryfikacja klienta na podstawie dokumentu tożsamości, obsługa papierowa list osób upoważnionych do wypłat były głównymi przyczynami poszukiwania nowej technologii. Spośród kilku firm oferujących takie rozwiązania za najlepszą uznano ofertę firmy Wincor Nixdorf, która wyposażyła swoje bankomaty w czytniki biometryczne układu naczyń krwionośnych palca japońskiej firmy Hitachi. Po wykonaniu testów w październiku 2009 PBS zdecydował się na wdrożenie usługi wypłat z bankomatów z wykorzystaniem biometrii w całej infrastrukturze PBS.

Pierwsze wypłaty biometryczne świadczeń socjalnych z bankomatu miały miejsce w 2010 roku. Od samego początku usługi biometryczne spotkały się z dużym zainteresowaniem. Podczas wybierania gotówki klienci nie muszą, bowiem znać kodu PIN, który jest często kłopotliwy do zapamiętania. Klient nie musi również nosić ze sobą żadnej karty płatniczej. Jest to bardzo wygodna metoda korzystania z bankomatu. Bank zyskał również wiele z tytułu wdrożenia biometrii do wypłat socjalnych. Klient nie musi stać w kolejce do wypłaty a tym samym nie zajmuje czasu pracownikowi, który w tym czasie może wykonywać inne czynności, jak np. sprzedaż produktów bankowych. Dodatkową zaletą usługi jest jej szybkość i duże bezpieczeństwo wykonywanych transakcji.

W marcu 2011 roku PBS wdrożył usługę wypłat lokalnych z konta bankowego. Klienci posiadający rachunki oszczędnościowo-rozliczeniowe (ROR) od tego momentu mogli dokonywać wypłat z bankomatu za pomocą czytnika układu naczyń krwionośnych palca. Klienci chętnie korzystają z tej formy wypłat, o czym świadczy dynamiczny wzrost liczby transakcji w bankomatach przy użyciu biometrii naczyń krwionośnych palca.

Już w 4 kwartale 2013 roku PBS planuje rozszerzyć ofertę o nowe rozwiązanie polegające na identyfikacji i autoryzacji klienta w okienkach bankowych za pomocą czytnika biometrycznego we wszystkich placówkach PBS. Klient nie będzie musiał posiadać przy sobie dowodu osobistego, aby autoryzować operację np. realizację wypłaty z konta. Nowe rozwiązanie będzie wygodne również dla klientów, którzy od tej pory nie będą musieli

pamiętać nr PESEL czy innych kłopotliwych do zapamiętania danych osobistych, aby załatwić sprawę w banku.

Każde wdrożenie nowej technologii jest ciekawym wydarzeniem zarówno dla PBS jak i jego klientów, choć budzi pewne wątpliwości dotyczące pozytywnego zaakceptowania. Informacja, która pojawiała się w mediach o tym, że PBS, jako pierwszy w Polsce wdrożył produkcyjnie usługę biometryczną, miała duży wpływ na promocję banku, jako instytucji innowacyjnej. Jak każda nowość dane rozwiązanie wzbudziło duże zainteresowanie wśród klientów. Początkowo traktowane jako ciekawostka czy też gadżet, obecnie stało się niejednokrotnie jedyną metodą korzystania z bankomatu. PBS będzie dalej rozwijać technologię biometryczną, wprowadzając kolejne innowacyjne rozwiązania.

W związku z wdrożeniem biometrii PBS otrzymał następujące prestiżowe nagrody:

1. „Projekt Roku 2010” - Nagroda główna w konkursie organizowanym przez Związek Banków Polskich (maj 2011),
2. „Złote Godło - Najwyższa jakość 2011 Quality International” w kategorii QI Services - usługi najwyższej jakości (lipiec 2011),
3. „Medal Europejski” za usługę biometrii (listopad 2011),
4. „Najciekawsza innowacja bankowa”, i miejsce w konkursie „Liderzy świata bankowości” organizowanym przez Polski Kongres Gospodarczy (marzec 2012),
5. Wyróżnienie w kategorii „Bankowość elektroniczna i e-finanse” w jubileuszowej edycji konkursu technologicznego „Gazety Bankowej” pt. „Lider Informatyki Instytucji Finansowych 2011” (marzec 2012).

8.1.2. Bank Polskiej Spółdzielczości S.A. (BPS)

Bank Polskiej Spółdzielczości S.A. będący w gronie podmiotów finansowych o najwyższym wskaźniku implementacji nowych rozwiązań informatycznych i innowacji z zakresu produktów bankowych, podjął w 2010 roku decyzję o wdrożeniu nowoczesnej technologii biometrycznej w bankomatach. Analiza rynku i ofert kilku firm posiadających rozwiązania z zakresu biometrii skutkowała podjęciem współpracy z firmą Wincor-Nixdorf. Dostawca systemu biometrycznego pod nazwą InterVein zaproponował funkcjonalność biometryczną opartą na rozwiązaniu firmy Hitachi - Finger Vein. System InterVein oparty jest na integracji urządzeń bankomatowych z czytnikami Finger Vein pozwalającymi na identyfikację i weryfikację klienta na podstawie wzoru jego naczyń krwionośnych palca. Klient po rejestracji w oddziale banku i złożeniu wzorca referencyjnego bazującego na wzorze naczyń krwionośnych, może korzystać z bankomatów wyposażonych w czytniki Finger Vein.



Rys.30: Bankomat biometryczny w oddziale Banku BPS na ul. Płockiej w Warszawie

Źródło: Wincor Nixdorf

Proces wypłaty środków z bankomatów składa się z dwóch etapów:

- **etap I** - identyfikacja klienta poprzez wprowadzenie karty bankomatowej lub wprowadzenie na klawiaturze kodu np. nr PESEL,
- **etap II** - weryfikacja klienta, czyli porównanie wzorców biometrycznych z bazy danych (wzorce złożone w banku podczas procesu rejestracji klienta w systemie) z wzorem naczyń krwionośnych żywego palca przyłożonego na czytniku FV zainstalowanym w bankomacie.

Dodatkowo bankomaty z funkcjonalnością biometryczną wyposażone są w dyspensery monet pozwalające na wypłatę nawet niewielkich kwot w postaci bilonu.

Pierwsze testowe uruchomienie w Banku BPS S.A. pojedynczego bankomatu wyposażonego w czytnik biometryczny miało miejsce w Centrali Banku wiosną 2010 roku. Wdrożenie systemu w banku rozpoczął proces wymiany wcześniejszych urządzeń bankomatowych oraz przygotowanie własnej infrastruktury związanej z dostosowaniem łączą dla nowego typu bankomatów wyposażonych w czytniki biometryczne FV. z początkiem roku 2011 rozpoczęto kolejny etap wdrożenia polegający na zebraniu wymogów banku w odniesieniu do nowego systemu InterVein, szczególnie na linii integracji systemu Inter Vein z funkcjonującym w banku

systemem finansowo-księgowym defBank. Dodatkowo utworzono trzy środowiska systemu InterVein: deweloperskie, testowe i produkcyjne.

Konfiguracja systemu biometrycznego przez integratorów firmy Wincor-Nixdorf została przygotowana według założeń zdefiniowanych przez departamenty biznesowe, bazując na obowiązujących w Banku BPS S.A. regulacjach wewnętrznych. Wypłata bankomatowa z wykorzystaniem danych biometrycznych adresowana jest do podmiotów fizycznych z uwzględnieniem zarówno klienta pojedynczego, jak i grupowego. Równocześnie system InterVein pozwala na wypłatę środków z kont uprawnionych współwłaścicieli i pełnomocników po uprzednim zarejestrowaniu się w bazie wzorców biometrycznych przechowywanych w banku w postaci zaszyfrowanego kodu. Ponadto system InterVein poprzez funkcję kompatybilności z zestawieniami (listy osobowych) w formatach używanych przez państwowie instytucje pomocowe (np. PUP, MOPS, GOPS) przygotowany jest na obsługę osób pobierających zasiłki dla bezrobotnych, bądź zasiłki pomocy socjalnej.

„Bankomaty z funkcjonalnością biometryczną wyposażone są w dyspensery monet pozwalające na wypłatę nawet niewielkich kwot w postaci bilonu”

Po skompletowaniu dokumentacji, przeprowadzeniu szeregu testów akceptacyjnych oraz szkoleniu pracowników będących użytkownikami oprogramowania, zdecydowano się na pilotażowe uruchomienie systemu. w lutym 2012 roku w dolnośląskim regionie Banku BPS S.A. podłączono do systemu 15 szt. bankomatów biometrycznych udostępniając funkcjonalność biometryczną pracownikom banku będących jednocześnie jego klientami (osoby posiadające konto debetowe w Banku BPS). Miesięczne użytkowanie systemu w ramach pilotażu pozwoliło na gruntowne jego sprawdzenie przed uruchomieniem w pozostałych placówkach bankowych i zaoferowaniem rozwiązania podstawowym klientom banku. Błędy aplikacji oraz niezgodne z założeniami banku ustawienia systemu, szczególnie w odniesieniu do części raportowej aplikacji wspoma-

gającej rozliczenie bankomatu i uzgodnienie sald dla transakcji zrealizowanych, zostały skorygowane i skonfigurowane z pierwotnymi wymaganiami banku.

W maju 2012 roku bank zakończył instalację czytników biometrycznych FingerVein we wszystkich placówkach, co pozwoliło na swobodną rejestrację klienta w każdym oddziale na terenie całej Polski. Liczba bankomatów Banku BPS wyposażonych w funkcjonalność biometryczną docelowo na koniec lipca 2012 roku wyniosła 65 szt.

Biometryczny system InterVein stanowi nie tylko nowoczesne, a wręcz rewolucyjne rozwiązanie pozwalające na łatwy, intuicyjny dostęp klienta do własnych środków poprzez sieć bankomatową z wyborem opcji wypłaty z użyciem karty lub bez karty. Główną zaletą systemu jest jednak jego niekwestionowany wysoki poziom bezpieczeństwa związany z identyfikacją właściwej osoby - właściciela rachunku, co w odniesieniu do usług bankowych otwiera przed biometrią dodatkowe możliwości łączenia związków związanymi produktami finansowymi Banku BPS S.A. proponowanymi swoim klientom.

8.1.3. Bank Spółdzielczy w Kielcach

Bank Spółdzielczy w Kielcach jest jednym z największych Banków Spółdzielczych w Polsce. w 2012 roku obchodził 110-lecie swojego istnienia. Główna siedziba Banku mieści się w Kielcach. Bank posiada na terenie województwa świętokrzyskiego 16 oddziałów, 14 filii i 5 punktów kasowych.

W 2011 r. Zarząd Banku zdecydował o zmianie modelu obsługi bankomatów i rozszerzeniu sieci urządzeń samoobsługowych o bankomato-wpłatomaty. Dotychczasowy model oparty na obsłudze transakcji wyłącznie międzynarodowymi kartami płatniczymi został uzupełniony o: obsługę gotówkowych transakcji lokalnych (wypłaty, wpłaty i wypłaty świadczeń łącznie z bilonem) i kontekstową prezentację reklam.

Zmiana modelu podyktowana była:

- Spadkiem rentowności bankomatów, spowodowanym obniżeniem interchange fee dla wypłat obcymi kartami.
- Poszukiwaniem nowych rozwiązań pozwalających na wydajniejsze wykorzystanie urządzeń, poprzez przeniesienie na nie większości operacji gotówkowych realizowanych w kasach Banku. Rozwiązań dedykowanych zwłaszcza dla klientów niekorzystających z kart płatniczych.
- Koniecznością udostępnienia usługi wypłaty świadczeń socjalnych w bankomatach (jednorazowa wypłata całości świadczenia z uwzględnieniem wypłaty bilonu), a także całodobowego przyjmowania wpłat gotówkowych na rachunki bankowe za pomocą wpłatomatów, przy wykorzystaniu lokalnych metod

uwierzytelniania tych transakcji.

- Uniezależnieniem urządzeń Banku od niedostępności centrów autoryzacyjnych (prace serwisowe, brak łączności, awarie), dzięki umożliwieniu w takich sytuacjach dokonania transakcji lokalnych.

Bank poszukiwał nowego, innowacyjnego środka uwierzytelniania lokalnych transakcji gotówkowych w urządzeniach samoobsługowych, będącego wygodną, przyjazną i bardziej bezpieczną alternatywą dla karty płatniczej. Zainteresowanie Banku wzbudziła biometryczna technologia *Finger Vein* dostarczana przez firmę Hitachi. Wiedza zdobyta w wyniku działalności grupy biometrycznej Forum Technologii Bankowych, a także sukcesy w zastosowaniu tej technologii w Banku Polskiej Spółdzielczości S.A., Podkarpackim Banku Spółdzielczym oraz tureckim Banku IS Bankası, zadecydowały o wyborze tego rozwiązania w projekcie Banku. Ta decyzja umożliwiła zaoferowanie klientom Banku innowacyjnej i bardzo bezpiecznej usługi autoryzacji transakcji lokalnych w urządzeniach Banku bez konieczności użycia fizycznego nośnika.

Bank zadecydował o wyborze komponentów do technologii biometrycznej od firmy Hitachi (czytniki bankomatowe, czytniki oddziałowe oraz serwer autoryzacyjny FV). Dostawcą i głównym koordynatorem projektu została firma NCR Polska. Dostarczyła ona 8 bankomatów-wpłatomatów (największa obecnie w województwie świętokrzyskim sieć wpłatomatowa wśród banków) i jeden bankomat. Urządzenia te posiadają dyspenser monet. Oprócz tego dostarczyła także komponenty do biometrii *Finger Vein* dla wszystkich 29 urządzeń banku. Dostawcą oprogramowania multivendorowego do urządzeń i hosta zarządzającego tymi urządzeniami (Novum Host), została firma Novum Sp. z o. o. z Łomży, w zakupionym rozwiążaniu, dostawca opracował interfejs współpracujący z komponentami biometrycznymi FV, umożliwiając uwierzytelnianie biometryczne. Przy wydatnej pomocy polskiego oddziału firmy Hitachi Europe Ltd implementacja zakończyła się pełnym sukcesem.

Realizacja Projektu „System lokalnej karty uwierzytelnianej biometrycznie w Banku Spółdzielczym w Kielcach” umożliwiła zaoferowanie klientom banku usługi karty lokalnej, co pozwala na przeprowadzanie transakcji lokalnych w urządzeniach banku:

- bez konieczności użycia nośnika fizycznego przy pomocy uwierzytelniania biometrycznego;
- przy pomocy nośnika fizycznego (karta) uwierzytelnianego biometrią lub 5 cyfrowym hasłem.

Klientowi, który wyrazi chęć korzystania z transakcji lokalnych w urządzeniach banku, przypisywana jest karta lokalna o następujących cechach:

- nie posiada ona dedykowanego nośnika fizycznego,
- ma 17 cyfrowy unikalny numer,
- przypisana jest do konkretnego rachunku bankowego,

- posiada określoną funkcjonalność, zależną od pełnomocnictwa do rachunku posiadanego przez użytkownika karty lokalnej:
 - wpłaty i wypłaty,
 - tylko wpłaty,
 - wypłata salda rachunku (zasiłki)
 - ma przypisany dzienny limit wypłat,
 - oraz sposób uwierzytelniania i blokowania karty lokalnej (palec blokujący)

Każdemu klientowi może być wydanych wiele kart lokalnych.

W przypadku uwierzytelnienia biometrycznego użytkownik karty lokalnej musi najpierw dokonać identyfikacji karty lokalnej w urządzeniu poprzez jeden z poniższych sposobów:

- Podanie przez użytkownika identyfikatora karty (będącego prostym rozszerzeniem identyfikatora użytkownika - unikalnego, znanego i łatwego do zapamiętania, wybranego przez niego w momencie uruchamiania usługi - np. numer telefonu)
- Włożenie do czytnika nośnika fizycznego (karty identyfikacyjnej) z przypisany do niego numerem karty lokalnej.



Rys.31: Naczelnik Wydziału Informatyki Banku BS Kielce (p. Janusz Kurczych) przy bankomacie biometrycznym wyposażonym w technologię *Finger Vein*

Źródło: BS Kielce

Po identyfikacji karty lokalnej w urządzeniu następuje prośba o jej uwierzytelnienie poprzez przyłożenie palca w czytniku FV urządzenia. Sam proces uwierzytelnienia trwa niecałe 2-3 sekundy. Przy testach szybkości obsługi uwierzytelnienie transakcji kartą płatniczą za pomocą pinu trwało dłużej niż użycie karty identyfikacyjnej uwierzytelnianej biometrią.

Po uwierzytelnieniu pojawia się menu z dostępnymi dla klienta operacjami, podobne jak przy transakcjach realizowanych kartą płatniczą, ale dodatkowo rozbudowane - np. o operacje wpłaty.

Serwer autoryzacyjny FV i serwer Novum Host posadowione są lokalnie w Banku. Serwer Novum Host zarządza pracą urządzeń Banku, wykorzystując centrum autoryzacyjne do autoryzacji transakcji kartami płatniczymi. Serwer autoryzacyjny FV wykorzystywany jest do uwierzytelniania biometrycznego i przechowywania wzorców biometrycznych klientów.

Klienci, którzy nie wyrażają zgody na uwierzytelnienie biometryczne, mogą autoryzować transakcje lokalne za pomocą karty identyfikacyjnej z uwierzytelnieniem 5 cyfrowym hasłem (klasyczna karta lokalna). Jest to rozwiązanie zgodne z sugestiami GŁODO, zakładającymi pełną dobrowolność decyzji klienta o wyborze biometrii. Według opinii Generalnego Inspektora Ochrony Danych Osobowych brak jednakowo płatnej alternatywy dla biometrii w tym przypadku traktowany jest, jako przymus ekonomiczny w stosunku do klienta.

Bank podniósł bezpieczeństwo transakcji lokalnych, poprzez wieloczynnikowe uwierzytelnianie. Rozwiązań oparte na podaniu identyfikatora klienta o z góry określonych charakterze np. data urodzenia albo PESEL, pomimo prawie 100% pewności biometrycznego uwierzytelnienia niesie ryzyko kradzieży tożsamości. W przypadku stanu nieświadomości klienta (nieprzytomność lub inne stany niepoczytalności), nadal będzie działać uwierzytelnienie biometryczne. Dane do identyfikacji można łatwo odczytać z dowodu osobistego, a palec blokujący może być niewystarczającym zabezpieczeniem. Bank, jako instytucja zaufania publicznego dbający o bezpieczeństwo konsumentów, musiał wziąć pod uwagę to ryzyko i proponuje klientowi samodzielny wybór identyfikatora (nie określając jego charakteru), z którego będzie korzystał w procesie identyfikacji. Klient zawsze może go zmienić w przypadku podejrzenia jego ujawnienia. Połączenie identyfikatora (to, co klient wie) z uwierzytelnieniem biometrycznym (to, kim jest), stanowi obecnie najbezpieczniejszy sposób uwierzytelnienia transakcji.

Oprogramowanie Novum Host umożliwia przeprowadzenie transakcji lokalnych w przypadku niedostępności centrum autoryzacyjnego autoryzującego transakcje kartami płatniczymi, a także w przypadku uszkodzenia łącznika teleinformatycznego, pomiędzy Bankiem a centrum autoryzacyjnym. W przypadku awarii sieci Bankomatowej Banku klienci nadal mogą korzystać z wypłat w bankomatach innych banków przy użyciu kart płatniczych.

W urządzeniach Banku następuje identyfikacja kart lokalnych klienta, a nie samego klienta. Wszystkie karty lokalne konkretnego klienta uwierzytelniamy tym samym wzorcem biometrycznym. Kartom lokalnym przy-

pisane są uprawnienia odpowiadające posiadanym pełnomocnictwom klienta do rachunków przypisanych do tych kart.

„ Za pomocą biometrii BS Kielce obsługuje też uwierzytelnianie we wpłatomatach

Za pomocą biometrii BS Kielce obsługuje też uwierzytelnianie we wpłatomatach. Transakcje realizowane kartą płatniczą, od realizowanych kartą lokalną w urządzeniach Banku różni tylko sposób autoryzacji i podmiot autoryzacyjny. Pozostała obsługa prowadzona jest przez oprogramowanie Novum Host identycznie. Nie ma konieczności rezerwowania części zasobów urządzenia wyłącznie na potrzeby danego typu transakcji. A więc nie ma konieczności podziału kaset, prowadzenia oddzielnych rozliczeń urządzeń i możliwe jest podłączenie i rozliczenie samoobsługowych recyclerów.

W I kwartale 2013 r. system był testowany pilotażowo przez pracowników Banku. Po zakończeniu tej fazy usługa została udostępniona klientom Banku. Bank planuje wkrótce wzbogacenie sieci urządzeń o samoobsługowe recyclerы wyposażone w czytniki biometryczne. Planowane jest także rozpoczęcie kampanii reklamowej zachęcającej do korzystania z urządzeń i kart lokalnych uwierzytelnianych biometrycznie. W przypadku dużego zainteresowania usługą planowana jest dalsza rozbudowa sieci urządzeń. W przypadku pojawienia się na rynku centrum autoryzacyjnego oferującego możliwość obsługi obcych, transakcji uwierzytelnianych biometrycznie w urządzeniach Banku lub obsługi biometrycznej klientów Banku w urządzeniach obcych, Bank nie wyklucza udziału w takim projekcie.

8.1.4. Powiślański Bank Spółdzielczy w Kwidzynie



Rys.32: Bankomat biometryczny w oddziale Powiślańskiego Banku Spółdzielczego w Kwidzynie

Źródło: Powiślański Bank Spółdzielczy

Łamiąc stereotypy mówiące, że nowoczesne technologie obce są bankom spółdzielczym, w czerwcu bieżącego roku Powiślański Bank Spółdzielczy w Kwidzynie, jako jedyny na Pomorzu i trzeci wśród wszystkich banków w Polsce, pilotażowo wprowadził do swojej oferty wypłaty gotówki bezpośrednio z konta poprzez bankomaty z funkcją *Finger Vein*, czyli weryfikacji danych biometrycznych. Pierwsze dwa bankomaty wykorzystujące tę technologię znajdują się w Centrali Banku przy ul. Kopernika w Kwidzynie i umożliwiają wypłatę gotówki bez użycia kart bankomatowych. Biometryczna weryfikacja danych oznacza, że nowoczesne bankomaty nie tylko nie potrzebują kart, ale również kodów PIN. W celu wypłaty pieniędzy wystarczy wpisać swoją datę urodzenia lub PESEL (tzw. wstępna weryfikacja), a następnie przyłożyć palec do czytnika znajdującego się na bankomacie. W ten prosty sposób dokonana zostanie przy użyciu wzoru naczyń krwionośnych palca (innego u każdego człowieka) ostateczna autoryzacja danych niezbędna do wypłaty gotówki. Amatorzy filmów grozy również mogą spać spokojnie – aby wypłacić pieniądze niezbędny jest żywy układ naczyń krwionośnych w palcu, nie wystarczą natomiast same linie papilarne, z których czytnik nie korzysta.

