IGOR TOMECKI*

Modelowy schemat silnego uwierzytelnienia użytkownika w kontekście europejskiej dyrektywy PSD2 oraz polskiej ustawy o usługach płatniczych

Streszczenie

Niniejszy artykuł poświęcony jest silnemu uwierzytelnieniu użytkownika, analizowanemu na gruncie drugiej dyrektywy o usługach płatniczych (*Payment Services Directive 2* – PSD2) oraz ustawy o usługach płatniczych. Obiektem badań były dostępne metody potwierdzania tożsamości użytkownika, które spełniają warunki narzucone przez legislaturę oraz są możliwe do wdrożenia przy obecnym poziomie rozwoju technologii. Celem artykułu jest wypracowanie modelowego schematu silnego uwierzytelnienia użytkownika spełniającego warunki narzucone przez europejskiego i krajowego legislatora. Zastosowaną metodą badawczą jest analiza źródeł wtórnych, m.in. książek, raportów oraz aktów prawnych. Z analizy wynika, iż najkorzystniejszym z punktu widzenia wszystkich interesantów jest oparcie silnego uwierzytelnienia użytkownika na weryfikacji biometryków fizycznych oraz biometryków behawioralnych. W myśl opinii wydanej przez European Banking Authority, mogą być one zaklasyfikowane jako elementy należące do dwóch różnych kategorii, przez co spełniają one wymagania silnego uwierzytelnienia użytkownika.

Słowa kluczowe: silne uwierzytelnienie użytkownika, ustawa o usługach płatniczych, Payment Services Directive (PSD2), biometria, biometria behawioralna, wykładnia prawa.

JEL: G210, K230, K240, O160, O330

Model blueprint for strong user authentication in the context of the European PSD2 Directive and the Polish Act on Payment Services

Abstract

This article is dedicated to the analysis of Strong Customer Authentication (SCA) in the context of the Payment Services Directive (PSD2) and the Payment Services Act. The subject

* lic. Igor Tomecki – Uniwersytet Warszawski, Wydział Zarządzania, Wydział Prawa i Administracji, ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa; Szkoła Główna Handlowa, al. Niepodległości 162, 02-554 Warszawa, Polska. ORCID: 0000-0002-9058-1552.

DOI: 10.7172/978-83-235-5939-9.swwz.13.2

of the research is the available methods of consumer identity confirmation that meet the conditions imposed by the legislature and that are possible to implement in the current state of technological development. This article aims to develop a model blueprint for Strong Customer Authentication that meets the conditions imposed by both European and national legislators. The research method used in the article is the analysis of secondary sources, including books, reports, and legal acts. Research indicates that the most beneficial for all parties involved is to base strong user authentication on the verification of both physical and passive behavioural biometrics. According to the opinion of the European Banking Authority, they can be classified as elements of two different categories, thus fulfilling Strong Customer Authentication requirements.

Keywords: Strong Customer Authentication (SCA), Act on Payment Services, Payment Services Directive (PSD2), biometrics, behavioural biometrics, Strong Customer Authentication model, law interpretation.

Wprowadzenie

Wraz z dynamicznym rozwojem nowych technologii, płatności elektroniczne nieustannie zyskują na popularności. Jak pokazują badania przeprowadzone przez Związek Banków Polskich, w IV kwartale 2021 roku liczba aktywnych klientów indywidualnych bankowości internetowej wyniosła aż 21 milionów, z bankowości mobilnej aktywnie korzystało zaś 16 milionów Polaków. Wartym podkreślenia jest, iż ponad połowa z użytkowników bankowych aplikacji mobilnych (a zatem blisko 10 milionów) to klienci *mobile only* (Związek Banków Polskich, 2021, s. 3–4). Jak wskazywał już Jakub Górka (2009, s. 179) „w segmencie płatności mobilnych kryje się duży potencjał z powodu popularności telefonów komórkowych". Nie jest to nowy trend, gdyż już na przełomie pierwszej i drugiej dekady XXI wieku płatności gotówkowe stanowiły mniejszość transakcji w sektorze *e-commerce* i *m-commerce* w Polsce (Górka, 2013, s. 91–92). Szybkiemu wzrostowi rynku płatności elektronicznych towarzyszy zacięta rywalizacja banków o nowych klientów korzystających z tego segmentu usług.

Jak wykazało badanie przeprowadzone przez Konrada Łuczaka (2017, s. 14–15), aż 4/5 użytkowników bankowości mobilnej wskazało, iż istotnym dla nich jest obsługa płatności elektronicznych z poziomu aplikacji bankowej. Jednym z najważniejszych elementów wpływających na wygodę użytkownika (*user experience*) podczas tej czynności jest wykorzystana do autoryzacji płatności metoda uwierzytelnienia. Dlatego, wychodząc naprzeciw potrzebom klientów bankowości elektronicznej, celem niniejszego artykułu jest wypracowanie modelowego schematu silnego uwierzytelnienia użytkownika, które spełnia wymagania stawiane przez dyrektywę Payment Services Directive 2 (PSD2) (Dyrektywa Parlamentu Europejskiego i Rady [UE] 2015/2366…, 2015) oraz krajową ustawę o usługach płatniczych, a także pozytywnie wpływa na bezpieczeństwo oraz *user experience*.

Zastosowaną metodą badawczą jest prawno-ekonomiczna analiza źródeł wtórnych, m.in. książek, raportów oraz aktów prawnych.

Dlatego też część pierwsza niniejszego artykułu poświęcona jest analizie scenariuszy wymagających zastosowania silnego uwierzytelnienia użytkownika, ze szczególnym uwzględnieniem ustawy o usługach płatniczych (Dz.U. 2021 poz. 1907 z pózn. zm.) wraz ze zmianami wprowadzonymi w ramach nowelizacji wynikającej z konieczności implementacji PSD2 do polskiego porządku prawnego. Bazując na wdrożonych przez europejskiego i krajowego regulatora przepisach prawnych, druga część artykułu zawiera rozważania dotyczące definicji samego silnego uwierzytelnienia użytkownika wraz z omówieniem poszczególnych, składających się na niego kategorii metod uwierzytelniania użytkownika. W kolejnej części przedstawione są narosłe wątpliwości dotyczące poprawnej klasyfikacji poszczególnych elementów do różnych kategorii. W ostatniej części dokonano porównania wszystkich dostępnych elementów silnego uwierzytelniania użytkownika, ze szczególnym uwzględnieniem ich zalet oraz wad. Podsumowanie zawiera wskazanie najkorzystniejszego modelu silnego uwierzytelnienia użytkownika, który spełnia warunki narzucone przez zarówno europejskiego, jak i krajowego regulatora.

1. Scenariusze wymagające użycia silnego uwierzytelnienia użytkownika

1.1. Zastosowania silnego uwierzytelnienia użytkownika

W kontekście analizy dopuszczalnych form uwierzytelniania za kluczowe należy uznać dwa artykuły ustawy o usługach płatniczych – art. 2 oraz art. 32i. Odnoszą się one bezpośrednio do pojęcia „silnego uwierzytelnienia użytkownika" (*Strong Customer Authentication*, SCA). Jak wskazuje treść art. 32i ust. 1, jest to pojęcie niezwykle ważne z punktu widzenia analizowanej w niniejszym artykule problematyki, ponieważ:

> „Art. 32i 1. Dostawca stosuje silne uwierzytelnianie użytkownika, w przypadku gdy *płatnik:*
> 1) uzyskuje dostęp do swojego rachunku w trybie on-line;
> 2) inicjuje elektroniczną transakcję płatniczą;
> 3) przeprowadza za pomocą kanału zdalnego czynność,
> która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć".

Przytoczony przepis zawiera enumeratywne wymienienie wszystkich przypadków, kiedy użycie silnego uwierzytelniania przez dostawcę jest obligatoryjne. Europejski prawodawca, któremu przyświecało stworzenie sprzyjającego otoczenia prawno-ekonomicznego dla sektora e-commerce i m-commerce, uznał, że

kluczową rolę w tym procesie odgrywa bezpieczeństwo płatności elektronicznych. Intencja ta została wyrażona wprost w motywie 95 preambuły dyrektywy PSD2, który stwierdza, iż „bezpieczeństwo płatności elektronicznych ma podstawowe znaczenie dla zapewnienia ochrony użytkowników i stworzenia solidnego otoczenia dla handlu elektronicznego. Wszystkie usługi płatnicze oferowane drogą elektroniczną powinny być wykonywane w sposób bezpieczny, z użyciem technologii będących w stanie zagwarantować bezpieczne uwierzytelnianie użytkownika i w jak największym stopniu ograniczyć ryzyko oszustw".

