Skutki prawne stosowania podpisu elektronicznego w praktyce obrotu gospodarczego

Jerzy Zygadło

Prawie codziennie każdy z nas podpisuje różnego rodzaju dokumenty, faktury, itp. Czynimy to własnoręcznie za pomocą pióra, długopisu, ołówka, kreśląc na papierze określone, charakterystyczne znaki pozwalające nas zidentyfikować. W najbliższej przyszłości powszechną sprawą stanie się podpisywanie dokumentów nowym rodzajem podpisu, którym jest podpis elektroniczny.

W przypadku elektronicznej wersji podpisu nie ma mowy o własnoręczności tegoż podpisu, nie ma także mowy o nawiązaniu w sposób bezpośredni do imienia czy nazwiska osoby go składającej. Dzieje się tak, ponieważ podpis elektroniczny odwołuje się do tych danych jedynie w sposób pośredni. Sam podpis jest tylko zbiorem bitów[1]. Lecz istota podpisu elektronicznego zakłada jego wiarygodność na tym samym poziomie, co podpis własnoręczny.

Pojęcie podpisu elektronicznego jest pojęciem, które pojawiło się stosunkowo niedawno. W polskim prawie pojęcie to funkcjonuje od 18 września 2001 roku, kiedy to Sejm RP uchwalił ustawę o podpisie elektronicznym, która weszła w życie z dniem 16 sierpnia 2002 roku.[2]

Zgodnie z art. 3 ust. 1. tej ustawy, podpis elektroniczny to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny. Podpis elektroniczny jest niczym innym, jak ciągiem cyfr powstałym poprzez zastosowanie algorytmu kryptograficznego do podpisywanej wiadomości (Stokłosa, 1998).

Prawo wspólnotowe rozróżnia pojęcia „podpisu cyfrowego" i „podpisu elektronicznego. Jednakże nie wyjaśnia różnicy między tymi pojęciami, wskazując jedynie, że „podpis elektroniczny" jest pojęciem szerszym (Szyndzielorz, 2001). Cechą, która wyróżnia go spośród podpisów elektronicznych jest fakt zastosowania w nim metod kryptografii polegającej na wykorzystaniu dwóch kluczy. Do wygenerowania podpisu elektronicznego stosuje się tzw. algorytm kryptografii z kluczem publicznym. Jest to system, w którym każdy użytkownik posiada parę unikalnych kluczy – klucz prywatny i klucz publiczny. Dostęp

[1] Bit – najmniejsza jednostka informacji. Przyjmuje wartość 0 lub 1.

[2] Ustawa z dnia 18 września 2001 roku o podpisie elektronicznym (Dz.U. Nr 130, poz. 1450).

do klucza prywatnego posiada tylko i wyłącznie jego właściciel, natomiast odpowiadający mu klucz publiczny musi być powszechnie dostępny.

Klucz prywatny służy przede wszystkim do zaszyfrowania wiadomości i w efekcie do stworzenia podpisu elektronicznego dla danego dokumentu. Stanowi on swoistą zaszyfrowaną pieczęć, która uniemożliwia niedostrzegalną zmianę treści dokumentu i identyfikuje posiadacza klucza, np. nazwisko, pseudonim, itp. Tak podpisana wiadomość może być odczytana i zweryfikowana przez odbiorcę za pomocą klucza publicznego. Odbiorca niejako przykładając klucz publiczny do podpisanej elektronicznej dokumentu może stwierdzić, czy wiadomość pochodzi od dysponenta klucza prywatnego (Barta, Markiewicz, 2000: 71).

Ustawa o podpisie elektronicznym, oprócz zwyczajnego podpisu elektronicznego, wprowadza także pojęcie bezpiecznego podpisu elektronicznego. W myśl ustawy jest on podpisem elektronicznym, który:

– pozwala na jednoznaczną identyfikację osoby składającej ten podpis, a identyfikacja to nic innego, jak potwierdzenie tożsamości osoby,
– winien być niepowtarzalny czyli tylko jedna osoba może dysponować identycznym popisem elektronicznym,
– jest sporządzany za pomocą – podlegających wyłącznej kontroli osoby składającej podpis elektroniczny – bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
– jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna,
– umożliwia wykrycie prób jego złamania podejmowanych po jego złożeniu (Borowicz, 2002: 98).

