Paweł Stańczyk

# PRAWNE I EKONOMICZNE ASPEKTY PODPISU ELEKTRONICZNEGO

Praca dyplomowa
napisana pod kierunkiem

**dr. Grzegorza Kotlińskiego**
Katedra Bankowości
Akademia Ekonomiczna w Poznaniu

POZNAŃ 2001

# O Autorze:

Paweł Stańczyk (ur. 1977)

## Absolwent

Uniwersytetu im. A Mickiewicza
Wydziału Prawa i Administracji
Kierunek: prawo

Akademii Ekonomicznej w Poznaniu
Wydziału Ekonomii
Kierunek: finanse i bankowość

Kontakt:
pawelstanczyk@go2.pl

# SPIS TREŚCI

# WSTĘP

Światowa gospodarka ulega licznym przeobrażeniom. Zmienia się przede wszystkim jej charakter. Istotnym elementem wymiany gospodarczej staje się informacja, którą można uznać za cenne dobro. Szybkość jej przesyłania ma coraz większe znaczenie, gdyż jest to sposób jego przekazywania. Szybka wymiana informacji prowadzi do powstania gospodarki nowego typu – opartej na wiedzy. Jednak aby móc ustalić wartość informacji trzeba znać jej źródło. Dlatego tak ważne jest właściwe ustalenie, skąd pochodzi przekazywana wiadomość, kto jest jej autorem. Nie ma z tym żadnego problemu w przypadku, gdy jesteśmy bezpośrednimi świadkami przekazywania informacji, na przykład w czasie wykładu. Gospodarcze wykorzystanie tego dobra wymaga jednak o wiele szybszego obiegu. Służą temu najnowsze techniki komunikacyjne, takie jak telefonia komórkowa czy Internet. To ostatnie medium jest szczególnie często wykorzystywane do szybkiego przesyłania danych na dużą odległość. Problemem jest jednak właściwa identyfikacja osób porozumiewających się za pomocą Internetu. Jego rozwiązaniem jest podpis elektroniczny, który staje się niezbędnym narzędziem w dzisiejszej gospodarce.

Tematem niniejszej pracy są prawne i ekonomiczne aspekty podpisu elektronicznego. Jest to zupełnie nowa, dotychczas nieznana, instytucja. Ma ona duże znaczenie dla podmiotów, które będą z niej korzystać najczęściej – banków. Ważna jest więc kompleksowa analiza tej problematyki. Tymczasem nie istnieją w Polsce całościowe opracowania dotyczące podpisu elektronicznego. Celem niniejszej pracy jest więc omówienie technicznych i prawnych zasad działania podpisu elektronicznego oraz wskazanie korzyści, kosztów oraz możliwych problemów z nim związanych. W zamyśle ma ona stanowić kompendium wiedzy na temat podpisu elektronicznego.

Rozdział pierwszy omawia zasady działania oraz funkcje podpisu elektronicznego. Przybliża pojęcie podpisu elektronicznego i określa funkcje, jakie ma on do spełnienia. Zawiera również opis zasad jego działania. W tym celu wyjaśnia na czym polega złożenie podpisu elektronicznego oraz jakie etapy składają się na ten proces. Szczególny nacisk kładziony jest na wskazanie roli kluczy prywatnego i publicznego w tworzeniu sygnatury elektronicznej. Określa się też funkcje i zadania systemu certyfikacji. Jako że bezpieczeństwo podpisu ma zasadnicze znaczenie dla powodzenia tej instytucji, rozdział pierwszy zawiera również analizę technik kryptograficznych stosowanych na potrzeby podpisu elektronicznego. Jej celem jest odpowiedź na pytanie o zakres pewności i bezpieczeństwa takiego podpisu dziś i w najbliższej przyszłości. Ze stosowaniem tego narzędzia wiąże się wiele korzyści dla banków. Ich wskazanie jest również celem tej części pracy. Banki będą musiały też ponieść określone koszty wdrażając odpowiednią

infrastrukturę, dlatego też opisano, jakiego rodzaju wydatki są związane z podpisem elektronicznym.

Podpis elektroniczny dla swej skuteczności wymaga uznania go przez system prawny. Chodzi w szczególności o zrównanie go pod względem wywoływanych skutków z podpisem własnoręcznym. Dlatego też rozdział drugi zajmuje się prawnymi aspektami podpisu elektronicznego. Jego celem jest określenie infrastruktury prawnej, w której on funkcjonuje. Za podstawę rozważań służy projekt Ustawy o podpisie elektronicznym w wersji uchwalonej przez Sejm 27 lipca 2001 roku. Rozdział drugi problematykę tę ujmuje w podziale na dziedziny prawa. Przede wszystkim omawia on cywilnoprawne skutki stosowania podpisu elektronicznego. Ze względu na bogactwo zagadnień o charakterze cywilnoprawnym, z konieczności jedynie sygnalizuje się pozostałe problemy, które mogą się pojawić w związku ze stosowanie tej instytucji. Szczególny nacisk kładzie się na kwestie administracyjnoprawne, które mają decydujące znaczenia dla bezpieczeństwa całego systemu. Stanowią one podstawową część regulacji ustawowej. W związku z prawdopodobnym przystąpieniem Polski do Unii Europejskiej, dokonuje się również analizy przepisów dotyczących uznawania podpisów elektronicznych tworzonych poza obszarem naszego kraju. W rozdziale drugim znajduje się też wskazanie norm, które nakładają odpowiedzialność karną za naruszenie określonych w Ustawie reguł. Rozważania te uzupełnione są o ich krytyczną analizę.

Wymiana informacji za pośrednictwem sieci komputerowych ma charakter międzynarodowy. W wielu krajach wprowadza się obecnie instytucję podpisu elektronicznego. W nielicznych ona już funkcjonuje. Rozdział trzeci umiejscawia polskie rozwiązania na tle rozwiązań międzynarodowych. Traktuje on zarówno o wytycznych o charakterze międzynarodowym, jak i o przykładowych unormowaniach w kilku krajach. W rozdziale tym szczególną uwagę kładzie się na zgodność polskiego systemu podpisu elektronicznego z wytycznymi Unii Europejskiej w tej sprawie. Dokonuje się w nim również analizy porównawczej, która ma na celu wskazanie, czy, i ewentualnie jakie problemy mogą wyniknąć ze stosowania innych, niż określają to wydane w Polsce przepisy, podpisów elektronicznych. Jej przedmiotem jest przede wszystkim samo pojęcie podpisu elektronicznego, jako że w różnych krajach termin ten oznacza różne rzeczy, co prowadzić może do wielu komplikacji.

Jak już wspomniano, nie istnieją całościowe opracowania w języku polskim dotyczące podpisu elektronicznego. Wymusza to konieczność korzystania z wielu cząstkowych opracowań, dotyczących poszczególnych wycinków tej problematyki. W zakresie wydawnictw zwartych wykorzystano przede wszystkim polskie wydania opracowań anglojęzycznych dotyczących zasad działania podpisu elektronicznego oraz technicznych kwestii z nim związanych, w szczególności

stosowanych metod kryptograficznych. Pomocne okazały się również prace polskich autorów dotyczące prawa komputerowego czy internetowego. Istotne wiadomości zaczerpnięte zostały z artykułów umieszczonych w czasopismach komputerowych (np. miesięcznik ENTER) lub bankowych (np. miesięcznik BANK). Cenne okazały się również artykuły zamieszczane w gazetach codziennych (przede wszystkim w „Rzeczpospolitej" i „Gazecie Wyborczej").

W niniejszej pracy ważną rolę zajęły dane, pochodzące od dwóch pierwszych, i jedynych polskich podmiotów świadczących usługi certyfikacyjne. Są to firma Unizeto z siedzibą w Szczecinie, która prowadzi Centrum Certyfikacji „Certum", oraz Centrum Certyfikacji „Signet", będące własnością Telekomunikacji Polskiej S.A. Stamtąd właśnie pochodzą dane na temat kosztów związanych z podpisem elektronicznym. Jednak powstanie tej pracy było możliwe tylko dzięki informacjom pochodzącym ze źródła, które samo w sobie jest powodem stworzenia podpisu elektronicznego, a mianowicie Internetu. Zamieszczono tam wiele opracowań, które w różnym stopniu dotykają istoty omawianej problematyki. Istnieje wiele serwisów internetowych poświęconych właśnie podpisowi elektronicznemu chociaż najczęściej są to serwisy zagraniczne. Z polskich domen internetowych wykorzystano przede wszystkim serwis „VaGla – Prawo i Internet" prowadzony przez Piotra Waglowskiego, a także serwis „Prawo komputerowe" prowadzony przez Adama Tochę, umieszczony w portalu Hoga.pl. Wśród wykorzystanych materiałów szczególną rolę odgrywają przepisy prawne, w tym przede wszystkim projekt polskiej Ustawy o podpisie elektronicznym. Wykorzystano także ustawy innych krajów, a także przepisy Unii Europejskiej oraz normy tworzone przez Komisję Narodów Zjednoczonych do spraw Międzynarodowego Prawa Handlowego. Skorzystano też z materiałów o takim charakterze, jak np. sprawozdanie komisji sejmowej z rozpatrzenia projektów ustaw o podpisie elektronicznym.

Praca ta zawiera, w zakresie polskiego ustawodawstwa, stan prawny na dzień 11 października 2001 roku. Uwzględnione zostały w niej postanowienia Ustawy z dnia 18 września 2001 roku o podpisie elektronicznym.

# Rozdział 1

# Zasady działania i funkcje podpisu elektronicznego

## 1.1. Pojęcie i funkcje podpisu elektronicznego

### 1.1.1. Pojęcie podpisu elektronicznego

Podpis elektroniczny to pojęcie nowe. Nie ma ugruntowanej treści w języku polskim. Co więcej kłóci się ono z potocznym rozumieniem słowa „podpis". Tradycyjnie, dokonując podpisu, czynimy to własnoręcznie, kreśląc określone znaki na papierze. Umożliwia to później identyfikację autentyczności poprzez zwykłe porównanie złożonych znaków z posiadanym wzorcem lub też poprzez szczegółową analizę grafologiczną. Podpis w formie elektronicznej nie ma jednak nic wspólnego z cechą „własnoręczności", możliwe jest nawet złożenie podpisu elektronicznego bez wykonywania jakiegokolwiek ruchu ręką. Treść podpisu tradycyjnego obejmuje najczęściej nazwisko, które bywa uzupełniane imieniem osoby dokonującej tego aktu. Jednak w przypadku podpisu elektronicznego nie ma w ogóle mowy o bezpośrednim nawiązywaniu do imienia czy nazwiska osoby go składającej, albowiem podpis elektroniczny odwołuje się do tych danych osobowych jedynie pośrednio, sam będąc tylko zbiorem bitów komputerowych. Nie znajdzie wreszcie swego odzwierciedlenia w podpisie elektronicznym cecha „pisemności", która nieodłącznie kojarzy się z podpisem w jego tradycyjnej formie.