Dzięki wprowadzeniu dyrektywy PSD2, znacząco zwiększono bezpieczeństwo, radykalnie ograniczając ryzyko wystąpienia oszustw dokonywanych z wykorzystaniem instrumentów płatniczych. W drodze kompromisu jednak, aby zapewnić wystarczające bezpieczeństwo, ale również poszerzyć dostępność i rozpropagowywać innowacyjne usługi płatnicze, a co za tym idzie znacząco polepszyć *user experience*, europejski prawodawca postanowił stworzyć szereg wyjątków od zasady silnego uwierzytelnienia użytkownika. Zostało to uzewnętrznione w podkreśleniu, iż silne uwierzytelnienie ma zastosowanie w sytuacji „która może wiązać się z ryzykiem oszustwa" (art. 32i ust. 1 ustawy o usługach płatniczych). Wyjątki wytypowano, opierając się na analizie poziomu potencjalnego ryzyka wynikającego z transakcji płatniczej, kanału płatności, kwoty czy powtarzalności operacji. Z tego też powodu na liście wyjątków znalazły się między innymi[1]: „transakcje płatnicze do odbiorców znajdujących się na liście zaufanych odbiorców utworzonej uprzednio przez płatnika, kolejne transakcje płatnicze (nie pierwsza) należące do serii transakcji cyklicznych opiewających na tę samą kwotę na rzecz tego samego odbiorcy, polecenia przelewu miedzy rachunkami będącymi w posiadaniu tej samej osoby fizycznej lub prawnej, zdalne elektroniczne transakcje nisko kwotowe, procesy i protokoły realizacji bezpiecznych płatności korporacyjnych, zdalne elektroniczne transakcje płatnicze, które dostawca uzna za charakteryzujące się niskim poziomem ryzyka zgodnie z mechanizmami monitorowania transakcji określonymi w rozporządzeniu RTS SCA" (Dybiński & Osajda, 2022).

Jednym z przypadków wymagających silnego uwierzytelnienia użytkownika, wymienionym w punkcie drugim analizowanego przepisu, jest inicjowanie elektronicznej transakcji płatniczej. Trudno uznać to sformułowanie za intuicyjnie jasne i zrozumiałe oraz pochodzące z języka potocznego, dlatego też, bez względu na sympatyzowanie z klasyfikacyjną czy derywacyjną koncepcją wykładni prawa, należy uznać zdefiniowanie zastosowanego zwrotu za istotne. Próżno szukać definicji legalnej czy nawet dalszego objaśnienia znaczenia pojęcia „elektronicznej transakcji płatniczej" na gruncie ustawy o usługach płatniczych. Koniecznym

[1] Europejski ustawodawca przewidział w sumie 9 wyjątków, kiedy stosowanie silnego uwierzytelnienia użytkownika, pomimo spełnienia jego przesłanek, nie jest wymagane. Są one enumeratywnie wymienione w postaci zamkniętego katalogu w przepisach art. 10-18 RTS dyrektywy PSD2.

w tym przypadku jest skorzystanie z wykładni systemowej, gdyż przy objaśnianiu omawianego sformułowania pomocnym okazuje się przepis art. 2 pkt 4 ustawy o świadczeniu usług drogą elektroniczną (Dz.U. 2020 poz. 344), który zawiera definicję legalną „świadczenia usług drogą elektroniczną" – „wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne" (art. 2 pkt 4 ustawy o świadczeniu usług drogą elektroniczną). W kolejnym punkcie omawianego artykułu zdefiniowane są zaś „środki komunikacji elektronicznej" jako „rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną" (art. 2 pkt 5 ustawy o świadczeniu usług drogą elektroniczną).

1.2. Dynamiczne łączenie w kontekście silnego uwierzytelnienia użytkownika

W wyjątkowym jednak przypadku, jakim jest sytuacja opisana w drugim punkcie analizowanego artykułu ustawodawca, postępując zgodnie z ustępem drugim artykułu drugiego dyrektywy PSD2, wprowadził *lex specialis*, które stanowi, że:

> „2. Jeżeli płatnik inicjuje elektroniczną transakcję płatniczą z wykorzystaniem połączenia z siecią Internet lub za pośrednictwem środków, które mogą być wykorzystywane do porozumiewania się na odległość, dostawca stosuje silne uwierzytelnianie użytkownika obejmujące elementy, które dynamicznie łączą transakcję płatniczą z określoną kwotą transakcji oraz określonym odbiorcą" (art. 32i ust. 2 ustawy o usługach płatniczych).

Warto zauważyć, iż w opozycji do art. 32i ust. 1 pkt 2, przytoczony przepis doprecyzowuje, że dynamiczne łączenie wymagane jest w przypadku elektronicznej transakcji płatniczej, inicjowanej „z wykorzystaniem połączenia z siecią Internet lub za pośrednictwem środków, które mogą być wykorzystywane do porozumiewania się na odległość" (art. 32i ust. 2 ustawy o usługach płatniczych). Rozumując zatem *a contrario*, należy stwierdzić, iż istnieją również przypadki, kiedy elektroniczna transakcja płatnicza nie jest inicjowana za pomocą Internetu czy za pośrednictwem środków komunikacji na odległość. Dzieje się tak na przykład w sytuacji zainicjowania płatności „w obecności płatnika, np. kartą w terminalu POS w punkcie sprzedaży, w bankomacie, czy w wyposażonym w terminal płatniczy urządzeniu samoobsługowym służącym do uiszczania opłat za postój lub za przejazd" (Dybiń-

ski & Osajda, 2022), a także w przypadku transakcji płatniczych dokonywanych przy użyciu bankomatu czy wpłatomatu, gdyż co do zasady wymagają one użycia karty opartej na elektronicznym chipie bądź użycia innego elektronicznego instrumentu płatniczego (np. wirtualnej portmonetki czy kodu BLIK).

Poddając niniejszy przepis dalszej analizie, za kluczowe w kontekście jego wykładni należy uznać interpretację słowa „dynamicznie" – „powinno być rozumiane w odróżnieniu od «statycznie», czyli zmienne, uzależnione od zmiennych cech danej transakcji" (Grabowski, 2020, s. 266). Zgodnie z tym silne uwierzytelnienie zawierające dynamiczne łączenie powinno obligatoryjnie zawierać informację o kwocie autoryzowanej transakcji oraz jej obiorcy, który może być identyfikowany na wiele odmiennych sposobów poprzez wyświetlenie m.in. numeru IBAN, numeru telefonu czy nazwy będącej unikatowym identyfikatorem odbiorcy (Grabowski, 2020, s. 267). W ostatnim przypadku możliwym jest również użycie jedynie fragmentu nazwy odbiorcy, pod warunkiem, że nadal spełnia on warunki dynamicznego łączenia[2]. Dopuszczalne jest także wyświetlenie więcej niż jednego elementu. W każdym z podanych przypadków jednak wyświetlone oznaczenie odbiorcy musi jednoznacznie wskazywać na konkretny podmiot.

Dynamiczne łączenie każdorazowo przypisywane jest do jednej konkretnej transakcji, której odbiorcą ma być określony beneficjent otrzymujący zdefiniowaną kwotę. Jakakolwiek modyfikacja warunków transakcji czy to kwoty, czy odbiorcy, wymaga ponownego utworzenia nowego dynamicznego łączenia, powiązanego z nowymi krytycznymi cechami transakcji. W każdej takiej sytuacji dostawca powinien zastosować najwyższe środki bezpieczeństwa gwarantujące użytkownikowi poufność, autentyczność i integralność – kwoty transakcji i odbiorcy na wszystkich etapach uwierzytelniania, jak również – informacji wyświetlanych płatnikowi na wszystkich etapach uwierzytelniania. Choć pierwotnie dynamiczne łączenie wykorzystywane było wyłącznie z elementem „posiadania", to zgodnie ze stanowiskiem European Banking Authority (EBA), możliwym jest zastosowanie z elementami „wiedzy" czy „cechy" (Grabowski, 2020, s. 267), co obecnie coraz częściej ma zastosowanie w praktyce.

2. Pojęcie „silnego uwierzytelnienia użytkownika"

2.1. Pojęcie „uwierzytelnienia"

Analizując zagadnienie „silnego uwierzytelnienia" nie sposób nie odnieść się do samego pojęcia „uwierzytelniania". Na gruncie polskiego prawa zostało ono

[2] Dokładne omówienie niniejszego zagadnienia zostało zawarte w odpowiedzi na pytanie do EBA, Question ID: 2019_4556.

wprowadzone w art. 2 ust 33b ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, któremu nadano brzmienie:

> „Art. 2 33b) uwierzytelnianie – procedurę umożliwiającą dostawcy usług płatniczych weryfikację tożsamości użytkownika lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających".