Zgodnie z ustawą, tylko bezpieczny podpis elektroniczny jest równoważny, pod względem skutków prawnych, podpisowi tradycyjnemu. Jak się można domyślać koszty uzyskania takiego podpisu będą wyższe niż w przypadku uzyskania „zwykłego" podpisu elektronicznego, lecz w zamian otrzymamy produkt o wyższym poziomie bezpieczeństwa.

W czasach, gdy nowoczesna technika informatyczna umożliwia niedostrzegalną zmianę i fałszowanie przekazywanych czy gromadzonych danych nikogo nie dziwią techniczne i prawne zabiegi oraz postulaty uczestników obrotu prawnego, którzy domagają się wprowadzenia oraz równouprawnienia „bezpiecznych" dokumentów elektronicznych. Podpis elektroniczny jest aprobowany przez system prawny i ułatwia obrót handlowy, a jednocześnie dokumenty opatrzone takim podpisem stają się bardziej wiarygodne od dokumentów z tradycyjnym podpisem.

W związku z powyższym podpis elektroniczny w elektronicznym obrocie handlowym (e-Commerce), a także w innych zastosowaniach, ma do spełnienia istotne funkcje, z których najważniejsze to:

– Poufność – jest to ochrona przesyłanych informacji przed ich poznaniem przez nieuprawnione osoby. Poufność można uzyskać poprzez zaszyfrowanie wiadomości,
– Integralność – czyli ochrona przed wprowadzeniem zmian do wiadomości przez osoby do tego nieuprawnione.

Każdy z nas – wysyłając lub odbierając wiadomość – chce mieć pewność, że treść tej wiadomości nie została lub nie zostanie zmieniona czy też zniekształcona przez osoby nieuprawnione.

– Uwierzytelnianie – funkcja ta polega na potwierdzeniu tożsamości danego użytkownika i/lub potwierdzenie prawdziwości przesyłanej wiadomości. W gruncie rzeczy uwierzytelnianie polega na sprawdzeniu, czy dany podpis został utworzony przy wykorzystaniu klucza prywatnego odpowiadającego kluczowi publicznemu,
– Niezaprzeczalność – uniemożliwia wyparcie się przez nadawcę faktu wysłania wiadomości o ustalonej treści.

Cecha ta ma szczególne znaczenie w przypadku zamówień dokonywanych np. w sklepach internetowych. W przypadku, gdy dana osoba podpisana jako nadawca – oświadczy, że nie wysyłała zamówienia o danej treści, wówczas odbiorca, w tym przypadku sklep, bez problemu jest w stanie udowodnić, że nikt inny nie mógł wysłać takiej wiadomości, ponieważ tylko nadawca może posługiwać się kluczem prywatnym, który został mu przydzielony, przy użyciu którego zostało wysłane zamówienie. Na tym etapie nie jest istotne to, kto rzeczywiście posłużył się kluczem prywatnym, ani też to, kim rzeczywiście jest nadawca (Bartosiewicz, 2001: 44 nn).