Adresat każdego dokumentu chciałby mieć pewność, że przesłana mu wiadomość rzeczywiście pochodzi od nadawcy podpisanego pod jej treścią. W przypadku dokumentu tradycyjnego jego nadawca po prostu podpisuje się własnoręcznie na papierze pod treścią przekazu. Wiadomość w postaci elektronicznej nie posiada jednak substratu materialnego, nie ma więc na czym złożyć podpisu. Problemem polega zatem na tym, czym opatrzyć taki przekaz, aby bez cienia wątpliwości można było stwierdzić od kogo pochodzi. Żeby komunikacja była skuteczna ważne jest również, aby wiadomość nie została zmieniona w drodze od nadawcy do adresata. O ile w przypadku dokumentów tradycyjnych spełnienie powyższego warunku nie jest trudne, o tyle w przypadku danych w postaci elektronicznej przesyłanych przy użyciu nowoczesnych sieci komputerowych zapewnienie ich bezpieczeństwa to już poważny problem. Tym celom ma służyć instytucja podpisu elektronicznego wykorzystująca nowoczesne techniki kryptograficzne.

Podpis elektroniczny (zwany również „podpisem cyfrowym" lub „e-podpisem") jest to ciąg cyfr powstały poprzez zastosowanie algorytmu kryptograficznego do podpisywanej wiadomości. Ów algorytm stosuje się wraz z kodem znajdującym się w posiadaniu osoby podpisującej, który jest najczęściej umieszczony na specjalnej karcie mikrochipowej. Podpis elektroniczny stanowi więc rodzaju pieczęć odciskana na wiadomości w formie elektronicznej. Stanowi go niepowtarzalny ciąg bitów, którego postać zależy od dwóch czynników:

a) od osoby, która wiadomość podpisuje (a ściślej od jej klucza prywatnego) oraz
b) od treści podpisywanej wiadomości (warto więc zaznaczyć, iż podpis elektroniczny będzie różny dla dwóch różnych wiadomości, nawet gdy podpisuje go ta sama osoba) [1].

Idea podpisu elektronicznego oparta jest na asymetrycznym systemie szyfrowania z wykorzystaniem dwóch, matematycznie powiązanych kluczy. Oczywiście nie mają one postaci materialnej, są jedynie ciągami odpowiednich cyfr. Pierwszy z nich to tzw. klucz prywatny (ang. *private key*) nadawcy, który służy przede wszystkim (ale nie tylko) do zaszyfrowania oryginalnej wiadomości i w konsekwencji do stworzenia podpisu elektronicznego dla danego dokumentu. Klucz ten jest tajny, może się nim posługiwać tylko jego posiadacz. Wytworzony przy jego zastosowaniu ciąg bitów, jako e-podpis, przesyłany jest wraz z dokumentem do jego adresata. Ten używa drugiego z pary kluczy – klucza publicznego (ang. *public key*) nadawcy. Klucz ten jest powszechnie dostępny. Używając go adresat jest w stanie stwierdzić, czy wiadomość pochodzi od dysponenta klucza prywatnego[2]. Klucz publiczny nadawcy staje się więc nieodłącznym komponentem tej instytucji, jest on bowiem niezbędny do weryfikacji autentyczności przesłanej poprzez sieć wiadomości. Para: klucz prywatny – klucz publiczny jest w ten sposób podstawowym elementem podpisu elektronicznego.

Twórcy polskiej Ustawy o podpisie elektronicznym z dnia 18.09.2001 (dalej: Ustawa) podobnie ujmują istotę tej instytucji, tak ją definiując: „Podpis elektroniczny – 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"[3]. Dokonując krótkiej analizy projektowanego przepisu warto zauważyć, iż określa on podpis elektroniczny jako pewne dane w postaci elektronicznej. Dane te to nic innego jak klucz prywatny nadawcy. Zostają one dołączone do innych danych, stając się podpisem elektronicznym. Owe „inne dane" to po prostu wiadomości w formie elektronicznej. To do nich jest niejako doklejany podpis elektroniczny

[1] J. Stokłosa , *Podpis elektroniczny można porównać do pieczęci*, Rzeczpospolita, 2.03.1998.
[2] J. Barta, R. Markiewicz, *Internet a Prawo*, Kraków 1998, str. 71.
[3] Art. 4 pkt. Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

jako swego rodzaju załącznik. Polska ustawowa definicja podpisu elektronicznego jest wyraźnie wzorowana na Dyrektywie Parlamentu Europejskiego i Rady (dalej: Dyrektywa) w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego[4]. Stanowi ona w artykule 4 punkcie 1, że „podpis elektroniczny oznacza dane w formie elektronicznej, które dodane są do innych danych elektronicznych lub są z nimi logicznie powiązane i służą do autoryzacji"[5]. Wydaje się, iż słusznie zauważono w dyrektywie, że e-podpis ma zastosowanie tylko w przypadku dokumentów o postaci elektronicznej. Podstawowa bowiem różnica pomiędzy obiema definicjami, polską i unijną, jest taka, że Dyrektywa Unii Europejskiej wymaga, aby podpis był stosowany tylko do danych elektronicznych. Polska Ustawa mówi jedynie o „danych", nie zawężając zakresu tego pojęcia do danych elektronicznych, co należałoby interpretować jako zgodę na stosowanie podpisu elektronicznego również wobec przekazu informacji o tradycyjnej postaci. Zdaniem Autora jest to zbyt szerokie ujęcie.

W myśl Ustawy o podpisie elektronicznym dane, mające stać się podpisem cyfrowym, muszą być dołączone do wiadomości lub być przynajmniej z nią logicznie powiązane. Wydaje się jednak, że spełnione powinny być jednocześnie obie przesłanki, bowiem przy spełnieniu tylko jednej z nich trudno sobie wyobrazić właściwe funkcjonowanie tej instytucji. Na przykład brak logicznego powiązania podpisu z wiadomością oznaczałby równoczesny brak jednego z czynników, który jest niezbędny do wyznaczenia podpisu elektronicznego. Dlatego zamiast użycia spójnika „lub" właściwsze wydaje się użycie spójnika „i", który sugeruje konieczność jednoczesnego wystąpienia obu tych zjawisk: zarówno logicznego powiązania danych elektronicznych z wiadomością elektroniczną jak też dołączenia danych do wiadomości. Tego mankamentu nie posiada rządowy projekt ustawy o podpisie elektronicznym[6], który w tym zakresie nie został uwzględniony. Omówione powyżej działania powinny „służyć do identyfikacji osoby składającej podpis elektroniczny".

W literaturze zwraca się uwagę, że pojęcia „podpis elektroniczny" i „podpis cyfrowy" nie są tożsame. Podpis cyfrowy jest tylko jednym z wielu możliwych rodzajów podpisu elektronicznego. Cechą wyróżniającą podpis cyfrowy wśród podpisów elektronicznych jest zastosowana w nim metoda kryptograficzna, polegająca na wykorzystaniu dwóch symetrycznych kluczy. Zastosowanie innej techniki kryptograficznej powoduje więc stworzenie nowego rodzaju podpisu

[4] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronical signature*, opublikowany w: *Official Journal of the European Communities* z 19.01.2000.
[5] *ibidem*, „Electronic signature – means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.".
[6] Por. art. 4 wstępnego rządowego projektu ustawy o podpisie elektronicznym z dnia 29.11.1999.

elektronicznego, który nie może być już nazywany podpisem cyfrowym[7]. Ani Ustawa, ani Dyrektywa Unii Europejskiej nie stoi na przeszkodzie takiemu rozumieniu podpisu elektronicznego. Realizuje się tym samym postulat neutralności technologicznej aktów prawnych – nie przesądza się szczegółowo tego, jakie techniki kryptograficzne będą używane. Tym niemniej, nie istnieją obecnie inne, rozpowszechnione metody znajdujące zastosowanie w podpisie elektronicznym. Dlatego też można jeszcze dziś stosować te pojęcia zamiennie. Tak też będą używane w niniejszej pracy.

Polska Ustawa określa warunki, jakie powinien spełnić podpis elektroniczny, aby mógł zostać uznany za „bezpieczny podpis elektroniczny"[8]. Stanowi ona, iż powinien on:

a) być przyporządkowany wyłącznie do osoby składającej ten podpis,
b) być sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
c) być powiązany z danymi, do których został dodany w taki sposób, że każda późniejsza zmiana tych danych jest rozpoznawalna.

Tylko bezpieczny podpis elektroniczny będzie mógł wywołać skutki prawne równoważne podpisowi tradycyjnemu[9]. Koszty funkcjonowania takiego podpisu będą z pewnością większe niż podpisu „zwykłego", ale to za cenę wyższego poziomu bezpieczeństwa i większej pewności obrotu handlowego i prawnego. Taki podpis będzie mógł być stosowany już nie tylko pomiędzy osobami prywatnymi, ale również w stosunku do wielu instytucji i urzędów publicznych (np. urzędów skarbowych), które będą miały obowiązek go honorować. Bezpieczny podpis elektroniczny będzie też stosowany w kontaktach z bankami, zakładami ubezpieczeniowymi i innymi podmiotami finansowymi. Krótko mówiąc wszędzie tam, gdzie bezpieczeństwo przesyłania danych ma istotne znaczenie.[10]

[7] Tak np. za niemiecką doktryną P. Szyndzielorz, *Elektroniczna forma czynności prawnych*, VaGla – Prawo i Internet, http://www.vagla.pl/.
[8] Art. 3 pkt. 2 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[9] Art. 5 ust 2. Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[10] Inaczej tę kwestię ujmował wstępny rządowy projekt ustawy, który nie dzieli podpisu elektronicznego na „zwykły" i „bezpieczny", lecz od razu stawia tej instytucji wyższe wymagania. Według tego projektu każdy podpis elektroniczny, żeby być skutecznie złożonym musi spełniać określone warunki. Powinien być jednoznacznie związany z podmiotem podpisującym, umożliwiać określenie tożsamości podmiotu podpisującego, być tworzony przy użyciu narzędzi, nad którymi podmiot podpisujący posiada całkowitą i wyłączną kontrolę oraz musi być powiązany z danymi, do których został dodany w taki sposób, że każda późniejsza zmiana tych danych będzie możliwa do stwierdzenia.

### 1.1.2. Funkcje podpisu elektronicznego

Instytucja podpisu elektronicznego ma do spełnienia ważne funkcje. Niektóre z nich są bezpośrednio związane z samym podpisem cyfrowym, inne są wynikiem mechanizmów związanych z funkcjonowaniem tej instytucji. Zależnie od przyjętych kryteriów funkcje można mnożyć i dzielić na wiele różnych sposobów.[11] Na potrzeby niniejszej pracy wystarczające wydaje się wskazanie podstawowych pięciu funkcji podpisu elektronicznego. Zadaniem sygnatury elektronicznej jest zapewnienie uwierzytelniania, niezaprzeczalności, integralności, identyfikacji oraz poufności.

Najbardziej charakterystyczną funkcją instytucji podpisu elektronicznego jest uwierzytelnianie (ang. *authentication*). Polega ona na ustaleniu, czy podpis elektroniczny został utworzony z użyciem klucza prywatnego odpowiadającego kluczowi publicznemu. Nadawca wiadomości używa swojego klucza prywatnego do złożenia podpisu na dokumencie. Po wysłaniu dokumentu adresat, wiedząc, kto jest domniemanym (na razie) nadawcą, używa klucza publicznego tegoż nadawcy (powszechnie dostępnego), aby stwierdzić, czy określone sumy kontrolne się zgadzają. Jeżeli tak jest, oznacza to, iż wiadomość została podpisana przy użyciu klucza prywatnego tego właśnie nadawcy. Nie znamy jeszcze dokładnie nadawcy, może on ukrywać się na przykład pod pseudonimem. Mamy natomiast pewność, iż wiadomość została podpisana przy użyciu jego klucza prywatnego.