Powyższy przepis, zawierający definicję legalną uwierzytelnienia wprowadzono, implementując przepis zawarty w art. 4 pkt 29 dyrektywy PSD2. Pojęcie to należy interpretować jako „procedurę bezpieczeństwa, która ma umożliwić dostawcy usług płatniczych sprawdzenie tożsamości użytkownika lub ważności konkretnego instrumentu płatniczego, w tym z wykorzystaniem spersonalizowanych danych uwierzytelniających użytkownika" (Byrski & Zalcewicz, 2021, s. 139). Jest to znaczenie jak najbardziej zgodne z definicją słowa „uwierzytelnianie" (*authentication*) – za Słownikiem Języka Polskiego PWN – które oznacza „czynić coś wiarygodnym"[3], czy „stwierdzać autentyczność"[4].

Warto w tym miejscu zaznaczyć, iż wbrew nasuwającemu się intuicyjnie tłumaczeniu angielskiego słowa *authentication*, w języku polskim oznacza ono nie „autoryzowanie", lecz „uwierzytelnianie". Taki właśnie błąd tłumaczeniowy został popełniony w tłumaczeniu transponowanej do polskiego porządku prawnego dyrektywy PSD1. Słowa uwierzytelnianie i autoryzowanie, choć blisko ze sobą związane, nie są tożsame i nie mogą być stosowane zamiennie, gdyż „uwierzytelnianie jest elementem procesu weryfikacji przez dostawcę usług płatniczych faktu wyrażenia przez płatnika zgody (autoryzacji) na wykonanie transakcji płatniczej, i jako takie, jest kluczową przesłanką dla udowodnienia przez dostawcę usług płatniczych, że transakcja została autoryzowana" (Blocher & Iwański, 2020).

Niestety analogiczna omyłka znalazła się również w znowelizowanej w 2018 roku, na bazie regulacji zawartych w dyrektywie PSD2, ustawie o usługach płatniczych. Implementując dyrektywę unijną do krajowego porządku prawnego, ponownie błędnie przetłumaczono w art. 45 ustawy o usługach płatniczych art. 72 dyrektywy PSD2, słowo *authentication* jako „autoryzacja", a nie uwierzytelnienie. Pomyłka ta dała pole do nadużyć dla klientów banków, gdyż wbrew intencji europejskiego prawodawcy, przerzuca ona na banki i innych dostawców usług płatniczych cały ciężar odpowiedzialności za transakcję, którą klient uznał za nieautoryzowaną. W związku z tym postulować należy prounijną wykładnię prawa, która naprawi błąd polskiego legislatora i podąży za pierwotnym *ratio legis* europejskiego prawodawcy (art. 72 dyrektywy w sprawie usług płatniczych). Dlatego

[3] https://sjp.pwn.pl/slowniki/uwierzytelnienie.html (pobrano: 19.04.2022).
[4] Ibidem.

też tym bardziej istotnym jest zwiększanie świadomości społecznej o różnicach pomiędzy uwierzytelnieniem a autoryzacją.

2.2. Silne uwierzytelnienie użytkownika

Niezwykle istotnym w kontekście analizowanego pojęcia „silnego uwierzytelnienia użytkownika" jest wyjaśnienie czym są elementy posiadania, wiedzy i cechy. Odpowiedź na to pytanie znajduje się w art. 2 ust. 26aa ustawy o usługach płatniczych, który stanowi:

> „Art. 2 26aa) silne uwierzytelnianie użytkownika – uwierzytelnianie zapewniające ochronę poufności danych w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:
> a) wiedza o czymś, o czym wie wyłącznie użytkownik,
> b) posiadanie czegoś, co posiada wyłącznie użytkownik,
> c) cechy charakterystyczne użytkownika
> – będących integralną częścią tego uwierzytelniania oraz niezależnych w taki sposób, że naruszenie jednego z tych elementów nie osłabia wiarygodności pozostałych".

Wprowadza on do obiegu prawnego pojęcie „silnego uwierzytelnienia", które oznacza „wzmocnioną procedurę weryfikacji tożsamości uprawnionego użytkownika usług płatniczych lub sprawdzenia ważności stosowania konkretnego instrumentu płatniczego" (Byrski & Zalcewicz, 2021, s. 124) oraz podział elementów uwierzytelniających na trzy kategorie: wiedzy, posiadania i cechy. Aby osiągnąć zamierzony cel, jakim jest wzrost bezpieczeństwa płatności, ustawodawca, podążając za wymaganiami wyznaczonymi przez europejskiego legislatora, ustanawia wymóg zastosowania „co najmniej dwóch elementów należących do (trzech wymienionych) kategorii" (art. 2 ust. 26aa ustawy o usługach płatniczych). Oczywistym jest, iż dla zachowania odpowiedniego poziomu bezpieczeństwa „elementy te powinny być od siebie niezależne, co oznacza, że ujawnienie lub utrata wiarygodności jednego z nich nie ma wpływu na wiarygodność pozostałych" (Stanisławska, 2022, s. 111–112). Intuicyjne wydawać by się mogło, iż w ten sposób ustawodawca narzuca wykorzystanie dwóch elementów, które jednak mogą należeć do jednej z wymienionych kategorii. Jak wskazuje jednak przeważająca opinia doktryny, potwierdzona ostatecznie przez opinię wydaną przez EBA 13.06.2018 (European Banking Authority, 2018, pkt 33), każdy z elementów musi pochodzić z innej kategorii, aby spełnić warunki silnego uwierzytelnienia użytkownika.

Jak *explicite* wskazuje analizowany przepis, w przypadku konieczności zastosowania silnego uwierzytelnienia, dostawca ma obowiązek oprzeć uwierzytelnienie na „co najmniej dwóch elementach" (art. 2 ust. 26aa ustawy o usługach płatniczych). Stosując wykładnię językową przytoczonego fragmentu przepisu, należy uznać, iż dozwolonym jest zastosowanie przez dostawcę więcej niż dwóch elementów

potwierdzających tożsamość użytkownika. Jednak ze względu na *user experience*, zgodnie z przytoczonymi we wstępie niniejszego artykułu badaniami podkreślającymi, jak niebagatelną rolę odgrywa dla użytkowników łatwość i wygoda sposobu uwierzytelniania, zastosowanie więcej niż dwóch elementów uwierzytelniających w zasadzie nie ma obecnie miejsca. W analogiczny sposób należy interpretować sytuację braku spełnienia przesłanek obowiązku użycia silnego uwierzytelnienia użytkownika, zawartych w art. 32i ust. 1, czy zaistnienie jednej z przesłanek wyłączających obowiązek jego użycia, zawartych w art. 10–18 RTS on SCA and CSC dyrektywy PSD2. Oznacza to, że w takiej sytuacji zastosowanie bądź niezastosowanie silnego uwierzytelnienia zależy od woli dostawcy.

2.3. Element wiedzy

Zgodnie z zamkniętym katalogiem zawartym w analizowanym przepisie, jednym z elementów wykorzystanym w procesie silnego uwierzytelnienia użytkownika może być „wiedza o czymś, co wie wyłącznie użytkownik" (art. 2 ust. 26aa ustawy o usługach płatniczych). Element ten – zgodnie z opinią EBA – powinien istnieć przed zainicjowaniem uwierzytelnienia, co oznacza, że za element wiedzy nie zostanie uznana np. znajomość kodu OTP. Również (z powodów bezpieczeństwa) za element wiedzy nie zostanie uznany numer identyfikacyjny użytkownika w sytuacji, gdy użytkownik korzysta z numeru identyfikacyjnego oraz hasła (European Banking Authority, 2019, pkt 34). W celu rozwiania najczęściej pojawiających się wątpliwości EBA w swojej Opinii z 21.06.2019 r., EBA-Op-2019-06 sporządziło niewyczerpującą listę dopuszczalnych elementów ze wszystkich kategorii. Przetłumaczone opracowania tabel zostały ujęte w tabeli 1.

Tabela 1. Niewyczerpująca lista dopuszczalnych elementów z kategorii „wiedza"

Sposób uwierzytelnienia użytkownika	Zgodność z silnym uwierzytelnieniem użytkownika
Hasło	tak
PIN	tak
Pytania oparte na wiedzy użytkownika	tak
Hasło słowne	tak
Wzór	tak
Adres email lub nazwa użytkownika	nie
Dane karty (wydrukowane na karcie)	nie
Kod jednorazowy wygenerowany lub otrzymany na urządzenie (kod SMS, token wygenerowany przez hardwarowy lub softwarowy generatora tokenów)	nie (dla obecnych zastosowań funkcjonujących na rynku)

Źródło: opracowanie własne na podstawie: Opinii European Banking Authority, 2019.