Za każdym razem, kiedy Klient będzie chciał skorzystać z bankomatu, jego palec prześwietlony zostanie przez niewidzialne i nieszkodliwe dla zdrowia światło bliskiej podczerwieni. Dzięki temu uzyskiwany będzie obraz wzoru naczyń krwionośnych palca, który będzie następnie analizowany i przetwarzany na unikalny wzorzec biometryczny. W wyniku tak indywidualnych i zaawansowanych zabezpieczeń jest to wyjątkowo bezpieczny sposób korzystania z bankomatu.



Rys.33: Pierwszy recycler biometryczny w Polsce w oddziale Powiślańskiego Banku Spółdzielczego w Kwidzynie

Źródło: Powiślański Bank Spółdzielczy

Udostępnienie usługi jest również bardzo prostą procedurą i trwa zaledwie kilka minut. Klient banku, który chciałby skorzystać z bankomatu wykorzystując *Finger Vein* powinien zgłosić się do Centrali Banku w Kwidzynie w celu pobrania wzorca biometrycznego oraz wprowadzenia go do systemu wraz z pozostałymi danymi osobowymi. Dane Klienta Banku wraz z wzorcem biometrycznym wprowadzane są jednorazowo do bazy danych, a następnie wykorzystywane przy wypłacie pieniędzy z bankomatu.

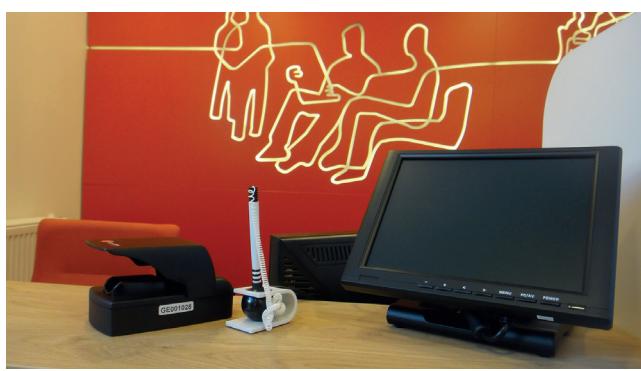
Powiślański Bank Spółdzielczy, jako pierwszy w Polsce uruchomił recycler biometryczny. Decyzja o uruchomieniu recyclera razem z biometrią nastąpiła w kwietniu 2012, a uruchomienie samego recyclera we wrześniu 2012 roku. Do tej pory Bank posiadał strefę bezobsługową gdzie znajdowały się dwa urządzenia Wincora

PC2000xe i PC3000xe czyli bankomat i wpłatomat. Ze względu na duże obciążenie urządzenia te musiały być codziennie obsługiwane, czyli bankomat musiał być doładowywany a wpłatomat rozładowywany. Poprzez zastosowanie recyclingu (Recycler CINEO firmy Wincor Nixdorf) obciążenie na tym urządzeniu nadal jest bardzo duże z tą różnicą, że urządzenie wymaga obsługi raz lub dwa razy w miesiącu. Biometria w Banku ma nadal status pilotażu - Bank obecnie korzysta z rozwiązaniu firmy Novum, jednakże planuje podłączenie do hosta biometrycznego w IT Card.

Wprowadzanie nowoczesnych technologii oraz dostosowywanie oferty do wciąż wzrastających oczekiwania i wymagań Klientów to główne priorytety Powiślańskiego Banku Spółdzielczego w Kwidzynie. Cieszy fakt, że również tym razem z sukcesem udało się połączyć zapotrzebowanie rynku z funkcjonowaniem unikatowego systemu obsługi klienta, wyznaczającego nowy trend w bankowości elektronicznej, z czego nawet wielkie, komercyjne placówki bankowe mogą brać przykład.

8.1.5. Bank BPH S.A.

BPH S.A. to jeden z największych banków komercyjnych w Polsce. Jako pierwszy bank w Europie BPH wprowadził biometrię do swoich oddziałów. W styczniu 2013 zakończyło się wdrożenie pierwszej generacji projektu „*Finger Vein*”, wprowadzającego w oddziałach Banku BPH uwierzytelnianie biometryczne oparte na unikalnym wzorcu naczyń krwionośnych wewnętrz ludzkiego palca. Dla klientów Banku BPH oznacza to, że ta nowoczesna i bezpieczna technologia jest od dnia dostępna we wszystkich 285 oddziałach Banku, na ponad 1700 stanowiskach.



Rys.34: Stanowisko biometryczne w oddziale BPH

Źródło: Hitachi

Bank BPH spośród różnych technologii biometrycznych wybrał technologię *Finger Vein*, jako najbardziej bezpieczną oraz zapewniającą przestrzeganie prywatności Klientów w najpełniejszym zakresie. Technologia ta wykorzystuje do identyfikacji klienta wzór naczyń krwionośnych palca. Wzór naczyń krwionośnych

w palcu jest unikalny dla każdego człowieka, nawet dla bliźniąt jednojajowych. Układ naczyń krwionośnych w palcu człowieka nie zmienia się z wiekiem. Nie ma też możliwości wykorzystania palca, w którym nie płynie krew (obciętego palca).

W ramach projektu każdy z oddziałów Banku BPH, każde stanowisko, zostało wyposażone w oddziałowy czytnik biometryczny *Finger Vein* oraz monitor kliencki. Czytnik pobiera oraz porównuje wzorce pobrane podczas potwierdzania tożsamości Klienta i autoryzacji transakcji z wzorcami przypisanymi do Kartotek Klientów. Monitor kliencki służy do wyświetlania danych transakcji, które klient będzie akceptował poprzez przyłożenie palca do czytnika. Na monitorze wyświetlane są również filmy instruktażowe na temat użycia technologii biometrycznej.

Technologia *Finger Vein* służy podniesieniu poziomu bezpieczeństwa, w tym zwiększeniu ochrony środków klientów banku, podniesieniu poziomu transparentności dokonywanych przez klienta czynności bankowych.

Dzięki wdrożeniu technologii FV w Banku BPH procesy potwierdzania tożsamości klienta i autoryzacji transakcji przebiegają zgodnie z poniższym opisem:

1. Potwierdzenie tożsamości klienta

Klient, przychodzący do oddziału Banku BPH podaje nazwisko, nr PESEL, CIF (nr identyfikacji w Banku BPH) lub inny unikalny identyfikator. Pracownik sprawdza w systemie, czy na poziomie Kartoteki Osobowej Klient posiada znaczek *Finger Vein*. Jeżeli tak, to następuje weryfikacja tożsamości Klienta poprzez przyłożenie palca do czytnika biometrycznego. Czytnik biometryczny porównuje pobrany wzorzec biometryczny układu naczyń krwionośnych palca klienta ze wzorcem referencyjnym znajdującym się w bazie Banku. Jeżeli w wyniku porównania nastąpi zgodność wzorców, wtedy na ekranie Klienta jak i doradcy pojawi się komunikat - weryfikacja klienta zakończona sukcesem.

2. Autoryzacja transakcji kasjerskich

Jeśli klient chce wykonać transakcję kasową, czyli wpłatę, przelew, wypłatę itp., doradca wprowadza do systemu dane transakcji. Po wpisaniu danych transakcji następuje ich wyświetlenie na ekranie klienckim. Klient sprawdza poprawność danych (numery kont, kwotę transakcji itp.). Po sprawdzeniu poprawności Klient przykłada palec do czytnika biometrycznego, jako potwierdzenie. Czytnik biometryczny porównuje pobrany wzorzec biometryczny układu naczyń krwionośnych palca Klienta z wzorcem referencyjnym znajdującym się w bazie banku. Jeżeli w wyniku porównania nastąpi zgodność wzorców wtedy doradca przykłada palec do czytnika i akceptuje transakcję. Autoryzacja transakcji z wykorzystaniem FV jest dostępna w sieci oddziałów Banku BPH od 3 kwartału 2013 roku. Dzięki temu czas obsługi klienta został zredukowany o 20%.

„ Po wdrożeniu ekranu kasjera zaobserwowano gwałtowny wzrost bazy klientów biometrycznych

Wyzwaniem w projekcie było zaplanowanie wdrożenia na produkcję, w całej sieci oddziałów w kontrolowany sposób tak, by nie zakłócić pracy oddziałów i nie przekroczyć budżetu. W tym celu zaplanowano pilotaż na małej grupie oddziałów, w czasie którego „szlifowano” rozwiązanie i procedury oraz zbierano doświadczenia, które pozwoliły lepiej zaplanować pełne wdrożenie. Zaplanowano szczegółowo logistykę, komunikację i wsparcie techniczne oraz przygotowano precyzyjną procedurę instalacji. Rozdzielono w czasie instalacje sprzętu Finger Vein w placówkach od faktycznego rozpoczęcia pracy z tym rozwiązaniem przez oddziały. Zostały również zaplanowane szkolenia w placówkach z użyciem zainstalowanych już tam czytników Finger Vein. Dzięki temu pierwsze użycie systemu w oddziale odbywało się pod okiem doświadczonych szkoleniowców z Pionu Operacji i Pionu Sprzedaży. Dzięki takiemu ostrożnemu i planowemu podejściu, styczniowe rozpoczęcie codziennej pracy z Finger Vein w całej sieci oddziałów przebiegło planowo i spokojnie.

W ramach pierwszej generacji projektu „Finger Vein” zostało zrealizowane 95% wszystkich prac i wydatków zaplanowanych w projekcie. Z dnia na dzień narasta baza wzorców biometrycznych klientów. W fazie pierwszej projektu, która umożliwiała jedynie biometryczną weryfikację tożsamości klientów uzyskano bazę 50 000 aktywnych klientów biometrycznych. Po wdrożeniu ekranu kasjera zaobserwowano gwałtowny wzrost bazy klientów biometrycznych. Poziom rejestracji klientów wzrósł nawet do 7000 klientów tygodniowo. Działające rozwiązanie, w połączeniu z dużą ilością korzystających z niego klientów, stanowi doskonały punkt wyjścia do dalszych inicjatyw wykorzystujących uwierzytelnianie biometryczne.

Na przyszły rok, tj. 2014 Bank planuje wprowadzenie potwierdzeń Finger Vein dla niektórych rodzajów umów zawieranych z klientem oraz wdrożenie biometrii Finger Vein w sieci partnerskiej, w której dotychczas stosowano kartę identyfikacyjną. Bank BPH jest również zainteresowany zastosowaniem biometrii w bankomatach.

Korzyści z wdrożenia projektu Finger Vein w BPH:

1. Zwiększenie **Bezpieczeństwa** transakcji bankowych, które wykonują nasi Klienci w oddziałach banku, tj.:
 - Odwiedzając oddziały BPH, klienci nie muszą używać żadnego dokumentu w celu identyfikacji. Nie jest potrzebna również weryfikacja podpisu odręcznego. Ryzyko błędnej identyfikacji Klienta jest wyeliminowane.
 - Bank chroni środki swoich klientów w oddziale banku przed nieuprawnionym dostępem osób trzecich.
 - Wzorzec biometryczny palca jest niemożliwy do skopiowania – jest unikalny nawet dla bliźniat jednojajowych.
 - Technologia oparta na wzorze naczyń krwionosnych palca jest najbezpieczniejszą metodą identyfikacji (bardziej niezawodną niż skanowanie siatkówki oka lub linii papilarnych).
2. Zwiększenie **Wygody** i oszczędność **Czasu** klientów BPH w trakcie wizyt w oddziałach banku:
 - Klienci BPH nie muszą nosić przy sobie karty płatniczej, dowodu osobistego, pamiętać kodu PIN ani żadnego innego dokumentu przy dokonywaniu wszystkich operacji w oddziałach.
 - Klienci nie muszą pamiętać wzoru podpisu złóżonego na bankowej Karcie Wzorów Podpisu.
 - Identyfikacja Klientów BPH przebiega w sposób wygodny i sprawny – przyłożenie palca do czytnika powoduje identyfikację każdego klienta w chronionej bazie danych. Nie ma konieczności wyszukiwania Klientów po takich kryteriach jak nr PESEL, nr dowodu osobistego, nazwisko.

Poprzez wdrożenie biometrii Finger Vein, Bank BPH:

- Ograniczył ilość papieru występującego w procesach bankowych,
- Eliminuje ryzyko związane z nieuprawnionym dostępem do rachunków,
- Skracą czas weryfikacji tożsamości Klienta,
- Ogranicza do zera błędную identyfikację Klienta.

8.1.6. Getin Bank

Getin Bank jest detaliczną częścią ogólnopolskiego Getin Noble Banku, należącego do najbardziej dynamicznie rozwijających się instytucji finansowych w Polsce. Oferta Getin Noble Banku jest skierowana do klientów indywidualnych, małych i średnich firm, samorządów oraz dużych korporacji. z usług Banku korzysta ponad 2,2 mln Klientów, a produkty są dostępne w ponad 550 oddziałach własnych i franczyzowych oraz w szerokiej sieci pośredników. Getin Noble Bank jest drugim największym bankiem z większościowym polskim kapitałem.



Rys.35: Nowe oddziały Getin Bank wykorzystujące biometrię

Źródło: Getin Bank

Getin Bank jest w tej chwili jednym z najnowocześniejszych banków w Polsce i może pochwalić się innowacyjnymi wdrożeniami w skali nie tylko krajowej, ale również międzynarodowej. Jednym z takich wdrożeń, jest wprowadzenie w nowej sieci oddziałów uwierzytelniania biometrycznego opartego na technologii *Finger Vein*. Biometria *Finger Vein* jest technologią opracowaną przez firmę Hitachi, która wykorzystuje wzorzec naczyń krwionośnych palca pobrany w procesie naświetlania światłem bliskiej podczerwieni do weryfikacji tożsamości. Poprzez zapewnienie maksymalnie możliwej precyzji i szybkości operacji, technologia ta jest najbardziej zaawansowanym sposobem uwierzytelniania na świecie w różnych sektorach rynku, w tym w bankowości. *Finger Vein* jest unikalnym rozwiązaniem, które wykorzystuje cechy ludzkie znajdujące się wewnątrz ciała i niewidoczne na zewnątrz. Jest więc nową generacją biometrii, która jest odporna na próby falsyfikacji i kradzieży tożsamości.



Rys.36: Czytnik biometryczny *Finger Vein* w Getin Bank

Źródło: Hitachi

Getin Bank zdecydował się na biometrię *Finger Vein* ze względu na to, że opiera się ona na unikalnej strukturze naczyń krwionośnych palca i uważana jest za najbezpieczniejszą metodę uwierzytelnienia w bankowości. Dodatkowo wykorzystywana może być nie tylko w oddziałowej obsłudze klienta, ale również, np. w bankomatach (w tej chwili jest ok. 80 tys. biometrycznych bankomatów na świecie), płatnościach czy nawet w bankowości internetowej. Jest to technologia o największych referencjach w światowej bankowości, powszechnie stosowana m.in. w Japonii, coraz bardziej popularna również np. w Turcji, Brazylii czy Polsce.

W Getin Banku system uwierzytelniania *Finger Vein* funkcjonuje w wybranych nowych placówkach od stycznia 2013 r. Wprowadzone rozwiązanie to wyjście naprzeciw oczekiwaniom Klientów nastawionych na nowoczesne rozwiązania i skok technologiczny umożliwiający Klientom skorzystanie z bezpiecznego, innowacyjnego i wygodnego sposobu uwierzytelniania. Weryfikacja tożsamości Klienta następuje wyłącznie w oddziale Banku, po podaniu przez Klienta informacji, umożliwiających jego identyfikację. Pozytywna weryfikacja tożsamości Klienta stanowi potwierdzenie jego tożsamości i wyłącza konieczność okazywania dokumentu tożsamości (np. dowodu osobistego czy paszportu).

W Getin Noble Bank ścieżka decyzyjna jest skrócona do niezbędnego minimum, co pozwoliło na bardzo szybkie zrealizowanie wdrożenia rozwiązania *Finger Vein* w nowych Oddziałach Getin Banku. We wrześniu 2012 r. została przedstawiona oferta Konsorcjum Hitachi - Wincor Nixdorf dla wdrożenia technologii *Finger Vein* w oddziałach Getin Banku, na początku października 2012 r. został podpisany list intencyjny, a już pod koniec października 2012 r. umowa wdrożeniowa. Prace implementacyjne rozpoczęły się w drugiej połowie listopada 2012 r., a już 25.01.2013 r. został przez Bank podpisany protokół odbioru i 30.01.2013 r. został uruchomiony pierwszy oddział Getin Banku z czytnikami biometrycznymi (oddział we Wrocławiu).

Główne zalety rozwiązania:

- biometria *Finger Vein* to szybki, bezpieczny i wygodny sposób uwierzytelniania klientów w oddziale Banku - proces uwierzytelniania trwa jedynie ok. 1,5 sekundy,
- integracja z wewnętrznym systemem banku zapewnia skrócenie procesu obsługi klienta w oddziale Banku,
- *Finger Vein* to bezpieczniejsza metoda uwierzytelnienia klienta niż wykorzystanie tradycyjnych metod (np. weryfikacja dowodu osobistego),
- urządzenia biometryczne *Finger Vein* są bardzo łatwe i przyjazne w obsłudze.

Do końca roku 2013 r. planowane jest uruchomienie 30 nowych oddziałów Getin Banku z usługą uwierzytelniania *Finger Vein*. Dodatkowo kolejną planowaną fazą rozwoju funkcjonalności systemu biometrycznego w Getin Banku, jest wdrożenie biometrycznego podpisu elektronicznego do końca 2013 roku. W przypadku wprowadzenia przez Bank takiej funkcjonalności, Klient będzie miał możliwość składania oświadczeń woli z wykorzystaniem danych biometrycznych w zakresie autoryzacji zleceń płatniczych oraz składania innych dyspozycji i zawierania nowych umów bez konieczności składania podpisu odręcznego. Możliwość składania dyspozycji oraz zawierania umów na podstawie podpisu biometrycznego pozwoli na usprawnienie i podniesienie bezpieczeństwa zawierania umów pomiędzy Bankiem, a Klientem oraz wyeliminowanie papierowego obiegu dokumentów, co będzie również przyczyniało się do ekologicznego aspektu funkcjonowania banku.

8.1.7. Asekuracja

Asekuracja Cash Handling Sp. z o.o. jest wiodącą firmą na rynku polskim w zakresie przeliczania, sortowania i transportowania wartości pieniężnych. Jest także pierwszą firmą w Polsce, która wykorzystuje biometryczny system służący do identyfikacji i uwierzytelniania pracowników pobierających gotówkę z sortowni. Wykorzystywana technologia *Finger Vein* wdrożona została już w warszawskich sortowniach firmy oraz w warszawskim oddziale konwojowym.

Kierownik grupy konwojowej odpowiedzialny jest za rejestrowanie nowych konwojentów i bieżącą modyfikację danych o swoich pracownikach np. zwolnienie z pracy. Pracownicy sortowni odpowiedzialni są za wykonanie biometrycznego uwierzytelnienia konwojentów, którzy przyjeżdżają do sortowni po odbiór gotówki. Wdrożenie systemu pozwoliło znacznie zwiększyć bezpieczeństwo sortowni i wyeliminowało zagrożenie wynikające z ewentualnej kradzieży tożsamości i „podszwania się” pod inną osobę przy wykorzystaniu podrobionych lub skradzionych dokumentów.

Asekuracja planuje rozszerzenie wykorzystywanej technologii i wdrożenie jej we wszystkich punktach, które odpowiedzialne są za przekazywanie gotówki. W ten sposób uruchomi największy i najbezpieczniejszy tego typu system w Polsce. W ramach rozwoju systemu planowane jest objęcie jego działaniem także innych firm sortujących i transportujących gotówkę. Dzięki temu pracownicy jednej firmy będą mogli być uwierzytelniani biometrycznie w sortowniach wszystkich innych firm na rynku.

8.2. Wdrożenia zagraniczne

8.2.1. Turcja - IS Bankasi



Rys.37: Bankomat IS Banku z usługą Biyokimlik

Źródło: Hitachi

W 2010 roku **IS Bankasi A.S.** rozpoczął wdrożenie największego projektu biometrycznego w Europie. IS Bankasi A.S. to największy bank komercyjny w Turcji posiadający aktywa w wysokości ponad 100 mld. USD. Posiada 17 mln. klientów (14 mln. aktywnych klientów), sieć 4700 bankomatów (Bankamatik), 1210 oddziały bankowe. IS Bank posiada też oddziały zagranicą w tym przede wszystkimi w Niemczech, Rosji i na Cyprze. IS Bank od początku istnienia jest liderem innowacji w tureckim sektorze bankowym. IS Bank wprowadził, bowiem m.in. pierwszy bankomat, pierwszą bankowość elektroniczną, pierwszy system iVR. IS Bank został również pierwszym bankiem w Turcji, który korzysta z biometrii w swoich kanałach sprzedaży.

Przyczyną zainteresowania banku IS biometrią była zwiększająca się obawa klientów banku wobec kradzieży tożsamości i fraudów w bankomatach. IS Bank posiada największą w Turcji sieć bankomatów, która jednak miała dosyć niskie obciążenie (tj. liczbę transakcji). IS Bank poszukiwał technologii, która będzie łatwa w użyciu (dla wszystkich typów klientów), bezpieczna oraz która będzie umożliwiała przeniesienie znaczącej części operacji z oddziału do bankomatu. Po wewnętrznych analizach bank zdecydował o wybraniu technologii *Finger Vein*. Projekt pilotażowy rozpoczął się w lipcu 2010 roku wraz z dedykowaną kampanią telewizyjną. Bank

brak przykład z wdrożeń w Polsce, goszcząc na wizycie referencyjnej m.in. oddziału banku PBS i BPS.



Rys.38: POS banku IS Bankası z biometrią Finger Vein

Źródło: IS Bankası A.S.