Inną, bardzo blisko związaną z powyższą, cechą związaną z funkcjonowaniem podpisu elektronicznego jest niezaprzeczalność (ang. *undeniability*). Funkcja ta umożliwia udowodnienie (w typowej sytuacji) faktu wysłania określonej wiadomości przez dana osobę. Zapobiega to przypadkom wypierania się przez nadawcę, że wysłał dokument o takiej to a takiej treści. Ma to szczególne znaczenie w przypadku zamówień kierowanych np. do sklepów internetowych. Jeżeli osoba podpisana jako nadawca oświadczy, że nie wysłała takiej wiadomości, wówczas adresat-sklep bez problemu wykaże, iż nikt inny prócz nadawcy nie mógł wysłać takiej wiadomości, gdyż tylko on może posługiwać się jemu przynależnym kluczem prywatnym, przy użyciu którego zostało wysłane zamówienie. Nie ważne jest na tym etapie ani to, kto rzeczywiście posłużył się kluczem prywatnym nadawcy, ani też to, kim rzeczywiście jest nadawca (jakie są jego dokładne personalia). Wystarczy, iż wiadomo, że do nadania wiadomości użyto określonego klucza prywatnego

[11] Por. np. J. Barta, R. Markiewicz, *Internet a Prawo*, Kraków 1998, str. 70; V. Ahuja, *Bezpieczeństwo w sieciach – Internet, Intranet, Firewall*, Warszawa 1997; A. Król, *Zawarcie umowy w internecie według kodeksu cywilnego*, http://www.prometeus.com.pl/prawo/; M. Bartosiewicz, *Bity Twojego podpisu*, ENTER, 2001, Nr 5, str. 44; Uzasadnienie do poselskiego projektu ustawy o podpisie elektronicznym złożonego przez posłów dnia 21.12.2000, str. 1.

jednoznacznie związanego z osobą nadawcy. Na tej podstawie można w sposób logiczny domniemywać (w sensie potocznym), że danym kluczem prywatnym posługuje się osoba, na którą go wystawiono.

Kolejną ważną funkcją podpisu elektronicznego jest integralność (ang. *integrity*). Funkcja ta polega na ochronie wiadomości przed wprowadzeniem do niej zmian przez osoby do tego nieupoważnione. Nadawca musi mieć pewność, że treść dokumentu nie została sfałszowana lub też, że nie doszło do przypadkowego jej zniekształcenia. Dokładnie rzecz biorąc zapewnienie integralności odbywa się jedynie pośrednio, albowiem możliwość wprowadzenia nieuprawnionych modyfikacji do wiadomości nie jest w żaden sposób utrudniona, z tym, że każda, choćby najmniejsza zmiana treści będzie od razu widoczna. Dzieje się tak, ponieważ nieodłącznym komponentem tworzenia podpisu elektronicznego jest wyznaczenie na podstawie samej wiadomości jej skrótu przy użyciu odpowiedniego algorytmu. W ten sposób powstaje unikalna dla danej wiadomości suma kontrolna, która dla dwóch różnych wiadomości będzie zawsze różna. Oznacza to, że każda modyfikacja treści wiadomości zmienia wartość skrótu, a zatem jest możliwa do wykrycia. Jest to tzw. jednokierunkowa funkcja skrótu.

Ważną funkcją, która wiąże się z instytucją e-podpisu, jest identyfikacja (ang. *identification*). Polega ona potwierdzeniu tożsamości nadawcy wiadomości. Pozwala ona stwierdzić, kto rzeczywiście jest zarejestrowany jako właściciel danego klucza prywatnego. Jest to możliwe dzięki istnieniu tzw. organów certyfikacji, które generują odpowiadające sobie pary kluczy, a następnie klucz prywatny przyznają osobie zainteresowanej, a klucz publiczny podają do powszechnej wiadomości. W ten sposób łatwo jest ustalić, kim jest nadawca, po prostu zwracając się do takiego organu z odpowiednim zapytaniem lub przeglądając publicznie dostępny rejestr certyfikatów[12], o ile taki istnieje. Tu trzeba jednak poczynić dwie uwagi. Po pierwsze, możliwe jest posługiwanie się pseudonimem przy użytkowaniu certyfikatu, a nawet przy jego uzyskiwaniu. Oznacza to, iż adresat będzie miał wprawdzie pewność, iż wiadomość pochodzi od podpisanej elektronicznie osoby, ale nie będzie mógł się dowiedzieć rzeczywistych i dokładnych personaliów nadawcy. Po drugie, w zamkniętym kręgu podmiotów istnienie organów certyfikacji nie jest w ogóle potrzebne, gdyż w takiej sytuacji wszyscy nawzajem znają swoje klucze publiczne i swoją tożsamość. Identyfikacja nadawcy będzie w takim przypadku dokonywana jednocześnie z uwierzytelnieniem wiadomości. Przykładem mogą być tu banki, które same między sobą, tworzą własną parę kluczy, zachowując sobie klucz prywatny, rozpowszechniając natomiast wśród pozostałych banków-kontrahentów klucz publiczny. Postępuje tak każdy bank w umawiającej się

[12] Por. art. 27 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

grupie. W ten sposób każdy z nich posiada klucz publiczny pozostałych banków, nie jest wtedy potrzebne odwoływanie się do jakiejkolwiek osoby trzeciej, pełniącej funkcje centrum certyfikacji.

Ostatnia funkcja – poufności (ang. *confidentiality*), jest funkcją, która nie musi być związana z podpisem elektronicznym. To, czy jest ona realizowana, czy nie, dla istnienia e-podpisu jest zupełnie obojętne. Tak się jednak składa, że często wraz z podpisywaniem wiadomości dokonuje się jej zaszyfrowania. Funkcja to polega bowiem właśnie na ochronie danych przed zapoznaniem się z nimi przez osoby trzecie. W ten sposób szyfrowanie dokonywane jest nie tylko wobec skrótu wiadomości, lecz także wobec niej samej, z tą jednak różnicą, iż używa się do tego klucza publicznego adresata, a rozszyfrowania dokonuje adresat swoim kluczem prywatnym (kierunek jest więc odwrotny).

## 1.2. Uwierzytelnianie i utajnianie

W systemie podpisu elektronicznego niezbędne jest istnienie układu dwóch powiązanych ze sobą matematycznie kluczy – prywatnego i publicznego. Służą one do szyfrowania i deszyfrowania wiadomości. Jest to tzw. system z szyfrem asymetrycznym (ang. *assymetric key encryption*). Jego przeciwieństwem jest system oparty o szyfr symetryczny (ang. *symmetric key encryption*), w którym to mamy do czynienia tylko z jednym kluczem, używanym zarówno do szyfrowania, jak i do odszyfrowywania wiadomości. Klucz ten jest znany zarówno nadawcy jak i odbiorcy, jednak dla pozostałych osób musi pozostać on tajny. System taki ma dwie zasadnicze wady z punktu widzenia podpisu elektronicznego:

a) w celach identyfikacyjnych można posługiwać się nim tylko w stosunkach między dwoma podmiotami; wiadomo wówczas, że tylko druga, znana odbiorcy, strona mogła posłużyć się danym szyfrem; w przypadku większej liczby podmiotów znających klucz (nawet gdyby było ich tylko trzech) nie można stwierdzić, kto rzeczywiście wiadomość podpisał, bowiem klucza mogły użyć przynajmniej dwie osoby,
b) istnieje problem, jak przekazać drugiej stronie stosowany klucz w taki sposób, aby nie poznały go osoby postronne; w szyfrowaniu z kluczem asymetrycznym drugiej stronie również jest przekazywany klucz, lecz już z założenia ma on charakter jawny; to niebezpieczeństwo więc nie występuje; problemem w obu przypadkach pozostaje nadal kwestia bezpiecznego przechowywania kluczy.

Ze względu na powyższe wady metoda szyfrowania z kluczem symetrycznym nie znajduje zastosowania w dziedzinie e-podpisu. Dlatego też w niniejszej pracy nie zostanie ona szerzej omówiona.

Klucz, zarówno prywatny jak i publiczny, to ciąg bitów komputerowych. Zasadniczo przyjmuje on postać ciągu zer i jedynek (zapis binarny), ale jako taki nie jest widoczny dla użytkownika komputerowego, gdyż jest on zaszyfrowany i uzupełniony ważnymi informacjami, tworząc tzw. certyfikat. Może on przybrać postać ciągu tekstowego. Oto przykład takiego certyfikatu[13]:


MIIC/TCCAmagAwIBAgIDAeiIMA0GCSqGSIb3DQEBBAUAMEMxCzAJBgNVBAYTAlBM
MRswGQYDVQQKEx7Vbml6ZXRvIFNwLiB6IG8uby4xFzAVBjNVBAMTDkNlcnR1bSBM
ZXZlbCBJMB4XDTAxMDIyNzAxMzQwMloXDTAxMDgyNjAxMzQwMlowYDELMAkGA1UE
BhMCUEwxGjA3agNVBAoTEVpvbGJveCBGcmVlIEVtYWlsMREwDwYDVQQDEwhrb211l
cmNqYTEiMCAGCSqGSIb3DQEJARYTa29tZXJjamFAcG9sYm94LmNvbTBcMA0GCSqG
SIb3DQEBAQUAA0sAMEgCQQC9Ejq2YHwEhYjQOAVtbzaINqCC2H6whRt9aHYnwzGB
LggO6N0y1+0rmrjKCQUebQFbLkOWt96c4wu2VxzfZzBbAgMBAAGjggEkMIIBIDAJ
BgNVHRMEAjAAMBEGCWCGSbGG+EIBAQQDAwIHgDAwBgNVHR8EKTAnMCWgI6Ahhh9o
dHRwOi8vY3JsLmNlcnR1bS5wbC9jbGFzczEuY3JsMIHNBgNVHSAEgcUwgcIwgb8G
CyqEaAGG9ncCAgEBMIGvMCQGCCsGAQUFBwIBFhhodHRwOi8vd3d3LmNlcnR1bS5w
bC9DUFMwgYYGCCsGAQUFBwICMHowGRYSVW5pemV0byBTcC4geiBvLm8uMAMCAQEa
XUVtYWlsIElEIGZvciBQZXJzb25hXE5vdCBWYWxpZGF0ZWQuIENvcHlyaWdodCAo
YykgMTk5OSBVbml6ZXRvIFNwLiB6IG8uby4gQWxsIHJpZ2h0cyByZXNlcnZlZDAN
BgkqhkiG9w0BAQQFAAOBgQBqK+8c6WWceNW3npz6n8DjFGCX2VSwPnqnxzOpq87L
aJwYjOnYcQmWqL8UdCeh4Ns2HJlvXnPls8R5QMsJB0tO2hm7zxQK4Tp6Z5NldTuS
LgH1N4NYQyShn+PlLkg5BTgrJ6LwVObHKa8MsoWH5b238i227jBUO+6Vfn0w9pOB
iQ==