2.4. Element posiadania

Jak wskazuje definicja legalna zawarta w analizowanym przepisie, za przedmiot posiadania należy uznać przedmiot posiadany jedynie przez użytkownika. Przytoczona definicja „nie ogranicza rzeczy, których posiadanie może być wykazane, nie ogranicza także czy dana rzecz ma stanowić własność użytkownika czy też może być własnością dostawcy lub (teoretycznie) – podmiotu trzeciego" (Grabowski, 2020, s. 257), co więcej nie narzuca ona, aby element posiadania stanowił przedmiot materialny. Może być nim zatem np. aplikacja, gdyż jak wskazuje pkt 6 preambuły do RTS on SCA and CSC dyrektywy PSD2 „czynnikiem posiadania może być specyfikacja algorytmu, długość klucza i entropia informacyjna" (Grabowski, 2020, s. 257). Aby móc uznać dany element za czynnik posiadania, dostawca powinien spełnić warunek przypisania przedmiotu do konkretnego użytkownika (np. w przypadku urządzeń elektronicznych poprzez zarejestrowanie numeru IP czy też w przypadku karty poprzez jej personalizację –

Tabela 2. Niewyczerpująca lista dopuszczalnych elementów z kategorii „posiadanie"

Sposób uwierzytelnienia użytkownika	Zgodność z silnym uwierzytelnieniem użytkownika
Posiadanie urządzenia potwierdzone przez kod jednorazowy otrzymany lub wygenerowany na urządzeniu (kod SMS, token wygenerowany przez hardwarowy lub softwarowy generatora tokenów)	tak
Posiadanie urządzenia potwierdzone przez podpis wygenerowany przez urządzenie (token hardwarowy lub softwarowy)	tak
Karta albo urządzenie potwierdzone poprzez kod QR (albo fotograficzny kod TAN) zeskanowany z urządzenia zewnętrznego lub karty	tak
Aplikacja lub przeglądarka, której posiadanie jest potwierdzone poprzez połączenie urządzenia – takie jak poprzez chip bezpieczeństwa wbudowany w urządzenie albo klucz prywatny łączący aplikację z urządzeniem albo rejestrację przeglądarki łączącą przeglądarkę z urządzeniem	tak
Posiadanie karty potwierdzone za pomocą czytnika kart	tak
Posiadanie karty potwierdzone jej dynamicznym kodem bezpieczeństwa	tak
Aplikacja zainstalowana na urządzeniu	nie
Posiadanie karty potwierdzone jej danymi (wydrukowanymi na karcie)	nie (dla obecnych zastosowań funkcjonujących na rynku)
Posiadanie karty potwierdzone wydrukowanym elementem (na przykład listą kodów jednorazowych)	nie (dla obecnych zastosowań funkcjonujących na rynku)

Źródło: jak tab. 1.

umieszczenie na niej danych użytkownika, jej numeru etc.) – „dostawca jest uprawniony do odebrania oświadczenia użytkownika, że jest jedynym użytkownikiem konkretnego urządzenia" (Grabowski, 2020, s. 257). Koniecznym jest także posiadanie przez dostawcę procedury uprawdopodobnienia, że dany przedmiot rzeczywiście jest w posiadaniu konkretnego użytkownika.

2.5. Element cechy

W przytoczonym przepisie pojawia się również pojęcie „cech charakterystycznych użytkownika", które oznacza „cechy klienta (coś, czym jest użytkownik)" (Grabowski, 2020, s. 260). Termin ten, zgodnie z zasadą neutralności technologicznej, jest pojęciem otwartym. Oznacza to, że tekst prawny wymienia w tym przypadku jedynie niektóre kryteria stosowalności dla powyższego terminu, a co za tym idzie wraz z rozwojem technologii możliwa jest zmiana zakresu normowania tegoż przepisu. Z analizowanym zagadnieniem nierozerwalnie wiąże się pojęcie „biometrii", czyli „technika dokonywania pomiarów istot żywych" lub badanie „cech populacji organizmów żywych, posługujące się metodami statystyki matematycznej" (*Słownik Języka Polskiego PWN*). Cechy posiadane przez organizmy żywe noszą nazwę biometryk. Dzielą się one na dwie podkategorie: biometryki fizyczne (bazujące na statycznych cechach charakterystycznych człowieka), oraz biometryki behawioralne (bazujące na wzorcach zachowań człowieka).

W skład pierwszej z grup – biometryków fizycznych – wchodzą niezmienne cechy człowieka odnoszące się do fizjologicznych cech organizmu oraz jego części, jak: linie papilarne, siatkówka czy tęczówka oka, geometra dłoni i twarzy etc. Druga grupa – biometryków behawioralnych – zawiera zaś wzorce zachowań człowieka, takie jak: sposób chodu, styl pisania na klawiaturze (np. tempo, siła i kąt nacisku, popełniane błędy), sposób trzymania i kąt nachylenia urządzenia etc. Specyfika obu metod wymusza różne podejście do ich implementacji. W przypadku biometryków fizycznych zbadanie cechy i porównanie jej z zapisanym wzorcem następuje jednorazowo, często w uświadomiony przez użytkownika sposób, w momencie dokonywania uwierzytelnienia. Biometryki behawioralne są powiązane z koncepcją tak zwanego „ciągłego uwierzytelniana" (*continuous authentication*), kiedy to zachowanie użytkownika nieustająco porównywane jest w tle z zapisanym wzorcem.

W odróżnieniu od pozostałych możliwych elementów uwierzytelnienia, weryfikacja biometryków nie bazuje na metodzie zero-jedynkowej, lecz „na odpowiednich dla cechy metodach porównawczych, które dopuszczają określony margines odchyleń od wzorca", gdyż „praktycznie niemożliwe jest uzyskanie wyników kolejnych pomiarów w 100% odpowiadających wzorcowi zapisanemu podczas rejestracji" (Kałużny & Stolarski, 2019, s. 146). Z tego też względu koniecznym jest dopuszczenie pewnego marginesu odchyleń zarejestrowanych danych od utrwalonego wzorca biometryka. Wyróżnić można dwa typy błędów: *False Rejec-*

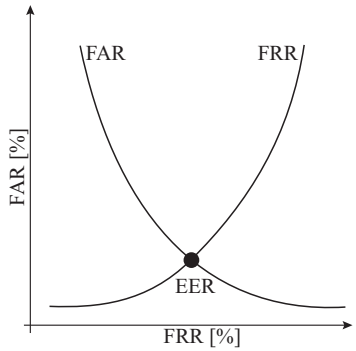
tion Rate (FRR) oraz *False Accept Rate* (FAR). Pierwszy z nich polega na „nie przyznaniu dostępu użytkownikowi, który faktycznie jest tym za kogo się podaje" (Kałużny & Stolarski, 2019, s. 146) i liczony jest jako stosunek tego zjawiska do wszystkich podjętych prób rozpoznania biometryka. Drugi zaś występuje w sytuacji „gdy nieuprawiony użytkownik (którego wzorzec jest podobny, lub który stara się imitować oryginalnego właściciela wzorca) uzyskuje dostęp do systemu" (Kałużny & Stolarski, 2019, s. 146). Jego wartość jest liczona w analogiczny sposób do FRR.

Analizując zagadnienie biometrycznych metod uwierzytelnienia spełniających warunek bycia elementem silnego uwierzytelnienia użytkownika, warto zauważyć, iż wartość błędu FRR będzie przekładać się na *user experience* użytkownika, gdyż będzie on wskazywać na to, w jakim odsetku przypadków biometryk użytkownika nie zostanie rozpoznany poprawnie i uniemożliwi dokonanie autoryzacji uprawnionemu użytkownikowi. Wartość FAR natomiast będzie ukazywać z jakim prawdopodobieństwem podrobiony czy podobny biometryk zostanie uznany za zgodny z zapisanym wzorcem, co zaś przełoży się bezpośrednio na bezpieczeństwo procesu uwierzytelniania. Biorąc pod uwagę jaką rolę w tym scenariuszu odgrywa poprawne rozpoznanie biometryka, bez wątpliwości za istotniejsze należy uznać prawdopodobieństwo wystąpienia błędu FAR, gdyż ma ono bezpośrednie przełożenie na szansę wystąpienia oszustwa. Intuicyjnie zrozumiałym jest, iż oba opisane błędy są współzależne i w przypadku analizowania jednego systemu, przy zmianie wartości jednego z błędów *ceteris paribus*, wartość drugiego również ulegnie zmianie, lecz w przeciwnym kierunku. Co do zasady nie jest to jednak zależność liniowa. W przypadku porównywania ze sobą skuteczności działania różnych systemów czy biometryków pod kątem bezpieczeństwa za bardzo pomocny należy uznać również *Equal Error Rate* (EER), czyli „poziom, dla którego wartości FAR i FRR są sobie równe" (Kałużny & Stolarski, 2019, s. 146), inaczej ujmowany jako punkt przecięcia krzywych FAR i FRR w przypadku konkretnego systemu. Znajomość wartości EER dla różnych systemów czy biometryków pozwala na ich proste i obiektywne porównanie pod względem skuteczności zastosowania i bezpieczeństwa.