Obecnie IS Bankası zaimplementował ponad 3000 bankomatów z biometrią Finger Vein. Biometria używana jest w zastępstwie kodu PIN przy operacji kartowej, jak i do uwierzytelniania transakcji bezkartowej. Usługa wypłaty biometrycznej (Biyokimlik) jest najpopularniejszą metodą wypłaty bezkartowej z bankomatów w Turcji. Już rok po wdrożeniu (10.2011) z biometrii korzystało ponad 100 000 klientów.

W 2011 roku IS Bank rozszerzył swój projekt biometryczny o płatności biometryczne. IS Bank posiada największą w Turcji sieć akceptacji (ponad 300 tysięcy terminali POS). Od 2011 IS Bank doposała swoje terminale POS w czytniki biometryczne Finger Vein, aby umożliwić swoim klientom płatności bezkartowe. W 2012 roku IS Bank otrzymał nagrodę „Innowacji w bankowości” od magazynu „Banker”.

8.2.2. Turcja - Ziraat Bankası

W 2010 roku bank Ziraat Bankası A.S. ogłosił rozpoczęcie wdrożenia bankomatów z zamkniętym obiegiem gotówki (ang. recycler) z uwierzytelnianiem biometrycznym. Ziraat Bank to największy państwowy bank w Turcji ze 100 mld. USD aktywów. Ziraat posiada ponad 32 mln. klientów, sieć 2700 bankomatów oraz ponad 1200 oddziałów.



Rys.39: Bankomat Ziraat Bankası z biometrią Palm Vein

Źródło: MIG

Bank szukał nowocesnej i bezpiecznej metody uwierzytelniania, która mogłaby być zaimplementowana w recycleraх oraz wirtualnych placówkach bankowych. W sierpniu 2010 roku, chińska firma GRG wygrała przetarg na dostawę 1500 recycleraх do banku Ziraat. Po przeprowadzeniu prac badawczych i testach zdecydowano się doposażyć recyclery w technologię Palm Vein. W czerwcu 2011 roku wdrożono pierwsze 900 recycleraх z biometrią PV. Planowano wdrożyć również 1400 stanowisk rejestracyjnych w oddziałach Ziraat Bank.



Rys.40: Biometryczny VTM w banku Ziraat

Źródło: Ziraat Bankası

Równocześnie bank rozpoczął wdrożenie wirtualnych oddziałów bankowych (VTM), jako pierwszy bank na świecie. Klienci mogli wykonać większość operacji oddziałowych w samoobsługowym urządzeniu. VTMy również zostały wyposażone w czytniki biometryczne. Niestety od początku projekt w Ziraat Bank zmagał się z wieloma problemami. Wśród głównych problemów bank wymieniał trudności z zebraniem bazy wzorców i zachęceniem klientów, oraz brakiem zaznajomienia klientów Banku z tą technologią. Po części z braku odpowiednich mechanizmów edukacyjnych, odnotowano bardzo dużą ilość aktów vandalizmu (np. czytniki były przypalane papierosami). z perspektywy czasu, projekt mimo dużych nakładów nie odniósł oczekiwanej sukcesu. Ze względu na problemy technologiczne do dzisiaj projektu nie rozszerzono o inne typy bankomatów Banku. z dostępnych informacji wynika, że usługa biometrii mimo 2 lat od wdrożenia nie jest dzisiaj aktywna.

8.2.3. Turcja - Vakif Bank



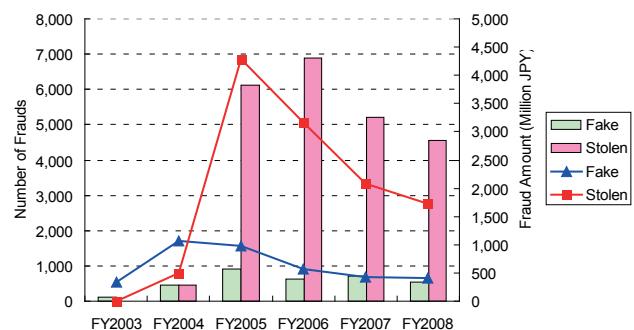
Rys.41: Bankomat w VakifBank z technologią Finger Vein

Źródło: MIG

Kolejnym bankiem tureckim, który zdecydował się na wdrożenie biometrii był **VAKIF Bankası**. Vakif Bank to szósty największy bank w Turcji. Vakif posiada 9 mln. klientów i sieć ponad 2300 bankomatów oraz 650 oddziałów. Vakif prowadził testy biometrii już od 2009 roku. Po prawie 2 latach testów, bank zdecydował o wyborze technologii *Finger Vein*. w ramach pilotażu bank wdrożył 15 bankomatów biometrycznych, w tym bankomatów na lotnisku w Istanbule. Dostawcą banko-

matów była firma NCR. w latach 2011-2012 Vakif Bank przygotowywał projekt pełnego rolloutu na wszystkie bankomyty (2300 szt.) . Obecnie ze względów budżetowych zdecydowano się na czasowe wstrzymanie projektu. Miały na to wpływ również prace administracji rządowej nad wprowadzeniem dowodu biometrycznego. Do dzisiaj jednak nie wybrano technologii biometrycznej (rozważano *Finger Vein*, *Palm Vein* i odcisk palca), a projekt dowodu tymczasowo wstrzymano.

8.2.4. Japonia - największy projekt biometryczny świata



Rys.42: Spadek przestępstw kartowych po wdrożeniu uwierzytelniania biometrycznego

Źródło: FSA Japan (Financial Services Agency)

Największy projekt biometryczny w światowej bankowości miał miejsce w Japonii. w latach 2004 - 2005 Japonia zmagała się z drastycznym wzrostem przestępstw kartowych, przede wszystkich związanych ze skimmingiem (kradzieżą danych z karty w celu nanieśienia ich na inne karty do nieautoryzowanych wypłat z bankomatów). Czarę goryczy przełał skandal na ekskluzywnym polu golfowym, gdzie zeskimmowane karty prezesów czołowych banków japońskich. Wzrastający niepokój społeczny oraz zmiany regulacji bankowych (odpowiedzialność za straty w wyniku sfałszowanych transakcji została przerzucona z klientów na banki) wymusił na bankach japońskich inwestycje w nowoczesne metody zabezpieczeń. Rząd japoński apelował do instytucji finansowych o zwiększenie poziomu bezpieczeństwa i wdrożenie biometrycznego uwierzytelniania do transakcji bankomatowych i tych realizowanych w placówce bankowej. Ze względu za brak akceptowalności społecznej, zrezygnowano z wykorzystania najbardziej znanej biometrii, tj. biometrii odcisku palca (ang. *Finger Print*). Zwróciło się do największych firm technologicznych, które miały opracować nową technologię biometryczną, która miała łączyć bezpieczeństwo, użyteczność i ochronę prywatności. Równocześnie rząd japoński przeprowadził zmiany w prawie (*data privacy laws*), które pozwoliły na użycie biometrii do uwierzytelniania transakcji bankomatowych.



Rys.43: Bankomat z uwierzytelnianiem *Palm Vein* w Bank of Tokyo Mitsubishi Ufj

Źródło: Mitsubishi

Ostatecznie wybrano dwie technologie, które obecnie dominują na rynku japońskim: *Finger Vein* (Hitachi) i *Palm Vein* (Fujitsu). Pierwszym bankiem, który wdrożył biometrię był **Bank of Tokyo-Mitsubishi UFJ**, jeden z największych banków japońskich. Wybrał on biometrię naczyń krwionośnych dloni (*Palm Vein*). Czytniki *Palm Vein* zostały zainstalowane na 6000 bankomatów banku. Mimo to inne czołowe banki japońskie takie jak **Mizuho Bank, Bank of Mitsui Sumitomo, Resona Bank, Bank of Kyoto** czy też największy bank japoński tj. **Japan Post Bank** wybrało biometrię naczyń krwionośnych palca (ang. *Finger Vein*), przede wszystkim ze względu na większą praktyczność rozwiązania. Obecnie 81% banków korzysta właśnie z technologii *Finger Vein*, a nie z *Palm Vein* (ok. 9%). z biometrii *Finger Vein* korzystają również banki zagraniczne, takie jak **CITI Bank** czy też **HSBC**.



Rys.44: Bankomat/VTM z uwierzytelnianiem *Finger Vein* w CITI Bank (japonia)

Źródło: Hitachi

Już w 2005 roku zainstalowano w Japonii 34 000 bankomatów biometrycznych i wydano milion inteligentnych kart chipowych zawierających wzorce biometryczne. W 2009 roku liczba bankomatów biometrycznych wzrosła do ponad 75 tysięcy. Według danych Związku Banków Japońskich liczba użytkowników biometrii w bankach wzrosła w 2011 roku do 44 milionów. W 2012 roku

w Japonii wdrożonych jest ponad 76 000 bankomatów z technologią *Finger Vein*.

Głównym zastosowaniem biometrii w japońskiej bankowości są bankomaty

Cechą charakterystyczną projektu w Japonii był sposób przechowywania i porównywania wzorców biometrycznych. Ze względu na bardzo rygorystyczne przepisy dotyczące przetwarzania danych biometrycznych, zapisywano je i porównywano na karcie inteligentnej. W Japonii wydawane były bowiem karty multiaplikacyjne (Multos, Java), które umożliwiały wgranie aplikacji biometrycznych. Takie rozwiązanie zapewnia najwyższe bezpieczeństwo i ochronę prywatności (wzorce referencyjne nigdy nie opuszczają karty). Dzięki takiemu rozwiązaniu można też osiągnąć większy zasięg usług biometrycznych i kompatybilność. Np. klienci banku Resona mogą korzystać z bankomatów biometrycznych banku Mizuho bez konieczności przełączania baz danych. Mimo to przez zastosowanie dwóch różnych technologii biometrycznych nie osiągnięto pełnej kompatybilności. Dlatego też niektóre banki stosujące mniejszościową technologię (*Palm Vein*) umożliwiają swoim klientom zapis dwóch rodzajów danych biometrycznych (także *Finger Vein*), aby jak najbardziej udostępnić klientom możliwość korzystania z usług biometrycznych. Podjęcie „kartowe” nie sprawdziło się jednak w Europie. Tutaj nawet dzisiaj, banki nie stosują drogich kart multiaplikacyjnych, co uniemożliwia wgranie aplikacji biometrycznej. Dlatego też dominują systemy przechowujące dane biometryczne w bezpiecznych systemach centralnych, a porównujące w czytniku biometrycznym bądź na serwerze. Kolejną różnicą jest sposób wykorzystania biometrii. W Japonii dominuje 3-stopniowe uwierzytelnianie poprzez kartę, kod PIN i biometrię. W Europie tak długi proces byłby niedopuszczalny. Dlatego też biometria w Europie pozycjonowana jest jako zastępstwo kodu PIN, a nawet karty (wyплатy bezkartowe).

Głównym zastosowaniem biometrii w japońskiej bankowości są bankomaty. Dopiero w ostatnich latach banki japońskie rozszerzają możliwości wykorzystania biometrii. Banki Resona i Bank of Kyoto wdrażają oddziały biometryczne, w których można uwierzytelniać operacje oddziałowe przy pomocy karty i biometrii. W niektórych bankach (np. Resona) bardzo popularne są bezpieczne skrytki depozytowe z uwierzytelnianiem biometrycznym.

8.2.5. Japonia - Resona Bank

Resona Bank, to grupa instytucji finansowych składająca się z trzech banków: Resona Bank Ltd., Saitama Resona Bank Ltd. oraz Kinki Osaka Bank Ltd., kontrolowanych przez Resona Holding Ing. Grupa Resona znana jest z wysokiej jakości usług i innowacyjności. Resona posiada sieć 583 oddziałów i 4250 bankomatów oraz 2,9 mln aktywnych kart płatniczych. Resona jest obecnie najbardziej innowacyjnym bankiem japońskim.



Rys.45: Bankomat biometryczny w Resona Bank

Źródło: Hitachi

Resona, podobnie jak inne banki japońskie miała mało wydajny sposób obsługi klientów, który w rezultacie prowadził do frustracji klientów, długich kolejek i wydłużonego czasu operacji bankowych przez wysoki stopień biurokracji. Bank przeprojektował i wdrożył zupełnie nową koncepcję swoich oddziałów, która miała na celu obniżenie kosztów oraz zwiększenie wydajność i poprawienie jakości obsługi klientów. Dla zwiększenia wydajności wprowadzono strefy szybkiej obsługi (ang. *Zero, Waiting Time*), wyeliminowano papier i gotówkę podczas obsługi przez konsultanta. Dodatkowo uruchomiono urządzenia „QuickNavi”, czyli specjalnie zaprojektowane bankomaty biometryczne, które w wydajny sposób obsługują standardowe operacje gotówkowe, do tej pory obsługiwane wyłącznie przez pracownika banku. „QuickNavi” wyposażony został w specjalny system, który miał na celu podpowiadać i pomagać klientom podczas przeprowadzania standardowych operacji gotówkowych. W ramach rozwoju oddziałów Resona wprowadził też innowacyjne stanowiska obsługi klienta, przy którym wszelkie operacje są dokonywane na ekranach dotykowych, a operacje są uwierzytelniane biometrycznie zarówno przez klienta i pracownika banku. Oddziały wyposażono w Bezpieczne Skrzynki Depozytowe (BSD) wyposażone w czytniki biometryczne. Pierwszy innowacyjny oddział otwarto w 2007 roku w centrum Tokio. Obecnie takie rozwiązania masowo stosuje się także w pozostałych oddziałach Resony.



Rys.46: Bezpieczna skrytka depozytowa (BSD) w oddziale Resona Bank w Tokio

Źródło: Hitachi

Resona to jeden banków, który masowo wdrożył biometrię *Finger Vein*. Jest to pierwszy bank w Japonii, który wprowadził biometrię nie tylko w bankomatach, ale w wielu usługach banku. Klienci Resona Bank używają jednej, biometrycznej karty płatniczej do obsługi zarówno transakcji bankomatowych, oddziałowych jak i obsługi Bezpiecznych Skrzynek Depozytowych (BSD). Dzięki takiemu rozwiązaniu bank promuje z usługi bezpiecznej biometrii bankowej, zachęca do odwiedzania swoich oddziałów, a także stara się upowszechnić korzystanie z BSD. Klienci banku są identyfikowani przez konsultanta przy użyciu karty, następnie autoryzacja odbywa się przy użyciu biometrii FingerVein. Od wieku lat Resona Bank ponosi duże nakłady, aby podnieść rozpoznawalność i użyteczność biometrii w bankowości. Aby nakłonić swoich klientów do masowego jej wykorzystania, Resona stosuje wiele usprawnień takich jak natychmiastowe wydawanie kart biometrycznych w oddziale banku, jeśli klient zgodzi się stosować biometrię. Resona, jako pierwszy bank w Japonii wprowadził biometrię zamiast kodu PIN. Teraz wszelkie operacje autoryzowane są tylko przy pomocy biometrii, a nie tak w innych bankach (PIN + biometria). W 2008 roku Resona Bank zainstalował bankomaty biometryczne *Finger Vein* we wszystkich zrzeszonych oddziałach banku. Resona Bank instaluje również bankomaty w niezrzeszonych oddziałach: w 2007 roku było to tylko 1,8% bankomatów, jednak w 2008 było to już 23,1%. Resona posiada 3750 bankomatów biometrycznych z *Finger Vein*. Ponad 40% nowych klientów korzysta aktywnie z biometrii.

8.2.6. Brazylia - Banco de Bradesco

Brazylijski bank **Banco de Bradesco** to drugi największy bank w Brazylii i jeden z największych banków świata. Bank wdrożył największy system uwierzytelniania biometrycznego w Ameryce Południowej, implementując czytniki biometrycznego w 90% ze swojej sieci 35 000 bankomatów. Czynnikiem, który wpłynął na podjęcie przez Banco de Bradesco decyzji o wprowadzeniu technologii biometrycznej do bankomatów było podniesienie stopnia bezpieczeństwa przeprowadzanych transakcji na bankomacie. Obecnie biometrii w Banco de Bradesco używa ponad 10 milionów klientów.



Rys.47: Bankomat biometryczny w Banco de Bradesco

Źródło: NCR

Mimo, że w Ameryce Południowej najbardziej popularną biometrią (także wśród bankowości) jest biometria odcisku palca, wybór padł na biometrię naczyń krwionośnych dłoni. Miało na to wpływ bezpieczeństwo i higiena użytkowania. Projekt w Banco de Bradesco jest największym projektem wykorzystującym biometrię *Palm Vein* na świecie (liczba bankomatów i użytkowników jest większa nawet niż w Japonii, gdzie *Palm Vein* jest w mniejszości i został zdominowany przez technologię *Finger Vein*). Czytniki biometryczne PalmSecure (FAT13M1S1) zaimplementowano w sieci bankomatów, zarówno na bankomatach NCR (NCR SelfServ22) jak i Wincor Nixdorf. Aby zapewnić niski poziom fałszywych odrzuceń (FRR) wbudowano specjalne podstawki przytrzymujące dłoń w stałej pozycji. Firma Wincor Nixdorf przygotowała specjalny typ bankomatu, w którym można było umieścić tak duży czytnik. W systemie Banku Bradeco dane biometryczne po pobraniu przez czytnik są porównywane na serwerze. Dodatkowym czynnikiem zabezpieczającym proces uwierzytelniania klienta jest wbudowany w czytnik detektor pulsu, który uniemożliwia pobranie próbki z martwego ciała. W banku została wprowadzona zasada, że wszystkie nowo instalowane bankomaty w Banco de Bradesco muszą być wyposażone w czytnik hand vein.

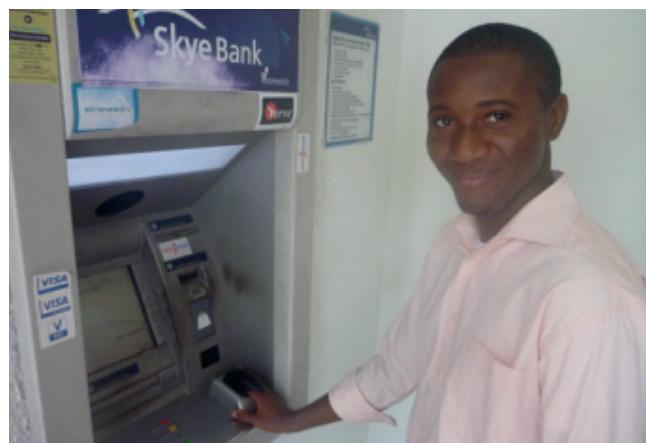
W chwili obecnej użytkownik musi dodatkowo autory-

zować się przy pomocy PINu, ale prowadzone są próby pilotowe rozwiązania niewymagającego podawania PINu.

8.2.7. Nigeria

Nigeria to najludniejszy kraj Afryki (oficjalnie ponad 175 mln obywateli). Nigeria, a dokładniej Lagos jest siedzibą największych banków afrykańskich, m.in. United Bank of Africa (UBA). Oficjalnie na terenie Nigerii funkcjonuje 20 banków, 8000 bankomatów i 6000 oddziałów bankowych. Nie jest to liczba oszałamiająca, biorąc pod uwagę szacowaną liczbę ludności na ponad 200 mln ludzi. Istnieje ok. 40 mln kont, z czego tylko 13 mln to realnie aktywne konta.

Biometria to obecnie bardzo gorący problem w nigeryjskiej bankowości. Sektor bankowy boryka się bowiem zarówno z problemem identyfikacji jak i uwierzytelniania operacji. Bardzo popularnym przestępstwem jest tutaj zakładanie kont czy branie kredytów pod fałszywą tożsamością. Stąd też od wielu lat zarówno rząd jak i Bank Centralny stara się wprowadzić identyfikację przy pomocy odcisku palca. Niestety wiele projektów pilotażowych dało złe rezultaty (duża liczba odrzuceń, zniszczone dlonie klientów itd.). Mimo to w 2012 roku Central Bank of Nigeria zarządził wprowadzenie do banków identyfikacji biometrycznej przy pomocy 10 odcisków palców przy zakładaniu nowego konta.



Rys.48: Bankomat biometryczny w Skye Bank

Źródło: Environ

W Nigerii istnieje jednak także inny poważny problem – uwierzytelniania operacji. Bezpieczeństwo transakcji, szczególnie w bankomacie jest bardzo małe. Począwszy od zainfekowanych bankomatów po skimming kart. Dlatego też największe banki w Nigerii nie chcąc czekać na przeciągający się projekt identyfikacji biometrycznej, rozpoczęły projekty pilotażowe na swoich bankomatach.

Skye Bank to jeden z największych banków w Nigerii, posiadający sieć 653 bankomatów. W 2011 roku Bank rozpoczął pilotaż w wybranych oddziałach i bankoma-

tach banku. w ramach pilotażu wdrożono system biometryczny *Finger Vein*. System przyjął się bardzo dobrze. Bank planuje pełny rollout w latach 2013-2014.

Kolejne banki nigeryjskie w tym **United Bank of Africa**, **Access Bank** czy **Diamond Bank** również przeprowadziły projekty pilotażowe z wykorzystaniem technologii *Finger Vein*. Jednakże część banków chciała być zgodna z metodą identyfikacji i zdecydowała się na pilotaż biometrii odcisku palca w bankomatach. Wśród takich banków były m.in.: **First Bank** i **Zenith Bank**.

8.2.8. Słowacja - Tatra Banka

Tatra Banka należący do grupy Raiffeisen International od dawna zmagał się z problemem niewygodnej i długotrwałej weryfikacji klientów na Infolinię. Ponad 90% wszystkich połączeń na Infolinię wymagało uwierzytelniania, więc średni czas rozmowy odgrywał istotną rolę. Strategicznie bank nie używa również usług IVR, więc zastosowano weryfikację głosową podczas zwykłej rozmowy telefonicznej z konsultantem. z punktu widzenia klienta rozmowa wygląda tak jak poprzednio, tylko, że konsultant nie zadaje już tylu niewygodnych pytań. Klient od razu przechodzi do wyjaśniania, w jakiej sprawie dzwoni a w tle zostaje uwierzytelniony przez system biometrii głosowej. Po pozytywnej weryfikacji, konsultant otrzymuje na swoim pulpicie informacje o uwierzytelnieniu danej osoby i spokojnie przechodzi do dalszej merytorycznej dyskusji z klientem. Bez konieczności zadawania tych wszystkich niewygodnych dla klienta pytań, Bank oszczędza średnio 30 sekund na każdej rozmowie i ponad 97% wszystkich dzwoniących klientów uwierzytelnianych jest automatycznie. Klienci docenili takie rozwiązanie i współczynnik NPS wzrósł z 41% do 62%. Dodatkowym czynnikiem motywującym wdrożenie alternatywnego rozwiązania uwierzytelniającego klientów i konsultantów jednocześnie była znacząca ilość nadużyć na transakcjach telefonicznych. Czyli oprócz zwiększenia satysfakcji klienta, poprawy jego wygody korzystania z usług Infolini bankowej, zwiększono dodatkowo bezpieczeństwo na Infolini.