System bazujący na szyfrze asymetrycznym polega na tym, że jeden klucz, zwany prywatnym, jest kluczem tajnym, znanym tylko jego właścicielowi. Przy pomocy tego klucza można przede wszystkim szyfrować wysyłane wiadomości. Odpowiadający jemu klucz publiczny jest natomiast kluczem powszechnie znanym. Służy on do odszyfrowywania wiadomości zaszyfrowanych kluczem prywatnym. Para kluczy ma jednak jeszcze jedno zastosowanie. Klucz prywatny może służyć również do deszyfrowania wiadomości przychodzących, które zostały uprzednio zaszyfrowane przy użyciu klucza publicznego. Klucz publiczny, jak widać, może więc służyć do szyfrowania wiadomości. Istotą tego systemu jest to, że dokument zaszyfrowany kluczem publicznym może zostać odczytany tylko z użyciem klucza prywatnego. Nikt więc poza właścicielem takiego klucza nie będzie miał możliwości odkodowania przekazu. Gwarantuje to

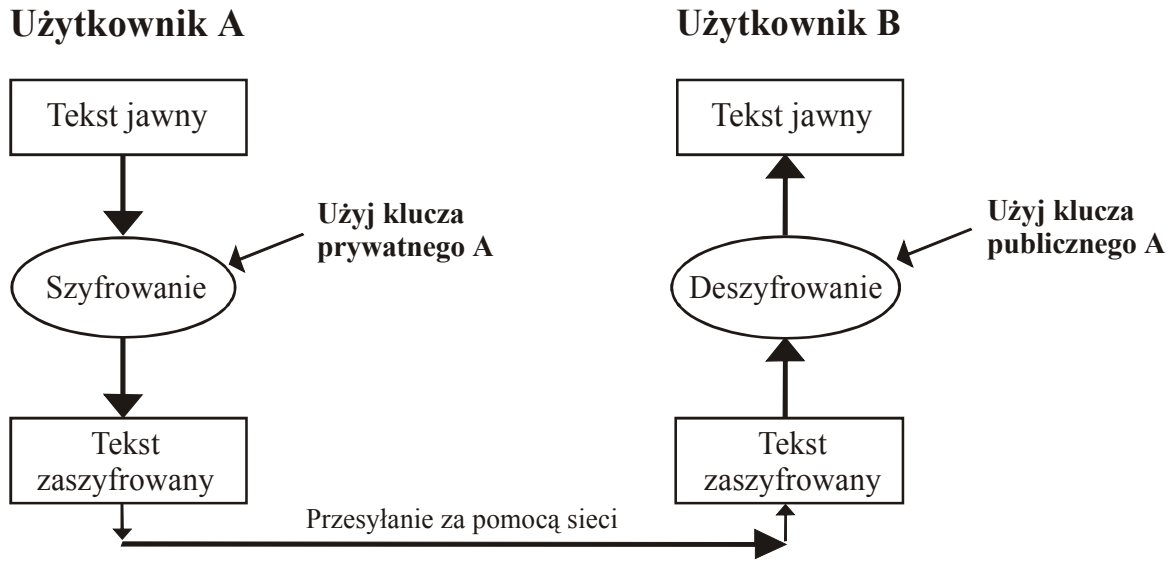
[13] Jako że jest to oryginalny certyfikat autora niniejszej pracy, ze względów bezpieczeństwa niektóre znaki uległy zmianie. O certyfikatach szczegółowo będzie mowa w rozdziale 1.4.

bezpieczeństwo komunikacji prowadzącej w kierunku „świat zewnętrzny" – właściciel klucza prywatnego[14]. Każdy bowiem może użyć do zaszyfrowania wiadomości klucza publicznego tej osoby, do której chce ją wysłać, jako że klucz ten jest powszechnie dostępny. Tylko jedna osoba – posiadacz klucza prywatnego będzie miała możliwość zrozumienia treści przekazu.

Rozpatrzmy to na przykładzie[15]. Załóżmy, że mamy dwie osoby A i B. Osoba A chce wysłać wiadomość do osoby B używając do tego metody szyfrowania z kluczem asymetrycznym. W tym celu A używa swojego klucza prywatnego do zaszyfrowania przekazywanej wiadomości. Ów klucz, jak wspomniano wyżej znany jest tylko jemu. Następnie odbiorca wiadomości, osoba B, deszyfruje wiadomość za pomocą powszechnie dostępnego klucza publicznego nadawcy A. Dzięki temu B ma pewność, że wiadomość rzeczywiście została wysłana przez A, jako że tylko A może się posługiwać swoim kluczem prywatnym. Procedura ta nazywana jest uwierzytelnianiem i przedstawia ją schemat 1. Domyślnie zakładamy, że A nie udostępnił osobie trzeciej swojego klucza jak też, że go nie zgubił i nie wszedł on w posiadanie nieuprawnionej osoby.

Schemat 1

Uwierzytelnianie wiadomości przy użyciu pary asymetrycznych kluczy




*Źródło: V. Ahuja, Bezpieczeństwo w sieciach - Internet, Intranet, Firewall, Warszawa 1997, str. 59.*

Warto zwrócić uwagę na to, że samo uwierzytelnianie nie zapewnia poufności przesyłanych danych. Deszyfracja następuje przecież przy użyciu powszechnie dostępnego klucza publicznego

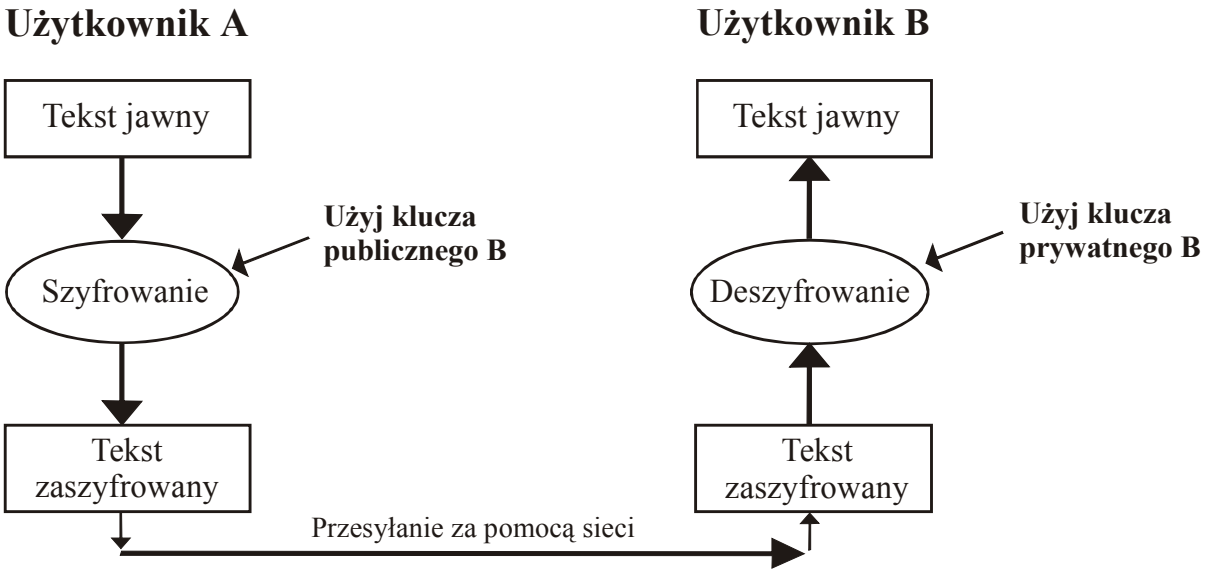
[14] M. Bartosiewicz, *Bity Twojego podpisu*, ENTER, 2001, Nr 5, str. 46.
[15] W przykładzie wykorzystano: Ahuja V., *Bezpieczeństwo w sieciach – Internet, Intranet, Firewall*, Warszawa 1997, str. 59 i n.

nadawcy. Jak wiadomo dostęp do tego klucza może uzyskać każdy, a to oznacza, że każdy może zapoznać się z ich treścią. Posiadacz klucza prywatnego nie może przy jego użyciu oczekiwać, że jego wiadomość nie zostanie odczytana przez niepowołane osoby.

Powstaje pytanie, czy w takim razie można zapewnić bezpieczeństwo takiej komunikacji przebiegającej od osoby A do osoby B. Posiadacz klucza prywatnego, jak już zostało to stwierdzone, nie może użyć własnego klucza prywatnego dla zapewnienia bezpieczeństwa przesyłanych danych. Może on natomiast odszukać klucz publiczny adresata i przy jego użyciu zaszyfrować i wysłać wiadomość, której treść będzie mogła zostać odszyfrowana tylko przy użyciu klucza prywatnego adresata. Tylko on zapozna się z wiadomością. W naszym przykładzie będzie to wyglądało następująco. Nadawca, czyli nadal osoba A, szyfruje przesyłaną wiadomość używając ogólnie dostępnego klucza publicznego odbiorcy B. Następnie przesyła wiadomość za pośrednictwem sieci. Odszyfrować wiadomość może jedynie osoba B będąca posiadaczem klucza prywatnego. Procedura ta nazywana jest utajnianiem. Jej przebieg ilustruje schemat 2.

Schemat 2

Utajnianie wiadomości przy użyciu pary asymetrycznych kluczy



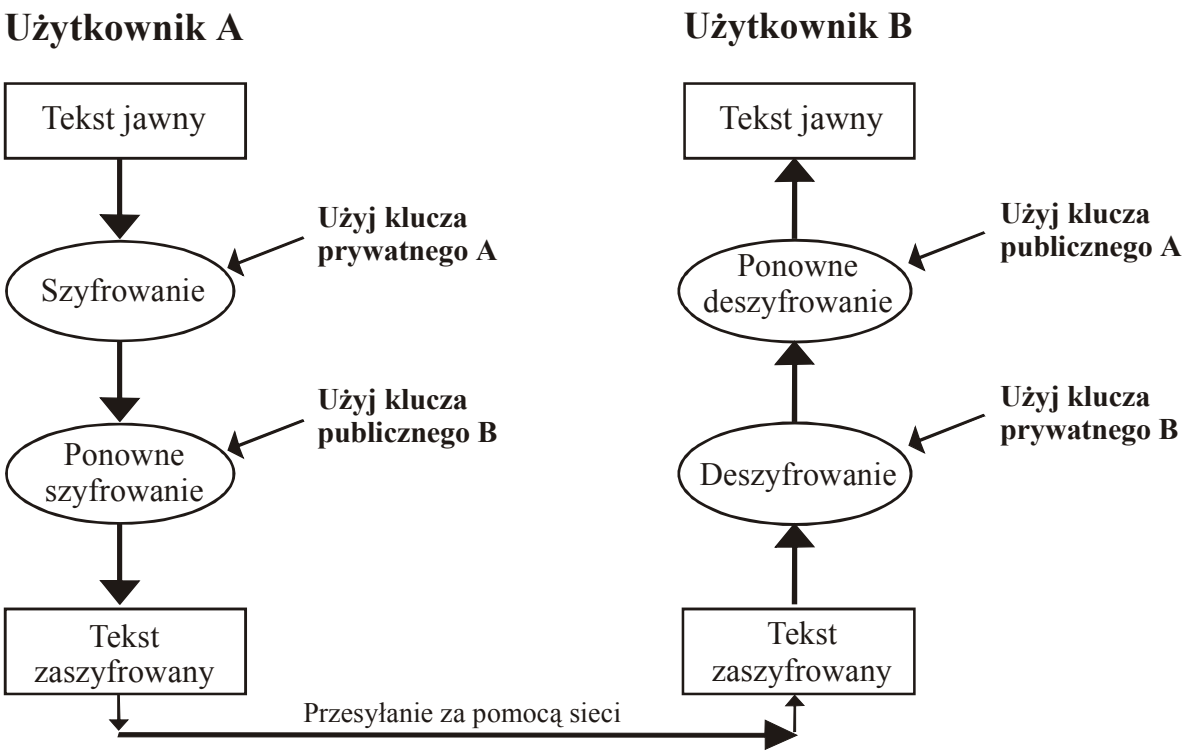

*Źródło: V. Ahuja, Bezpieczeństwo w sieciach - Internet, Intranet, Firewall, Warszawa 1997, str. 59.*

Minusem procedury utajniania jest to, że każdy może użyć ogólnie dostępnego klucza publicznego B, stąd też odbiorca B nie wie, od kogo rzeczywiście pochodzi wiadomość. Zostaje więc zachowana poufność, jednak nie można w ten sposób stwierdzić tożsamości nadawcy.

