Wrocław, dn. 19 stycznia 2020 r.

OPINIA PRAWNA

Praktyczne zastosowanie podpisu elektronicznego w odniesieniu do produktu *SignOnTheGo*

sporządzona na zlecenie Smartech-IT sp. z o.o. z siedzibą we Wrocławiu

+48 606 200 512
+48 71 759 33 92
piotr@szkulik.pl
www.szkulik.pl

Kancelaria Adwokacka
adw. Piotr Szkulik
ul. Sądowa 12/4
50-046 Wrocław

SignOnTheGo – bezpieczna rewolucja w zawieraniu umów

Innowacyjne rozwiązania pozwalają na zawieranie umów bez wychodzenia z domu, dzięki zastosowaniu urządzeń elektronicznych. Nie ulega jednak wątpliwości, że nowe technologie w początkowym okresie ich stosowania mogą wywoływać obawy co do wypełniania przez nie wymogów formalnych przewidywanych przez normy prawne prawodawstwa polskiego i unijnego.

Naprzeciw potrzebom zapewnienia kompromisu pomiędzy szybkością i wygodą, a bezpieczeństwem obrotu gospodarczego wychodzi aplikacja SignOnTheGo. Gwarancję bezpieczeństwa w aplikacji zapewnia technologia blockchain, która umożliwia identyfikację i weryfikację autentyczności dokumentów. Każdy podpisany w aplikacji SignOnTheGo dokument opatrzony jest metryką, która umożliwia śledzenie zmian wprowadzanych do jego treści przed podpisaniem. Cyfrowy kod certyfikacji QR, weryfikowany za pomocą technologii blockchain daje gwarancję autentyczności, a dodatkowe zabezpieczenie w postaci blokady podpisanego dokumentu w PDF sprawia, że wszelkie próby zmiany treści dokumenty po jego podpisaniu doprowadzą do unieważnienia podpisu cyfrowego.

Niniejsze opracowanie ma na celu przybliżenie istoty instytucji podpisu elektronicznego, jak również wyjaśnienie jego roli i prawnej skuteczności w kontekście rewolucyjnego wręcz rozwoju technologii. Przedstawiona redakcja prowadzi potencjalnego użytkownika aplikacji SignOnTheGo od ogólnych regulacji dotyczących podpisów elektronicznych i ich rodzajów, poprzez rozważania dotyczące technologii wykorzystywanych przy tworzeniu podpisów elektronicznych, aż do wyjaśnienia sposobu funkcjonowania SignOnTheGo, jego roli w zawieraniu zobowiązań umownych, by na zakończenie rozwiać wszelkie wątpliwości i obawy dotyczące skuteczności umów zawieranych poprzez aplikację.

I. PODSTAWA PRAWNA OPINII

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE „eIDAS" (Dz. U. UE L 257, 28.8.2014);
2. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U.2019.1145, 2019.06.19) ze szczególnym uwzględnieniem nowelizacji, która weszła w życie 8 września 2016 r., tj. ustawy z dnia 10 lipca 2015 r. o zmianie ustawy - Kodeks cywilny, ustawy - Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz. U. z 2015 r. poz. 1311);
3. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2016 r., poz. 1579).

II. PODPIS ELEKTRONICZNY W ŚWIETLE PRZEPISÓW PRAWA

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U.UE.910/2014) podpis elektroniczny są to dane, które użyte są przez podpisującego jako podpis, ale - jednocześnie - są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej. Owe "inne dane" to dane zawarte w certyfikacie elektronicznym, poświadczającym niezaprzeczalny związek podpisu z konkretną, dającą się jednoznacznie zidentyfikować osobą fizyczną (składającą podpis).

W świetle powołanego wyżej rozporządzenia rozróżniamy trzy rodzaje podpisów elektronicznych, a mianowicie podpis elektroniczny (zwykły, niekwalifikowany), zaawansowany podpis elektroniczny oraz kwalifikowany podpis elektroniczny. Powyższy opis definiuje zwykły podpis elektronicznego, jeżeli chodzi natomiast o dwie pozostałe formy podpisu elektronicznego, to przypisuje się im dodatkowego kryteria nieujęte w powyższej definicji.

Zaawansowany podpis elektroniczny to podpis elektroniczny, spełniający następujące kryteria: umożliwia ustalenie tożsamości podpisującego, jest unikalnie przyporządkowany podpisującemu, jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna, jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą.

Kwalifikowany podpis elektroniczny oznacza zaś zaawansowany podpis elektroniczny, który jest dodatkowo składany za pomocą kwalifikowanego urządzenia do składania

podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego;

Choć zgodnie z obowiązującymi przepisami jedynie kwalifikowany podpis elektroniczny kreuje skutki prawne tożsame ze skutkami podpisu własnoręcznego, to w świetle powołanego rozporządzenia niezależnie od wybranej formy żadnemu „**podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych**", o czym wyraźnie i jednoznacznie mówi treść art. 25 ust. 1 Rozporządzenia eIDAS.