Warto zwrócić uwagę, że biometria głosowa jako sposób uwierzytelniania klientów, została wbudowana w całą spójną strategię podniesienia satysfakcji klientów. Wraz z wprowadzeniem biometrii głosowej, odświeżono brand Infolinni „Dialog Live”, prowadzono kampanie marketingowe w telewizji, radio, prasie i w oddziałach bankowych. Pracownicy zostali odpowiednio przeszkoleni z benefitów wprowadzonej nowej usługi, co zaowocowało wysokim współczynnikiem zgód na rejestrację próbek biometrycznych podczas kontaktu z Infolinią „Dialog Live”.

8.2.9. Rumunia - ING Bank

Bank **ING** w Rumunii od wielu lat próbował zwiększyć ilość osób załatwiających sprawy bankowe samodzielnie w IVR. Niestety, aplikacja IVR była w taki sposób zbudowana, że jedynie 4% klientów korzystało z tej metody. Dodatkowo Bank zmagał się z problemem wysokiego współczynnika nadużyć. z pomocą przyszły połączone rozwiązania biometrii głosowej, nawigacji głosowej i przekierowania głosowych, których celem było podniesienie współczynnika poziomu samoobsług. Nowa aplikacja spotkała się z pozytywnym przyjęciem przez klientów ING Bank. Współczynnik samoobsług wzrósł z 4% do 38% a współczynnik nadużyć został znacznie zredukowany i pozwolił osiągnąć 15 miesięczny zwrot z inwestycji przy jedynie 45 stanowiskach konsultantów.

8.2.10. Wielka Brytania - Barclays

Najbardziej spektakularny przykład wykorzystania biometrii głosowej w sektorze bankowym w ostatnim czasie. **Barclays** chciał podnieść jakość obsługi klientów oraz poprawić pozytywne doświadczenie klientów w kontaktach z Infolinią. Najpierw przez kilka miesięcy intensywnie testował rozwiązania biometrii głosowej na wybranej grupie klientów i ostatecznie w roku 2013 uruchomił możliwość biometrycznego uwierzytelnienia podczas zwykłej rozmowy klientów z konsultantami.

Bank Barclays jest **pierwszą instytucją finansową na świecie**, która wdrożyła pasywne rozwiązania biometrii głosowej, jako podstawowy sposób uwierzytelniania klientów. Za wdrożenie innowacyjnej usługi Barclays zdobył ważną i prestiżową Nagrodę Financial Services UK w kategorii „Najlepsze wykorzystanie technologii w obsłudze klienta” za zastosowanie biometrii głosowej w procesie uwierzytelniania klientów. Nagroda została przyznana w kwietniu 2013 roku i stanowi dowód uznania środowiska dla inicjatywy Barclays w wyznaczaniu nowych standardów obsługi klienta.

Od momentu wdrożenia ponad 85% klientów Barclays zarejestrowało swój głos w banku do celów weryfikacji, a 95% z nich zostało pozytywnie zweryfikowanych już przy pierwszym telefonie do banku. Barclays zyskał jednak coś więcej niż tylko poprawę bezpieczeństwa. Aż 93% klientów dało Barclays ocenę 9 lub 10 za szybkość, łatwość obsługi i bezpieczeństwo nowego systemu uwierzytelniania.

8.2.11. Indonezja - Bank Negara Indonesia (Persero) Tbk

Pod koniec 2011 roku, indonezyjski **Bank Negara Indonesia (Persero) Tbk** wprowadził możliwość automatycznego resetu hasła z użyciem biometrii głosowej. Rozwiążanie obsługuje język Indonezyjski (Bahasa) i używane jest przez pracowników banku BNI do uwierzytelniania podczas resetu hasła. Rozwiążanie pozwoliło zwiększyć wygodę pracowników i jednocześnie zwiększyć bezpieczeństwo wewnętrzne banku.

Biometria głosowa była naturalnym wyborem z uwagi na możliwość jej wykorzystania przez telefon

Bank działa od 1946 roku i został utworzony przez rząd Indonezji, jako pierwszy w kraju. Dział IT banku BNI od dawna stara się zapewnić najlepszą jakość usług dla klientów BNI i jego pracowników. W ostatnim czasie zwiększono politykę bezpieczeństwa dla pracowników, co doprowadziło do tego, że tysiące osób zaczęły notorycznie zapominać swoje hasła i coraz częściej trzeba było je resetować. Proces resetu hasła był z miesiąca na miesiąc coraz bardziej uciążliwy dla działu help desk BNI jak i samych pracowników. Podczas każdego resetu trzeba sprawdzać tożsamość osoby, z którą rozmawia konsultant w help desk. W pewnym momencie stało się jasne, że trzeba było znaleźć lepsze rozwiązanie.

Biometria głosowa była naturalnym wyborem z uwagi na możliwość jej wykorzystania przez telefon. Wysoki współczynnik bezpieczeństwa i wygoda korzystania została potwierdzona już przez miliony użytkowników.

8.2.12. Izrael

Bank HaPoalim, Bank Leumi oraz **Discount Bank** uruchomiły aplikacje zwiększające bezpieczeństwo dostępu do zdalnych usług opierając się o biometrię głosową.

Bank HaPoalim uruchomił aplikacje umożliwiające automatyczne resetowanie PINu oraz umożliwiające dostęp do usług bankowych poprzez Contact Center bez konieczności wprowadzania PINu w ogóle.

Bank Leumi wprowadził samoobsługowe resetowanie hasła dla aplikacji eBanking oraz wykrywanie oszustów w czasie rzeczywistym (wykorzystuje tzw. ciche powiadomienie służb bezpieczeństwa w banku o nadużyciach).

Discount Bank z kolei, wprowadził wielostopniowe uwierzytelnienie oparte o biometrię głosową dla transakcji wysokiego ryzyka.

9. Wybrane studia przypadków wdrożeń biometrii w innych sektorach

9.1. Polska - T-Mobile

T-Mobile, jako pierwszy w Polsce uruchomił usługę opartą o biometrię głosową. U operatora zastosowano technologię firmy Nuance.

T-Mobile uruchomił usługę głosowej weryfikacji użytkownika na potrzeby wewnętrznego systemu automatycznego resetu haseł dostępowych w sieci wewnętrznej. Całodobowa dostępność usługi ułatwia codzienną pracę pracownikom biur i sklepów polskiego operatora.

Wdrożenie zostało przeprowadzone przez zespół Algo-tech specjalizujący się w biometrii głosowej. Zastosowane rozwiązanie pozwala na automatyczną i zdальną weryfikację tożsamości użytkownika na podstawie unikalnych cech jego głosu. System sprawdza, czy dana osoba rzeczywiście jest tą, za którą się podaje, porównując jej głos w trakcie wypowiedzi z zachowanym wcześniej wzorcem głosu, uzyskanym w trakcie jednorazowej rejestracji. Zaletą systemu jest to, że nie ma konieczności zadawania już szeregu pytań dotyczących danych osobowych związanych z użytkownikiem, weryfikowanych dotychczas w trakcie procedur bezpieczeństwa i wymagających kontaktu ze specjalistą. Operacja jest dokonywana w całości automatycznie, możliwa do przeprowadzenia 24 godziny na dobę, 7 dni w tygodniu, a czas procedury resetu hasła skrócił się do ok. 20 sekund. Oszczędza się zatem nie tylko czas użytkowników, ale także pracowników wsparcia informacyjnego firmy jednocześnie podnosząc bezpieczeństwo operacji resetu hasła.

9.2. Węgry - T-Mobile

Na wiosnę 2012 roku **T-Mobile** na Węgrzech udostępnił usługę weryfikacji klientów z użyciem biometrii głosowej. Aby się zarejestrować, klient musi wyrazić zgodę na poniesienie jednorazowego kosztu w wysokości ok. 1,50 zł. w ten sposób znacznie wzmacniono bezpieczeństwo dostępu do usług i transakcji w Contact Center, gdzie uprzednio uwierzytelnienie oparte było na numerze identyfikacyjnym osoby dzwoniącej oraz pytaniach kontrolnych (zamkniętego zestawu pytań). Klienci zyskali zatem zwiększenie bezpieczeństwa i jednocześnie uzyskali łatwiejszy dostęp do swoich usług. w ciągu pierwszego miesiąca zarejestrowało się 12000 osób, a obecnie tempo nowych rejestracji utrzymuje się na poziomie ok. 9000 rejestracji miesięcznie.

9.3. Turcja - Global Bilgi

Global Bilgi to firma usługowa będą własnością operatora telefonii komórkowej Turkcell. Rozpoczął on implementację biometrii głosowej od aplikacji resetu hasła dla pracowników Global Bilgi. Po nabraniu niezbędnych doświadczeń z rozwiązaniami biometrii głosowej, postanowiono uruchomić uwierzytelnienie biometryczne dla wszystkich klientów. Rozwiązanie spotkało się w Turcji z tak dobrym przyjęciem, że dziś korzysta z niego ponad 10 milionów klientów i jest to największy na świecie przykład wdrożenia na szeroką skalę systemu biometrii głosowej.

9.4. Turcja - SGK



Rys.49: Czytnik biometryczny BioMIG na bazie technologii Finger Vein dedykowany dla SGK

Źródło: MIG International

SGK (Sosyal Guvenlik Kurumu) to turecki odpowiednik zakładu ubezpieczeń społecznych. SGK należy do Ministerstwa Pracy i Ubezpieczeń Społecznych. SGK odpowiada za narodowy system ubezpieczeń, ubezpieczenia zdrowotne, wyznaczanie polityk społecznych, współpracę z Unią Europejską w zakresie porozumień dotyczących ubezpieczeń społecznych, wdrażanie nowych reguł prawnych itd. SGK obejmuje ubezpieczenia krótkoterminowe (np. urlop macierzyński, urlop wyhowawczy, urlop zdrowotny) oraz długoterminowe (np. emerytury, renty). SGK pokrywa też koszty wszelkich usług medycznych dla mieszkańców Turcji.

Narodowy system zdrowia w Turcji boryka się jednak z ogromnymi problemami: rosnącym deficytem i kolsalną liczbą fraudów, ok. 15 mld USD rocznie. Dlatego też SGK zdecydował się wprowadzić uwierzytelnianie dostępu do usług medycznych dla obywateli w każdym punkcie usługowych (szpitale, przychodnie, apteki itd.). Jedynie poprawne uwierzytelnianie umożliwia ubieganie się o zwrot kosztów dla usługodawcy. Jako metodę uwierzytelniania wybrano biometrię. 1 września 2013 wprowadzono odpowiednie ramy prawne. Dzięki wprowadzeniu uwierzytelniania biometrycznego SGK chce osiągnąć redukcję fraudów, lepszą kontrolę nad wydawaniem środków społecznych jak i wprowadzić jednolitą metodę uwierzytelniania.



Rys.50: Uwierzytelnianie biometryczne *Palm Vein* w jednym z punktów medycznych

Źródło: Fujitsu

W taki sposób uruchomiono największy projekt biometryczny na świecie, który ma objąć 5000 szpitali, 24 000 aptek, 5000 salonów optycznych, 35 000 gabinetów prywatnych, 7000 punktów medycznych oraz 1500 biur SGK w 81 miastach, co daje kilkaset tysięcy czytników. Rynek ten jest podzielony między kilku dostawców systemów biometrycznych, którzy pomyślnie przeszli proces certyfikacyjny. Wśród nich liderami są Hitachi (*Finger Vein*) i Fujitsu (*Palm Vein*) wraz ze swoimi partnerami (np. MIG International dla Hitachi), którzy uzyskali akredytację i rozpoczęli dostawy do szpitali. Założeniem projektu jest, że stroną kupującą nie jest SGK a bezpośrednio instytucja medyczna. SGK jedynie dopuszcza dane rozwiązań i wyznacza warunki. Projekt SGK daje możliwość dostępu do największego projektu biometrycznego na świecie, jednakże jest bardzo wymagający dla dostawców. Dostawcy systemów biometrycznych musieli opracować specjalne urządzenia wg wymagań SGK, wdrożyć na własną rękę system centralny przechowujący bezpiecznie wzorce biometryczne i komunikujący się z systemem SGK oraz utrzymać system i urządzenia przez 5 lat. To wszystko miało być umieszczone w cenie per urządzenie.

9.5. Europa - Biometria w systemach informacyjnych Unii Europejskiej

Unia Europejska bardzo wcześnie doceniła wartość stosowania biometrii w zakresie identyfikacji i uwierzytelnienia tożsamości w systemach informacyjnych obejmujących ewidencję obywateli samej Unii Europejskiej jak i obywateli innych krajów przebywających czasowo na jej terenie bądź ubiegających się o taki pobyt. Już w 1990 roku podjęto decyzję o wdrożeniu Europejskiego Zautomatyzowanego Systemu Identyfikacji Odcisków Palców, od roku 1999 trwają prace nad systemami informacyjnymi dla strefy Schengen szeroko wykorzystującym biometrię oraz wizowy system informacyjny. Od roku 2004 podjęto intensywne działania dla opracowania europejskiego biometrycznego paszportu elektronicznego. Systemy te w wyniku wieloletniego doświadczenia zawierają bardzo dobre rozwiązania technologiczne i organizacyjne a ich stabilność jest zapewniona przez opracowane standardy, stale doskonalone. Rozwiązania te mogą być wzorcem dla wielu projektów biometrycznych, zwłaszcza o dużym zakresie ilościowym jak i terytorialnym. Warto więc studiować te rozwiązania, aby nie wyważać otwartych drzwi. Szczególnie użycie infrastruktury klucza publicznego (PKI) do ochrony wrażliwych danych biometrycznych w systemie paszportowym wydaje się być godnym polecienia.

- **Eurodac - Europejski System Identyfikacji Odcisków Palców**

System identyfikacji odcisków palców azylantów i nielegalnych imigrantów na obszarze Unii Europejskiej, gromadzi dane na temat obserwowanych, podejrzanych lub ściganych osób oraz przedmiotów (skradzionych pojazdów, broni, dokumentów).

W ramach Eurodac istnieje centralna komputerowa baza danych, do której dostęp mają pracownicy odpowiednich służb we wszystkich krajach członkowskich.

Eurodac, to baza opracowana na potrzeby Konwencji Dublińskiej o azylu z 1990 r. Państwa członkowskie zostały zobowiązane do pobierania odcisków palców każdego obywatela, który złożył wniosek o azyl lub został zatrzymany w związku z nielegalnym przekroczeniem granicy. System uruchomiono 15 stycznia 2003 r. i obecnie aktywnie uczestniczą w nim wszystkie kraje strefy Schengen, oraz Irlandia i Wielka Brytania.

- **System Informacyjny Schengen SIS 1+ i SIS II**

SIS, (ang. Schengen Information System) – jest największą w Europie komputerową bazą danych (zawiera ponad 37 milionów wpisów, i stale się powiększa o około 3% danych miesięcznie), która pozwala na sprawdzenie, czy osoby lub przedmioty przekraczające granicę Strefy Schengen, bądź już znajdują-

ce się na jej terenie, nie są poszukiwane, niejawnie nadzorowane lub czy nie dotyczy ich zakaz wstępu.

Dostęp do niej mają policja i urzędy konsularne oraz straż graniczna i służba celna z państw członkowskich układu z Schengen. SIS składa się z narodowych sekcji w każdym z krajów członkowskich oraz z układu centralnego. Centralny serwer SIS znajduje się w Strasburgu.

W bazie SIS1+ gromadzone są informacje dotyczące: osób poszukiwanych (w celu wydania lub ekstradycji, poniesienia odpowiedzialności za czyny, za które są np. ścigane); osób zaginionych; utraconego lub skradzionego mienia; zakazu wjazdu dla obywateli państw trzecich.

Obejmuje swoim zasięgiem niemal całą Unię Europejską jak również Norwegię, Islandię i Szwajcarię.

Od roku 1999 trwają prace nad nowym systemem (SIS II). Druga generacja SIS (SIS II) umożliwi przetwarzanie obok danych tekstowych również danych biometrycznych (fotografii i odcisków palców). Polska bierze aktywny udział w realizacji projektu SIS II, Architektura SIS II będzie oparta o system centralny, systemy krajowe i infrastrukturę komunikacyjną. Dane są wprowadzane, modyfikowane, usuwane i wyszukiwane za pośrednictwem systemów krajowych, a system centralny będzie odpowiedzialny za operacje związane z centralnym przechowywaniem i udostępnianiem danych - baza referencyjna.

- **Wizowy System Informacyjny¹² VIS**

VIS to system służący wymianie danych wizowych dotyczących wiz krótkoterminowych między Państwami Członkowskimi Schengen. VIS zapewnia wymianę informacji o osobach starających się o wizę i wydanych wizach między państwami tworzącymi strefę Schengen, VIS to: uproszczenie procedury rozpatrywania wniosków wizowych, ułatwienie waliki z nadużyciami, ułatwienie odpraw na przejściach granicznych na granicach zewnętrznych państw członkowskich i na terytoriach państw członkowskich, pomoc w identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium państw członkowskich lub też przestały spełniać te warunki, skuteczniejsze zapobieganie zagrożeniom bezpieczeństwa wewnętrznego każdego z państw członkowskich.

W VIS rejestrowane są: dane biograficzne, fotografia osoby ubiegającej się o wizę, odciski palców (10), odsyłacze do innych wniosków. W pierwszej kolejności wdrożenie Systemu zostało dokonane w krajach Afryki Północnej: oraz w Armenii, Azerbejdżanie oraz Malezji. Wnioskodawca musi stawić się osobiście w konsulacie, by udostępnić swoje dane biometryczne. Dane te będą ważne przez 5 lat i mogą być ponownie wykorzystywane w przypadku składania kolejnych wniosków, chyba, że nastąpią uzasadnione wątpliwości dotyczące tożsamości wnioskodawcy.

VIS pozwala na usprawnienie współpracy pomiędzy państwami członkowskimi m.in. w zakresie: wspólnej polityki wizowej, zapobiegania handlu wizami, identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium UE.

Systemem VIS został operacyjnie uruchomiony w 2011 r. i zapewnia dostęp do danych dla służb odpowiedzialnych za zapobieganie, ściganie, zwalczanie przestępcości i terroryzmu. VIS jest oparty na decentralizowanej architekturze obejmującej Centralny Wizowy Systemem Informacyjny, a także interfejs w każdym państwie oraz infrastrukturę komunikacyjną między Centralnym Wizowym Systemem Informacyjnym i interfejsami krajowymi. Zarządzanie VIS będzie realizowane na poziomie centralnym UE przez utworzoną w tym celu instytucję unijną - ta sama, co w przypadku SIS.

„VIS pozwala na usprawnienie współpracy pomiędzy państwami członkowskimi

W VIS są gromadzone dane dotyczące wnioskodawcy wizy oraz informacji nt.: wniosku wizowego, wizy: wydanej, anulowanej, cofniętej lub przedłużonej, a także, której wydania odmówiono, fotografie, odciski palców (10), odsyłacze do poprzednich wniosków oraz do wniosków osób podróżujących wspólnie.

Dostęp do VIS w celu wprowadzania, modyfikowania, usuwania i przeglądania danych jest zagwarantowany wyłącznie dla organów wizowych oraz organom - właściwych do przeprowadzania odpraw na przejściach granicznych na granicach zewnętrznych, organom odpowiedzialnym za udzielanie azylu oraz kontrolę legalności pobytu na terytorium państwa, dla organów odpowiedzialnych za zapobieganie przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywanie oraz ściganie. Obecnie do korzystania z VIS uzyskało ponad 16 instytucji krajowych np. Straż Graniczna, konsulowie, wojewodowie, Policja, sądy, prokuratury, ABW, BOR oraz CBA.

- **Paszport biometryczny**

Paszport biometryczny posiada tą samą formę i cechy jak paszport tradycyjny a ponadto w paszport ten wbudowany jest Chip RFID (RF Radio Frequency, ID Identification). Chip RFID jest to odpowiednik

12 ang. Visa Information System

bezstykowej karty elektronicznej inaczej mikroprocesor połączony z anteną, poprzez którą kontaktuje się z czytnikiem. Ponadto antena generuje prąd wystarczający, aby zasilać ten mikroprocesor. Chip jest wyposażony w koprocesor kryptograficzny umożliwiający wykonywanie wszystkich niezbędnych operacji kryptograficznych a to z kolei zapewnia wysoki poziom bezpieczeństwa.

• Od Paszportu do biometrycznego e-Paszportu

Międzynarodowa organizacja lotnictwa cywilnego ICAO (*International Civil Aviation Organization*) rozpoczęła prace nad paszportem biometrycznym w 1997. Po 11 Września 2001, wystąpiło pilne zapotrzebowanie na lepszą metodę identyfikacji i uwierzytelnienia. Rząd USA zażądał od krajów uprawnionych do ruchu bezwizowego na wprowadzenie ePaszportu z jedną cechą biometryczną - wizerunkiem twarzy. Wymagania te spełniono dopiero w 2006.

W wyniku prowadzonych przez ICAO prac normalizacyjnych dotyczących MRTD (w tym paszportów i wiz) powstają raporty techniczne zawierające zalecenia, które powinny być brane pod uwagę przez kraje wydające takie dokumenty.¹³

Rada Europejska wydała ROZPORZĄDZENIE RADY (WE) NR 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie¹⁴. Rozporządzenie reguluje zagadnienia ogólne a bardziej szczegółowe zasady są ujmowane w specyfikacjach i standardach.

I tak utworzono ujednolicone techniczne specyfikacje dla elektronicznych paszportów i wiz, które wprowadzono: „Decyzją Komisji Europejskiej, której załącznikiem jest Zastosowanie biometrii w paszportach UE. UE - Specyfikacje dla paszportu¹⁵.