Połączenie obu tych procedur gwarantuje zarówno poufność danych, jak i pozwala właściwie uwierzytelnić ich nadawcę. W naszym przykładzie najpierw nadawca A szyfruje wiadomość za pomocą swojego klucza prywatnego, potwierdzając tym samym swoją tożsamość (uwierzytelnianie). Następnie osoba A szyfruje już zaszyfrowaną wiadomość przy użyciu klucza publicznego odbiorcy – osoby B, zapewniając w ten sposób poufność – tylko odbiorca B przy pomocy swojego klucza prywatnego będzie mógł odczytać wiadomość (utajnianie). Tak zaszyfrowana wiadomość jest przesyłana elektronicznie do osoby B. Odbiorca deszyfruje wiadomość najpierw przy użyciu swojego klucza prywatnego w celu jej odtajnienia, a następnie używa klucza publicznego nadawcy A by stwierdzić jednoznacznie od kogo pochodzi informacja. Połączenie uwierzytelniania i utajniania prezentuje schemat 3.

Schemat 3

Uwierzytelniane i utajnianie wiadomości przy użyciu pary asymetrycznych kluczy




*Źródło: V. Ahuja, Bezpieczeństwo w sieciach - Internet, Intranet, Firewall, Warszawa 1997, str. 59.*

Można uznać, iż w powyższej metodzie z podpisem elektronicznym będziemy mieli do czynienia w chwili, gdy nadawca zaszyfruje wiadomość wykorzystując w tym celu swój klucz prywatny. Tu warto zaznaczyć, że omawiany mechanizm nie został stworzony na potrzeby e-podpisu, a funkcjonuje już od wielu lat, znajdując zastosowanie w wielu różnych dziedzinach. Cała

powyższa procedura jest jednak dosyć pracochłonna, szczególnie ze względu na to, że algorytm podpisu stosowany jest do całej wiadomości. W przypadku wysyłania serii bardzo długich wiadomości ich szyfrowanie i deszyfrowania może być nie lada problemem obliczeniowym, w szczególności dla słabszych procesorów. Dla istnienia instytucji podpisu elektronicznego nie jest jednak wymagane zapewnienie poufności – wystarczy zapewnienie integralności przesyłanych danych. Innymi słowy, musi istnieć pewność, że podpis złożono pod dokładnie tą samą treścią, którą widzi odbiorca. Dlatego też w praktyce stosuje nieco odmienny tryb postępowania. Nadal jego podstawą jest system z kluczem asymetrycznym, nieco jednak wzbogacony. Tryb ten zostanie opisany w następnym podrozdziale.

## 1.3. Zasady działania podpisu elektronicznego

Dla powstania podpisu elektronicznego konieczne jest uprzednie istnienie odpowiedniej wiadomości. W odróżnieniu od podpisu tradycyjnego nie jest możliwe złożenie e-podpisu *in blanco*, albowiem jego ważnym elementem jest niezmienialność podpisanych danych. Raz podpisana wiadomość, nawet gdyby była pusta, nie może zostać uzupełniona treścią, gdyż wówczas dołączony do niej podpis elektroniczny przestałby do niej pasować. Tak więc pierwszym elementem niezbędnym do stworzenia podpisu jest sama wiadomość (dane elektroniczne). Zakładamy również, że nadawca posiada już własną parę kluczy, a dokładniej klucz prywatny. Wysłanie takiej informacji następuje w kilku etapach[16].

Najpierw nadawca tworzy przy pomocy specjalnego programu skrót wiadomości. Streszczenie to będzie zawsze posiadać stałą długość, która, co najciekawsze, będzie niezależna od długości samej wiadomości. Najczęściej skrót wiadomości będzie liczył 128 lub 160 bitów[17]. W jego tworzeniu używa się technik kryptograficznych w postaci specjalnych algorytmów. Najczęściej jest to tzw. *Secure Hash Algorithm-1* (SHA-1) lub, rzadziej, *Massage Digest 5* (MD5). Efektem ich zastosowania jest cyfrowe streszczenie wiadomości. Wykorzystywana jest tu tzw. jednokierunkowa funkcja skrótu, która tworzy unikalną dla wiadomości sumę kontrolną właśnie w postaci skrótu. Funkcja skrótu posiada trzy, bardzo ważne dla podpisu elektronicznego własności. Po pierwsze, każda, choćby najmniejsza, zmiana oryginalnej wiadomości powoduje nieprzewidywalną zmianę skrótu. Jakakolwiek modyfikacja oryginalnej treści spowoduje zatem

[16] M. Bartosiewicz, *Bity Twojego podpisu*, ENTER, 2001, Nr 5, str. 44 i n.
[17] Bit to najmniejsza możliwa jednostka informacji, która może przyjmować tylko jedną z dwóch wartości: zero lub jeden. 8 bitów tworzy 1 bajt. Tak więc 128 bitów=16 bajtów, a 160 bitów=20 bajtów.

zmianę sumy kontrolnej i będzie łatwa do wykrycia. Po drugie, niemożliwe jest obliczenie (odtworzenie) oryginalnej wiadomości tylko na podstawie samego skrótu. Własność ta nazywana jest jednokierunkowością, stąd też pochodzi nazwa całej funkcji[18]. Po trzecie, żadne dwie różne wiadomości nie mogą w praktyce dać identycznego skrótu. Jest to tzw. bezkolizyjność funkcji skrótu. Tworzenie cyfrowego streszczenia wiadomości ma dwa cele:

a) zapewnienie integralności przesyłanych danych – niemożliwa jest bowiem modyfikacja danych, która nie pociągała by za sobą zmiany skrótu,
b) szybkość procedury – podpis elektroniczny zostanie obliczony już nie dla całej wiadomości, lecz tylko dla jej skrótu.

W następnym etapie nadawca tworzy podpis elektroniczny dla wysyłanej wiadomości. Wykorzystuje on do tego własny, unikalny klucz prywatny. Istnieje przynajmniej kilka technicznych sposobów przechowywania i używania klucza. Może mieć on postać pliku zapisanego w komputerze lub, lepiej, na osobnej dyskietce. Może też być zawarty na specjalnej karcie mikroprocesorowej, która będzie w trakcie podpisywania wiadomości umieszczana w odpowiednim czytniku. W najbardziej rozpowszechnionej postaci klucz po prostu integruje się (zostaje zapamiętany) z programami służącymi do komunikacji sieciowej (np. Outlook Express) i nie ma wówczas każdorazowej potrzeby jego wczytywania. To ostatnie rozwiązanie nie charakteryzuje się jednak najwyższym poziomem bezpieczeństwa i jest godne polecenia dla użytkowników domowych, których ewentualne straty z tytułu użycia przez nieuprawnioną osobę (np. kolegę współużywającego komputera) ich e-podpisu nie będą zbyt wielkie. Przy pomocy klucza prywatnego komputer szyfruje utworzony w poprzednim etapie skrót wiadomości. Tak zaszyfrowany skrót staje się podpisem cyfrowym danej wiadomości. Jak widać, wartość podpisu, czyli jego ostateczny kształt dla danej wiadomości, zależy dwóch czynników:

a) skrótu wiadomości, a dokładniej od samej wiadomości, bowiem to ona była podstawą utworzenia skrótu; dla każdej wiadomości podpis będzie więc różny,
b) klucza prywatnego nadawcy[19].

Kolejnym etapem jest przesłanie przez nadawcę przekazu do odbiorcy drogą elektroniczną. Przesłana zostaje wiadomość wraz z jej zaszyfrowanym skrótem. Najczęściej będzie to plik zawierający właściwą treść wraz z załącznikiem zawierającym podpis elektroniczny dla danej wiadomości. Możliwe jest jednak również osobne przesyłanie obu elementów w postaci odrębnych plików. Nie musi być ono nawet równoczesne – drugi z elementów można dosłać nawet po dłuższym okresie. Jednak do czasu otrzymania obu nie będzie możliwa weryfikacja podpisu.

[18] *Wielka Internetowa Encyklopedia Multimedialna* – http://www.wiem.onet.pl.
[19] J. Stokłosa , *Podpis elektroniczny można porównać do pieczęci*, Rzeczpospolita, 2.03.1998.

Odbiorca wiadomości musi najpierw posłużyć się kluczem publicznym nadawcy. To, gdzie taki klucz będzie mógł adresat znaleźć, zostanie wskazane w następnym podrozdziale. Przy pomocy klucza publicznego nadawcy odbiorca rozszyfrowuje uprzednio zaszyfrowany skrót wiadomości otrzymując jego pierwotną wersję. Dokonuje się tu procedura uwierzytelnienia. Ma ona jednak charakter wstępny i nie jest jeszcze ostateczna, gdyż odbiorca otrzymał dopiero skrót, który jest dla niego niezrozumiałym „bełkotem" o postaci pozornie przypadkowych cyfr i liter. Nie może więc stwierdzić, czy klucze pasują do siebie – podobny (dla człowieka) rezultat otrzymałby bowiem również i wtedy, gdyby użyto innego, niż nadawcy, klucza prywatnego. Dlatego powinien wykonać jeszcze jeden, przedstawiony poniżej, krok.