Stosunkowo powszechną, acz nieprawidłową praktyką jest utożsamianie wspomnianej funkcji **identyfikacyjnej** osoby składającej podpis elektroniczny z czynnością prawną wyrażenia woli przez tę osobę. Podpis elektroniczny może bowiem spełniać kilka funkcji, w tym właśnie potwierdzać wyrażenie woli przez składającą go osobę fizyczną, ale wynikać to musi z kontekstu i charakteru działania, w którym podpis był użyty. O ile funkcją bezwarunkową podpisu elektronicznego jest **zapewnienie integralności podpisywanych danych** - z podpisu (ściślej, z wystawionego przez tzw. zaufaną stronę trzecią certyfikatu towarzyszącego podpisowi), dzięki stosowanym rozwiązaniom technicznym, o których mowa poniżej, jednoznacznie wynika, kto złożył podpis – to dopiero z treści podpisywanych danych wynika cel złożenia podpisu. Od charakteru podpisywanych danych (np. zdjęcie, tekst, obraz, oprogramowanie, zbiór plików w archiwum .zip – z których każde w postaci elektronicznej jest pewnym zbiorem danych binarnych tj. skończoną sekwencją zer i jedynek) i ich zawartości merytorycznej zależna będzie kwalifikacja wyłącznie jako czynności technicznej mającej na celu zapewnienie integralności i wskazania osoby lub podmiotu, która tego zapewnienia integracji dokonała, czy też jako czynności stanowiącej wyrażenie woli tego podmiotu.

Jedynie na marginesie zasygnalizować można (niniejsze nie stanowi bowiem przedmiotu niniejszej opinii), że rozporządzenie eIDAS obok podpisu elektronicznego wprowadza także definicję innej, szczególnie doniosłej dla działalności podmiotów posiadających osobowość prawną instytucji, a mianowicie pieczęci elektronicznej. W sposób tożsamy jak dla podpisu elektronicznego, w stosunku do pieczęci elektronicznej Rozporządzenie eIDAS również rozróżnia trzy rodzaje: zwykłą, zaawansowaną i kwalifikowaną. Powołując w ślad za słownikiem Rozporządzenia: za zwykłą pieczęć elektroniczna należy uznać „dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych". Pieczęć elektroniczna może znacznie usprawnić funkcjonowanie podmiotu prawnego. Można nią opatrywać firmową korespondencję elektroniczną, elektroniczne faktury, dokumenty dotyczące funkcjonowania danego podmiotu (jak statuty czy sprawozdania finansowe), jak również dokumenty prawne, oferty handlowe, foldery reklamowe, czy dokumentację bankową. Posługiwanie się pieczęcią elektroniczną niesie za sobą wiele

zalet. Zapewnia bowiem wiarygodność, bezpieczeństwo, oszczędność czasu i kosztów, pozytywnie wpływa również na wizerunek danego podmiotu.

III. FORMA PISEMNA

Pisemną formę czynności prawnych konstytuuje przepis art. 78 § 1 k.c. Stanowi on, że do zachowania pisemnej formy czynności prawnej wystarcza złożenie własnoręcznego podpisu na dokumencie obejmującym treść oświadczenia woli. Do zawarcia umowy wystarcza wymiana dokumentów obejmujących treść oświadczeń woli, z których każdy jest podpisany przez jedną ze stron, lub dokumentów, z których każdy obejmuje treść oświadczenia woli jednej ze stron i jest przez nią podpisany.

Jak rozumieć własnoręczność? Czy nazwę należy rozumieć literalnie i czy w związku z tym do zachowania pisemnej formy czynności prawnych konieczne jest wykorzystanie konkretnego nośnika informacji, a mianowicie, czy dokument musi być sporządzony na kartce papieru, czy też może znaleźć zastosowanie inny nośnik, o ile umożliwi wymaganą przez przepis wymianę dokumentów?

Również i przedmiotowa kwestia zostanie rozważona w dalszej części niniejszej opinii.

IV. ELEKTRONICZNA FORMA CZYNNOŚCI PRAWNYCH

5

Problematyka kwalifikacji formy czynności prawnych dokonywanych za pomocą środków elektronicznych początkowo budziła wątpliwości w doktrynie i judykaturze. Podejmowano próby odpowiedzi na pytanie, czy składanie podpisów w formie elektronicznej kreuje nową, odrębną od pisemnej, formę czynności prawnej, czy też stanowi odmianę tej drugiej. Wszelkie wątpliwości rozwiało prowadzenie przepisu art. 78^1 k.c., który w sposób niebudzący wątpliwości rozróżnił formę elektroniczną od formy pisemnej, jednocześnie zrównując skutki prawne oświadczeń woli składanych w formie elektronicznej z oświadczeniami pisemnymi.