Istotne rozstrzygnięcia dotyczą wyboru technologii dla układów scalonych, które stanowią integralną część dokumentu podróży - są to procesorowe bezstykowe układy zbliżeniowe o „plikowej” architekturze zasobów pamięciowych i logicznym protokole komunikacji ze „światem zewnętrznym” zgodnymi

13 ICAO NTWG, Development of a Logical Data Structure-LDS for optional capacity expansion technologies, Technical Report, Revision 1.7, 18 May 2004. ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read Only Access, Technical Report, Version 1.1, 1 October 2004

14 Ang. wersja: COUNCIL REGULATION (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

15 Ang. wersja: Biometric Deployment of EU-Passports, EU-Passport Specification (working document), Advanced Security Mechanisms for MRTD, Technical Report (Technical Report version0.85).Biometric Deployment of EU-Visa and EU Residence Permits, EU Visa Specification (w przygotowaniu)

z odpowiednimi normami ISO/IEC¹⁶. Dokument podrózny, czyli MRTD składa się więc z „klasycznej” części dokumentu, która umożliwia stwierdzenie тожsamości na podstawie oceny wzrokowej, zaś układ scalony ma dodatkowo zwiększać wiarygodność tego procesu.

Biometria w dokumentach podróżnych

Biometria została wybrana, jako metoda identyfikacji i uwierzytelnienia z uwagi na następujące zalety:

- Bardzo trudno wykonać duplikat dokumentu, aby dokonać sfałszowania trzeba zarówno pokonać zabezpieczenia dokumentu klasycznego jak i cały system zabezpieczeń informatycznych w tym chipa.
- Występuje bardzo silne powiązanie pomiędzy dokumentem a jego posiadaczem
- Paszport elektroniczny stwarza możliwości do prowadzenia automatycznej kontroli granicznej, co może usprawnić przepływ osób.
- Umożliwia zidentyfikowanie podróżnych i imigrantów, którzy zagubili swoje dokumenty podróżne, (jeśli przeszli oficjalną kontrolę graniczną)

Weryfikacja autentyczności dokumentów, ochrona dostępu do danych, uwierzytelnienie podmiotów.

Dla zapewnienia kompleksowego bezpieczeństwa wydawania i użytkowania dokumentów zawierających dane biometryczne, należy kontrolować dostęp do danych, sprawdzać ich autentyczność, ale również badać wiarygodność urządzeń czytających. Mechanizmy zabezpieczające dostęp do danych, a także ich integralność, autentyczność i/lub wiarygodność oraz poufność podzielono na 4 kategorie: **uwierzytelnienie bierne, uwierzytelnienie aktywne (mikroprocesora), podstawowa kontrola dostępu oraz rozszerzona kontrola dostępu (terminala)**.

Uwierzytelnienie bierne jest wymagane dla wszystkich danych (obligatoryjny zakres bezpieczeństwa dla sygnatariuszy ICAO). Polega ono na weryfikacji podpisu cyfrowego złożonego przez wydawcę paszportu pod danymi zawartymi w strukturze danych chipa. Zapewnia, że dane w chipie są autentyczne i niezmienione, jednakże nie chroni przed skopiowaniem lub podmianą chipa, przed nieupoważnionym dostępem oraz przed przeglądaniem danych

Uwierzytelnienie aktywne według specyfikacji ICAO umożliwia uwierzytelnienie układu scalonego względem systemu kontroli za pomocą kryptografii asymetrycznej i protokołu „wyzwanie-odpowiedź”, a zatem jest to metoda sprawdzenia, czy układ scalony nie zo-

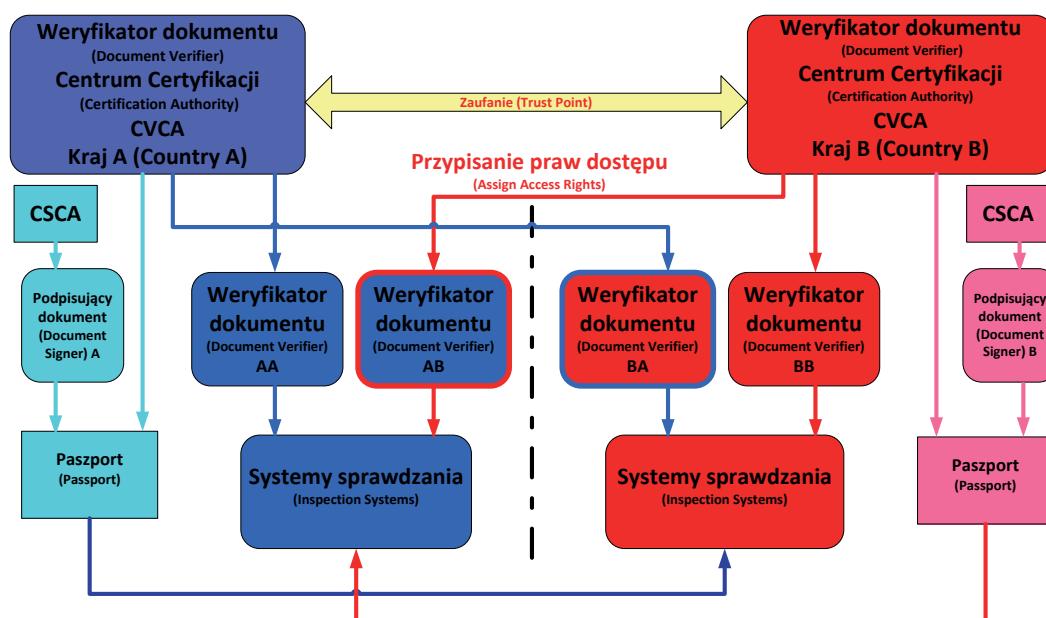
16 16ISO/IEC 14443, części 1-4, Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards ISO/IEC 7816, części 4, 5, 8, 9 i 15, Identification Cards -Integrated Circuit(s) Cards with Contacts

stał podmieniony. Sporządzenie „klona” wydaje się więc praktycznie niemożliwe. Uwierzytelnienie aktywne wymaga zastosowania chipa z kooprocesorem kryptograficznym i wygenerowania kluczy kryptograficznych dla każdego chipa. Specyfikacja UE wprowadziła alternatywną metodę uwierzytelnienia chipa (*chip authentication*), która oprócz powyższych właściwości podnosi poziom bezpieczeństwa przesyłanych danych.

Podstawowa kontrola dostępu wymagana jest dla wszystkich danych. Ma ona zapobiegać odczytowi danych z układu scalonego przez podmioty nieuprawnione (np. nawiązując komunikację z układem scalonym bez „otwierania” paszportu, bądź „posłuchując” legalną komunikację między MRTD a systemem sprawdzania paszportu). Zapobiega podsłuchiwaniu komunikacji pomiędzy MRTD i systemem sprawdzania (w trakcie komunikacji ustalany jest szyfrowany sesjowy kanał). Nie chroni przed skopiowaniem lub podmianą chipa.

authentication) dzięki wykorzystaniu dodatkowej infrastruktury PKI, w której wydawane są certyfikaty dla weryfikujących dokumenty.

Najważniejszymi elementami tej struktury są krajowe centra certyfikacji. Istnieją dwa rodzaje narodowych centrów certyfikacji. Pierwsze to CSCA (Country Signing Certificate Authority) czyli centrum, które wydaje certyfikaty dla wydawcy paszportu (DS - Document Signer). Wydawca paszportu przy ich pomocy podpisuje dane umieszczone w paszporcie w celu zapewnienia biernego uwierzytelnienia. Centrum to przekazuje swój autocertyfikat (samopodpisany) wszystkim odpowiednikom z pozostałych krajów. Drugie centrum to DVCA (Document Verifier Certificate Authority), czyli Centrum, które wydaje certyfikaty zarówno krajowym weryfikatorom dokumentów (DV Document Verifier, np. Straży Granicznej), a ci z kolei wydają certyfikaty dla systemu sprawdzania (Inspection System, np. sys-



Materiały: Franciszek Wołowski

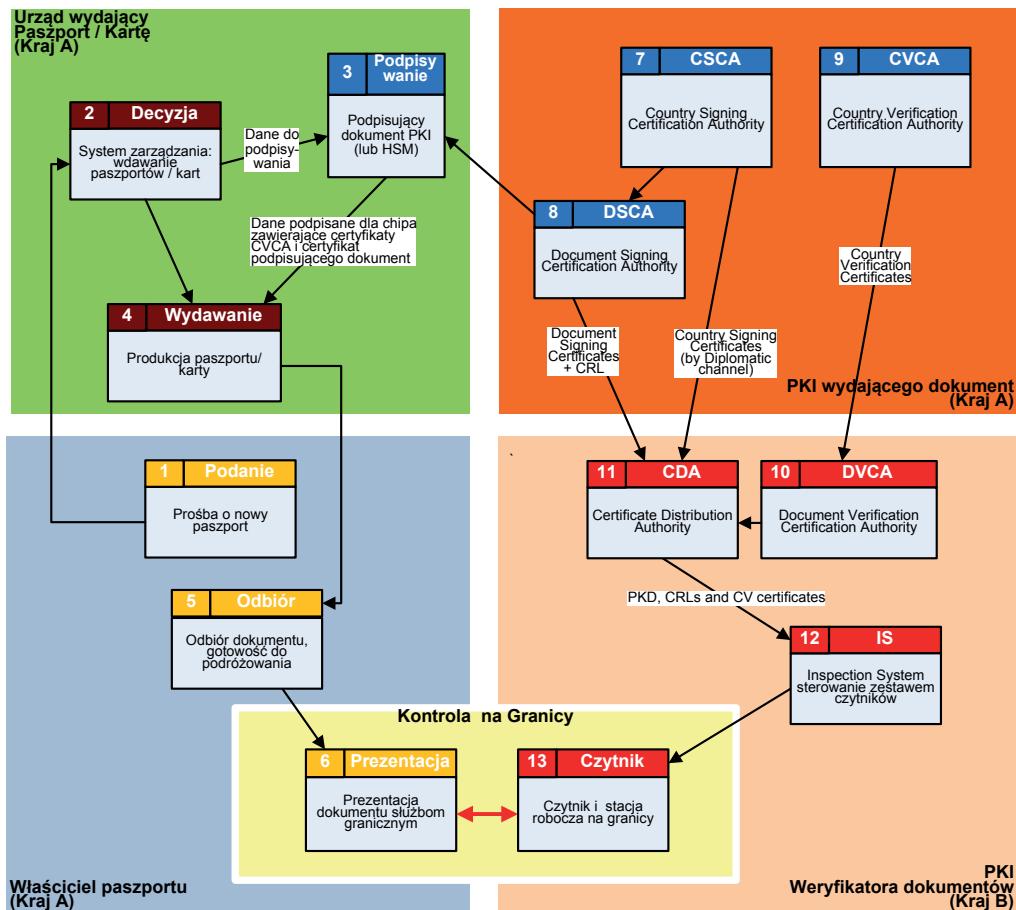
Rys.51: Struktury PKI dwóch krajów i ich współdziałanie

Źródło: PWPW

Rozszerzona kontrola dostępu (Extended Access Control) jest wymagana dla dostępu do odcisków palca – uznawanych za dane wrażliwe - jako ochrona dodatkowa. Jest to opcjonalne wymaganie ICAO, jednakże UE przyjęła je, jako obowiązkowe po wprowadzeniu do paszportów odcisków palców. Zakłada się, że kontrola dostępu do tych danych powinna być tak skuteczna, jak to możliwe. Prace ekspertów europejskich zaowocowały propozycją alternatywnego aktywnego uwierzytelniania. Chodzi o uwierzytelnianie terminala (terminal

mom zainstalowanym na przejściach granicznych), ale również, a raczej przede wszystkim, wydają certyfikaty wszystkim zagranicznym weryfikatorom dokumentów, aby można było zamknąć ścieżkę zaufania i zrealizować rozszerzoną kontrolę dostępu, co można by bardziej przystępnie określić, jako nadawanie uprawnień zagranicznym służbom do czytania paszportów obywateli określonego kraju.

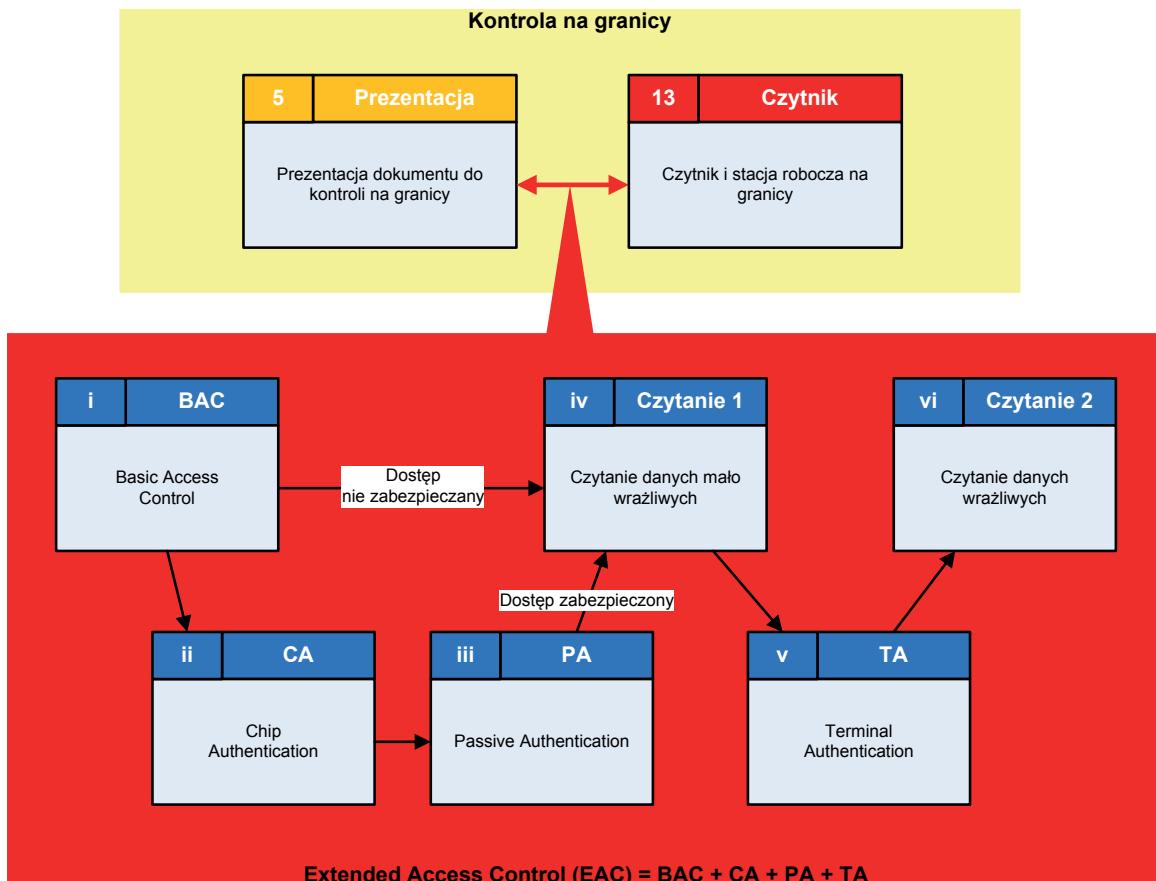
Cały system wydawania i użytkowania paszportów biometrycznych jest więc dosyć skomplikowany, bo obejmuje gromadzenie danych, ich weryfikację, podsystem zabezpieczenia przed oszustwami i nieuprawnionym dostępem, produkcję dokumentów i ich dystrybucję i w końcu weryfikację tych dokumentów i tożsamości ich właścicieli.



Rys.52: System wydawania i użytkowania paszportów biometrycznych

Źródło: PWPW

Kontrola na granicy z zastosowaniem paszportu biometrycznego nie została jeszcze określona w sposób dokładny, gdyż może być ona bardzo różnorodna, począwszy od np. wyświetlenia na ekranie zawartości wizerunku twarzy zapisanego w chipie paszportu i porównanie go z zdjęciem w paszporcie oraz twarzą podróżnego do całkowicie zautomatyzowanej kontroli z wykorzystaniem procesu dopasowywania wzorców. w kontroli mogą być stosowane obie cechy biometryczne razem (podnosi to efektywność kontroli) lub każda z nich oddzielnie. Sposób kontroli będzie również uzależniony od środowiska, w którym będzie ona realizowana, inaczej będzie realizowana kontrola w portach lotniczych i morskich a inaczej w zatłoczonym pociągu (np. jadącym z Lwowa do Medyki) lub na leśnym przejściu w niekorzystnych warunkach atmosferycznych (deszcz, śnieg, wiatr, mróz).

**Rys.53: Schemat weryfikacji paszportu na granicy**

Źródło: PWPW

Podstawowym dokumentem zawierającym regulacje związane z działalnością tej struktury jest raport techniczny (por. poz. 5 Bibliografii). Dokument ten został opracowany, uzupełniany i aktualizowany przez grupę roboczą ds. PKI i EAC, której Komitet Artykułu 6 nadał oficjalny status i która przyjęła nazwę Brussels Interoperability Group (BIG). Grupa ta intensywnie pracowała do 2012 roku opracowując niezbędne dokumenty takie jak polityki certyfikacji, profile ochrony, specyfikacje testów itp. oraz dokumenty dla zapewnienia interoperacyjności paszportów wszystkich państw członkowskich UE. Dla uzyskania pełnej kompatybilności i interoperacyjności zostały opracowane plany testów zgodności paszportów z standardami (ePassport Conformity test), czytników (Reader Conformity test) jak również testów wzajemnych (Cross over test) dla weryfikacji poprawności sprawdzania paszportów na różnorodnych urządzeniach. Zrealizowano kilka międzynarodowych sesji testowych. Po każdej z sesji aktualizowano zarówno plany testów jak i same standardy.

Wdrożenie polskiego paszportu biometrycznego

Rozporządzenie Rady (WE) nr 2252/2004 to dokument obligatoryjny dla wszystkich krajów członkowskich. W związku z tym, w roku 2005 rozpoczęto prace mające na celu wypełnienie obowiązków Polski w kwestii wydawania paszportów biometrycznych. Proces ten podzielono na dwa etapy. W pierwszym etapie - do sierpnia 2006 - zobowiązało wydawanie paszportu z wizerunkiem twarzy. Drugi etap do czerwca 2009 - dotyczył wydawania paszportów z dwoma cechami biometrycznymi, czyli wizerunkiem twarzy i odciskami palców.

Pierwszy etap wdrożenia polskiego paszportu biometrycznego

Dla uniknięcia popełnienia błędów na dużą skalę, zdecydowano się na pilotażowe wdrożenie dla paszportów dyplomatycznych i służbowych. Dla tej wybranej grupy stworzono system informatyczny służący do przyjmowania wniosków, pozyskiwania danych, przesyłania wniosków paszportowych w postaci elektronicznej do Centrum Personalizacji Dokumentów, przesyłania infor-

macji zwrotnej o etapie osiągniętym w procesie wydania paszportu oraz rejestracji danych o dokumencie w bazie danych, system personalizacji, infrastrukturę klucza publicznego PKI, system komunikacji oraz system zarządzania bezpieczeństwem obejmujący każdy z tych elementów i zabezpieczający komunikację pomiędzy wymienionymi elementami. System pilotażowy sprawdził się przy wydawaniu paszportów dyplomatycznych i służbowych, więc bez większych zmian został przekształcony w system produkcyjny do wydawania wszystkich rodzajów paszportów i na początku 2006 roku rozpoczęto wydawanie wszystkich rodzajów e-paszportów.

Oprócz problemów merytorycznych musiano również uwzględnić protest stowarzyszenia fotografów, którzy nie zgodzili się na instalację profesjonalnych kabin do pobierania wizerunku twarzy.

Drugi etap wdrożenia polskiego paszportu biometrycznego

Odciski palców są powszechnie uważane za bardzo wrażliwą cechę.. z tego względu jej zastosowanie UE obwarowała bardzo restrykcyjnymi zabezpieczeniami (część opcjonalnych wymagań ICAO UE przyjęła za obligatoryjne). Zabezpieczenia te dotyczą zarówno ochrony danych przed fałszerstwem, jak i przed nieuprawnionym dostępem do nich a w szczególności nielegalnym ich gromadzeniem. z tych względów zastosowane w pierwszym etapie metody zarządzania bezpieczeństwem systemu (BAC i PA) należało rozwinąć i uzupełnić (CA i TA). Wiązało się to z koniecznością uzupełnienia danych w chipie nie tylko o same odciski palców, ale i o dodatkowe klucze oraz certyfikaty, z modyfikacją systemu operacyjnego chipa w celu umożliwienia realizacji dodatkowych protokołów, ale przede wszystkim z zbudowaniem nowych struktur PKI umożliwiających uwierzytelnienie podmiotów weryfikujących dokumenty i zapewniających odpowiednią kontrolę dostępu do tych wrażliwych danych. Opracowany system i procedury zostały poddane rygorystycznym testom i po niezbędnych modyfikacjach zostały przekazane do produkcji. w ten sposób od 2009 roku w Polsce wydawane są e-paszporty z dwoma cechami biometrycznymi, czyli wizerunkiem twarzy i odciskami dwóch palców a wszystko to zostało wykonane bez rozgłosu i akcji PR, część społeczeństwa nie zdaje sobie nawet z tego sprawy.



Oprócz problemów merytorycznych musiano również uwzględnić protest stowarzyszenia fotografów

10. Aspekty prawne biometrii

10.1. Biometria w bankowości

Obecnie rozwiązania biometryczne w polskiej bankowości, mimo iż wciąż stanowią **względną nowość, są faktem**. Niemniej jednak wydaje się, że ich zastosowanie może być rozszerzone na wiele procesów bankowych. Wskazuje się, iż oprócz weryfikacji tożsamości klientów banków w oddziale, wypłaty środków pieniężnych w bankomatach, uwierzytelniania transakcji, dane biometryczne umożliwiają składanie oświadczeń woli, minimalizację papierowego obiegu dokumentacji, zaświadczenie dostępu do pomieszczeń i krytycznych elementów systemów banku, wymagających szczególnej ochrony.

Od czasu opublikowania raportu pt. „*Prawne Aspekty Biometrii*”¹⁷ przez działającą w ramach Związku Banków Polskich Grupę ds. Biometrii poczyniono wiele dodatkowych badań i ustaleń dotyczących zagadnień prawnych, których wybrane wyniki zostaną wskazane w niniejszej edycji raportu, dopełniającego poprzednią jego wersję.