Adresat otrzymał wiadomość oryginalną w postaci niezaszyfrowanej. W związku z tym oblicza on we własnym zakresie jej skrót, używając do tego tego samego algorytmu, którego użył nadawca. Teraz odbiorca musi porównać oba skróty: ten pierwszy, pochodzący od nadawcy a odszyfrowany w poprzednim etapie przy użycie klucza publicznego i ten drugi, obliczony przez siebie. Jeżeli są identyczne oznacza to, że:

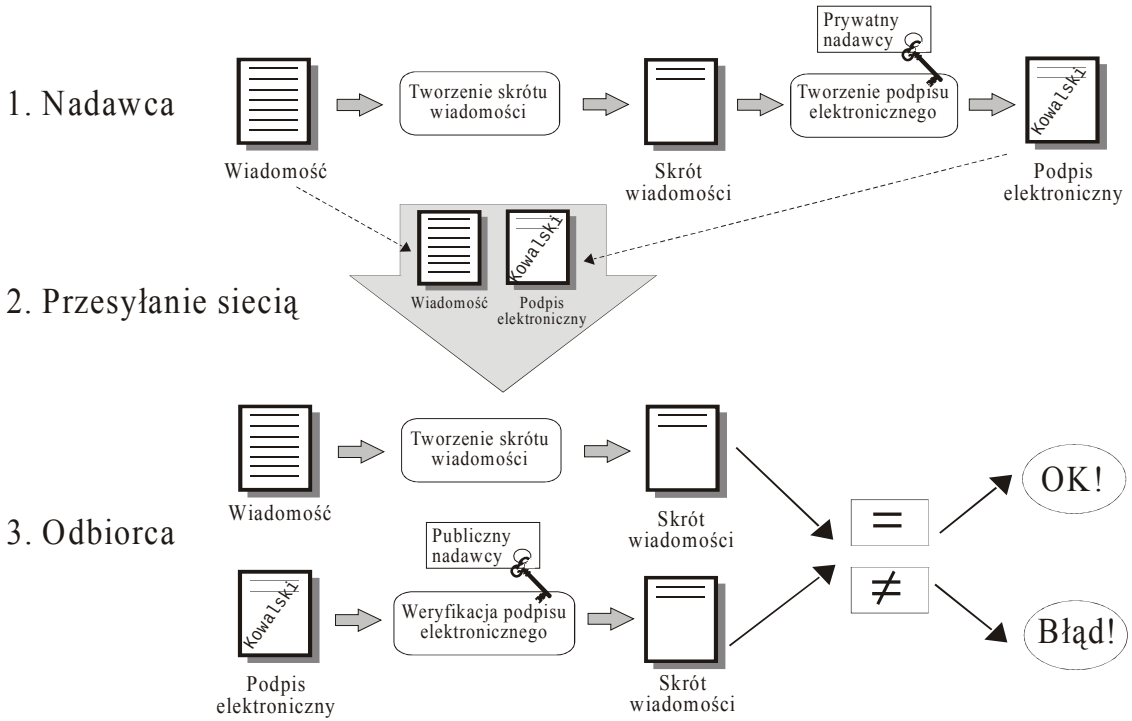
a) wiadomość pochodzi od osoby, która się podpisała elektronicznie pod wiadomością (a ściśle: od osoby, która jest posiadaczem danego klucza prywatnego),
b) wiadomość nie została zmodyfikowana w drodze od nadawcy, gdyż oba skróty (sumy kontrolne) są sobie równe[20].

Podpis, dla którego oba skróty będą równe, uznać można za autentyczny. Natomiast w przypadku ich niezgodności podpis należy odrzucić. W praktyce wszystkie powyższe etapy wykonywane są samoczynnie przez komputer, który przejmuje na siebie szyfrowanie, deszyfrowanie i porównywanie wyników. Rola nadawcy sprowadza się do wydania komputerowi polecenia „podpisz wiadomość' i ewentualnie do wybrania tego podpisu, który chcemy zastosować. Każdy może bowiem mieć więcej niż jeden podpis elektroniczny, które będzie stosował w zależności od tego, co i dla kogo będzie podpisywał, np. inny będzie używany w stosunkach koleżeńskich, a inny w stosunkach służbowych, czy w sytuacjach oficjalnych. Rola odbiorcy sprowadza się do pobrania z sieci klucza publicznego i wydania komputerowi odpowiedniego polecenia w celu weryfikacji autentyczności podpisu i wiadomości. W razie potrzeby komputer jest w stanie automatycznie połączyć się z siecią, odszukać niezbędny klucz i pobrać go. Po przeprowadzeniu niezbędnych obliczeń zostanie wyświetlona informacja o tym, czy dany podpis elektroniczny można uznać za autentyczny, a w ślad za tym, czy można samą wiadomość uznać za niezmienioną. Omówioną powyżej procedurę przedstawia schemat 4.

[20] M. Bartosiewicz, *Bity Twojego podpisu*, ENTER, 2001, Nr 5, str. 44 i n.

Schemat 4

## Tworzenie i zasady działania podpisu elektronicznego

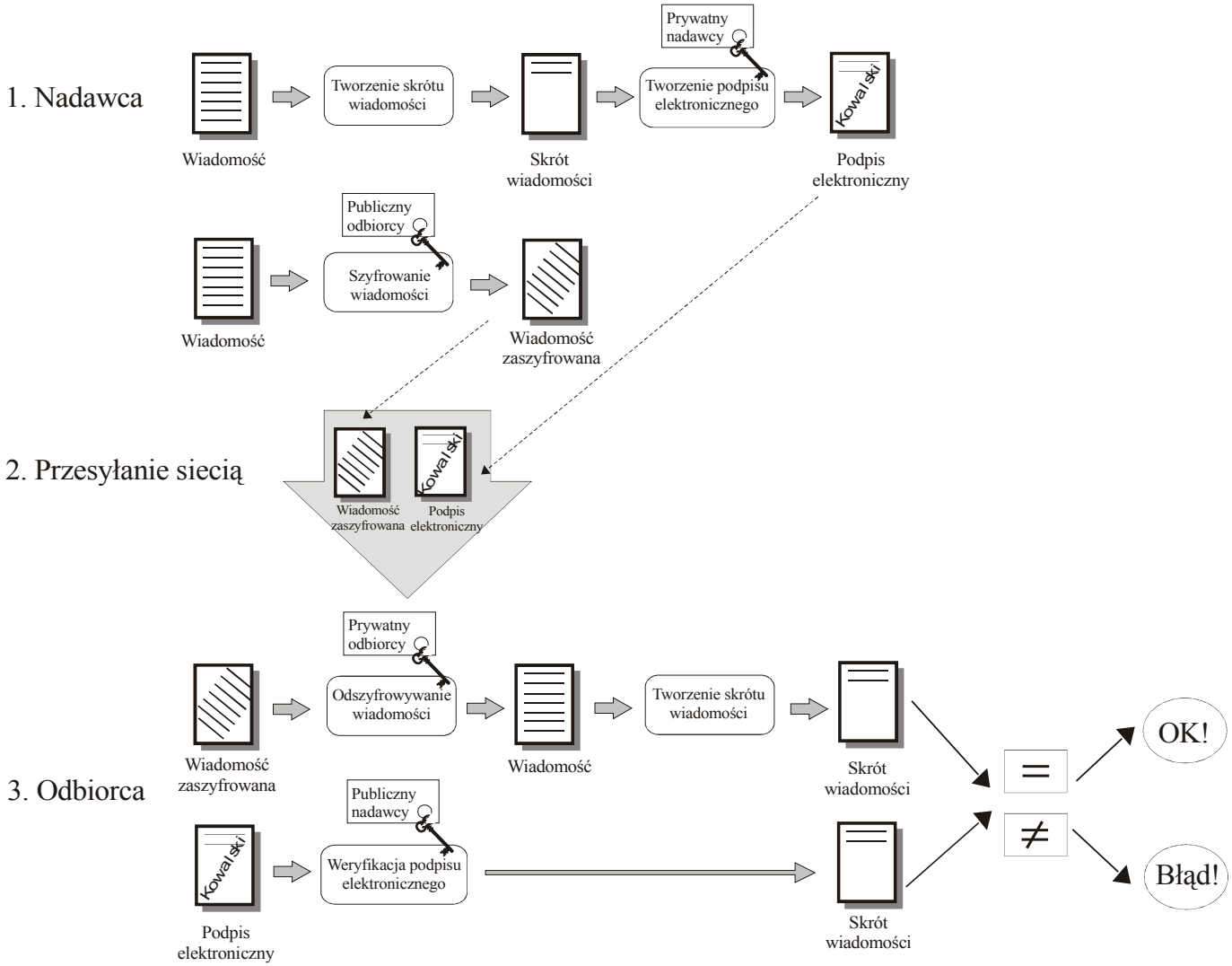



*Źródło: M. Bartosiewicz, Bity Twojego podpisu, „ENTER" 2001, Nr 5, str. 45*

Omówiona właśnie procedura gwarantuje integralność przesyłanych danych. Żadna osoba, która przechwyci taką wiadomość, nie będzie miała możliwości zmienić jej w sposób niezauważony. Jeśli chodzi o podpis elektroniczny *sensu stricto* jest to w zupełności wystarczające i tu można by zakończyć rozważania. Warto sobie jednak uświadomić, iż skoro już zachodzi potrzeba używania specjalnych technik w celu uwierzytelnienia danych, to najprawdopodobniej są to na tyle ważne informacje, iż nadawca (lub odbiorca) nie chciałby, aby trafiły one w niepowołane ręce. Przykładowo, płatnik składek ZUS, który płaci swoje składki w formie elektronicznej czy podatnik wysyłając swoje oświadczenie podatkowe do Urzędu Skarbowego w formie elektronicznej z pewnością wolałby, aby przekazywane przez niego informacje pozostały tajne. Również wiele instytucji komercyjnych potrzebuje rozwiązań gwarantujących nie tylko integralność, ale i poufność przesyłania danych. Szczególną grupą podmiotów są tu banki, dla których bezpieczeństwo ich danych ma kluczowe znaczenie. Przesyłane przez nie informacje na drodze bank-klient (np. informacja o stanie konta klienta), jak i na drodze klient-bank (np. polecenie przelewu) muszą spełniać warunek zachowania tajemnicy bankowej, a więc powinny być przesyłane w takiej formie, aby zapewnić zachowanie ich w tajemnicy. W przypadku powyższej procedury osoba, która przechwyci wiadomość, będzie mogła swobodnie zapoznać się z jej treścią. Istnieje wiele metod zapobieżenia tej niedogodności. Często stosowaną metodą jest szyfrowanie całego przekazu i tworzenie tzw. bezpiecznego połączenia (np. przy użyciu modułu *Secret Socket Layer*). Do tego celu można również wykorzystać opisany w poprzednim podrozdziale mechanizm utajniania.

Po stworzeniu podpisu elektronicznego nadawca wysyła m.in. niezaszyfrowaną wiadomość. Może on jednak zapewnić poufność przekazu używając klucza publicznego odbiorcy. W tym celu przed wysłaniem wiadomości powinien ją zaszyfrować przy użyciu wspomnianego klucza. Przesłaniu ulega wówczas podpis elektroniczny i zaszyfrowana wiadomość. Tylko odbiorca, jako jedyny posiadacz klucza prywatnego będzie mógł ją odczytać. Będzie on zmuszony najpierw użyć swojego klucza aby uzyskać oryginał wiadomości poprzez jej odszyfrowanie. Dalej powinien on postępować zgodnie z opisanymi wcześniej wskazówkami. Na schemacie 5 pokazano algorytm postępowania w przypadku tworzenia i weryfikacji podpisu elektronicznego z użyciem procedury utajniania.

## Utajnianie w procesie podpisu elektronicznego




*Źródło: opracowanie własne na podst. M. Bartosiewicz, Bity Twojego podpisu, „ENTER" 2001, Nr 5, str. 45*

## 1.4. Certyfikaty i rola centrów certyfikacji

Do uwierzytelnienia nadawcy i wysłanej przez niego wiadomości potrzebny jest jego klucz publiczny. Powstaje pytanie, gdzie należy takiego klucza szukać i skąd pewność, że dany klucz rzeczywiście przynależy do konkretnej osoby. Wiemy bowiem, że w przeciwieństwie do podpisu odręcznego podpis cyfrowy nie ma bezpośredniego związku z osobą nadawcy. Jest on jedynie ciągiem bitów. Zatem, kiedy już przy pomocy klucza publicznego stwierdzimy, że wiadomość została podpisana przy pomocy klucza prywatnego osoby X, nadal nie wiemy, czy ktoś nie podszył się pod osobę X uzyskując prawo do danego klucza prywatnego. Innymi słowy, musimy stwierdzić, czy rzeczywiście podpis elektroniczny należy do osoby X, a nie do kogoś, kto się za nią podaje. Temu służą certyfikaty i system certyfikacji.