Zasada działania podpisu elektronicznego

W celu użycia podpisu elektronicznego lub cyfrowego konieczne jest uprzednie przygotowanie wiadomości, którą mamy zamiar cyfrowo podpisać. Pierwszym krokiem jest stworzenie przez nadawcę, za pomocą specjalnego programu, skrótu wiadomości. Poprzez zastosowanie jednokierunkowej[3] funkcji skrótu otrzymujemy cyfrowe „streszczenie" dokumentu. Istotą cechą streszczenia jest to, że skrót zawsze ma stałą długość, niezależną od długości wiadomości. Najczęściej jest to 16 lub 20 bajtów (czyli 128 i 160 bitów). Dzięki temu zabiegowi programowa implementacja algorytmu podpisu elektronicznego staje się szybsza. Dzieje się to w wyniku tego, że podpis obliczany jest tylko dla kilkunastu bajtów skrótu dokumentu. W praktyce okazuje się, że żadne dwie różne wiadomości nie mają tego samego skrótu. Dodatkowo funkcja skrótu gwarantuje wykrycie nieuprawnionych modyfikacji. Oznacza to, że w przypadku ingerencji nieuprawnionej osoby w treść podpisanej cyfrowo wiadomości lub zmiany pojedynczego bitu tej wiadomości, wartość funkcji skrótu zmienia się w sposób nieprzewidywalny.

Podczas generacji podpisu, ta ostatnia cecha pozwala traktować skrót wiadomości na równi z pierwowzorem. Do skracania wiadomości używane są techniki kryptograficzne w postaci algorytmów. Najczęściej stosuje się algorytm SHA-1 (*Secure Hash Algorithm-1*) generujący wynik o długości 128 bajtów lub MD5 (*Message Digest 5*) generujacy wynik o długości 160 bajtów (Dąbrowski, Kowalczuk, 2002: 35 nn.).

[3] Jednokierunkowa, gdyż niemożliwe jest odtworzenie oryginalnej wiadomości na podstawie samego skrótu.

Certyfikaty i organy certyfikacyjne

Tożsamość osoby podpisanej kluczem prywatnym pod dokumentem elektronicznym winna być poświadczona przez niezależny podmiot świadczący usługi certyfikacyjne. Usługi świadczone przez te podmioty polegają na wydawaniu certyfikatów poświadczających tożsamość osoby korzystającej z określonego podpisu elektronicznego (Barta, Markiewicz, 2000: 74; Jacyszyn, Przetocki, Wittlin, Zakrzewski, 2002: 225) Certyfikat może otrzymać jedynie osoba fizyczna, gdyż tylko osoba fizyczna może składać oświadczenia woli z użyciem podpisu elektronicznego i skutki prawne będą dotyczyły konkretnej osoby fizycznej (Świerczyński, 2002: 9).

Kwalifikowany podmiot świadczący usługi certyfikacyjne może oferować następujące usługi:

– „Zwykły" podpis elektroniczny będącym najtańszym i prostym rozwiązaniem, służącym głównie do zabezpieczenia danych przesyłanych pocztą elektroniczną. Takiemu oświadczeniu woli z tym podpisem, jak stwierdza art. 8 omawianej ustawy, nie można odmówić ważności i skuteczności, tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu. „Zwykły" podpis elektroniczny i oświadczenie woli potwierdzone tym podpisem nie będzie miało takiej wartości dowodowej, jak oświadczenia woli potwierdzone bezpiecznym podpisem z kwalifikowanym certyfikatem, czyli można mu odmówić ważności i skuteczności, jeżeli wcześniej strony nie umówiły się co do jego ważności i skuteczności (Świerczyński, 2002: 8).
– Kwalifikowany – bezpieczny podpis elektroniczny, spełniający warunki określone przepisami ustawy o podpisie elektronicznym, czyli weryfikowany przy pomocy kwalifikowanego certyfikatu i sporządzony za pomocą podlegających wyłącznej kontroli osoby składającej podpis bezpiecznych urządzeń i danych[4] służących do składania podpisu elektronicznego. Bezpieczny podpis elektroniczny jest równoważny pod względem skutków prawnych dokumentom podpisanym własnoręcznie.
– Instytucja znakowania czasem – jest elektroniczną formą daty pewnej, która nadaje formie pisemnej walor kwalifikowany w rozumieniu przepisów kodeksu cywilnego. Polega na dołączeniu do danych w postaci elektronicznej – logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym – oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę. Ową usługę certyfikacyjną pełnią podmioty kwalifikowane wedle cech określonych w ustawie o podpisie elektronicznym. W szczególności – w odróżnieniu od daty pewnej uregulowanej w art. 81 kodeksu cywilnego – podmiotami takimi mogą być podmioty prawa prywatnego nie mające kompetencji do sporządzania dokumentów urzędowych w rozumieniu art. 244 kodeksu po-