Wydaje się, iż **ogólne wykorzystywanie danych biometrycznych**, które immanentnie wiąże się z koniecznością należytego postępowania i poszanowania prywatności oraz ochrony danych osobowych, **w celu zwiększenia bezpieczeństwa w bankowości (w relacji bank - klient banku) budzi obecnie coraz mniej kontrowersji**. Na potwierdzenie takiego poglądu można przywołać różnorodne wystąpienia Generalnego Inspektora Ochrony Danych Osobowych podczas konferencji dotyczących tej tematyki (np. *Spring Biometric Summit 2012*, *Spring Biometric Summit 2013*), jak również jeden z pierwszych poglądów przedstawiony w prasie o zasięgu ogólnopolskim w tym zasięgu:

„(...) Uważam, że były, są i będą takie dziedziny życia, w których zbieranie danych biometrycznych będzie adekwatne i słuszne. Tak jest m.in. wszędzie tam, gdzie zadania wykonywane przez pracowników wiążą się z tajemnicą państwową. **Takie dane mogą być też zabezpieczeniem najistotniejszych miejsc w bankach.** w takich wypadkach również wyrażamy zgodę na ich stosowanie (...)”¹⁸.

¹⁷ Zob.: R. Kaszubski, M. Sudoł, T. Woszczyński, Z. Marcinkowski, J. Ratajczak, A. Czajka, Prawne Aspekty Biometrii, Warszawa 2011, http://www.hitachi.pl/veinid/documents/OK_Raport_Biometria.pdf

¹⁸ Artykuł GIODO (Michał Serzycki) w Rzeczypospolitej z dnia 25.01.2010 r., „Sfera prywatna jest ważnym dobrem osobistym”, <http://www.giodo.gov.pl/>

Mając na uwadze bezpieczeństwo prawne, czy inaczej ujmując - zapewnienie ochrony sfer prawnych użytkowników systemów biometrycznych stosowanych w bankowości, należy wyjść od generalnego stwierdzenia, że **wykorzystywanie danych biometrycznych w sektorze bankowym podlega będzie przepisom ustawy z dnia 29 sierpnia 1997 r. prawo bankowe**¹⁹ w związku z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej „*u.o.d.o.*” lub „*ustawa*”)²⁰, której konieczność stosowania przez banki (przy założeniu braku jakichkolwiek wyłączeń) wynika niej samej, tj. z art. 3 ust 2 pkt.1²¹.

Co istotne, jeżeli wykorzystywane przez bank dane biometryczne będą służyły do dokonywania **przez bank operacji zaliczanych do czynności bankowych, o których mowa w art. 5 prawa bankowego**, to wszystkie informacje dotyczące czynności bankowej (w tym **dane biometryczne stanowiące informacje o charakterze podmiotowym**²² zвязane z czynnością bankową) objęte będą również ochroną przewidzianą dla tajemnicy bankowej. Tak więc wszelkie dane (informacje) dotyczące czynności bankowej uzyskane przez bank podczas negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje objęte będą tajemnicą bankową.

Nie bez znaczenia jest fakt, iż polski system prawnego przyjmuje maksymalizację ochrony tego rodzaju danych. Świadczyć o tym może uregulowanie relacji pomiędzy przepisami ustawy o ochronie danych osobowych i przepisami ustaw szczególnych²³.

Zgodnie z art. 5 ustawy o ochronie danych osobowych, „*jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw*”. **Jest to więc równoznaczne z traktowaniem w tym przypadku przepisów zapewniających dalej idącą ochronę, jako lex specia-**

¹⁹ Ustawa z dnia 29 sierpnia 1997 r. prawo bankowe (Dz.U. 1997 nr 140 poz. 939, ze zm.)

²⁰ Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 ze zm.).

²¹ Por. „ustawę stosuje się również do: (...) osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych” oraz „które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej”

²² B. Smykla, *Prawo bankowe, Komentarz*, Warszawa 2006, s. 332.

²³ Por. Wyrok NSA z dnia 4 kwietnia 2003 r., II SA 2935/02; M. Swora Glosa do wyroku II SA 2935/02, Państwo i Prawo nr 1 z 2004 r., s.124.; Opinia Generalnego Inspektora Nadzoru Bankowego z 2 czerwca 2000 r. nr NB/BPN/I/237/00, Glosa nr 8 z 2000 r., s.26.

*lis w stosunku do ustawy o ochronie danych osobowych*²⁴. Natomiast do kwestii nieuregulowanych w ustawie szczególnej (np. prawie bankowym), nie obejmujących większą ochroną danych osobowych lub w przypadkach braku kolizji ustawy szczególnej (prawa bankowego) z ustawą o ochronie danych osobowych zastosowanie będą miały przepisy ustawy o ochronie danych osobowych.

Przyjmując, że art. 104 -106b i 106d prawa bankowego przewidują dalej idącą ochronę niż ustawa o ochronie danych osobowych , ostatnia z wymienionych regulacji nie będzie miała w tym przypadku zastosowania. Za takim stanowiskiem mogą przemawiać przepisy prawa bankowego statujące sankcje za naruszenie obowiązku zachowania tajemnicy bankowej wynikającego z art. 104 ustawy Prawo bankowe (np. poprzez ujawnienie podmiotowi nieuprawnionemu, niewymienionemu w wyłączeniu zawartym w art. 104 ust.2).

Jedynie dla porządku należy wskazać, iż w przypadku naruszenia tajemnicy bankowej będą mogły mieć zastosowanie sankcje karne, cywilnoprawne i administracyjnoprawne, tj. **sankcje personalne** (art. 171 ust.5: grzywna do 1 000 000 złotych i kara pozbawienia wolności do lat 3.), **odpowiedzialność odszkodowawcza** na zasadach ogólnych oraz **sankcje nadzorcze** (nakłady przez KNF).

W przypadku jednak stwierdzenia, że art. 104 -106b i 106d prawa bankowego nie przewidują dalej idącej ochrony, chociażby ze względu na wyłączenia od tajemnicy bankowej zawarte w prawie bankowym, koniecznym będzie równolegle stosowanie przepisów ustawy o ochronie danych osobowych i związane z tym m.in. wypełnienie przesłanek legalizujących (np. uzyskanie zgody klienta banku na przetwarzanie danych biometrycznych w konkretnym celu), dochowanie obowiązków informacyjnych wobec klienta banku, zabezpieczenie danych zgodnie z wymogami przewidzianymi przez przepisy ustawy o ochronie danych osobowych i rozporządzeń wykonawczych do niej.

Niemniej jednak, należy stwierdzić, że mimo tego, iż przepisy prawa nie zawierają definicji legalnej danych biometrycznych i ich powszechnie wykorzystanie w sektorze bankowym nie było możliwe do przewidzenia na etapie ich uchwalania, wykorzystywanie danych biometrycznych w sektorze bankowym w relacji bank - klient banku będzie możliwe po **wypełnieniu generalnych wymogów określonych przez dotychczasowe regulacje zawarte w przepisach ustawy o ochronie danych osobowych lub przepisach prawa bankowego**. Dopóki nie zostanie wprowadzona szczegółowa regulacja w tym zakresie, ustalona praktyka lub powszechnie przyjęta rekomendacja, podejście do danych biometrycznych, będzie rządziło się **takimi**

²⁴ Por. M. Krzysztofek, Tajemnica bankowa i ochrona danych osobowych w praktyce bankowej, Warszawa 2010, s. 18.

samymi zasadami jak dotychczasowe podejście do innych danych osobowych (lub odpowiednio: informacji objętych ochroną przewidzianą dla tajemnicy bankowej).

10.2. Biometria a ochrona danych osobowych

Wprowadzenie

W ramach polskiego systemu prawa ochrona danych osobowych przewidziana jest przepisami prawa powszechnie obowiązującego o różnej randze i zasięgu obowiązywania.

Na poziomie krajowym przetwarzanie danych osobowych oraz prawa osób fizycznych, których dane mogą być przechowywane w zbiorach danych, określają przede wszystkim przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej „**u.o.d.o.**” lub „**ustawa**”)²⁵. Równocześnie, należy mieć na uwadze, iż wybrane dane osobowe mogą być również informacjami, których **ochronę gwarantuje zasada prawa do prywatności** przewidziana przez art. 47 Konstytucji Rzeczypospolitej Polskiej (dalej „**Konstytucja**”)²⁶, uzupełniana przez ochronę „informacji dotyczących osoby” na podstawie art. 51 Konstytucji. Uregulowanie problematyki danych osobowych na poziomie konstytucyjnym świadczy o istotności tego zagadnienia i uznaniu potrzeby zagwarantowania ochrony prawnej przed zagrożeniami, które mogą wyniknąć z ewentualnych nadużyć w tym zakresie.

Na uwagę zasługuje fakt, iż Karta Praw Podstawowych Unii Europejskiej²⁷ wprowadziła *expressis verbis* **oddzielny od ochrony prywatności przepis prawný statujący wprost ochronę danych osobowych i traktujący prawo do ochrony takich danych**, jako - prawo podstawowe - wyróżniane, respektowane i podlegające ochronie w ramach Unii Europejskiej.

Dane osobowe a dane biometryczne

Definicja legalna danych osobowych została skonstruowana w art. 6 u.o.d.o., zgodnie z którym dane osobowe to „**wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej**”²⁸.

Należy zaznaczyć, że możliwa do zidentyfikowania jest osoba, której tożsamość może być określona **bezpo-**

²⁵ Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 ze zm.).

²⁶ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r. (Dz.U. 1997 nr 78 poz. 483).

²⁷ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:pl:PDF>

²⁸ Tak art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 ze zm.).

Średnio lub pośrednio. Może się to przejawiać poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka indywidualnych właściwości określających jej cechy fizyczne, umysłowe, fizjologiczne, kulturowe, ekonomiczne lub społeczne.

Jednakże informacji nie uważa się za umożliwiającą określenie tożsamości osoby, gdy wymaga to nadmiernych kosztów, czasu lub działań²⁹.

Na podstawie wskazanych powyżej przepisów u.o.d.o. można stwierdzić, że dane osobowe to wszelkie informacje dotyczące osoby fizycznej, które identyfikują lub chociażby pozwalają bez większego wysiłku tę osobę zidentyfikować, mimo tego, iż nie jest ona precyjnie wskazana³⁰.

W kontekście danych biometrycznych, należy wskazać, że u.o.d.o. nie zawiera definicji legalnej tych danych, ani bezpośredniego odwołania do nich. Dlatego, w ogólnym i modelowym ujęciu, ich kwalifikacja w ramach definicji „dane osobowe” może nie być jednoznaczna biorąc pod uwagę ich liczbę, różnorodność, specyficzne właściwości, cel i sposób wykorzystywania. Niemniej jednak, zdaniem autorów niniejszej części raportu, biorąc pod uwagę:

- dane biometryczne przeznaczone do wykorzystania w sektorze bankowym
- (np. naczynia krwionośne palca, naczynia krwionośne dłoni, odcisk palca, biometria głosu);
- możliwość, a właściwie konieczność połączenia danych biometrycznych z innymi danymi i informacjami o konkretnych klientach banków udzielających zgody na wykorzystywanie ich danych biometrycznych przez banki; oraz
- podążając za wskazaną powyżej definicją danych osobowych,

należy stwierdzić, iż dane biometryczne mogą być traktowane jako dane osobowe, gdyż umożliwiają zidentyfikowanie (a właściwie zweryfikowanie, które w myśl ustawy wydaje się być stosowane synonimcznie) określonej osoby na podstawie unikalnych cech.³¹

W art. 6 u.o.d.o. za **dane osobowe uznano zatem wszelkie informacje, które mogą zostać powiązane**

29 Tak art. 6 ust. 3 ustawy z dnia 29 sierpnia 1997 r. ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 ze zm.). Por. także: szersze rozważania dotyczące testu proporcjonalności w kontekście danych biometrycznych: R. Kaszubski, M. Sudoł, T. Woszczyński, Z. Marcinkiewicz, J. Ratajczak, A. Czajka, *Prawne Aspekty Biometrii*, Warszawa 2011, http://www.hitachi.pl/veinid/documents/OK_Raport_Biometria.pdf.

30 Por. także poprzednią wersję raportu: R. Kaszubski, M. Sudoł, T. Woszczyński, Z. Marcinkiewicz, J. Ratajczak, A. Czajka, *Prawne Aspekty Biometrii*, Warszawa 2011, http://www.hitachi.pl/veinid/documents/OK_Raport_Biometria.pdf.

31 A.Kowalik, *ABC Ochrony Danych Osobowych*, Warszawa 2007, s. 8 i nast.

z osobą fizyczną, tj. także dane utrwalone jako obraz lub dźwięk, odciski palców, informacje o kodzie genetycznym, czyli także informacje biometryczne.³²

Mimo wszystko, każdorazowo jednak, w odniesieniu do **danych biometrycznych** niezbędne jest sprawdzenie na podstawie wymienionego art. 6 u.o.d.o., czy **wybрана do dokonania pomiaru cecha, jest daną osobową**, czy tylko informacją pochodząą od osoby, niepodlegającą ustawowej ochronie.³³

Należy zatem przeprowadzić badania, sprawdzające daną cechę pod względem zawierania **informacji, umożliwiającej zidentyfikowanie konkretnej osoby fizycznej** (art. 6 ust. 1 u.o.d.o.). Ustaleniu podlega również fakt, czy tożsamość zidentyfikowanej osoby można określić bezpośrednio lub pośrednio, przez powołanie się na specyficzne czynniki określające m. in. jej cechy fizyczne (art. 6 ust. 2 u.o.d.o.).

Ustawa formułuje również **zasadę proporcjonalności**, która wskazuje, iż informacja nie jest uważana za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.³⁴

Uwzględniając wskazania Rekomendacji Komitetu Ministrów Rady Europy³⁵, w epoce rozwijających się technik informatycznych, kryterium proporcjonalności kosztów traci na swojej istocie jako odniesienie, które pozwala ustalić możliwość zidentyfikowania danej osoby fizycznej. Ustalenie nadmiernych kosztów, czasu lub działań, należy każdorazowo dokonywać z uwzględnieniem konkretnego administratora danych osobowych. Informacja tego samego rodzaju może być zatem dla jednego podmiotu, wystarczająca do szybkiego ustalenia tożsamości danej osoby, dla innego natomiast mogą być to działania nieproporcjonalne.³⁶

Dane biometryczne, spełniające ustawowe warunki wskazane powyżej „miesząc się w definicji danych osobowych”. Nie można jednak uznać, że wszystkie dane biometryczne wymagają zastosowania takiej samej ochrony. Ze względu na konieczność zweryfikowania dodatkowych przesłanek, przewidzianych przez ustawę oraz wynikających z konkretnych właściwości poszczególnych biometrii i zastosowanych metod, służących zabezpieczeniu wzorców biometrycznych należy poddać je indywidualnej ocenie.³⁷

32 A. Drozd, *Komentarz do art. 6 ustawy o ochronie danych osobowych*, LexPolonica 2008.

33 Prof. dr hab. R.W. Kaszubski, „Biometria w bankowości”, Konferencja Spring Biometric Summit 2011, 14-15 kwietnia 2011, Warszawa.

34 Ibidem.

35 Rekomendacja No R (97) 5 dotycząca ochrony danych medycznych przyjęta 13.2.1997 r.

36 P. Barta; P. Litwiński, *Komentarz do art. 6 ustawy o ochronie danych osobowych*, Legalis 2009

37 Ibidem.

„Każda metodę biometrycznego uwierzytelnienia oraz informację, którą za sobą niesie, należy zbadać indywidualnie”

Dane „zwykłe” i dane „szczególnie chronione”

Opisując pojęcie danych biometrycznych należy zwrócić uwagę na rozróżnienie danych osobowych na dane „zwykłe” i dane „szczególnie chronione”. Przytoczone pojęcia nie są zdefiniowane bezpośrednio w ustawie o ochronie danych osobowych, jednak wynikają przywołanej ustawy.³⁸

Dane szczególnie chronione zwane również „wrażliwymi” zostały opisane w art. 27 ust.1 u.o.d.o. Należą do nich informacje o rasowym lub etnicznym pochodzeniu człowieka, poglądach religijnych, politycznych, filozoficznych, wyznaniu, przynależności partyjnej lub związkowej, stanie zdrowia, kodzie genetycznym, a także nałogach, życiu seksualnym, skazaniach, orzeczeniach o ukaraniu, mandatach i innych orzeczeniach wydanych w postępowaniu przed sądem lub urzędem.³⁹

Kryterium wyróżnienia informacji jako danych objętych szczególną ochroną należy doszukiwać się w uwarunkowaniu, iż związane są one ze sferami należącymi do prywatności czy nawet intymności osoby fizycznej, jak również wysokim poczuciem zagrożenia oraz niebezpieczeństwem na polach związanych z ochroną danych. **Należy zaznaczyć, iż przepisy polskiej ustawy wykraczają poza zakres pojęcia danych „wrażliwych” ukształtowanych w Dyrektywie 95/46/WE, obejmując ochroną również informacje o kodzie genetycznym i nałogach.**⁴⁰

Dane „zwykłe” są to natomiast informacje o osobach niewymienione w art. 27 ust. 1 przywołanej ustawy. Zaliczamy do nich m. in. imię, nazwisko, numer PESEL. Dane te podlegają ochronie, jednak nie są poddane szczególnej ochronie ze względu na ich charakter oraz fakt, iż nie dotykają intymnych dla człowieka sfer.⁴¹

38 A.Kowalik, *ABC Ochrony Danych Osobowych*, Warszawa 2007, s. 9-10.

39 Ibidem.

40 Por. E. Kulesza, *Ochrona danych o stanie zdrowia w świetle ustawodawstwa europejskiego i polskiej ustawy o ochronie danych osobowych*, Prawo i Medycyna 2000, Nr 5.

41 A.Kowalik, *ABC Ochrony Danych Osobowych*, Warszawa 2007, s. 9-10.

Klasyfikując dane biometryczne, należy stwierdzić, iż nie można jednoznacznie określić do której grupy będą one należały. **Zależy to od indywidualnego charakteru danej biometrii oraz faktu zawartej lub możliwej do odczytania informacji, która zdeterminuje czy są to dane szczególnie chronione, czy dane „zwykłe”.**

Informacją/wartością prawnie chronioną poddaną ustawowej, szczególnej ochronie jest m.in. **stan zdrowia osoby fizycznej**. Dla przykładu, wydaje się, że metodą biometryczną, która ze względu na sposób przeprowadzenia i zapisu jest nośnikiem danych na temat zdrowia może być **biometria tęczówki oka**. Na obrazie tęczówki zapisany jest stan narządów wewnętrznych i zewnętrznych oraz informacja o tym, jakimi chorobami dana osoba jest dziedzicznie zagrożona. **Irydolog**, lekarz zajmujący się oceną zdrowia na podstawie wyglądu tęczówki, jest w stanie określić kondycje każdego układu i narządów wewnętrznych oraz stwierdzi na jaką chorobę obecnie cierpi dana osoba.

W świetle ustawy należy uznać, że **informacje uzyskane na podstawie biometrii tęczówki oka mogą być danymi osobowymi szczególnie chronionymi**. Bez wątpienia były by nimi również biometrie opierające swoje działanie o kod DNA. Spełnione są bowiem przesłanki zarówno z art. 6 u.o.d.o., decydującej o przynależności informacji do **definicji danych osobowych**, jak i z art. 27 ust.1 u.o.d.o., które pozwalają określić te dane jako „wrażliwe”, poddane szczególnej ochronie.

Ze względu na spełnienie ustawowych przesłanek z art. 6 u.o.d.o danych osobowych należą również odciski palców, czy też biometrie naczyniowe. Wydają się to jednak być dane biometryczne zaliczane do danych osobowych „zwykłych”, gdyż, według wiedzy autorów, sposób i techniki ich wykorzystania nie wymagają i **nie opierają swojego działania, czy też nie pozwalają na odczytanie istotnych informacji** wymienionych w art. 27 ust.1 ustawy.

Powyższe przykłady pokazują, że **każda metodę biometryczną uwierzytelnienia oraz informację, którą za sobą niesie, należy zbadać indywidualnie**. Jest to niezbędne do dokonania właściwej klasyfikacji czy dana metoda mieści się w definicji danych osobowych i jakiej ewentualnej ochronie podlega.

Należy zwrócić uwagę, na kolejne istotne pojęcie w zakresie wykorzystywania danych biometrycznych, jakim jest ich przetwarzanie. Pod uregulowanym w ustawie pojęciem przetwarzania danych osobowych, a zarazem danych biometrycznych mieści się wykonywanie na nich jakichkolwiek operacji. **Przetwarzaniem jest zatem już samo przechowywanie danych, nawet jeśli nie są one faktycznie wykorzystywane**. W definicji przetwarzania mieści się także ich zmiana, udostępnianie, zbieranie, modyfikowanie, przekazywanie, utrwalanie, a zwłaszcza operacje wykonywane w systemach informatycznych. Ustawa definiuje pojęcie „**przetwarzanie**”

rzania”, brak jest natomiast definicji poszczególnych postaci przetwarzania, takich jak: udostępnianie, przekazywanie. Wydaje się, że należy je zatem przyjmować zgodnie z ich słownikowym znaczeniem.⁴²

Wymóg dopuszczalności przetwarzania danych z art. 23 u.o.d.o. jak i **zakaz przetwarzania** zawarty w art. 27 ust. 2 tej ustawy, stanowią istotne zadanie do spełnienia dla każdego administratora danych osobowych, w tym biometrycznych. Podstawową przesłanką uchylającą zakaz przetwarzania danych „wrażliwych”, jak i dopuszczającą przetwarzanie danych „zwykłych”, jest zgoda osoby, której dane dotyczą.

Pojęcie „**zgody**” zdefiniowane jest w art. 7 pkt. 5 u.o.d.o., rozumie się przez nie **oświadczenie woli zainteresowanej osoby**, wyrażające zgodę na przetwarzanie jej danych osobowych. **Zgoda ta nie może być domniemana**, a także dorozumiana z oświadczenia woli o innej treści złożonego przez daną osobę fizyczną.