W systemie certyfikacji najważniejszym ogniwem jest Organ Certyfikacji (ang. *Certification Authority*, CA), który pełni rolę tzw. zaufanej osoby trzeciej (ang. Trusted Third Party, TTP)[21]. Zadaniem tego organu jest potwierdzenie tożsamości osoby ubiegającej się o wydanie jej certyfikatu (tzw. subskrybenta) oraz potwierdzenie faktu, iż będący w jej posiadaniu klucz publiczny rzeczywiście do niej należy. Dzięki temu odbiorca wiadomości po otrzymaniu podpisanej wiadomości jest w stanie zidentyfikować właściciela certyfikatu, który podpis ten złożył[22]. Organ Certyfikacji tworzy stosowne bazy użytkowników. Aby uzyskać certyfikat użytkownik musi podać swoje dane, które następnie podlegają weryfikacji przez organ. Wydanie certyfikatu następuje dopiero po należytym sprawdzeniu informacji przedstawionych przez subskrybenta – po jego dostatecznej identyfikacji. Dokonywać tego może sam Organ Certyfikacji, często jednak zajmuje się tym wyspecjalizowana komórka – Organ Rejestracji (ang. *Registration Authority*, RA), dokonujący weryfikacji danych użytkownika, a następnie jego rejestracji. Po zarejestrowaniu użytkownika przez Organ Rejestracji następuje wydanie certyfikatu subskrybentowi. Możliwe są dwie sytuacje:

a) Organ Certyfikacji sam generuje parę kluczy, przekazując następnie klucz prywatny subskrybentowi wraz z wystawionym certyfikatem; przekazanie może odbywać się za pomocą przesyłki pocztowej, specjalnej przesyłki kurierskiej lub też przy użyciu sieci informatycznej, np. Internetu,
b) użytkownik we własnym zakresie generuje klucz prywatny i klucz publiczny za pomocą specjalnego oprogramowania, po czym przedstawia organowi

[21] Signet – http://www.signet.pl/bezpieczenstwo/pki/pki.html.
[22] Certum – http://www.certum.pl/pl/dokumentacja/pc/index.html.

wygenerowany klucz publiczny do certyfikacji; organ po identyfikacji użytkownika, wystawia mu certyfikat; jego przesłanie odbywa się tak, jak wyżej.

To drugie rozwiązanie charakteryzuje się większym poziomem bezpieczeństwa, gdyż od samego początku tylko użytkownik ma dostęp do własnego klucza prywatnego, nie następuje też w żadnym momencie jego przesyłanie. Certyfikat (w standardzie X.509) zawiera przede wszystkim następujące elementy[23]:

a) numer wersji – określa wersję formatu certyfikatu,
b) numer seryjny – numer ten jest przydzielany użytkownikowi, a dokładnie jego certyfikatowi, przez Organ Certyfikacji; numer ten jest niepowtarzalny – tylko jeden certyfikat wydany przez dany organ posiada taki numer,
c) identyfikator algorytmu – określa algorytm użyty do podpisania certyfikatu i związane z nim parametry,
d) wystawca – zawiera nazwę Organu Certyfikacji, który wydał certyfikat,
e) okres ważności certyfikatu – wyznaczany jest przez dwie daty; certyfikat nie jest ważny przed nastaniem pierwszej daty i po upływie drugiej,
f) osoba (użytkownik, temat) – określa osobę, której wydano certyfikat,
g) klucz publiczny – zawiera klucz publiczny użytkownika oraz określa algorytm wykorzystywany przez ten klucz,
h) podpis Organu Certyfikacji – powstaje on za pomocą klucza prywatnego Organu Certyfikacji; jego zadaniem jest uwierzytelnienie pochodzenia danego certyfikatu.

Certyfikat, najogólniej rzecz biorąc, to nic innego, jak „elektronicznie podpisany klucz”[24]. Jest to bowiem klucz publiczny subskrybenta wraz z dołączonym do niego podpisem wystawcy certyfikatu. Certyfikat jest więc, w pewnym uproszczeniu, zaszyfrowanym, przy użyciu klucza prywatnego Organu Certyfikacji, kluczem publicznym subskrybenta. Dlatego też odbiorca wiadomości podpisanej elektronicznie powinien, oprócz sprawdzenia poprawności wiadomości pochodzącej od adresata, również sprawdzić, czy certyfikat klucza publicznego nadawcy jest poprawny. Będzie mógł to uczynić za pomocą klucza publicznego Organu Certyfikacji, którym sprawdzi wiarygodność klucza prywatnego tego organu, widniejącego pod certyfikatem. Taki certyfikat może zostać przesłany odbiorcy przez samego nadawcę, wraz z wiadomością i podpisem elektronicznym. Jeżeli nadawca tego nie uczyni, wówczas adresat będzie musiał skorzystać z usług tak zwanego repozytorium. Są to dostępne w trybie on-line bazy danych zawierające certyfikaty Organu Certyfikacji, Organu Rejestracji i, co najważniejsze, wszystkich subskrybentów Organu

[23] V. Ahuja, *Bezpieczeństwo w sieciach – Internet, Intranet, Firewall*, Warszawa 1997, str. 63 in.
[24] M. Bartosiewicz, *Bity Twojego podpisu*, ENTER, 2001, Nr 5, str. 44 i n.

oraz związane z nimi inne informacje, m.in. listy certyfikatów unieważnionych (także innych subskrybentów), politykę certyfikacji, listy punktów rejestracji[25].

Przyznawane użytkownikom certyfikaty mogą być zróżnicowane, w zależności od poziomu bezpieczeństwa, jaki oferują. Wiąże się to ściśle ze sposobem, w jaki Organy Certyfikacji dokonują identyfikacji przyszłego subskrybenta. Najmniej bezpieczne, ale i najtańsze, często wręcz bezpłatne, certyfikaty przeznaczone są dla podpisywania prywatnej poczty e-mail. Ten typ danych nie wymaga wysokiego stopnia zaufania do jego nadawcy. Odbiorcy z reguły wystarczy pewność, że z danego adresu e-mail przysłała mu wiadomość ta osoba, która używała go do tej pory. Tę pewność daje mu sposób, w jaki identyfikowany jest subskrybent. Przyszły subskrybent podaje Organowi Certyfikacji, oprócz swoich danych, adres e-mail, dla którego, chce stworzyć podpis cyfrowy. Organ Certyfikacji w zasadzie nie sprawdza danych podanych przez użytkownika. Wyjątkiem jest tu sam adres e-mail, na który Organ wysyła elektroniczną wiadomość podając w niej określone hasło, potrzebne do procesu wydania certyfikatu. Jeżeli użytkownik rzeczywiście podał konto pocztowe, do którego ma prawo, nie powinien mieć problemu z poznaniem hasła i jego użyciem. Warto zwrócić uwagę, że identyfikacja osoby odbywa się pośrednio, za pomocą jej adresu e-mail. Podpis elektroniczny jest w praktyce wydawany dla danego konta pocztowego, ten sam użytkownik nie może się podpisać tym samym e-podpisem wysyłając wiadomość przy użyciu innego, choćby własnego, konta pocztowego. Istnieją również takie certyfikaty, dla otrzymania których niezbędne jest osobiste stawienie się w Organie Certyfikacji wraz z kompletem dokumentów. Certyfikat zostaje wystawiony dopiero po pozytywnej weryfikacji tych danych przez Organ Certyfikacji.

System certyfikacji składa się na tak zwaną Infrastrukturę Klucza Publicznego (IKP). W jej skład wchodzą: Organy Rejestracji, Organy Certyfikacji i Repozytoria. Zależnie od przyjętego systemu prawnego może istnieć jeden Centralny Organ Certyfikacji zależny od państwa, może istnieć również mnogość takich Organów, działających na zasadach komercyjnych. Zaufanie obywateli do Organów Certyfikacji decyduje o powodzeniu instytucji podpisu elektronicznego. Dlatego też zapewnienie szybkiego rozwoju bezpiecznej i funkcjonalnej Infrastruktury Klucza Publicznego jest ważnym zadaniem, wymagającym odpowiedniej regulacji prawnej.

[25] Kodeks Postępowania Certyfikacyjnego firmy Certum – http://www.certum.pl/.

## 1.5. Bezpieczeństwo podpisu elektronicznego

Głównym wymogiem stawianym instytucji podpisu elektronicznego jest jej bezpieczeństwo. Ma ono dwa aspekty. Po pierwsze, ważne jest stosowanie takich metod kryptograficznych, które na podstawie podpisu zapewnią przede wszystkim pewną identyfikację osoby podpisującej i integralność przesyłanej wiadomości, a także praktyczną niemożliwość jego złamania. Chodzi tu więc o bezpieczeństwo podpisu rozumianego jako zbiór technik i kluczy kryptograficznych. Po drugie, istotne jest to, aby system certyfikacji charakteryzował się wysokim poziomem zaufania jego uczestników. Musi być on tak skonstruowany, aby funkcjonowanie nieuczciwych wystawców nie było w ogóle możliwe, bądź przynajmniej jak najkrótsze. Nie może bowiem dochodzić do wystawiania fałszywych certyfikatów lub nieprawdziwego znakowania czasem.

Każdemu podpisowi, nie tylko elektronicznemu, stawia się określone wymogi. Muszą one być spełnione, aby można było powiedzieć, że dany rodzaj podpisu jest bezpieczny. Powstaje pytanie, co należy rozumieć przez „bezpieczeństwo". Innymi słowy, jakie są to wymogi, które powinien spełniać podpis, aby mógł on sprawnie funkcjonować w obrocie handlowym. W odpowiedzi na to pytanie należałoby podać następujące cechy[26]:

a) podpis powinien być niepodrabialny – oznacza, to, że nie istnieje możliwość niezauważalnego złożenia podpisu osoby podpisywanej przez inną osobę niż podpisujący,
b) podpis powinien być autentyczny – nie powinno być możliwości użycia własnego podpisu jako cudzego,
c) podpis nie powinien nadawać się do ponownego użycia – jako część dokumentu nie może być przeniesiony na inny dokument,
d) podpisany dokument powinien być niezmienialny – po podpisaniu dokument nie może zostać zmieniony,
e) nie można wyprzeć się podpisu – podpis i dokument istnieją realnie. Osoba podpisująca nie może później oświadczyć, że go nie podpisała.

Można zauważyć, że nawet w stosunku do podpisu odręcznego żaden z powyższych warunków nie jest spełniony całkowicie. Podpis własnoręczny można przecież sfałszować, a wykrycie takiego faktu nie jest łatwe i wymaga często specjalistycznej wiedzy. Przy użyciu sprzętu poligraficznego, czy choćby zwykłego ksero, można podpis przenosić z jednego kawałka papieru na inny. Nie stanowi żadnego problemu zmiana treści dokumentu już po jego podpisaniu. Pomimo

[26] B. Schneider, *Kryptografia dla praktyków*, Warszawa 1995, str. 53.

tych mankamentów podpis tradycyjny jest powszechnie używany, a to ze względu na trudności w oszukiwaniu i ryzyko wykrycia. Wyjaśnić zatem należy, czy podpis elektroniczny spełnia powyższe warunki i, jeżeli tak, co powoduje, że można go uważać za bezpieczną metodę podpisywania się.