Zgodnie z treścią przepisu do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym. Podkreślić więc należy, że podpis elektroniczny wywołuje skutki prawne równorzędne z podpisem własnoręcznym, gdy stanowi on tzw. bezpieczny podpis elektroniczny weryfikowany za pomocą kwalifikowanego certyfikatu, względnie, gdy posiada cechy indywidualne, pozwalające na weryfikację tożsamości autora.

W związku z powyższymi rozważaniami, które doprowadziły do wniosku o wyodrębnieniu elektronicznej formy czynności prawnych, której skutki prawne są tożsame z formą pisemną, w piśmiennictwie podjęto próbę wyróżnienia podpisów elektronicznych sensu stricte, obejmujących w istocie bezpieczne, weryfikowane za pomocą kwalifikowanego certyfikatu podpisy elektroniczne oraz podpisów

elektronicznych sensu largo, a zatem podpisów składanych (technicznie rzecz ujmując) w formie elektronicznej, nie spełniających jednakże kryteriów pozwalających za uznanie ich za bezpieczne podpisy elektroniczne. Celem rozjaśniania wskazuję, że podpisami elektronicznymi sensu largo będą między innymi: podpisy skanowane, które powstają w wyniku skanowania dokumentu zawierającego podpis własnoręczny, podpisy manualne, które są tworzone przy użyciu pióra cyfrowego, które przenosi elementy indywidualne do podpisu własnoręcznego do pamięci komputera, podpisy PIN-owe, które są składane za pomocą osobistego numeru identyfikacyjnego (kodu PIN) wraz z numerem karty elektronicznej w celu potwierdzenia takowej dyspozycji, podpisy biometryczne, które zawierają w sobie charakterystyczne dla danej osoby cechy fizyczne, np. odcisk linii papilarnych, czy obraz tęczówki, podpisy kryptograficzne, tworzone w oparciu o kryptograficzne karty mikroprocesorowe. Skutki prawne podpisów elektronicznych sensu largo są co do zasady tożsame do skutków wywoływanych przez użycie faksymile zamiast podpisu własnoręcznego.

Konsekwencją rozróżnienia na podpisy elektroniczne sensu strice i largo jest wyodrębnienie dwóch rodzajów form elektronicznych czynności prawnych, a zatem formy elektronicznej sensu largo, która obejmowałaby wszelkie dokumenty sygnowane elektronicznie oraz formę elektroniczną sensu stricte, czyli dokument elektroniczny opatrzony kwalifikowanym podpisem elektronicznym.

Powyżej przedstawiony podział skłania do dalszych rozważań, które pozwolą dokonać
6 analizy wpływu wybranej formy elektronicznej sensu largo i podpisywania dokumentów w aplikacji *Sign-On-The-Go* na ważność zawieranych w ten sposób umów, które to rozważania zawarte zostały w dalszych punktach niniejszego opracowania.

V. DOKUMENTOWA FORMA CZYNNOŚCI PRAWNYCH

Wraz z wejściem w życie ustawy nowelizującej Kodeks cywilny (co nastąpiło w dniu 8 września 2016 r.) wprowadzona została nowa forma umożliwiająca zawieranie czynności prawnych, a mianowicie forma dokumentowa.

W myśl art. 77^2 k.c. do zachowania dokumentowej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie.

Zgodnie z kolei z przepisem art. 77^3 k.c. dokumentem jest nośnik informacji umożliwiający zapoznanie się z jej treścią.

Cytowane przepisy dają w istocie możliwość zawierania umów i składania oświadczeń woli i wiedzy w odformalizowany sposób. Ustawodawca na mocy wprowadzonej nowelizacji sanuje bowiem sposób zawierania czynności prawnych, który w praktyce funkcjonował już od dawna.

W ramach niniejszego opracowania rozważaniom poddana zostanie również możliwość uznania skuteczności czynności prawnych zawieranych poprzez aplikację

Sign-On-The-Go w sytuacji, kiedy nie spełni ona wymogów formy pisemnej ani elektronicznej sensu stricte.

VI. PODPIS ELEKTRONICZNY, A PODPIS TRADYCYJNY

Pewność obrotu gospodarczego związana jest z możliwością wspomnianej wyżej identyfikacji podpisującego dokument elektroniczny. Wzmiankowana identyfikacja służy zapewnieniu bezpieczeństwa obrotu elektronicznego, a w sferze stosunków publicznoprawnych – uwiarygodnieniu elektronicznego podpisania określonego pisma przez konkretną osobę.