Ponadto, nie tylko zgoda będzie mogła stanowić przesłankę legalizacji przetwarzania danych biometrycznych. Kolejna, autonomiczna przesłanka legalizująca przetwarzanie danych osobowych zawarta w art. 23 i 27 ustawy stanowi, że dopuszczalne jest przetwarzanie danych w sytuacji, gdy jest to niezbędne dla realizowania **uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa**. Dodatkowo w odniesieniu do danych „wrażliwych” zawartych w art. 27 ust. 2 pkt. u.o.d.o. zaznaczono, iż przepis prawa musi także stwarzać **pełne gwarancje ochrony**.

Ponadto w niektórych przypadkach, pod rozwałgę można poddać legalizację przetwarzania danych biometrycznych na podstawie pownie usprawiedliwionego celu administratora danych, o ile możliwym bedzie jego wykazanie przez tegoż administratora.

Wykorzystanie **danych jest dopuszczalne**, jeżeli zostanie spełniona opisana wyżej przesłanka wyrażenia **zgody** osoby, której dane dotyczą (art. 27 ust. 2 pkt 1 u.o.d.o. lub jeśli **zezwala na to przepis szczególny** innej ustawy, dający pełne gwarancje ochrony tych danych lub chociażby administrator danych będzie w stanie wykazać swój prawnie usprawiedliwiony cel takiego przetwarzania).

Przetwarzanie danych biometrycznych, poddanych szczególnej ochronie ustawy dopuszcza się również m.in., jeśli celem jest **ochrona żywotnych interesów** osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, fizycznie lub prawnie nie jest w stanie wyrazić zgody, do czasu ustanowienia opiekuna prawnego albo kuratora (art. 27 ust. 2 pkt 3 u.o.d.o.).

Analizując przedstawiony podział na **dane „zwykłe”** oraz **dane szczególnie chronione** zwane „wrażliwymi”, od strony *ratio legis* nie można takiemu rozróżnie-

niu zarzucić braku zasadności. Paradoksalnie, należy jednak zaznaczyć, iż ten dwupodział jest nieco sztuczny, co sprawia, iż nie zawsze spełniony jest cel, w jakim został ten podział wprowadzony. **Czasami bowiem dane, które należą do sfery mniej chronionej mogą nieść istotniejsze informacje**, których ujawnienie/utrata pociągnie za sobą więcej szkód.⁴³

Szeroki zakres ustawowych wyjątków od potrzeby uzyskania zgody na przetwarzanie danych osobowych może wiązać się z pewnym ryzykiem dostania się **ważnych informacji** w niepowołane ręce. Dlatego niezwykle istotne jest ciągle **doskonalenie przepisów prawa przez ustawodawcę**, doskonalenie sposobu ich rozumienia przez teorię prawa oraz doskonalenie sposobu och i stosowania przez praktykę prawa w oparciu o szeroko poczynione badania różnych dziedzin życia. Jak i absolutne **przestrzeganie prawa** i związanego z nim bezpiecznego przetwarzania danych biometrycznych przez administratora takich danych.

10.3. Biometria a prawo pracy

Wprowadzenie

O ile wykorzystywanie biometrii w bankowości w relacji bank - klient banku budzi obecnie coraz to mniejsze wątpliwości, o tyle inaczej sprawa przedstawia się na gruncie relacji pracowniczych w banku. Wątpliwości te związane są ze sposobem interpretacji art. 22¹ Kodeksu pracy. Zgodnie z tym artykułem:

§ 1.

“**Pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:**

- 1) imię (imiona) i nazwisko,
- 2) imiona rodziców,
- 3) datę urodzenia,
- 4) miejsce zamieszkania (adres do korespondencji),
- 5) wykształcenie,
- 6) przebieg dotychczasowego zatrudnienia.

§ 2.

Pracodawca ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w § 1, **także**:

- 1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,
- 2) numeru PESEL pracownika nadanego przez Rzą-

42 Ibidem.

43 Ibidem.

dowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL).

§ 3.

Udostępnienie pracodawcy danych osobowych następuje w **formie oświadczenia osoby**, której one dotyczą. Pracodawca ma **prawo żądać udokumentowania** danych osobowych osób, o których mowa w § 1 i 2.

§ 4.

Pracodawca **może żądać podania innych danych osobowych** niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

§ 5.

W zakresie nieuregulowanym w § 1-4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych.

W kontekście wykorzystywania danych biometrycznych pracowników rozstrzygał m.in. Naczelnego Sądu Administracyjnego w wyroku z dnia 1 grudnia 2012 r., sygn. akt i OSK 249/09. Sąd stwierdził, że:

1. Brak równowagi w relacji pracodawca pracownik **stawia pod znakiem zapytania** dobrowolność wyrażenia zgody na pobieranie i przetwarzanie danych osobowych (biometrycznych). z tego względu ustawodawca ograniczył przepisem art. 22¹ Kodeksu Pracy katalog danych, których pracodawca **może żądać** od pracownika. Uznanie faktu wyrażenia zgody na podstawie art. 23 ust. 1 pkt. 1 ustawy o ochronie danych osobowych, jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. 22¹ Kodeksu pracy, stanowiłoby obejście tego przepisu;
2. Rzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro **zasada proporcjonalności** wyrażona w art. 26 ust. 1 pkt. 3 ustawy o ochronie danych osobowych, jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych, **do kontroli czasu pracy pracowników** jest nieproporcjonalne do zamierzonego celu ich przetwarzania.

Sąd powziął wskazane powyżej poglądy w następujących okolicznościach faktycznych:

1. Pracodawca pozyskał i wykorzystywał dane biometryczne **w celu ewidencji czasu pracy**;
2. Pracodawca wykorzystywał do ewidencji czasu pracy **odciski palca**;

3. Przetwarzanie odcisków palca pracowników w celu ewidencji czasu pracy oparł na podstawie **zgody pracownika**.

Wykorzystywanie biometrii do celów innych niż rejestracja czasu pracy

Należy zaznaczyć, iż przy formułowaniu tezy dotyczącej proporcjonalności, ocena została zawężona do celu, w jakim w przedmiotowej sprawie zostały zebrane dane biometryczne, tzn. do ewidencji czasu pracy. Przy formułowaniu tej tezy, wydaje się, że przedmiotem oceny sądu nie była ocena zasady proporcjonalności w kontekście innych możliwych celów wykorzystania biometrii.

W szczególności niewłaściwą wydaje się być automatyczna ocena nieproporcjonalności zastosowania biometrii w przypadku, w którym biometria wykorzystywana jest do innego celu, np. zwiększenia poziomu bezpieczeństwa. W szczególności, jeżeli weźmiemy pod uwagę sektor bankowy, posiadający szczególne prawa i obowiązki nałożone przez ustawodawcę.

Na kwestię tego, iż ocena proporcjonalności uzależniona jest od celu, w jakim wykorzystywane są dane biometryczne zdaje się również zwracać uwagę Generalny Inspektor Ochrony Danych Osobowych. Dla przykładu warto przywołać kilka opublikowanych wypowiedzi w tym zakresie:

- 1) „(...) w przypadku danych biometrycznych istotne jest określenie, czy pozyskiwanie jest uzasadnione **ze względu na cel**, jaki chce w ten sposób uzyskać pracodawca. W większości przypadków należy na to pytanie odpowiedzieć negatywnie. Np. Czytniki biometryczne nie powinny być stosowane na potrzeby ewidencji czasu pracy. z drugiej strony wydaje się, że **można je stosować, jeśli w ten sposób pracodawca chce w pełni kontrolować dostęp pracowników np. do tajnych informacji lub niebezpiecznych materiałów (...)**”⁴⁴.
- 2) „(...) Konsekwentnie twierdzę, że dane biometryczne nie mogą być wykorzystywane na potrzeby stosunku pracy, czyli np., w celu mierzenia czasu pracy pracownika. Takie jest też stanowisko Naczelnego Sądu Administracyjnego i wojewódzkich sądów administracyjnych. **Ten sam pracodawca może jednak dane biometryczne wykorzystywać, np. do celów związanych z zapewnieniem bezpieczeństwa** jakichś szczególnych pomieszczeń np. takich, w których przechowywane są materiały wybuchowe, chemikalia, wirusy czy bakterii, a nawet dokumenty zawierające tajemnice

⁴⁴ Artykuł GŁODO (dr Wojciech Wiewiórowski) w Dzienniku Gazeta Prawna 12.08.2010 r. , o kontrolowaniu pracowników przez pracodawców, <http://www.giodo.gov.pl/>

przedsiębiorstwa (...)"⁴⁵

3) „(...) Uważam, że były, są i będą takie dziedziny życia, w których zbieranie danych biometrycznych będzie adekwatne i słuszne. Tak jest m.in. wszędzie tam, gdzie zadania wykonywane przez pracowników wiążą się z tajemnicą państwową. **Takie dane mogą być też zabezpieczeniem najistotniejszych miejsc w bankach.** w takich wypadkach również wyrażamy zgodę na ich stosowanie (...)"⁴⁶

4) „(...) Coraz częściej na potrzeby ewidencji czasu pracy firmy instalują czytniki linii papilarnych, struktury dłoni, tęczówki oka itp. Czy mogą stosować takie rozwiązania?

- Siegnięcie po tak wrażliwe dane osobowe, jakimi są dane biometryczne, jest zbyt dużą ingerencją w sferę prywatną pracownika. Dlatego nie każdy pracodawca może wprowadzić w miejscu pracy takie czytniki wystąpić do pracowników o przekazanie swoich danych biometrycznych.

Kto w takim razie może je instalować?

-Np. banki, kancelarie tajne czyli instytucje, które muszą szczególnie dbać o bezpieczeństwo posiadanych informacji. Natomiast wykorzystywanie danych biometrycznych tylko po to, aby należycie sprawdzać czas pracy, jest nieadekwatne w stosunku do celu, jaki pracodawca chce uzyskać.

A jeśli pracownik zgodzi się na stosowanie takich czytników?

- Zgoda zawsze może być wymuszona, bo pracodawca jest silniejszą stroną stosunku pracy. Pracownik może się bać, że przełożony zwolni go, jeśli nie zgodzi się na takie rozwiązanie. (...) Dlatego rozwiązaniem bezpieczniejszym byłoby uregulowanie tej kwestii w przepisach (...)"⁴⁷.

Jeżeli natomiast odnieść się do tezy wyroku dotyczącej odmówienia zgody pracownika cech dobrowolności, nie wydaje się aby zawsze w relacjach pracownik-pracodawca zgoda nie mogła mieć charakteru dobrowolnego. Mogą bowiem istnieć sytuacje, gdy mimo przewagi pracodawcy nad pracownikiem (raczej w ujęciu ekonomicznym, niekoniecznie prawnym) **zgodzie będzie można przypisać przymiot dobrowolności.** Wydaje się, iż cecha taka będzie spełniona w szczególności, gdy w związku z brakiem zgody pracownika nie spotkają

45 Artykuł GIODO (dr Wojciech Wiewiórowski) w Dzienniku Gazeta Prawna, 0201.2012, Głów zapach styl pisma mogą podlegać ochronie, <http://www.giodo.gov.pl/>

46 Artykuł GIODO (Michał Serzycki) w Rzecznopolskiej 25.01.2010 r., sfera prywatna jest ważnym dobrem osobistym, <http://www.giodo.gov.pl/>

47 Artykuł GIODO (Michał Serzycki) w Dzienniku Gazeta Prawna 20.10.2008 r. „Pozykiwanie danych biometrycznych pracowników jest niezgodne z prawem” <http://www.giodo.gov.pl/>

istotne negatywne konsekwencje, sankcje, nie będą na nim stosowane środki nacisku i w związku z tym będzie miał możliwość samodzielnego oceny sytuacji i dokonania realnego wyboru w zakresie wyrażenia lub odmowy zgody.

Ponadto, posługując się literalną interpretacją art. 22¹ Kodeksu pracy, należy zwrócić uwagę, że przepis stanoiwi o **braku możliwości żądania** przez pracodawcę dodatkowych danych/informacji. Oznacza to, że po stronie pracownika nie ma korelatywnie sprzążonego obowiązku do przekazania takich danych. Innymi słowy stwierdzenie, że pracodawca ma prawo żądać, oznaczałoby, że pracownik jest obowiązany do udzielenia żądanego informacji⁴⁸ (danych). Nie wydaje się jednak słusznym interpretowanie tego przepisu, w ten sposób, że pracodawca nigdy nie może wykorzystywać innych danych, przekazanych nawet za zgodą pracownika. Wydaje się, że w myśl przepisu pracodawca nie ma jedynie właściwego uprawnienia do polecenia pracownikowi przekazania takich danych, ani możliwości stosowania sankcji w stosunku do osób, które odmówią wyrażenia zgody na przekazanie takich danych.

Wykorzystywanie biometrii do rejestracji czasu pracy

Chociaż ocena przez orzecznictwo wykorzystywania biometrii do rejestracji czasu pracy jest negatywna, to jednak debata w tym zakresie nie wydaje się być zamknięta. Rozwój tego rodzaju systemów biometrycznych hamowany jest w Polsce przede wszystkim przez istniejące przepisy prawa i ich stosowanie.

Znane są co najmniej trzy prawomocne wyroki sądów administracyjnych wydane wobec: zakładu produkcyjnego [1], szpitala [2] oraz urzędu skarbowego [3]. Każda ze spraw miała swoje źródło w skardze na decyzję GIODO nakazującą zaprzestania przetwarzania biometrycznych danych osobowych. Wszystkie trzy wyroki, w odniesieniu do biometrii, są do siebie bardzo podobne i dlatego mogą być wspólnie omawiane. We wszystkich tych przypadkach stosowano urządzenia wykorzystujące biometrię linii papilarnych oraz starano się, aby pracownicy mieli swobodę wyboru sposobu rejestracji swojej obecności w pracy: z zastosowaniem technik biometrycznych lub w inny sposób. Przy wyborze biometrii pracownicy wyrażali pisemną zgodę w formie oświadczenia.

„Z oświadczenia tego wprost wynika, że osoba je składająca wyraża zgodę na przetwarzanie jej danych osobowych, którymi w tym przypadku są jej linie papilarne.” [1]

GIODO w swoich decyzjach kwestionował podstawy prawne do stosowania technik biometrycznych wobec osób pozostających w stosunku pracy i nakazywał

48 Por. K. Jaśkowski, E. Maniewska, Kodeks pracy. Komentarz. Ustawy towarzyszące z orzecznictwem. Europejskie prawo pracy z orzecznictwem. T.I, wyd. VIII, Lex 2012.

zaprzestania użytkowania biometrycznych systemów ewidencji czasu pracy. Skargi pracodawców, którzy odwoływali się od decyzji GIODO do sądów administracyjnych zostały oddalone.

Oprócz ogólnych regulacji, pod które można dokonać subsumpcji nowego stanu faktycznego, jaki tworzą systemy biometryczne, w Polsce nie ma bowiem kompleksowych przepisów prawa regulujących stosowanie biometrii (z wyjątkiem ustawy o policji), co powoduje, że pracodawcy, GIODO i sądy posługują się niejako zastępco, czy też pośrednio ogólnymi przepisami prawa, które w momencie ich stanowienia nie uwzględniały takiego rozwoju techniki i nie przewidywały wielu sytuacji dziś spotykanych, albo zostały uznane za tak oczywiste, iż nie wymagają regulacji prawnych.

Podstawowym zarzutem prawnym przeciw stosowaniu biometrii w RCP jest wg GIODO treść art. 22¹ Kodeksu Pracy [4] wskazanego na początku niniejszego rozdziału.

Wojewódzki Sąd Administracyjny w swoim uzasadnieniu wyroku [2] oddalenia skargi na decyzje GIODO stwierdził, że:

- 1) „na enumeratywnej liście z § 1 nie ma innych niż wymienione danych osobowych, w tym danych biometrycznych stąd, zdaniem GIODO, wynika zakaz stosowania biometrycznych systemów rejestracji czasu pracy. Wśród argumentów za taką interpretacją przepisów stoi przekonanie, że wzorce powstałe w wyniku przetworzenia obrazów cech biometrycznych (w tym przypadku linii papilarnych) do postaci ciągu bajtów - wzorca są danymi osobowymi w świetle art. 6 ust. 1 Ustawy o ochronie danych osobowych”.
- 2) „Ponadto, stosownie do art. 22¹ § 4 ustawy – Kodeksu pracy, pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów. Organ stwierdził, że zakres danych osobowych, jaki pracodawca może pozyskiwać od osoby zatrudnionej na podstawie umowy o pracę stanowi katalog zamknięty, szczegółowo określony przez przepisy prawa pracy. Wskazał, że pracodawca może pozyskiwać dodatkowe dane dotyczące pracownika, tylko w sytuacji, jeżeli obowiązek ich podania wynika z odrębnych przepisów prawa.”
- 3) „pisemna zgoda pracowników nie ma znaczenia, bowiem nie można mówić o równości pomiędzy pracodawcą i pracownikiem, jest zatem możliwe niejawne wymuszanie na pracownikach takiej zgody”.

Podobnej treści stwierdzenia można znaleźć w uzasadnieniach wyroków [1] i [3] Naczelnego Sądu Administracyjnego dotyczących stosowania technik biometrycznych w RCP.

W kontekście rejestracji czasu pracy, nieuzasadniony jest argument przytoczony w punkcie 1. Daje się

zauważać brak dostatecznego rozeznania aspektów technicznych i funkcjonalnych biometrii i technik biometrycznych, co w konsekwencji prowadzi do nieadekwatnych do rzeczywistości wniosków.

Wciąż bowiem panuje przekonanie o tym, że wzorce biometryczne są danymi osobowymi w rozumieniu art. 6 pkt.1 Ustawy o ochronie danych osobowych [5], bez dostatecznego uzasadnienia wynikającego z przeprowadzonych w tym zakresie analiz.

Z technicznego punktu widzenia, wzorzec biometryczny nie powstaje poprzez proste przetworzenie obrazu cechy biometrycznej do ciągu bajtów. Nim powstanie wzorzec, obraz cechy biometrycznej jest poddawany ekstrahowaniu punktów charakterystycznych, następnie przetworzeniu funkcją, zazwyczaj jednokierunkową, do postaci, która pozwala na łatwiejsze porównywanie wzorców i, przede wszystkim, uniemożliwia odtworzenie źródłowych cech biometrycznych. Na koniec przetwarzania wzorzec jest szyfrowany. W rezultacie wzorzec jest ciągiem bajtów, z których niemożliwe jest odtworzenie cechy biometrycznej.

Zatem koniecznym wydaje się przeprowadzenie dodatkowych rozważań w kontekście art. 6 pkt.3 Ustawy o ochronie danych osobowych [5] (*Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań*) czy rzeczywiście wzorce biometryczne nie są czy też nie są danymi osobowymi. Na podobny aspekt, w kontekście modelowego ujęcia (korzystania z wzorców biometrycznych przy systemach semianonomicznych) zwracano uwagę również w poprzedniej edycji raportu, pt. „Prawne Aspekty Biometrii”⁴⁹.

Dodatkowo należy również zwrócić uwagę, że przetwarzanie cechy biometrycznej - będącej daną osobową - do wzorca - mogącego nie stanowić już danej osobowej - jest wykonywane doraźnie, wyłącznie ze względów technicznych (w rozumieniu art. 2 ust. 3 UoODO). Biorąc pod uwagę taki punkt widzenia i proces powstawania wzorców, należałoby stwierdzić, że przywołana lista z art. 6 §1 Kodeksu Pracy [4] nie powinna mieć w takim przypadku zastosowania.

Argumenty przedstawione w punkcie 2 również budzą zastrzeżenia. Stwierdzenie, „że zakres danych osobowych, jaki pracodawca może pozyskiwać od osoby zatrudnionej na podstawie umowy o pracę stanowi katalog zamknięty, szczegółowo określony przez przepisy prawa pracy” może się wydawać słuszy, ale nie jest pozbawiony poważnego mankamentu. Otóż, gdy wymieniane są rodzaje technik biometrycznych, w każdym podręczniku, w każdym opracowaniu na ten temat, na każdej stronie internetowej zawsze można znaleźć na

⁴⁹ Por. R. Kaszubski, M. Sudoł, T. Woszczyński, Z. Marcinkowski, J. Ratajczak, A. Czajka, Prawne Aspekty Biometrii, Warszawa 2011, http://www.hitachi.pl/veinid/documents/OK_Raport_Biometria.pdf.

liście technik podpis odręczny. Niewątpliwie podpis odręczny jest cechą biometryczną, a co za tym idzie daną osobową, a jak podpis jest wyraźny, to do identyfikacji osoby składającej podpis nie potrzeba posiadać umiejętności grafologa.

„Problematyczna jest zatem stosowana w bardzo wielu przedsiębiorstwach i powszechnie usankcjonowana praktyka wykorzystywania do ewidencji czasu pracy tradycyjnej listy obecności

Stosując ściśle wykładnię wynikającą z przywołanego powyżej orzecznictwa, wniosek jaki się jawi jest paradoksalny: O ile pracodawca nie ma upoważnienia ustawowego do żądania podpisu pod konkretnym dokumentem, to pracodawca ten na podstawie zgody pracownika nie ma prawa do przetwarzania dokumentów pracowników sygnowanych ich podpisem. Podpis odreźnego nie ma bowiem na zamkniętej liście z art. 6 § 1 k. p. a podpis taki jest ewidentnym nośnikiem danych biometrycznych.

Problematyczna jest zatem stosowana w bardzo wielu przedsiębiorstwach i powszechnie usankcjonowana (jak dotychczas) praktyka wykorzystywania do ewidencji (rejestracji) czasu pracy tradycyjnej listy obecności. Taka papierowa lista ewidencji czasu pracy jest w istocie biometryczną listą obecności. Czyżby i ta „technologia” była na cenzurowanym? Należy wskazać, że obowiązek prowadzenia ewidencji czasu pracy wynika bezpośrednio z art. 149. § 1 k. p. [4]. Ustawa – Kodeks Pracy – natomiast nie preczyje sposobu prowadzenia ewidencji czasu pracy – dlatego też można dodatkowo rozważyć czy w takim przypadku nie zachodzi podstawa do zastosowania art. 22¹ § 4 k.p..

10.4. Podpis biometryczny

W kontekście aspektów prawnych powyższe rozważania dotyczyły głównie sfera publicznonarodowej ochrony prywatności i danych osobowych, która dotyczy dopełnienia wymogów regulacyjnych (np. dane osobowe, tajemnica bankowa),

Natomiast wykorzystywanie biometry do tworzenia tzw. Podpisu biometrycznego dotyczy sfery prywatnoprawnej, związanej w tym kontekście z zapewnieniem skuteczności oświadczeń woli związań czynnościami bankowymi (relacja bank-klient, relacja bank-pracownik, relacja bank/klient - administracja publiczna).