[4] Dane to niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez ową osobę do składania podpisu elektronicznego i używane są również do weryfikacji podpisu i identyfikacji osoby składającej podpis elektroniczny.

stępowania cywilnego. Znakowanie czasem stwarza niewzruszalne domniemanie, że podpis elektroniczny złożony został nie później niż w chwili dokonania tej usługi (Krawczyk, 2003: 295). Jednakże ze względu na to, że podstawą tego domniemania jest zaświadczenie certyfikacyjne, nie istnieje ono po ustaniu ważności tego certyfikatu, poza tym, gdy zostało przedłużone przez wydanie kolejnego lub kolejnych certyfikatów (Radwański, 2001: 1107).

Swoboda składania oświadczeń woli w postaci elektronicznej

Kolejna nowela kodeksu cywilnego[5] w dodanym § 2 do art. 61 stwierdza, że oświadczenie woli wyrażone w postaci elektronicznej jest złożone innej osobie z chwilą, gdy wprowadzono je do środka komunikacji elektronicznej w taki sposób, żeby osoba ta mogła zapoznać się z jego treścią. Zgodnie z treścią art. 78 § 2 k. c. oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne z oświadczeniem woli złożonym w formie pisemnej. Artykuł 661 § 1 k. c. stwierdza, iż oferta złożona w postaci elektronicznej wiąże składającego, jeżeli druga strona niezwłocznie potwierdzi jej otrzymanie. Natomiast przedsiębiorca składający ofertę w postaci elektronicznej jest obowiązany przed zwarciem umowy poinformować drugą stronę w sposób jednoznaczny i zrozumiały o:

– czynnościach technicznych składających się na procedurę zawarcia umowy,
– skutkach prawnych potwierdzenia przez drugą stronę otrzymania oferty,
– zasadach i sposobach utrwalania, zabezpieczania i udostępniania przez przedsiębiorcę drugiej stronie treści zawieranej umowy,
– metodach i środkach technicznych służących wykrywaniu i korygowaniu błędów we wprowadzonych danych, które jest obowiązany udostępnić drugiej stronie,
– językach, w których umowa może być zawarta,
– kodeksach etycznych, które się stosuje, oraz o ich dostępności w postaci elektronicznej.

Powyższe zasady stosuje się odpowiednio również, jeżeli przedsiębiorca zaprasza drugą stronę do rozpoczęcia negocjacji, składania ofert albo do zawarcia umowy w inny sposób. Należy podkreślić, że przepisy art. 611 § 1–3 kodeksu cywilnego nie mają zastosowania do zawierania umów przy użyciu poczty elektronicznej albo podobnych środków indywidualnego porozumiewania się na odległość; poza tym nie stosuje się ich także w stosunkach między przedsiębiorcami, jeżeli strony tak postanowiły.

Za miejsce zawarcia umowy w trybie ofertowym uważa się w razie wątpliwości miejsce otrzymania przez składającego ofertę oświadczenia o jej przyjęciu, a jeżeli dojście do składającego ofertę oświadczenia o jej przyjęciu nie jest wymagane albo oferta jest składana w postaci elektronicznej – w miejscu zamieszkania albo w siedzibie składającego

[5] Ustawa z dnia 14 lutego 2003 roku o zmianie ustawy – Kodeks cywilny oraz niektórych innych ustaw (Dz. U. Nr 49, poz. 408), która weszła w życie z dniem 25 września 2003 roku.

w chwili zawarcia umowy. Jest to reguła interpretacyjna i ma zastosowanie tylko wtedy, gdy strony nie ustaliły, co jest tym miejscem zawarcia umowy (Turek, 2003: 16).