W przeciwieństwie do podpisu tradycyjnego, który jest zazwyczaj stawiany w tym samym miejscu, a konkretnie pod treścią dokumentu, który opatruje, jest taki sam dla wszystkich dokumentów oraz nie może być oddzielony od dokumentu, który sygnuje, podpis elektroniczny jest funkcją zawartości dokumentu, zależy od najdrobniejszych szczegółów dokumentu, więc dla każdego dokumentu będzie inny, chociaż złożony przez tę samą osobę. Podpis elektroniczny może być przesyłany i przechowywany niezależnie od dokumentu, a jedna osoba może posługiwać się wieloma podpisami elektronicznymi. Podpis elektroniczny od tradycyjnego od odróżnia również to, że nie może być złożony *in blanco* na dokumencie, który następnie zostanie uzupełniony określoną treścią. Oryginał podpisanego dokumentu i jego kopia są natomiast identyczne, nie można rozróżnić oryginału i kopii.

Podpis elektroniczny może dawać nawet większą – w porównaniu do podpisu tradycyjnego – możliwość ustalenia pochodzenia dokumentu elektronicznego (konkretnie – jego autora). Korzystanie z tej formy umożliwia nadto weryfikację ewentualnych modyfikacji treści dokumentu po jego podpisaniu.

VII. TWORZENIE PODPISU ELEKTRONICZNEGO

Bezpieczeństwo korzystania z podpisu elektronicznego zapewnia odpowiednie szyfrowanie, do którego stosuje się **kryptografię asymetryczną**. Metoda ta wiąże się z użyciem parametrów, zwanych kluczami – mianowicie klucza prywatnego – znanego tylko jego właścicielowi i służącego do podpisywania dokumentów oraz ochrony jego treści oraz klucza publicznego – który jest ogólnodostępny, a jego rola sprowadza się do weryfikowania podpisów i potwierdzenia treści dokumentów.

Nadawca podpisuje się pod dokumentem elektronicznym stosując swój klucz prywatny. Natomiast odbiorca tego dokumentu, posługując się kluczem publicznym nadawcy, może sprawdzić, czy rzeczywiście dokument został podpisany przez osobę uwidocznioną w tym dokumencie jako jego autor oraz czy po podpisaniu dokumentu nie zostały wprowadzone do jego treści jakiekolwiek modyfikacje, tak przez samego autora, jak również przez inną osobę.

Techniczna możliwość pewnego i jednoznacznego udzielania odpowiedzi na pytanie o pochodzenie dokumentu oraz jego późniejsze modyfikacje pozwoliła na prawną akceptację sygnowanych w ten sposób dokumentów elektronicznych, na równi z dokumentami sygnowanymi w tradycyjny sposób. Podpis elektroniczny, który spełnia ustawowe, przewidziane w przepisie art. 78^{1k}.c. wymogi, stanowi zatem prawnie aprobowany sposób przekształcenia dokumentu elektronicznego w znaczeniu materialno-technicznym w dokument w znaczeniu formalno-prawnym.

VIII. KRYPTOGRAFIA, A *SIGN-ON-THE-GO*

W aplikacji *Sign-On-The-Go*, celem zapewnienia bezpieczeństwa obiegu podpisywanych dokumentów zastosowano technologię blockchain. Jej działanie polega na tym, że po podpisaniu dokumentu przez wszystkich partnerów, ten w pełni wykonany dokument zostaje opublikowany w sieci publicznej. Następnie dokument ten jest poddawany weryfikacji (która ma umożliwić ocenę jego autentyczności). Przebieg procesu weryfikacji został opisany szerzej na stronie internetowej: https://signonthego.pl/weryfikacja/.

Poniższe rozważania mają na celu wyjaśnienie fenomenu technologii w oparciu o którą funkcjonuje aplikacja *Sign-On-The-Go* oraz odpowiedzieć na pytanie, czy wykorzystanie technologii blockchain faktycznie zapewnia bezpieczeństwo i w jaki sposób.

Blockchain bardzo intensywnie i skutecznie wykorzystuje znane koncepty kryptograficzne.

Pierwszym z nich jest tworzenie unikalnych i jednoznacznych "odcisków" danych za pomocą jednokierunkowych funkcji skrótu (tzw. funkcji haszujących). Są to funkcje znane i wykorzystywane w informatyce już od ponad 27 lat, a ich działanie polega na wyliczaniu na podstawie wspomnianych funkcji hashujących „skrótów" danych zawartych w dokumentach. Tak uzyskany „skrót" będzie odporny na kolizje - dwa różne zestawy danych nie dadzą tego samego skrótu i nie ma praktycznej możliwości wygenerowania zestawu danych o takim samym skrócie jak wskazany zestaw danych oraz jednokierunkowy i nieodwracalny, bowiem nie da się odtworzyć oryginalnej wiadomości znając jej skrót.