Zdefiniowawszy i wytłumaczywszy model rozpoznawania biometryków oraz obarczających go błędów koniecznym jest przeanalizowanie, jak kształtują się ich wartości dla poszczególnych biometryków. Ze względu na ich zróżnicowane cechy, uzasadnionym wydaje się podział ich na trzy kategorie: biometryki fizyczne oraz biometryki behawioralne z podpodziałem na aktywne (wymagające podjęcia działania ze strony użytkownika w celu dokonania uwierzytelnienia) i pasywne (niewymagające żadnego dodatkowego działania ze strony użytkownika w celu uwierzytelnienia – zgodnie z koncepcją *continuous authentication*, potwierdzanie tożsamości użytkownika trwa nieustannie i odbywa się w tle)[5] oraz przedstawienie ich podstawowych cech w formie tabeli.

[5] Podział na biometryki behawioralne aktywne i pasywne wprowadzony przez autora.

Rysunek 1. Zależność FAR względem FRR, z zaznaczeniem wartości EER (punktu w którym FAR = FRR)



Źródło: Śliwa, Bożek, Szyszka & Trzeciak, 2018, s. 16.

Tabela 3. Charakterystyka metod biometrycznych z podziałem na podkategorie i uwzględnieniem ich kluczowych cech w kontekście wykorzystania ich jako zabezpieczenie w procedurze silnego uwierzytelnienia użytkownika

Cecha	FAR [%]	FRR [%]	EER [%]	Czas trwania uwierzytelnienia (w sekundach)	Ryzyko replikacji	Implementacja w urządzeniu mobilnym
Biometryki fizyczne						
Tęczówka	0,001	0,1	<2	1	niskie	trudna
Linie papilarne	1	0,000002	b.d.	1	średnie	umiarkowanie łatwa
Twarz	6	0,1	b.d.	1	wysokie	łatwa
Biometryki behawioralne (aktywne)						
Gest	b.d.	b.d.	2	2	wysokie	łatwa
Podpis	b.d.	b.d.	<2	3	średnie	łatwa
Głos	3	0,10	2	2	średnie	łatwa
Biometryki behawioralne (pasywne)						
Dynamika pisma	b.d.	b.d.	<2	natychmiastowo	niskie	łatwa
Profil dotyku	b.d.	b.d.	<4	natychmiastowo	niskie	łatwa
Styl chodu	3,92	11,76	5,60	natychmiastowo	niskie	łatwa
Profilowanie behawioralne	b.d.	b.d.	<5	natychmiastowo	bardzo niskie	łatwa

* W przypadku odmiennych wyników różnych badań w tabeli umieszczono najgorszy otrzymany wynik i oznaczono go jako poziom maksymalny.

Źródło: opracowanie własne na podstawie: Kałużny & Stolarski, 2019, s. 147–153.

W zależności od badania konkretnego systemu rozpoznawania danego biometryka, czy samych założeń badania, otrzymane wyniki mogą się od siebie różnić. Dlatego też w tabeli 3 pesymistycznie przyjęto najgorsze uzyskane rezultaty dotychczasowych badań i oznaczono je jako wartość maksymalną. Warto jednak odnotować, że wraz z dynamicznym rozwojem nowych technologii, a co za tym idzie i technologii biometrycznych, wartości wszystkich podanych błędów będą z czasem się obniżać. Zapewne już dziś możliwym jest, nawet w komercyjnym użyciu, uzyskanie niższych współczynników błędów, gdyż dane zamieszczone w tabeli bazują na wynikach badań, które ukazały się w latach 2014–2018. Dodatkowo wykorzystując sztuczną inteligencję i zlecając jej analizę obszernych baz danych, zawierających różne próbki konkretnego typu biometryków, możliwym jest osiągnięcie wartości błędu EER na poziomie 0% (Salloum & Jay Kuo, 2017, s. 2065).

Po przeanalizowaniu technicznych uwarunkowań związanych z rozpoznawaniem cech biometrycznych, niezwykle istotnym, w kontekście zagadnień rozważanych na kartach niniejszego artykułu, jest zarysowanie uwarunkowań prawnych dotyczących biometrii zawartych w regulacjach zarówno na poziomie europejskim, jak i krajowym, ze szczególnym uwzględnieniem opinii wydawanych przez organy stosujące prawo. Dlatego też w tabeli 4 przedstawiono niewyczerpującą listę biometryków uznawanych przez EBA za element cechy użytkownika w kontekście silnego uwierzytelnienia użytkownika.

Tabela 4. Niewyczerpująca lista dopuszczalnych elementów z kategorii „cecha charakterystyczna”

Sposób uwierzytelnienia użytkownika	Zgodność z silnym uwierzytelnieniem użytkownika
Skanowanie odcisku palca	tak
Rozpoznawanie głosu	tak
Rozpoznawanie układu naczyń krwionośnych	tak
Geometria dłoni i twarzy	tak
Skanowanie siatkówki i tęczówki	tak
Dynamika pisania	tak
Tętno lub inne wzorce ruchu ciała potwierdzające tożsamość użytkownika (w odniesieniu np. do urządzeń ubieralnych)	tak
Kąt, pod którym trzymane jest urządzenie	tak
Informacje przesłane za pomocą protokołu komunikacyjnego (np. EMV® 3-D Secure)	nie (dla obecnych zastosowań funkcjonujących na rynku)
Wzór	nie

Źródło: jak tab. 1.

3. Wątpliwości interpretacyjne

Choć *prima facie* przyporządkowanie poszczególnych metod uwierzytelnienia użytkownika do konkretnych kategorii wydaje się intuicyjnie oczywiste, to, jak wskazuje praktyka użycia, częstokroć istnieją wątpliwości co do prawidłowej klasyfikacji sposobów uwierzytelniania. Najczęściej spotykanym z nich jest choćby kontrintuicyjne uznanie kodu SMS nie za element wiedzy (wszakże koniecznym jest jego znajomość, aby autoryzacja się powiodła), lecz za element posiadania, gdyż zgodnie ze stanowiskiem EBA kod ten potwierdza posiadanie karty SIM, która przypisana jest do konkretnego numeru telefonu konkretnego użytkownika (*2018_4039 Qualification of SMS OTP as an authentication*, 2018).

Analogicznie nieintuicyjnie i jeszcze bardziej intrygująco prezentuje się kwestia odcisku palca, a w zasadzie (rozumując *per analogiam*) wszystkich biometryków. Choć oczywistym wydaje się, iż powinny one należeć wyłącznie do kategorii cechy użytkownika, to ich kwalifikacja „do odpowiedniej kategorii będzie zależeć od podejścia danego dostawcy" (Stanisławska, 2022, s. 112). Pomimo, iż rzeczywiście najczęściej biometryki kwalifikowane są jako cecha użytkownika, to w pewnych określonych sytuacjach mogą być także uznane za element posiadania. Może się tak stać w sytuacji, gdy dostawca nie weryfikuje biometryku samodzielnie, lecz wykorzystuje do tego oprogramowanie zainstalowane na urządzeniu mobilnym użytkownika weryfikujące zgodność próbki ze wzorcem – „w takim przypadku możliwa jest interpretacja, zgodnie z którą (…) (biometryk) jedynie potwierdza korzystanie przez użytkownika z danego urządzenia mobilnego" (Stanisławska, 2022, s. 112). Dopuszczalną jest jednak, także w takiej sytuacji, gdy „dostawca na potrzeby SCA korzysta z technologii podmiotu trzeciego jakim jest producent urządzenia mobilnego lub producent oprogramowania" (Stanisławska, 2022, s. 113), interpretacja biometryka jako cechy użytkownika. Podobnych wątpliwości nie wzbudza sytuacja, gdy użytkownik na potrzeby korzystania z bankowości mobilnej podaje dostawcy wzór swojego wybranego biometryka, a następnie dostawca każdorazowo weryfikuje stan biometryka użytkownika, porównując go z zapisanym wcześniej wzorem.

4. W poszukiwaniu modelowego rozwiązania

Przeanalizowawszy uwarunkowania prawne ukształtowane przez zarówno europejskiego, jak i krajowego legislatora oraz wyjaśniwszy narosłe wokół nich wątpliwości, a także przedstawiwszy obecnie dostępne możliwości technologiczne, należy uznać za słuszne wskazanie modelowego schematu silnego uwierzytelnienia użytkownika, które będzie pozytywie wpływać na *user experience*, jednocześnie będąc zgodnym z obowiązującym prawem, a także możliwym do

wdrożenia. W tym celu rozsądnym wydaje się przeanalizowanie wszystkich możliwości spełniających narzucone prawnie dostawcom wymagania.