Internet Banking

Postępująca od połowy lat 90. popularność i dostępność Internetu spowodowała, że banki zainteresowały się również i tym medium, widząc w nim łatwy dostęp do rynku detalicznego i indywidualnego klienta. I rzeczywiście, bankowość internetowa, znana także jako *Internet Banking*, stała się bardzo szybko nowym, a przy tym tanim kanałem dystrybucyjnym dla wielu banków. Obecnie coraz częściej bankowość internetowa na świecie zastępuje lub dokompletuje dotychczas stosowane rozwiązania – tzw. bankowości domowej (*Home Banking*), czy też *Phone Banking*. Kierowana jest głównie do klientów indywidualnych. *Home Banking* zezwala klientowi banku na dostęp do swojego konta bankowego przy użyciu specjalnego oprogramowania, które łącząc się bezpośrednio z serwerem banku przesyła wszelkie potrzebne dane. *Internet Banking* pozwala robić to samo bez użycia specjalnego oprogramowania i potrzeby nawiązywania bezpośredniego połączenia z bankiem – dostęp do konta odbywa się poprzez Internet, za pomocą przeglądarki www (Gregor, Stawiszyński, 2002: 163). Z konta w wirtualnym oddziale banku może korzystać praktycznie każdy, kto dysponuje komputerem klasy PC z dostępem do Internetu i zainstalowaną przeglądarką www (Netscape Navigator, MS Internet Explorer). *Internet Banking* umożliwia dokonywanie wszystkich klasycznych operacji bankowych bez wychodzenia z domu i – co najważniejsze – często taniej niż w tradycyjny sposób (Wiaderek, 2000: 141). Transmisja danych jest szyfrowana. Stosowane są różne formy uwierzytelniania klientów (zarówno silne, jak i słabe). Na rysunku 1 przedstawiono główną stronę wirtualnego banku mBank.

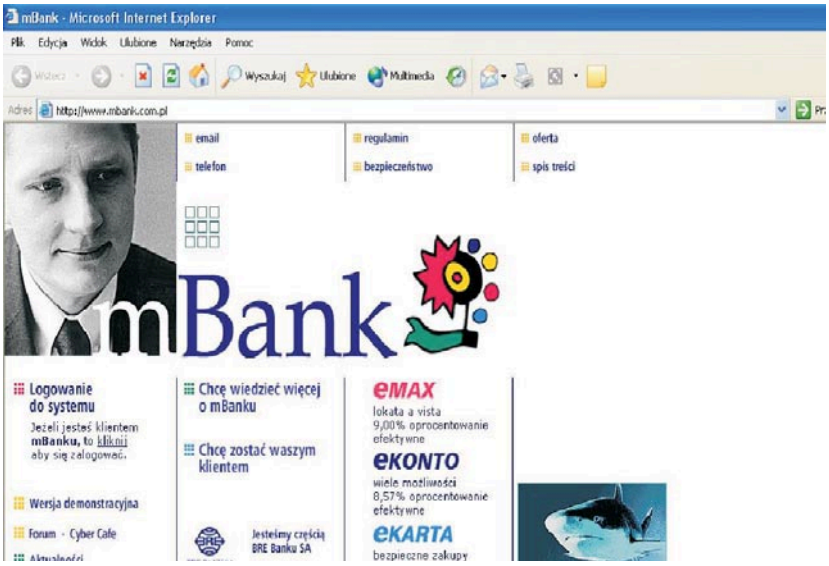
Instytucja podpisu elektronicznego winna znaleźć szerokie zastosowanie w bankowości. Pojawiają się jednak wątpliwości wobec stosowania kwalifikowanych technologii podpisu elektronicznego. Funkcjonowanie instytucji podpisu elektronicznego będzie pociągało za sobą określone koszty. Sami użytkownicy nie będą zainteresowani ponosić dużych nakładów na finansowanie czytników elektronicznych i kart chipowych. Najbardziej predestynowanym do tego rodzaju nakładów będzie sektor bankowy, gdyż stosowanie podpisu elektronicznego niesie za sobą szereg korzyści (Hoeren, 2003: 160). Wynikają one z faktu, iż instytucja e-podpisu przyspieszy rozwój dochodowego działu bankowości – bankowości elektronicznej[6].