Obie te cechy skrótów danych wyliczonych za pomocą funkcji haszujących są w praktyce wykorzystywane do szybkiej identyfikacji danych cyfrowych (w tym interesujących dokumentów wprowadzanych i podpisywanych za pomocą aplikacji *SignOnTheGo*). Dzięki zastosowanej technologii nawet najmniejsza zmiana w danych źródłowych, choćby zmiana jednego tylko bitu, będzie powodowała, że wyliczony hash będzie różnił się od skrótu danych źródłowych.

Drugim ważnym składnikiem technologii blockchain jest opisana powyżej kryptografia asymetryczna pozwalająca zabezpieczyć wymianę informacji, czy wręcz zaszyfrować

informacje wymieniane między dwiema stronami, bez konieczności uzgadniania przez te strony jednego wspólnego klucza zabezpieczającego.

Trzecim elementem ze świata kryptografii zaadaptowanym przez technologię blockchain jest znakowanie czasem. Następuje tutaj bowiem synchronizacja czasu w sieci blockchain między uczestnikami sieci (czyli między partnerami – stronami potencjalnej umowy). Zarówno transakcje, jak i same bloki są znakowane czasem. Dzięki temu wszystkie obiekty i zdarzenia w blockchain są bardzo precyzyjnie umieszczone na zsynchronizowanej osi czasu i razem tworzą wiarygodną, ułożoną chronologicznie historię.

Kolejnymi filarami zapewniającym unikalne cechy funkcjonalne blockchain są mechanizmy konsensusu i inteligentne kontrakty (smart contracts). Mechanizm konsensusu to w dużym skrócie mechanizm zatwierdzania transakcji i dołączania nowych bloków do łańcucha, wykonywany przez oprogramowanie węzłów sieci blockchain. W tradycyjnych rozwiązaniach, aby potwierdzić zajście pewnych zdarzeń (zatwierdzić transakcje) konieczne jest ustanowienie zaufanej trzeciej strony, która gromadzi wszelkie dane pozwalające jej rozstrzygać, która wersja zdarzeń przedstawiona przez uczestników danego procesu zostanie uznana za obowiązującą. Niewątpliwą zaletą blockchain jest eliminacja potrzeby takiej zaufanej osoby trzeciej, którą zastąpiono uzgodnieniem dokonywanym automatycznie pomiędzy węzłami sieci, nazywanym właśnie konsensusem. Spotykamy dwa główne typy mechanizmów konsensusu. Pierwszy to tzw. “konsensus Nakamoto” polegający na przeprowadzeniu dla każdego nowego bloku pewnego rodzaju loterii i wyborze węzła-lidera, który będzie mógł zaproponować nowy blok przeznaczony do dołączenia do łańcucha, a po zatwierdzeniu tego bloku przez inne węzły uzyskać wynagrodzenie za dodanie tego bloku.

Najbardziej znaną implementacją konsensusu tego typu jest tzw. “dowód pracy” (proof-of-work) wykorzystywany w Bitcoin czy Ethereum. Drugi typ konsensusu bazuje na klasycznym algorytmie bizantyjskich generałów wykorzystywanym w sieciach rozproszonych i polega na wykonywaniu przez węzły sieci rund głosowań w celu uzyskania konsensusu. Wyspecjalizowane programy, rezydujące w sieci blockchain odpowiadają za wykonywanie podczas przetwarzania transakcji dodatkowych operacji zapisanych w ich kodzie programistycznym. Dzięki inteligentnym kontraktom sieć blockchain uzyskuje dodatkowe możliwości funkcjonalne, pozwalające na dużo bardziej skomplikowane przetwarzanie niż tylko transfer podstawowej kryptowaluty danej sieci. Smart contract może zarówno definiować zupełnie nowe, nieznane wcześniej kryptowaluty o praktycznie dowolnych funkcjonalnościach, ale może także stać się nośnikiem czy składnicą niefinansowych walorów cyfrowych oraz cyfrowej reprezentacji wartości materialnych. Taka elastyczna funkcjonalność sieci blockchain uzyskana dzięki inteligentnym kontraktom jest dzisiaj wielką obietnicą zupełnie nowych, prawdziwie innowacyjnych rozwiązań budowanych w oparciu o technologię blockchain.