4.1. Element wiedzy

Zgodnie z przedstawioną w jednym z poprzednich punktów tabelą 1, zaczerpniętą z opinii wydanej przez EBA, elementy wiedzy użytkownika można uogólnić do różnego typu haseł lub pytań zabezpieczających. Jak wskazuje zaś wiele niezależnych badań, „hasła są zazwyczaj ponownie używane przez użytkowników do zabezpieczenia różnych kont" (Han i in., 2018, s. 309), gdyż „typowy użytkownik może skutecznie zapamiętać jedynie 4–5 haseł" (Gouda i in., 2005, s. 2). Co gorsza „użytkownicy konsekwentnie stosują bardzo uproszczone, łatwe do przewidzenia praktyki podczas konstruowania i używania haseł. Obejmuje to używanie znaczących słów lub dat osobistych, które są łatwe do zapamiętania (…), używanie nazw własnych lub słów powszechnie występującego w słowniku lub powiązanie hasła z rodzajem konta, do którego jest przypisane (…). Takie przewidywalne i systematyczne praktyki są łatwiejsze do zapamiętania dla użytkownika, ale poświęcają bezpieczeństwo konta, które hasło ma zapewnić" (Riley, 2006, s. 1). W jednym z przeprowadzonych badań wykazano, iż „74,9% respondentów (…) zadeklarowało, że ma zestaw wcześniej ustalonych haseł, których często używają, z czego 98,3% (…) zadeklarowało posiadanie średnio 3,1 (SD = 2,028) hasła. Ponad połowa (59,7%) stwierdziła, że nie tworzy haseł o różnej złożoności w zależności od rodzaju witryny, z której korzystają, na przykład nie ustala silniejszego hasła do internetowego konta bankowego w porównaniu z programem do czatu online. Przeciętny czas, przez jaki użytkownicy nieprzerwanie korzystali z tego samego swojego podstawowego hasła do użytku osobistego wyniósł 31,07 miesięcy (SD, 28,01), w przybliżeniu dwa lata i siedem miesięcy. Na pytanie «Jak często regularnie zmieniasz hasło, gdy nie jest to wymagane przez system?» 52,7% (…) odpowiedziało «Nigdy»" (Riley, 2006, s. 2). Podobny poziom bezpieczeństwa (jeśli nawet nie niższy) przedstawiają pytania zabezpieczające. Co do zasady orbitują one wokół prostych zagadnień, o których wiedza jest powszechnie dostępna wśród najbliższego kręgu użytkownika, a jej zdobycie nie nastręczy potencjalnemu przestępcy większego problemu – na czele z najczęściej chyba używanym w bankowości pytaniem o nazwisko panieńskie matki.

Przedstawione powyżej wyniki badań i analiz jasno wskazują, iż uznanie elementu wiedzy za skuteczny element uwierzytelnienia w wielu (czy nawet większości) przypadków okazuje się niemożliwe. Oczywiście istnieje możliwość narzucenia użytkownikowi pewnych warunków, które musi spełnić hasło, np. posiadanie wymienionej liczny konkretnych elementów (małych i wielkich liter, cyfr, znaków specjalnych), brak powiązania z portalem i kontem, do któ-

rego jest ono przypisane czy też zakaz korzystania z haseł słownikowych oraz obowiązek regularnej zmiany hasła na nowe. Takie praktyki spotykają się jednak co do zasady z negatywną reakcją użytkowników z powodu pogorszenia się *user experience*, a także doprowadzają do o wiele częstszej konieczności przywracania hasła, co również może być wektorem ataku, zmniejszając bezpieczeństwo chronionego konta. Pozwala to zatem sądzić, iż w poszukiwaniu optymalnego modelu silnego uwierzytelniania użytkownika należy rozważyć alternatywne rozwiązania.

4.2. Element posiadania

Drugą z wymienionych możliwych składowych silnego uwierzytelniania jest element posiadania. Opierając się na tabeli 2 zaczerpniętej z opinii EBA, a zawierającej przykładowy katalog elementów posiadania, można wysnuć wniosek, iż najczęściej bazuje on na dostępie do zaufanego urządzenia (smartphone, komputer) czy zainstalowanej na nim aplikacji lub przeglądarki bądź posiadaniu fizycznej karty. Oczywistą wadą tego typu rozwiązania jest możliwość utracenia przez prawowitego właściciela elementu potwierdzającego posiadanie, np. karty, telefonu czy laptopa, co może niezmierne ułatwić przestępcy dokonanie włamania na konto, a także dokonanie czynności wymagających silnego uwierzytelnienia. Szczególnie zagrożenie niesie za sobą utrata karty, na której odwrocie znajduje się kod CVC2/CVV2, który zgodnie z przyjętą wykładnią nie stanowi elementu wiedzy, lecz potwierdzenia posiadania karty. Służy on do autoryzacji płatności przez Internet i w przypadku niższych kwot transakcji (niepodlegających rygorom silnego uwierzytelnienia użytkownika) może być wystarczający do dokonania płatności.

Oczywiście dostawca ma obowiązek „posiadać procedurę uprawdopodobnienia, że dany przedmiot rzeczywiście znajduje się w posiadaniu użytkownika" (Grabowski, 2020, s. 257). Najczęściej jednak potwierdzenie takie następuje na przykład w postaci wpisania kodu PIN zabezpieczającego aplikację bankową czy też przesłania kodu SMS na numer użytkownika. Pomimo iż aplikacje mobilne banków są rekomendowane przez ekspertów od cyberbezpieczeństwa, ich użycie eliminuje bowiem ryzyko *spoofingu*[6], to metoda ta często napotyka problem opisany w powyższych akapitach tego artykułu. Niepozbawioną swoich wad jest także metoda bazująca na kodach SMS. Pomijając niebagatelne koszty, jakie pociągają za sobą hurtowe ilości wysłanych wiadomości SMS z kodami (koszt zakończenia wiadomości SMS w rozliczeniach międzyoperatorskich [*SMS Termination Rate*] to

[6] Jest to oszustwo polegające na podszyciu się przez hakera pod zaufany podmiot – w tym przypadku poprzez spreparowanie np. wiadomość e-mail i portalu banku użytkownika. Może być wykorzystane do wyłudzenia danych klienta czy zainfekowania urządzenia.

5 groszy, a koszt dla użytkownika końcowego – w tym przypadku banku – może sięgać nawet 10 groszy, co jest związane z marżą operatora telekomunikacyjnego, a także agregatora-pośrednika, który jest bezpośrednim dostawcą usługi dla banku) (Body of European Regulators for Electronic Communication, 2021, s. 44), które mogą iść w miliony złotych miesięcznie. Za zdecydowanie największą wadę tego rozwiązania, należy jednak uznać zagrożenie związane z atakami SIM swappingowymi.

Zjawisko SIM swappingu, które po raz pierwszy „zostało zgłoszone w USA i Europie w 2013 r." (Awale & Gupta, 2019, s. 995), jak wskazuje „Raport IOCTA 2020 (*Internet Organised Crime Threat Assement*), (…) wymienia się jako jeden z kluczowych trendów wśród przestępstw dotyczących płatności" (Zubańska, 2021, s. 559). Oszustwo to polega na „oszukaniu operatora telefonii komórkowej, zwykle podczas rozmowy telefonicznej z infolinią operatora, że prawowity właściciel abonamentu komórkowego musi otrzymać duplikat swojej karty SIM. Dzwoniący może na przykład twierdzić, że telefon został utracony za granicą i musi jak najszybciej odzyskać dostęp do swojego numeru przy pomocy nowo nabytego telefonu i nowej karty SIM" (Jover, 2020, s. 51). Oszuści z niezwykłą biegłością posługują się manipulacją i metodami nacisku psychologicznego na konsultanta, który chcąc rozwiązać problem dzwoniącego klienta, częstokroć nagina narzucone przez krajowego regulatora normy postępowania czy też wewnętrzne procedury bezpieczeństwa przedsiębiorstwa. Nierzadko zdarza się również, że działanie takie nie jest niezbędne, gdyż użytkownik samodzielnie dzieli się w swoich ogólnodostępnych mediach społecznościowych swoimi poufnymi danymi, które mogą zostać wykorzystane do uzyskania duplikatu karty SIM. Wykorzystując metody „phishingowe, czy inwigilację celu, aby zebrać dane osobowe, oszuści mogą podszyć się pod tę osobę" (Russo, 2019).

Po udanym przeprowadzeniu pierwszej części ataku i otrzymaniu przez oszusta duplikatu karty SIM „do momentu aż ofiara zauważy utratę zasięgu i skontaktuje się z obsługą klienta, wszystkie wiadomości i połączenia telefoniczne będą kierowane do oszusta (…), w związku z tym wszystkie kody SMS będą otrzymywane przez oszusta" (Jover, 2020, s. 51). Pozwala to na pokonanie dwuelementowego, silnego uwierzytelnienia użytkownika i dokonanie przez oszusta na przykład przelewu środków z rachunku.