Najczęściej to banki na mocy umów z organami certyfikacji przejmą na siebie koszty związane z uzyskaniem przez swoich klientów podpisów elektronicznych[7], gdyż takie działanie pozostaje w interesie banków, którym winno zależeć na bezpiecznych metodach identyfikacji swoich klientów (Stańczyk, 2001).

---

[6] W Banku BZWBK przelew elixir w okienku kosztuje 7 zł natomiast przelew za pośrednictwem Internetu to tylko 1,5 zł.

[7] PKO BP S. A. 2002, Referencje dla Unizeto Sp. z o. o., http://www.certum.pl/programy_partnerskie/referencje/pkobp.htlm



Rys. 1

Główna strona internetowego banku mBank w 2003 roku

Podpis elektroniczny to bezpieczny sposób uwierzytelniania klienta. Ustawa o podpisie elektronicznym pozwoli bankom na rozwijanie działalności w zakresie bankowości elektronicznej.

Bibliografia

[1] Barta J., Markiewicz R. 2000: *Internet a prawo*, Universitas, Kraków.

[2] Bartosiewicz M. 2001: *Bity Twojego podpisu*, ENTER, Nr 5.

[3] Borowicz K. 2002: *Komentarz. Ustawa o podpisie elektronicznym*, Park, Bielsko-Biała.

[4] Dąbrowski W., Kowalczuk P. 2002: *Podpis elektroniczny*, Mikom, Warszawa.

[5] Gregor B., Stawiszyński M. 2002: *e-Commerce*, Branta, Bydgoszcz-Łódź.

[6] Hoeren T. 2003: *Zagadnienie prawne handlu elektronicznego. Wprowadzenie*, tłum. J. Krieger [w:] T. Zasępa, R. Chmura (red.): *Internet i nowe technologie – ku społeczeństwu przyszłości*, Wyd. Święty Paweł, Lublin.

[7] Jacyszyn J., Przetocki J., Wittlin, A., Zakrzewski S. 2002: *Podpis elektroniczny. Komentarz do ustawy z 18 września 2001 r.*, LexisNexis, Warszawa.

[8] Krawczyk T.L. 2003: *Ustawa o podpisie elektronicznym- omówienie z krótkim komen- tarzem*, [w:] T. Zasępa, R. Chmura (red.): *Internet i nowe technologie – ku społeczeństwu przyszłości*, Święty Paweł, Lublin.

[9] Radwański Z. 2001: *Elektroniczna forma czynności prawnej*, Monitor Prawniczy nr 22.

[10] Skubisz R. (red.) 2000: *Internet 2000 prawo – ekonomia – kultura*, Serba, Lublin.

[11] Stańczyk P. 2001: *Prawne i ekonomiczne aspekty podpisu elektronicznego*, Poznań http://www.vagla.pl.

[12] Stokłosa J. 1998: *Podpis elektroniczny można porównać do pieczęci*, „Rzeczpospolita", 2 marca.

[13] Szyndzielorz P. 2001: *Elektroniczna forma czynności prawnych*, Poznań, http://www.vagla.pl.

[14] Świerczyński M. 2002: *Podpis elektroniczny w praktyce handlowej*, [w:] „Gospodarka elektroniczna", Monitor Prawniczy nr 24.

[15] Turek P. 2003: *Zawieranie umowy w drodze elektronicznej, w trybie ofertowym, według kodeksu cywilnego*, http://www.vagla.pl.

[16] Wiaderek G., 2000: *Internetowe czynności bankowe a forma pisemna czynności prawnych* [w:] R. Skubisz (red): *Internet 2000 prawo – ekonomia – kultura*, Serba, Lublin.

[17] Zasępa T. Chmura R. (red.) 2003: *Internet i nowe technologie – ku społeczeństwu przyszłości*, Wyd. Święty Paweł, Lublin.