Aplikacja *SignOnTheGo* łączy opisane składowe: funkcje haszujące, drzewa skrótów, kryptografię asymetryczną, znakowanie czasem, mechanizm konsensusu i inteligentne kontrakty w jedną całość. Systemy wykorzystywane w *SignOnTheGo* tworzą niezmienne, znakowane czasem wpisy w rozproszonej bazie danych dla każdej kiedykolwiek wykonanej, pojedynczej transakcji. Dzięki temu każda transakcja i odpowiadający jej rekord danych są łatwo i jednoznacznie identyfikowalne, przeciwdziałając jednocześnie oszustwom, nadużyciom oraz innym rodzajom manipulacji na danych transakcji.

IX. PODPIS BIOMETRYCZNY

Podpis biometryczny stanowi digitalizację charakterystycznych dla danej osoby cech fizycznych, tj. odcisku linii papilarnych, obrazu tęczówki, barwy głosu czy kształtu twarzy.

Obecnie największą popularność zyskuje biometria podpisu odręcznego. Jej użycie jest bowiem wygodne, szybkie i daje możliwości zastosowania w szerszym spektrum działań gospodarczych. W najprostszym ujęciu praktyczne wykorzystanie biometrii w interesującym nas i stanowiącym przedmiot niniejszego opracowania zakresie, tj. w sygnowaniu dokumentów i zawieraniu umów, sprowadza się do złożenia odręcznego podpisu na dokumencie za pośrednictwem dedykowanego tabletu, wykorzystującego specjalne oprogramowanie, które umożliwia jego wierne odwzorowanie w formie elektronicznej i związanie z dokumentem w systemie.

Powyższe skłania do analizy prawnego znaczenia i charakteru podpisu biometrycznego. W szczególności rozważyć należy, czy podpis biometryczny spełnia wymogi pozwalające na uznanie go za podpis własnoręczny.

Stanowisko Sądu Najwyższego dotyczące zagadnienia własnoręczności jest jednolite, powszechnie aprobowane i ugruntowane w orzecznictwie. W ślad za jednym z judykatów należy przyjąć, że podpis własnoręczny to „***znak pisarski, umożliwiający identyfikację osoby, od której pochodzi, przynajmniej według takich kryteriów jak cechy indywidualne i powtarzalne***”. W tych minimalnych wymaganiach nie określa się konieczności użycia papieru czy długopisu albo pióra. Podpis własnoręczny musi być zatem znakiem pisarskim (nie ma nawet wymogu, żeby podpisywać się pełnym imieniem i nazwiskiem), który ma na tyle indywidualne i powtarzalne cechy, że zawsze ten znak pisarski da przypisać jednej i tej samej osobie.

Innymi słowy, żeby podpis był własnoręczny, musi być taki, żeby się dało jednoznacznie stwierdzić, że ten podpis złożyła właśnie ta, konkretna osoba. **Jeśli więc podpis biometryczny pozwala ustalić jego autora, to jest podpisem własnoręcznym**.

Skoro judykatura co do zasady zezwala na potraktowanie podpisu biometrycznego jako podpisu własnoręcznego, to bez wątpienia kluczem do sukcesu będzie

stosowanie odpowiednich rozwiązań technologicznych, które umożliwią wykazanie wymaganej identyfikacji autorstwa.

X. UWIERZYTELNIANIE PRZY UŻYCIU BIOMETRII, A UWIERZYTELNIANIE TRADYCYJNE

Dokonując identyfikacji lub uwierzytelnienia określonej osoby w sposób tradycyjny, należy wykazać się posiadaniem dokumentu, klucza, karty lub pamiętać swój PIN, PESEL albo inny identyfikator. Weryfikacja za pomocą hasła nie identyfikuje osoby. Osoba podająca hasło niekoniecznie musi być osobą uprawnioną do jego używania, może wejść w posiadanie hasła (karty, klucza, tokena) nielegalnie. Przy weryfikacji za pomocą hasła (zapisanego na karcie czy wpisanego z pamięci) podaje się określone, dobrze rozpoznawalne znaki (liczby, litery itd.). Wynik weryfikacji jest dokładny. Jeżeli wszystkie znaki hasła są takie same jak we wzorze hasła zapisanym w bazie danych, następuje uwierzytelnienie. Jest to porównanie dwóch „informacji cyfrowych", które system automatyczny jest w stanie wykonać dokładnie. Hasło służące do weryfikacji może zostać przejęte (np. kradzież kartki z zapisanym hasłem). Dokonując weryfikacji za pomocą hasła należy zapamiętać hasło lub nabyć karty identyfikujące ich właściciela. Negatywną stroną takiej weryfikacji jest możliwość zgubienia karty lub podejrzenia hasła w czasie jego wprowadzania przez osoby nieuprawnione do jego posiadania. Pozytywną stroną jest ciągłość korzystania z haseł – w przypadku kompromitacji hasła istnieje możliwość jego zmiany i korzystania z nowego. Warto również zaznaczyć, że zarówno kartę z hasłem, jak i samo hasło można powierzyć osobie trzeciej, chociaż co do zasady hasło lub klucz jest tajny.