Warto w tym miejscu jednak zauważyć i pochwalić praktyki zminimalizowania ryzyka SIM swappingu, jakie stosuje polski MNO (*Mobile Network Operator*) Play. Każdorazowo w przypadku pojawienia się żądania wydania duplikatu karty SIM, przed zmianą przypisanego do numeru telefonu użytkownika numeru IMSI (*International Mobile Subscriber Identity*)[7], operator wysyła wiadomość SMS na

[7] Unikatowy numer przypisany konkretnej, fizycznej karcie SIM, na podstawie którego jest ona rozpoznawana w sieci telekomunikacyjnej. Informacja o numerze IMSI zakodowana jest na

starą kartę SIM z informacją o złożonym wniosku o wydanie duplikatu. Pozwala to użytkownikowi na zauważenie w porę próby przejęcia numeru telefonu i podjęcie wraz z operatorem stosowych kroków, mających zapobiec oszustwu.

Opisanemu powyżej elementowi posiadania, choć jak się często zdaje bezpieczniejszemu niż element wiedzy, nadal można przypisać pewne wady. Częściowo wynikają one ze specyfiki metod, które *prima facie* zakwalifikowalibyśmy jako element wiedzy, jednak w myśl zarówno wykładni dyrektywy PSD2, jak i krajowej ustawy o usługach płatniczych stanowią jedynie potwierdzenie elementu posiadania – wszelkie wady wynikające z ułomności haseł, kodów czy pytań zabezpieczających. Ponadto w wielu przypadkach metoda ta jest także bardzo podatna na ataki oszustów (choćby wspomniany SIM swapping), jak również najzwyklejszą kradzież zaufanego urządzenia (np. smartphone czy karta bankowa) bądź zainstalowanie na nim wirusa. Jak wykazały jednak rozważania zawarte w poprzednim punkcie, nie są to jedyne sytuacje, które w myśl wykładni logicznej prawa opartej na opiniach wydanych przez EBA oraz rozumowaniu *argumentum a simile*, mogą być uznane za element posiadania. Rozwiązanie to przeanalizowane będzie jednak w kolejnych akapitach.

4.3. Element cechy

Ostatnim z możliwych rozwiązań, koniecznych do przeanalizowania w poszukiwaniu modelowego schematu silnego uwierzytelnienia użytkownika, które będzie pozytywie wpływać na *user experience*, jednocześnie będąc zgodnym z obowiązującym prawem, a także możliwym do wdrożenia, jest wykorzystanie biometryków. Jak zaznaczono w punkcie 2.5 niniejszego artykułu, jest to dość zróżnicowana kategoria, która w uogólnieniu odnosi się do cech fizycznych użytkownika (biometryki fizyczne) bądź jego zachowań (biometryki behawioralne).

Zdecydowanie najbardziej rzucającą się w oczy zaletą biometrycznych metod uwierzytelniania użytkownika jest ich wygoda i szybkość, co niezwykle pozytywnie wpływa na *user experience*. Użytkownik nie musi pamiętać żadnych informacji, nie istnieje również szansa, aby przez przypadek komuś je zdradził. Nie ma także możliwości, by zapomniał zabrać ze sobą posiadany przez siebie element, utracił go lub zniszczył, natomiast złodziej nie może mu go też ukraść. Cechy biometryczne to immanentna część człowieka – to użytkownik jest kluczem. Niebagatelną zaletą jest również czas trwania uwierzytelnienia: w przypadku biometryków fizycznych wynosi on około sekundy, biometryków behawioralnych aktywnych – do 3 sekund, natomiast w przypadku pasywnych odbywa się natych-

karcie SIM; znajduje się także na serwerze operatora, który na jego podstawie łączy numer telefonu z konkretnym urządzeniem.

miastowo, gdyż tożsamość użytkownika jest potwierdzana cały czas w tle. Są to wartości nieosiągalne dla pozostałych metod uwierzytelniana.

Drugim z istotnych aspektów, pod kątem którego w badanym kontekście powinny być rozpatrywane metody biometryczne, jest bezpieczeństwo jakie gwarantują użytkownikowi. W odróżnieniu od elementów innych kategorii, weryfikacja próbki ze wzorcem nie przebiega zero-jedynkowo – dopuszczalne jest pewne odchylenie. Może budzić to pewne obawy co do bezpieczeństwa gwarantowanego przez tę metodę. Biorąc jednak pod uwagę ryzyko wiążące się z innymi powszechnie stosowanymi metodami zabezpieczeń (szansa na odgadnięcie standardowego kodu PIN to 0,01%), a także powszechnym wykorzystaniem wielu z biometrycznych metod uwierzytelniania użytkownika (na przykład skanowanie odcisku palca), należy uznać oferowany przez nią poziom bezpieczeństwa za wystarczający.

Co więcej, w odróżnieniu od innych metod uwierzytelniania, metody biometryczne pozwalają na bardzo łatwe łączenie weryfikacji wielu biometryków na raz, bez znaczącego wpływu na wygodę użytkownika i czas trwania uwierzytelnienia. Jak wykazały badania, niesie to za sobą ogromną zaletę, jaką jest istotne zwiększenie bezpieczeństwa – „na przykład użycie kombinacji skanu odcisku palca oraz twarzy pozwala osiągnąć lepsze bezpieczeństwo niż w przypadku weryfikacji jednego biometryka, poprawiając dokładność z 2,3% do 0,1% FAR" (Saevanee i in., 2015, s. 236). Opierając się na danych zawartych w tabeli 3, ukazującej podstawowe cechy wybranych biometryków, można stwierdzić, iż wykorzystując łącznie wszystkie biometryki behawioralne pasywne w niej wymienione i łącząc je w jedną metodę uwierzytelnienia, już kilka lat temu możliwym było osiągnięcie wartości błędu FAR na poziomie zaledwie 0,000224%. Wraz z dynamicznym rozwojem nowych technologii i coraz szerszym wykorzystaniem sztucznej inteligencji oraz obszernych baz danych, zawierających różne próbki konkretnego typu biometryków, możliwym jest osiągnięcie wartości błędu EER na poziomie 0% (Salloum & Jay Kuo, 2017, s. 2065). Choć technologia nie osiągnęła jeszcze takiego poziomu zaawansowania, to szansa na uzyskanie dostępu przez osobę nieuprawnioną jest o dwa rzędy wielkości niższa niż w przypadku standardowego kodu PIN (przy dodatkowym założeniu, że kod nie został wykradziony oraz nie stanowi on na przykład łatwej do zgadnięcia dla atakującego daty urodzenia), co pozwala uznać zaproponowaną metodę za niezwykle bezpieczną. Jednocześnie cały opisany proces jest zupełnie niezauważalny dla użytkownika, nie wymaga od niego podjęcia żadnej akcji, a do tego dzieje się natychmiastowo.

W kontekście silnego uwierzytelniania użytkownika przeprowadzanego za pomocą biometryków, konieczna jest jego analiza przez pryzmat dyrektywy PSD2 oraz polskiej ustawy o usługach płatniczych, a także opinii wydawanych przez EBA. Co sygnalizowano już w poprzednim punkcie, w zależności od

zastosowanego mechanizmu weryfikacji autentyczności, biometryk może zostać uznany za potwierdzenie elementu posiadania bądź element cechy. Jeśli proces nie jest przeprowadzany bezpośrednio przez dostawcę, lecz wykorzystywane jest do tego oprogramowanie podmiotu trzeciego zainstalowane na urządzeniu mobilnym użytkownika, które weryfikuje zgodność próbki ze wzorcem, to uwierzytelnianie może zostać uznane za potwierdzenie posiadania zaufanego urządzenia, za pomocą którego dokonywane jest potwierdzenie autentyczności biometryka. W sytuacji zaś, gdy użytkownik na potrzeby korzystania z bankowości mobilnej poda dostawcy wzór swojego wybranego biometryka, a następnie dostawca każdorazowo będzie weryfikować stan biometryka użytkownika, porównując go z zapisanym wcześniej wzorem, biometryk bezsprzecznie zostanie zakwalifikowany jako cecha użytkownika. Choć opinia EBA, na której bazuje ten pogląd, dotyczyła *explicite* odcisku palca, to w opinii autora, wyrażonej już w punkcie 3 niniejszego artykułu, poprawnym i uzasadnionym jest w tym przypadku rozumowanie *per analogiam* i rozszerzenie tej wykładni na wszystkie biometryki.

Do kwestii tej nie odniesie się najprawdopodobniej przygotowywana obecnie nowelizacja dyrektywy PSD2. Jak wskazuje EBA w opinii z 23 czerwca 2022 roku w sprawie rewizji dyrektywy o usługach płatniczych (PSD2), pomimo wskazania na wiele aspektów obecnie obowiązującej regulacji, które w opinii EBA powinny zostać zmienione w przypadku wdrożenia nowelizacji PSD2, Urząd w jasny sposób wskazuje, iż zagadnienie silnego uwierzytelnienia użytkownika nie wymaga nowelizacji czy dalszego uszczegółowienia, gdyż wydane do tej pory opinie i zalecenia Europejskiego Urzędu Nadzoru Bankowego można uznać za wystarczające (European Banking Authority, 2022, pkt 328). W odczuciu autora jest to stanowisko słuszne i uzasadnione.