Na bazie ustawy o podpisie elektronicznym wyróżniamy dwa rodzaje podpisu elektronicznego:

- podpis elektroniczny weryfikowany certyfikatem kwalifikowanym,
- podpis elektroniczny weryfikowany certyfikatem niekwalifikowanym.

Podpis elektroniczny weryfikowany certyfikatem kwalifikowanym, jeśli złożony jest zgodnie z wymaganiami tej ustawy, zapewnia skutek prawnego podpisu elektronicznego równoważny z podpisem odreźnym. Zapisy art. 48 tej ustawy eliminują jednak możliwość zastosowania podpisu kwalifikowanego w systemie podpisu serwerowego, w którym klucze prywatne użytkowników przechowywane są centralnie.

Z kolei podpis elektroniczny weryfikowany certyfikatem niekwalifikowanym nie zapewnia równoważności formy elektronicznej z papierową podpisanego dokumentu.

Jednakże banki, działające w oparciu o prawo bankowe mają możliwość zapewnienia składania oświadczeń woli w formie elektronicznej, który będzie równoważny z podpisem pidemnym zastrzeżonym pod rygorem nieważności na podstawie art. 7 prawa bankowego. Takie uprawnienie wynika wprost z art. 7 ust. 1 prawa bankowego.

Co więcej, przy spełnieniu warunków określonych w prawie bankowym oraz Rozporządzenia Rady Ministrów z dnia 26 października 2004 r. w sprawie sposobu tworzenia, utrwalania, przekazywania przechowywania i zabezpieczania dokumentów związanych z czynnościami bankowymi na elektronicznych nośnikach informacji⁵⁰, banki uprawnione są do sporządzania dokumentów na elektronicznych nośnikach danych.

W związku z powyższymi, wykorzystanie biometrii w kontekście postanowień prawa bankowego i rozporządzeń wykonawczych do nich, może umożliwić znaczną automatyzację i digitalizację wielu dotychczasowych procesów/czynności bankowych dokonywanych w sposób tradycyjny, tj. papierowy.

50 Dz. U. z 2004 r., nr 236, poz. 2364.

10.5. Biometria a prawo podatkowe

Nieuwzględniany - jak dotąd - w literaturze przedmiotu podatkowy aspekt biometrycznych metod uwierzytelniania przejawia się m.in. w regulacji dotyczącej tzw. ulgi technologicznej, przewidzianej w art. 18 b ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych⁵¹. Przybliżenie tego zagadnienia wydaje się o tyle istotne, że jak wskazuje raport Ministerstwa Gospodarki „Przedsiębiorczość w Polsce” w wrześniu 2011 r., spośród 100 przedsiębiorców działających w sektorach, w których najczęściej korzystano z ulgi 43% nie wiedziało o możliwości korzystania z ulgi⁵². Niewątpliwie ważny wydaje się również fakt, że podatnicy podatku dochodowego od osób prawnych odnoszą z tytułu nabycia nowych technologii korzyść nie tylko z tytułu **odliczenia wydatków** na ich nabycie, lecz także - na zasadzie wyjątku - z racji **odpisów amortyzacyjnych**.

Wydatki poniesione na nabycie technologii biometrycznych przez podatnika podatku dochodowego od osób prawnych mogą podlegać odliczeniu od podstawy opodatkowania (art. 18b ust. 1 p.d.o.p.), o ile spełniają ustawową definicję nowych technologii.

Zgodnie z definicją legalną wprowadzoną na mocy art. 18b ust. 2 p.d.o.p., za nowe technologie uważa się wiedę technologiczną w postaci wartości niematerialnych i prawnych, w szczególności wyniki badań i prac rozwojowych, która umożliwia wytwarzanie nowych lub udoskonalanie wyrobów lub usług.

W rozumieniu tego przepisu warunkiem koniecznym dla uznania technologii - w tym biometrycznej - za nową jest również jej **niestosowanie na świecie przez okres dłuższy niż ostatnich 5 lat**. Obligatoryjne jest również uzyskanie **opinii niezależnej od podatnika jednostki naukowej** w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki⁵³ w przedmiocie innowacyjności (okresu stosowania, nie istnienia⁵⁴) technologii. Stosownie do art. 2 pkt. 9 tej ustawy, jednostki naukowe to prowadzące w sposób ciągły badania naukowe lub prace rozwojowe:

- a) podstawowe jednostki organizacyjne uczelni w rozumieniu statutów tych uczelni;
- b) jednostki naukowe Polskiej Akademii Nauk w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o Polskiej Akademii Nauk⁵⁵;

51 Tj. Dz. U. z 2011 r., Nr 74, poz. 397 z późn. zm., dalej: p.d.o.p.

52 http://www.mg.gov.pl/files/upload/14678/MG_DAP_SM%20BP%20www_Rop2011_20111011.pdf, dostęp z dnia 30 maja 2012 r., godz. 12:05.

53 Dz. U. Nr 96, poz. 615 z późn. zm.

54 A. Mariański, Komentarz do art. 18b p.d.o.p. w: A. Mariański, D. Strzelec, M. Wilk „Ustawa o podatku dochodowym od osób prawnych: komentarz”, Wolters Kluwer Polska, Warszawa 2011 r., s. 473.

55 Dz. U. Nr 96, poz. 619 z późn. zm.

- c) instytuty badawcze (np. Instytut Maszyn Matematycznych);
- d) międzynarodowe instytuty naukowe utworzone na podstawie odrębnych przepisów, działające na terytorium Rzeczypospolitej Polskiej;
- e) Polską Akademię Umiejętności;
- f) inne jednostki organizacyjne, niewymienione w lit. a-e, posiadające osobowość prawną i siedzibę na terytorium Rzeczypospolitej Polskiej, w tym przedsiębiorców posiadających status centrum badawczo-rozwojowego, nadawany na podstawie ustawy z dnia 30 maja 2008 r. o niektórych formach wspierania działalności innowacyjnej⁵⁶.

Odnosząc się do formy dokumentu przedmiotowej opinii należy przytoczyć stanowisko Naczelnika Pierwszego Urzędu Skarbowego w Szczecinie zawarte w interpretacji z dnia 27 listopada 2006 r., IUS.PO/423/4/EK/2006. Naczelnik Urzędu stwierdził, że opinia powinna stanowić załącznik do faktury zakupu, jednak przepisy prawa podatkowego nie określają, czy musi to być oryginał, czy potwierdzona kserokopia opinii⁵⁷.

Odliczeniu podlega nabycie nowej technologii (w tym biometrycznej), przez co ustawodawca rozumie nabycie praw do wiedzy technologicznej, o której mowa w ust. 2, w drodze umowy o ich przeniesienie, oraz korzystanie z tych praw (art. 18b ust. 2a p.d.o.p.).

Dopuszczalna **wielkość odliczenia** związanego z nabyciem nowej technologii nie może przekroczyć 50% kwoty wydatków poniesionych przez podatnika na nabycie tej technologii, uwzględnionych w wartości początkowej, w części, w jakiej została zapłacona podmiotowi uprawnionemu w roku podatkowym, w którym nową technologię wprowadzono do ewidencji środków trwałych oraz wartości niematerialnych i prawnych lub w roku następującym po tym roku, oraz w której nie została zwrócona podatnikowi w jakiejkolwiek formie (art. 18b ust. 4 i 7 p.d.o.p.). Przedpłaty (zadatki) dokonane przez podatnika na poczet powyższych wydatków w roku poprzedzającym rok, w którym wprowadzono nową technologię do ewidencji środków trwałych oraz wartości niematerialnych i prawnych, uznaje się dla potrzeb podatkowych za poniesione w roku wprowadzenia nowej technologii do tej ewidencji (art. 18b ust. 5 p.d.o.p.).

Zgodnie z art. 18b ust. 6 p.d.o.p. odliczenia dokonywane są w **zeznaniu za rok podatkowy, w którym poniesiono wydatki** na nabycie nowych technologii. Ponadto, gdy podatnik osiąga za rok podatkowy stratę lub wielkość dochodu z pozarolniczej działalności podatnika jest niższa od kwoty przysługujących mu odliczeń, odliczenia odpowiednio w całej kwocie lub w pozostałej części dokonuje się w zeznaniach za kolejno następu-

56 Dz. U. Nr 116, poz. 730 z późn. zm.

57 LEX OMEGA nr 25331.

jące po sobie trzy lata podatkowe licząc od końca roku, w którym nową technologię wprowadzono do ewidencji środków trwałych oraz wartości niematerialnych i prawnych.

Ustawodawca podatkowy wyłączył zastosowanie art. 16 ust. 1 pkt 48 p.d.o.p. do przypadku odliczeń na nabycie nowych technologii. Kosztem uzyskania przychodów będą zatem - w przypadku technologicznej wiedzy biometrycznej uznanej za nową technologię w świetle art. 18b ust. 1 p.d.o.p. - odpisy z tytułu zużycia wartości niematerialnych i prawnych dokonywane, według zasad określonych w art. 16a-16m p.d.o.p., od tej części ich wartości, która odpowiada poniesionym wydatkom na nabycie tych wartości niematerialnych i prawnych, odliczonym od podstawy opodatkowania podatkiem dochodowym albo zwróconym podatnikowi w jakiejkolwiek formie. Powyższe oznacza, że nowe technologie biometryczne podlegają amortyzacji u ich nabywców.

Zastosowanie ulgi technologicznej podlega pewnym ograniczeniom. Na mocy art. 18b ust. 3 p.d.o.p. prawo do odliczenia nie przysługuje podatnikowi prowadzącemu w roku podatkowym lub w roku poprzedzającym działalność na terenie specjalnej strefy ekonomicznej na podstawie zezwolenia⁵⁸.

Ustawodawca przewidział ponadto szereg stanów faktycznych, których wystąpienie skutkuje utratą prawa do ulgi technologicznej. Podatnik traci prawo do odliczeń, jeśli udzieli w jakiejkolwiek formie lub części innym podmiotom prawa do nowej technologii, przy czym nie dotyczy to przeniesienia prawa w wyniku przekształcenia formy prawnej oraz łączenia lub podziału dotychczasowych przedsiębiorców, dokonywanych na podstawie przepisów Kodeksu spółek handlowych (art. 18b ust. 8 pkt 1 p.d.o.p.). Utrata tego prawa związana jest też ze zwrotem wydatków na nową technologię w jakiejkolwiek formie (art. 18b ust. 8 pkt 3 p.d.o.p.). Także ogłoszenie upadłości obejmującej likwidację majątku podatnika oraz postawienie w stan likwidacji powoduje utratę prawa do ulgi (art. 18b ust. 8 pkt 2 p.d.o.p.). Powyższe przesłanki nie będą jednak skutkować utratą prawa do ulgi, o ile opisane zdarzenia prawne nastąpią po upływie upływu trzech lat podatkowych licząc od końca roku podatkowego, w którym podatnik wprowadził nową technologię do ewidencji środków trwałych oraz wartości niematerialnych i prawnych (art. 18b ust. 8 p.d.o.p. *a contrario*).

Ustawodawca przewidział ponadto szereg stanów faktycznych, których wystąpienie skutkuje utratą prawa do ulgi

W przypadku zaistnienia okoliczności skutkujących utratą prawa do odliczenia, podatnik jest obowiązany w zeznaniu podatkowym składanym za rok, w którym wystąpiły te okoliczności, do zwiększenia podstawy opodatkowania o kwotę dokonanych odliczeń, do których utracił prawo, a w razie poniesienia straty - do jej zmniejszenia o tę kwotę (art. 18b ust. 9 p.d.o.p.). W przypadku utraty ulgi z uwagi na zwrot wydatków, kwotę odliczeń, do której podatnik utracił prawo, określa się proporcjonalnie do udziału zwróconych wydatków w wartości początkowej nowej technologii. Zasada ta znajduje zastosowanie odpowiednio w razie utraty przez podatkową grupę kapitałową⁵⁹ statusu podatnika - obowiązek zwiększenia podstawy opodatkowania ciąży wówczas na spółce, która wprowadziła nową technologię do ewidencji środków trwałych oraz wartości niematerialnych i prawnych (art. 18b ust. 10 p.d.o.p.).

Odnosząc się do ograniczeń związanych z omawianą ulgą technologiczną zasadne będzie przywołanie rozważań Wojewódzkiego Sądu Administracyjnego we Wrocławiu, który podkreślił m.in., że „*Premiując podatkowo wprowadzanie przez przedsiębiorców nowych technologii ustawodawca nie objął ulgą całości wydatków, jakie podatnik musi ponieść, by z nowych technologii skorzystać, ale ich specyficzną kategorię, tj. te które, najogólniej ujmując, wiążą się z uzyskaniem dostępu i praw do wiedzy i rezultatów badań. Taki charakter ulgi wyraźnie potwierdza też ust. 2a art. 18 b, w którym mówiąc o nabyciu nowych technologii, w kontekście omawianej ulgi, ustawodawca wskazuje, że chodzi o nabycie praw do wiedzy technologicznej, o której mowa w ust. 2. Objęte ulga wydatki na nowe technologie zostały więc znowu w tym przepisie portraktowane wąsko i sprowadzone do wydatków na nabycie "praw do wiedzy"*”⁶⁰.

W kontekście powyższych rozważań, należy stwierdzić, że korzyści podatkowe może także odnieść podmiot (w tym bank) nabywający licencję np. na zakup oprogramowania serwerowego do uwierzytelniania bio-

58 Zezwolenie wydawane jest na prowadzenie działalności gospodarczej na terenie danej strefy przez ministra właściwego do spraw gospodarki stosownie do przepisów rozdziału 4 ustawy z dnia 20 października 1994 r. o specjalnych strefach ekonomicznych (tj. Dz. U. z 2007 r., Nr 42, poz. 274 z późn. zm.).

59 Dotyczy to podatkowej grupy kapitałowej, o której mowa w art. 1a p.d.o.p.

60 Wyrok WSA we Wrocławiu z dnia 6 października 2010 r., sygn. akt i SA/Wr 763/10, <http://orzeczenia.nsa.gov.pl/do-c/7F02561E1D>.

metrycznego. Nabyte i nadające się do gospodarczego wykorzystania w dniu przyjęcia do używania licencje o przewidywanym okresie używania dłuższym niż rok, wykorzystywane przez podatnika na potrzeby związane z prowadzoną przez niego działalnością gospodarczą albo oddane przez niego do używania na podstawie umowy licencyjnej (sublicencji), umowy najmu, dzierżawy lub umowy określonej w art. 17a pkt 1 p.d.o.p.⁶¹, zwane wartościami niematerialnymi i prawnymi zgodnie z art. 16b ust. 1 pkt 5 p.d.o.p. **podlegają bowiem amortyzacji**⁶².

Niezależnie z kolei od przewidywanego okresu używania podlegają amortyzacji **także koszty prac rozwojowych** zakończonych wynikiem pozytywnym, który może być wykorzystany na potrzeby działalności gospodarczej podatnika (art. 16b ust. 2 pkt 3 p.d.o.p.). W takim przypadku **odpisu amortyzacyjnego dokonuje podmiot, który tworzy nowe technologie biometryczne**.

Przez prace rozwojowe należy rozumieć, zgodnie z art. 2 pkt 4 ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki⁶³ nabywanie, łączenie, kształcanie i wykorzystywanie dostępnej aktualnie wiedzy i umiejętności z dziedziny nauki, technologii i działalności gospodarczej oraz innej wiedzy i umiejętności do planowania produkcji oraz tworzenia i projektowania nowych, zmienionych lub ulepszonych produktów, procesów i usług. Warunkiem zastosowania odpisu amortyzacyjnego w przypadku kosztów prac rozwojowych jest **łączne spełnienie trzech warunków**:

- a) Produkt lub technologia wytwarzania zostały ścisłe ustalone, a dotyczące ich koszty prac rozwojowych wiarygodnie określone.
- b) Techniczna przydatność produktu lub technologii została stwierdzona i odpowiednio udokumentowana i na tej podstawie podmiot podjął decyzję o wytwarzaniu tych produktów lub stosowaniu technologii.
- c) Koszty prac rozwojowych zostaną pokryte spodziewanymi przychodami ze sprzedaży tych produktów lub zastosowania technologii.

Według najlepszej wiedzy i oceny autorów niniejszej części opracowania, w odniesieniu do wybranych technologii biometrycznych istnieją silne argumenty promawiające za uznaniem ich za produkt innowacyjny,

61 Przepis ten dotyczy umowy leasingu, przez którą prawodawca podatkowy rozumie umowę nazwaną w kodeksie cywilnym, a także każdą inną umowę, na mocy której jedna ze stron (finansującej), oddaje do odpłatnego używania albo używania i pobierania pożytków na warunkach określonych w ustawie drugiej strонie, (korzystający), podlegające amortyzacji środki trwałe lub wartości niematerialne i prawne, a także grunty oraz prawo wieczystego użytkowania gruntów.

62 Odpisy amortyzacyjne to odpisy z tytułu zużycia środków trwałych oraz wartości niematerialnych i prawnych i stanowią one koszt uzyskania przychodów (art. 15 ust. 6 p.d.o.p.).

63 Dz. U. Nr 96, poz. 615 z późn. zm.

zwiększający poziom bezpieczeństwa, polepszający jakość usług i niemający zastosowania na świecie przed okresem dłuższy niż 5 ostatnich lat. W związku ze spełnieniem wskazanych powyżej cech/wymogów istnieje możliwość zakwalifikowania wybranych technologii biometrycznych w ramach definicji legalnej „nowe technologie” w rozumieniu art. 18b p.d.o.p.

Powыższe stanowisko zostało również potwierdzone przez niezależną jednostkę naukową⁶⁴, z której pracami i dokumentami autorzy mieli okazję zapoznać się na etapie doradztwa prawnego świadczonego w zakresie wdrożenia jednej z technologii biometrycznych.

Biorąc pod uwagę stopień i okresy rozwoju poszczególnych technologii biometrycznych, możliwość zakwalifikowania ich w ramach „nowych technologii” i uzyskania z tego tytułu „korzyści podatkowych” wydaje się mieć zastosowanie i być zasadna w szczególności w stosunku do:

- a) technologii bazujących na „nieprzechwytywalnych” wzorcach biometrycznych⁶⁵; lub
- b) w odniesieniu do tzw. „odpisu biometrycznego” opierającego swoje działanie o wykorzystywanie wzorców o których mowa w punkcie (a) powyżej.

Podsumowując, przedsiębiorca zamierzający nabycie „nowe technologie biometryczne” może skorzystać z ulgi technologicznej oraz z odpisów amortyzacyjnych. Twórcy „nowych technologii biometrycznych” przysługuje natomiast uprawnienie do dokonania amortyzacji kosztów prac rozwojowych.

Korzyści podatkowe dla

nabywcy technologii	twórcy technologii
<ul style="list-style-type: none"> • odliczenie wydatków poniesionych na nabycie technologii biometrycznych art. 18b ust. 1 p.d.o.p. • amortyzacja kosztów prac rozwojowych art. 16b ust. 2 pkt 3 p.d.o.p. 	<ul style="list-style-type: none"> • amortyzacja zużycia nowych technologii art. 18b ust. 11 w zw. z art. 16 ust. 1 pkt 48 a contrario p.d.o.p.

64 Por. Opinia Instytutu Maszyn Matematycznych z dnia 23 marca 2011 r. potwierdzająca innowacyjność technologiczną systemu biometrycznego podpisu elektronicznego bazującego na technologii Finger vein, <http://www.hitachi.pl/veinid/bioPKI.html>

65 Por. szerzej o nieprzechwytywalności wzorców biometrycznych: R. Kaszubski, M. Sudół, T. Woszczyński, Z. Marcinkowski, J. Ratajczak, A. Czajka, *Prawne Aspekty Biometrii*, Warszawa 2011, http://www.hitachi.pl/veinid/documents/OK_Report_Biometria.pdf.

11. Autorzy raportu

11.1. Redakcja

- **Tadeusz Andrzej Woszczyński** – redaktor prowadzący i merytoryczny, współautor
Przewodniczący Grupy ds. Biometrii, Członek Prezydium Forum Technologii Bankowych ZBP Dyrektor Regionalny CEE i CIS, Grupa Systemów Informatycznych, Hitachi Europe Ltd.
- **Zbigniew Marcinkowski** – redaktor merytoryczny, współautor
Wiceprzewodniczący Grupy ds. Biometrii, Członek Prezydium Forum Technologii Bankowych ZBP Wiceprezes Zarządu, Algotech Polska Sp. z o.o.
- **Mariusz Sudoł** – redaktor merytoryczny i autor części prawnej
Ekspert Forum Technologii Bankowych ZBP

11.2. Współautorzy

- **Krzysztof Arciszewski**, IBM (obecnie KPMG)
- **Beata Bińkowska-Artowicz**
- **Sylwester Cekała**
- **Michał Czechowski**, KŁOS Nowoczesne Technologie Bankowe (obecnie NoaTech Sp. z o.o.)
- **Waldemar Częścik**, Powiślański Bank Spółdzielczy
- **Łukasz Hoppe**, Wasko S.A.
- **Przemysław Izwicki**, Wincor Nixdorf Sp. z o.o.
- **Wojciech Kujawa**, Podkarpacki Bank Spółdzielczy
- **Janusz Kurczych**, BS Kielce
- **Leszek Modzelewski**, BPH S.A.
- **Szymon Myśliński**, BiotrustIS Sp. z o.o. (obecnie ABB)
- **Mariusz Olszewski**, BPS S.A.
- **Daria Pawęda**, Getin Noble Bank S.A.
- **Robert Poznański**, Instytut Maszyn Matematycznych
- **Lech Szczeciński**, NCR Polska Sp. z o.o.
- **Michał Waluś**, ING Bank Śląski / Politechnika Śląska
- **Franciszek Wołowski**, PWPW S.A.
- **Jarosław Wójtowicz**, Instytut Maszyn Matematycznych

11.3. Koordynacja ze strony Związku Banków Polskich

- **Martyna Kubiak**, Sekretarz FTB
- **Ewelina Stępnik**, p.o. Sekretarza FTB



06.2014



ZWIĄZEK BANKÓW POLSKICH