Dla uwierzytelnienia z użyciem metod biometrycznych nie trzeba podawać hasła ani wykazywać się posiadaniem jakichkolwiek przedmiotów identyfikacyjnych. Należy tylko udostępnić swoją biometrykę, która zostaje następnie zidentyfikowana poprzez jej przetworzenie na postać cyfrową i wyekstrahowanie jej reprezentacji, czyli szablonu biometrycznego, a następnie utrwalenie i przetworzenie rzeczywistej biometryki na reprezentatywną postać cyfrową.

Czynność ta wykonywana jest za pomocą czytnika, czyli np. cyfrowego aparatu fotograficznego, czytnika linii papilarnych, czy rysika stosowanego do podpisywania dokumentów na tablecie.

Hipotetycznie możliwe jest, że pozytywnie zweryfikowanych szablonów z bazy będzie więcej niż jeden. Istotne znaczenie ma wybór kompromisu pomiędzy bezpieczeństwem, a kosztem urządzenia i jego późniejszej eksploatacji czy też bezpieczeństwem a czasem uwierzytelniania. Wybór zależny jest od rodzaju zastosowania urządzenia uwierzytelniającego. Podszycie się pod cudzą biometrykę wymaga nie tylko kradzieży tej biometryki (co często jest łatwe, gdyż biometryka nie jest sekretem), lecz także wykonanie atrapy w celu oszukania czytnika, co może być bardzo trudne technicznie, a czasem niemożliwe.

XI. WZMOCNIENIE PODPISU ELEKTRONICZNEGO ZA POMOCĄ BIOMETRII.

Najprostszym sposobem włączenia biometrii do procesu tworzenia podpisu elektronicznego jest uzależnienie dostępu do klucza prywatnego od pozytywnego wyniku biometrycznej weryfikacji użytkownika.

Weryfikacja ta polega na porównaniu szablonu uzyskanego z próbki biometrycznej tylko z jednym szablonem właściciela klucza i tylko właściciel może być zweryfikowany pozytywnie. Ta niezaprzeczalna autoryzacja tożsamości użytkownika uniemożliwia późniejsze wyparcie się użycia klucza. Nie jest też możliwe użycie klucza przez osoby nieupoważnione.

Rozróżnia się dwie możliwości automatycznej analizy podpisu: off-line, czyli podpisy statyczne, już istniejące na papierze, fotografii czy skanie oraz on-line, czyli podpisy składane przy użyciu specjalnego urządzenia dostarczającego na bieżąco dodatkowych informacji o dynamicznych cechach podpisu (nacisk, położenie pióra, czas i płynność wykonania podpisu).

Analiza off-line wykorzystuje typowe algorytmy do analizy obrazu, podczas gdy analiza on-line działa w oparciu o statystyczną metodę klasyfikacji sekwencji zdarzeń, używaną również przy rozpoznawaniu mowy oraz tzw. dynamiczne marszczenie czasu – polegające na porównywaniu podpisów jako funkcji czasu. Tempo pisania każdej osoby jest bez wątpienia inne, dlatego aby porównanie było właściwe, wprowadza się indywidualne czasy przez zniekształcenie (marszczenie) rzeczywistego czasu. Mimo że analiza on-line jest bardziej skomplikowana i wymaga zastosowania specjalistycznego oprzyrządowania – a co za tym idzie – jest też bardziej kosztowna, to nie ulega wątpliwości, że jest bardziej miarodajna. Analiza off-line jest bardziej podatna na podrabianie podpisu. Poziomy błędów zrównoważonych dla systemów on-line zawierają się w 2% i są dziesięciokrotnie mniejsze niż w przypadku systemów off-line.

W praktyce analizę on-line umożliwiają tablety graficzne, rejestrujące podpisy w systemach on-line. Rejestracja podpisu odręcznego uwzględnia charakterystykę tabletu, szybkość podpisywania, sposób trzymania długopisu.

XII. *SIGN-ON-THE-GO*, A WAŻNOŚĆ UMÓW PODPISYWANYCH PRZY UŻYCIU APLIKACJI

Rozróżnienie formy elektronicznej sensu stricte i sensu largo pozwala stwierdzić, że choć uznanie podpisu elektronicznego za kwalifikowany daje pewność spełnienia funkcji identyfikującej podpisującego, zapewniając tym samym pewność co do integralności dokumentu oraz tego, że podpis został złożony przez osobę uprawnioną, to nie umniejsza to roli jaką w związku z postępem technologicznym i możliwościami jakie zapewnia technologia blockchain odgrywa forma elektroniczna sensu largo. Co najważniejsze – nie deprecjonuje to skutków prawnych umów zawieranych i podpisywanych w aplikacji *Sign-On-The-Go*.