Podsumowanie – modelowy schemat silnego uwierzytelnienia użytkownika

Przeanalizowawszy wszystkie możliwe metody uwierzytelniania użytkownika, zarówno pod kątem technologicznym, prawnym, jak i z uwzględnieniem względów bezpieczeństwa oraz wpływu na *user experience*, możliwym jest wskazanie modelowej metody silnego uwierzytelnienia użytkownika zgodnego z dyrektywą PSD2 oraz prawem krajowym. Autor niniejszego artykułu postuluje o wykorzystanie połączenia weryfikacji wybranego biometryka fizycznego (na przykład odcisku palca, siatkówki oka czy zaawansowanego skanu twarzy 3D) za pomocą systemu informatycznego banku, co spełniałoby przesłanki elementu cechy z art. 2 ust. 26aa ustawy o usługach płatniczych, z weryfikacją za pomocą oprogramowania podmiotu trzeciego, zainstalowanego na urządzeniu, wybranej

grupy biometryków behawioralnych pasywnych, co wyczerpywałoby znamiona elementu posiadania z art. 2 ust. 26aa ustawy o usługach płatniczych. Zaprezentowana wykładnia pozwala na spełnienie wymagań stawianych przez PSD2 w kontekście silnego uwierzytelnienia użytkownika przy wykorzystaniu jedynie weryfikacji różnych biometryków użytkownika, gdyż w rozumieniu ustawy i unijnej dyrektywy wyczerpują one przesłanki do zakwalifikowania ich do dwóch różnych kategorii, co jest warunkiem koniecznym do określenia procesu uwierzytelniania jako silnego uwierzytelnienia użytkownika.

W opinii autora jest to najlepszy model, gdyż biometryki wysuwają się na zdecydowane prowadzenie pod kątem *user experience*, oferując praktycznie natychmiastowe potwierdzenie tożsamości użytkownika, jednocześnie nie wymagając od niego pamiętania czy posiadania jakichkolwiek elementów. Gwarantują one również co najmniej zadowalający poziom bezpieczeństwa, zwłaszcza biorąc pod uwagę wyeliminowanie ryzyka użycia hasła słownikowego, zapisanie hasła przez użytkownika w miejscu, z którego może być łatwo przechwycone (na przykład na kartce przyklejonej do monitora lub w nieszyfrowanym pliku na pulpicie o wiele mówiącej nazwie „hasła") czy wycieku hasła zastosowanego w wielu miejscach oraz utraty elementu posiadania. Co więcej, wraz z rozwojem technologii informatycznych oraz sztucznej inteligencji, współczynnik błędów FAR i FRR, a co za tym idzie i EER, będzie się jeszcze diametralnie zmniejszać, gwarantując poziom bezpieczeństwa coraz bliższy ideałowi.

Bibliografia

2018_4039 Qualification of SMS OTP as an authentication. (2018). European Banking Authority. Pobrano 19 kwietnia 2022 z https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039.

2019_4556 Definition of payee for dynamic linking. (2019). European Banking Authority. Pobrano 19 kwietnia 2022 z https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4556.

Awale, S.M. & Gupta, P. (2019). Awareness of Sim Swap Attack. *International Journal of Trend in Scientific Research and Development*, *3*(4), 995–997. https://doi.org/10.31142/ijtsrd23982.

Biometria – definicja, synonimy, przykłady użycia. (b. d.). Słownik języka polskiego PWN. Pobrano 19 kwietnia 2022 z https://sjp.pwn.pl/slowniki/biometria.html.

Blocher, M. & Iwański, W. (2020). Nieautoryzowane transakcje płatnicze. *Monitor Prawniczy*, (9), https://doi.org/10.32027/MOP.20.9.4.

Body of European Regulators for Electronic Communication. (2021). *Termination rates at European level, January 2021*(Raport BoR (21) 71). https://www.berec.europa.eu/en/document-categories/berec/reports/termination-rates-at-european-level-january-2021.

Byrski, J. & Zalcewicz, A. (red.). (2021). *Ustawa o usługach płatniczych. Komentarz*. Wolters Kluwer.

Dybiński, J. & Osajda, K. (red.). (2022). *Ustawa o usługach płatniczych. Komentarz*. C.H. Beck.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG), L 337/35 (2015) (Parlament europejski i Rada Unii Europejskiej). https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32015L2366.

European Banking Authority. (2018). *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC* (EBA-Op-2018-04). https://www.eba.europa.eu/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer-authentication-and-common-and-secure-communication.

European Banking Authority. (2019). *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* (EBA-Op-2019-06). https://www.eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2.

European Banking Authority. (2022). *Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)* (EBA/Op/2022/06). https://www.eba.europa.eu/eba-replies-european-commission%E2%80%99s-call-advice-%C2%A0-review-payment-services-directive.

Gouda, M.G., Liu, A.X., Leung, L.M. & Alam, M.A. (2005). *Single Password, Multiple Accounts* (niewydany artykuł). The University of Texas. http://www.cse.msu.edu/~alexliu/publications/Password/password.pdf.

Górka, J. (2009). *Konkurencyjność form pieniądza i instrumentów płatniczych*. CeDeWu.

Górka, J. (2013). *Efektywność instrumentów płatniczych w Polsce*. Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego.

Grabowski, M. (2020). *Ustawa o usługach płatniczych. Komentarz*. C.H. Beck.

Han, W., Li, Z., Ni, M., Gu, G. & Xu, W. (2018). Shadow Attacks Based on Password Reuses: A Quantitative Empirical Analysis. *IEEE Transactions on Dependable and Secure Computing*, *15*(2), 309–320. https://doi.org/10.1109/TDSC.2016.2568187.

Jover, R.P. (2020). Security Analysis of SMS as a Second Factor of Authentication: The challenges of multifactor authentication based on SMS, including cellular security deficiencies, SS7 exploits, and SIM swapping. *ACM Queue*, *18*(4), 37–60. https://doi.org/10.1145/3424302.3425909.

Kałużny, P. & Stolarski, P. (2019). Biometria behawioralna i „tradycyjna" w mobilnych usługach bankowych – stan oraz przyszłe możliwości zastosowania. *Bezpieczny Bank*, *1*(74), 139–161. https://doi.org/10.26354/bb.7.1.74.2019.

Łuczak, K. (2017). *Determinanty rozwoju aplikacji mobilnych w bankowości detalicznej* (niepublikowany autoreferat). Wydział Zarządzania Uniwersytetu Warszawskiego.

Riley, S. (2006). Password security: What users know and what they actually do. *Usability News*, *8*(1), 2833–2836.

Russo, T. (2019). *SIMulated Trust: How Malicious Actors Take Advantage of Cellular Carriers to Perform SIM Swapping Attacks* (niepublikowany artykuł). https://www.cs.tufts.edu/comp/116/archive/fall2019/trusso.pdf.

Saevanee, H., Clarke, N., Furnell, S. & Biscione, V. (2015). Continuous user authentication using multi-modal biometrics. *Computers & Security*, *53*, 234–246. https://doi.org/10.1016/j.cose.2015.06.001.

Salloum, R., & Jay Kuo, C.-C. (2017). ECG-based biometrics using recurrent neural networks. *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2062–2066. https://doi.org/10.1109/ICASSP.2017.7952519.

Stanisławska, M. (red.). (2022). *Ustawa o usługach płatniczych. Komentarz*. C.H. Beck.

Śliwa, P., Bożek, A., Szyszka, & Trzeciak, K. (2018). Biometria i biometryczne systemy zabezpieczeń. W L. Leniowska (red.), *Ogólnopolska Konferencja Naukowa Młodych Inżynierów* (13–23). Koło Naukowe Mechatron-SEP, Uniwersytet Rzeszowski.

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. 2020 poz. 344 (2020) (Polska).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz.U. 2021 poz. 1907 z późn. zm. (2021) (Polska).

Uwierzytelnienie – definicja, synonimy, przykłady użycia. (b.d.). Słownik Języka Polskiego PWN. Pobrano 19 kwietnia 2022 z https://sjp.pwn.pl/slowniki/uwierzytelnienie.html.

Zubańska, M. (2021). Kryminalistyka w dobie przyspieszenia naukowo-technicznego i technologicznych nadużyć – przytłaczająca wizja zmian czy inspiracja do rozwoju? *Studia Prawnoustrojowe*, (52), 549–568. https://doi.org/10.31648/sp.6577.

Związek Banków Polskich. (2021). *Raport NetB@nk, 4 kwartał 2021: bankowość internetowa i mobilna, płatności bezgotówkowe* (s. 3–4). https://www.zbp.pl/getmedia/ebf7bd37-fd02-47ad-95f0-514cc79709bc/Raport-Netbank_Q4-2021.