Obydwa rodzaje podpisu mogą być składane w taki sam sposób. Jednak, w przeciwieństwie do podpisu elektronicznego sensu largo – kwalifikowany podpis elektroniczny wymaga bezpiecznych urządzeń i bezpiecznego oprogramowania dostarczanych wyłącznie przez upoważnione (certyfikowane) do tego podmioty. Wymaga to jednakże znacznie większych – w porównaniu z podpisami elektronicznymi sensu largo – nakładów finansowych.

Skutki prawne zawierania umów w aplikacji są w istocie uzależnione od formy, jaką przepisy prawa przewidują dla umów konkretnego rodzaju (pisemną lub równaną z nią elektroniczną) i pod jakim rygorem forma ta jest przewidziana (rygor nieważności, czy dla celów dowodowych).

Zawarcie umowy, która dla swej ważności nie wymaga formy pisemnej, a zatem: umowy o współpracy, umowy zlecenia, w tym umowy zlecenia działań marketingowych (nie przenoszącej majątkowych praw autorskich), umowy zlecenia z osobami fizycznymi (lekarze, farmaceuci etc.), umowy najmu, umowy serwisowej, umowy o świadczenie usług, umowy długoterminowej, umowy sponsoringu, umowy ramowej, czy też aneksu do tej umowy, umowy badań rynku, umowy o dzieło (nie przenoszącej majątkowych praw autorskich), umowy o zachowaniu poufności, umowy na analizy HTA, zamówienia składanego na podstawie ustawy Prawo Zamówień Publicznych, zgody o przetwarzanie danych osobowych (po 25 maja 2018 r.), będzie dopuszczalne poprzez złożenie podpisu na tablecie lub za pomocą myszki na ekranie komputera. Właśnie w tym momencie klarowne staje się podobieństwo skutków prawnych czynności prawnych zawieranych przy użyciu podpisów elektronicznych sensu largo z tymi, które zostają urzeczywistnione przy użyciu faksymile. Również i istota opatrywania dokumentów podpisem elektronicznym sensu largo jest zbliżona do użycia faksymile, z tym zastrzeżeniem, że mechanizmy używane podczas składania podpisów elektronicznych niejako automatyzują cały proces odbicia podpisu.

Jeśli natomiast zawarta ma być umowa, której ważność jest uzależniona od zachowania formy pisemnej (dla przykładu: umowa leasingu, umowa darowizny, zgoda o przetwarzaniu danych osobowych (przed 25 maja 2018 r.), to odpowiedź na pytanie dotyczące możliwości jej zawarcia poprzez złożenie podpisu na tablecie warto poprzedzić powtórzeniem stanowiska Sądu Najwyższego dotyczącego wymogów jakie musi spełniać podpis, by mógł zostać uznany za własnoręczny. Należy rozważyć spełnienie wymogów podpisu własnoręcznego, a zatem posiadania przez podpis cech indywidualnych i powtarzalnych, umożliwiających identyfikację jego autora. Podpis biometryczny bez wątpienia te kryteria spełnia, w związku z czym należy dojść do konkluzji, iż zawarcie umowy dla której ważności ustawodawca przewidział formę pisemną w dalszym ciągu może nastąpić poprzez złożenie podpisu na tablecie, z tym zastrzeżeniem, że przy jego składaniu urządzenie (a właściwie aplikacja je obsługująca) musi zbierać dane dynamiczne związane z podpisem (tj. w szczególności poziom nacisku rysika, ale również prędkość składania podpisu i in.)., które pozwolą zidentyfikować osobę składającą podpis. Konkludując, jeżeli ustawa przewiduje dla

danej czynności prawnej formę pisemną, to opatrzenie podpisem biometrycznym pozwoli zachować tę przepisaną prawem formę.

Bez wątpienia wykorzystanie Aplikacji *Sign-On-The-Go* pozwoli uczynić zadość formie dokumentowej. Aplikacja umożliwia bowiem tak ustalenie osoby, która składa oświadczenie, jak również zapoznanie się z jego treścią. Tożsamość osoby jest bowiem weryfikowana już poprzez dane wprowadzane do Aplikacji podczas rejestracji konta. Podczas podpisywania zbierany jest również adres IP, który również pozwala na identyfikację autora. Co istotne, po zakończeniu edycji dokumentu i zwieńczeniu go podpisem Aplikacji – dokonywanie zmian w treści dokumentu jest niemożliwe, a poczynienie takich prób unieważni e-podpis. Nośnik informacji i zapisanie dokumentów w „chmurze" umożliwia natomiast wymianę dokumentów i daje dostęp do treści w nich zawartych.

adw. Piotr Szkulik