Funkcjonowanie podpisu elektronicznego opiera się na parze asymetrycznych kluczy, z których jeden, zwany prywatnym, znany jest tylko podpisującemu się, a drugi, zwany publicznym, jest powszechnie dostępny. Nadawca wysyła wiadomość podpisując go swoim kluczem prywatnym. Po pierwsze więc, podpis jest niepodrabialny, gdyż tylko sam nadawca zna swój klucz prywatny. Po drugie, podpis jest też autentyczny, gdyż tylko nadawca, i nikt inny, może go użyć. Odbiorca weryfikując wiadomość za pomocą klucza publicznego nadawcy wie, że to on ją podpisał. Po trzecie, w systemie podpisu cyfrowego dany podpis nie może być ponownie użyty, a to dlatego, że jego wartość zależy każdorazowo od podpisywanej wiadomości. Dla dwóch różnych przekazywanych informacji podpis będzie miał zawsze inną postać, albowiem podpis funkcjonuje tylko razem z konkretnym dokumentem. Przeniesienie go do innego dokumentu jest bardzo łatwe do wykrycia. Po czwarte, dokument podpisany elektronicznie jest niezmienialny – dowolna jego modyfikacja spowoduje błąd przy weryfikacji autentyczności za pomocą klucza jawnego. Wreszcie po piąte, nie można wyprzeć się podpisu. Dany klucz prywatny przynależy do określonej osoby. Podpis cyfrowy, choć jest w postaci elektronicznej, jest matematycznie trwale związany z wiadomością i dopóki ona istnieje, dopóty będzie można stwierdzić, przy użyciu jakiego klucza prywatnego została podpisana. Można więc uznać podpis elektroniczny za bezpieczny, jako że spełnia postawione na początku wymogi. Mając to na uwadze nie można jednocześnie zapominać, iż w rzeczywistości mogą, i na pewno będą zdarzać się różnego rodzaju oszustwa czy, przykładowo, kradzieże kart chipowych zawierających klucze prywatne. Tym niemniej, łatwość zablokowania skradzionego klucza i uzyskania nowego, przy względnie dużej trudności w oszukiwaniu, decyduje o uznaniu e-podpisu za bezpieczny. Bardzo duże znaczenie ma tu sposób funkcjonowania systemu certyfikacji, o czym później.

Należy się tu wyjaśnienie, jak to się dzieje, że system oparty na szyfrowaniu asymetrycznym charakteryzuje się tak wysokim poziomem bezpieczeństwa. Podstawowym pojęciem jest tu klucz prywatny, który powinien być niepowtarzalny. Chodzi o to, aby każdy użytkownik podpisu posiadał własny, unikalny ciąg bitów, który będzie jednocześnie jedyny na całym świecie. Przy czym chodzi nie o rzeczywistą niepowtarzalność, gdyż jej zapewnienie jest praktycznie niemożliwe, ale o to, aby prawdopodobieństwo wystąpienia dwóch identycznych kluczy było bliskie zeru. Jest to możliwie dzięki postaci klucza, który jest niewyobrażalnie dużą liczbą. Najczęściej obecnie stosowane klucze prywatne mają długość 1024 bitów. Przekładając zapis w systemie dwójkowym na system dziesiętny otrzymujemy $2^{1024}$ możliwych kombinacji –

taka liczba zawiera 308 cyfr. Dla porównania liczba mieszkańców Ziemi znajduje się w przedziale pomiędzy $2^{32}$ a $2^{33}$ ludzi (około 6 miliardów).

Bezpieczeństwo podpisu elektronicznego polega na oparciu go na szyfrowaniu systemem z kluczem asymetrycznym. Jego podstawy opracowali dwaj amerykańscy matematycy-informatycy – Whitfield Diffie i Martin Hellman[27]. Miało to miejsce w 1976 roku. Istota tego systemu polega na złożoności obliczeniowej określonych problemów matematycznych. Trudność polega tu na obliczeniu jednego klucza (prywatnego) znając jedynie klucz jawny. Trudność ta nie znika nawet wtedy, gdy posiada się wiadomość zaszyfrowaną kluczem prywatnym i jej niezaszyfrowany oryginał. Żadnej trudności nie sprawia natomiast obliczenie klucza jawnego mając do dyspozycji klucz prywatny (tajny). Można spotkać problemy obliczeniowe różnego rodzaju. Najczęściej wykorzystywane na potrzeby podpisu elektronicznego są dwa algorytmy: DSA i RSA.

Najprostszym przykładem funkcji o powyższej charakterystyce jest mnożenie liczb całkowitych. Każdy, nawet najsłabszy, komputer jest w stanie wykonać taką operację bardzo szybko. Powiedzmy, że mnożymy dwie liczby $p$ i $q$. Wystarczy wprowadzić je do komputera, rozdzielić znakiem „*" i nacisnąć klawisz ENTER. Operacja odwrotna do mnożenia jest trudna do wykonania nawet przez najlepsze komputery, oczywiście przy założeniu stosowania odpowiednio dużych liczb[28].

Funkcjonowanie algorytmu DSA (ang. *Digital Signature Algorithm*), który może być stosowany tylko do podpisów cyfrowych, dobrze opisali I. Sitnicki oraz M. Srebrny[29]. Według nich, jego istotą jest „obliczanie reszty z dzielenia liczby postaci $g^x$ przez pewną liczbę $p$, przy czym $g$ i $p$ są starannie dobranymi liczbami pomocniczymi. Zapisuje się to jako $y = g^x \bmod p$. Obliczenie potęgi i reszty z dzielenia jest prostym zadaniem arytmetycznym. Funkcja odwrotna, czyli obliczanie $x$, mając dane $y$ oraz pomocnicze $g$ i $p$, nazywa się logarytmem dyskretnym. Jest to funkcja określona na liczbach całkowitych i o wartościach całkowitych, dla której nie jest znany algorytm obliczający ją w czasie możliwym do realizacji w praktyce. Dla odpowiednio dobranych $g$, $p$ i $y$ nie jest możliwe w praktyce wskazanie $x$ takiego, że $y = g^x \bmod p$. Nic nie pomaga informacja, iż takie $x$ istnieje.". Liczba $y$ jest tu kluczem publicznym – obliczenie na jej podstawie wartości klucza prywatnego, czyli $x$, nie jest możliwe w rozsądnym czasie.

Najpopularniejszym algorytmem z kluczem jawnym jest RSA. Nazwa wzięła się od pierwszych liter nazwisk autorów tego algorytmu – Rivest, Shamir, Adleman. Może on być

[27] V. Ahuja, *Bezpieczeństwo w sieciach – Internet, Intranet, Firewall*, Warszawa 1997, str. 57.
[28] I. Sitnicki, M. Srebrny, *Nie taki diabeł straszny, jak go malują*, „Rzeczpospolita" 8.02.2001.
[29] ibidem.

stosowany zarówno do szyfrowania jak i do podpisów cyfrowych[30]. Opiera się on na problemie faktoryzacji (ang. *factorization*), czyli rozkładu na czynniki pierwsze dużej liczby $n$, o której wiadomo, że jest iloczynem dwóch dużych liczb pierwszych $p$ i $q$[31]. Nie jest znany algorytm, który dla określonej liczby całkowitej umożliwiałby dokonanie jej rozkładu na czynniki pierwsze w możliwym do zaakceptowania czasie. Obecnie systematycznie dokonuje się faktoryzacji liczb o około 140-150 cyfrach. Przykładowo, klucz o długości 512 bitów to 155 cyfr. Rozkład liczby o długości 664 bitów na czynniki pierwsze wymaga $10^{23}$ kroków. Gdyby przyjąć, że komputer wykonuje milion operacji w ciągu jednej sekundy oraz że zadanie to wykonuje sieć złożona z miliona takich komputerów, faktoryzacja zajęłaby prawie 4000 lat. Jeżeli liczba ta miałaby długość 1024 bity, ta sama sieć komputerów potrzebowałaby $10^{10}$ lat na dokonanie faktoryzacji tej liczby[32]. Komputery stają się jednak coraz szybsze. W sierpniu 1996 roku poinformowano o złamaniu RSA z kluczem wielkości 155 cyfr dziesiętnych (512 bitów)[33]. Tym niemniej, klucze 1024-bitowe powszechnie uważa się za bezpieczne w perspektywie przynajmniej najbliższych kilku lat.

Należy poczynić dwie uwagi. Po pierwsze, trzeba stwierdzić, iż jedynie podejrzewa się, że bezpieczeństwo zapewnianie przez RSA zależy od problemu faktoryzacji dużych liczb. Nigdy nie zostało bowiem udowodnione matematycznie, że należy rozłożyć dużą liczbę $n$ na czynniki pierwsze, aby obliczyć klucz prywatny i pierwotną wiadomość. Możliwe jest, że zostanie odkryty jakiś inny, o wiele prostszy niż faktoryzacja, sposób obliczenia odpowiednich liczb. Jednak jeżeli pozwalałby on na wydedukowanie klucza prywatnego, to mógłby on być także wykorzystywany jako nowy sposób faktoryzacji dużych liczb[34]. Po drugie, to że w tej chwili nie jest znany żaden szybki algorytm (zarówno dla RSA, jak i DSA) nie oznacza, że nie będzie on znany w przyszłości. To wymaga ciągłego doskonalenia stosowanych technik i używania kluczy o coraz większej liczbie cyfr. Obecnie za bezpieczne uważa się klucze prywatne wielkości 160 bitów i klucze publiczne wielkości 1024 bity[35].

Drugi aspekt bezpieczeństwa podpisu elektronicznego, o którym wspomniano na początku, ma charakter instytucjonalny. Przyjęte rozwiązania prawne dotyczące podmiotów świadczących usługi certyfikacyjne powinny tworzyć warunki do powstania godnego zaufania systemu certyfikacji. Jego nieprawidłowe funkcjonowanie może wywołać poważne komplikacje o charakterze prawnym. Ramy prawne powinny dotyczyć zarówno uregulowania cywilnoprawnych

[30] B. Schneider, *Kryptografia dla praktyków*, Warszawa 1995, str. 31.
[31] M. Bartosiewicz, *Bity Twojego podpisu*, „ENTER" 2001, Nr 5, str. 44 i n.
[32] Przykład i wyliczenia za B. Schneider, *Kryptografia dla praktyków*, Warszawa 1995, str. 341 i n.; warto jednak zauważyć, iż moc obliczeniowa komputerów od czasu wydania tej pozycji (1995) znacząco wzrosła.
[33] Informacja za I. Sitnicki, M. Srebrny, *Nie taki diabeł straszny, jak go malują*, Rzeczpospolita, 8.02.2001.
[34] B. Schneider, *Kryptografia dla praktyków*, Warszawa 1995, str. 34.
[35] I. Sitnicki, M. Srebrny, *Nie taki diabeł straszny, jak go malują*, Rzeczpospolita, 8.02.2001.

skutków podpisu elektronicznego, administracyjnych ram działania wystawców certyfikatów, jak też i przestępstw związanych z podpisem elektronicznym. Tym kwestiom zostanie poświęcony cały rozdział drugi.

Na tym tle warto wspomnieć o znakowaniu czasem. Jest to jedna z usług świadczonej przez wystawców certyfikatów. W swojej najprostszej wersji polega ona na przesłaniu do odpowiedniego podmiotu świadczącego usługi certyfikacyjne dokumentu (a dokładnie jego skrótu) z poleceniem zaopatrzenia go w tzw. znacznik czasu. Zawiera on datę i czas przedstawienia dokumentu do znaczenia z dokładnością co do sekundy. Znacznik taki staje się częścią dokumentu, który następnie zostaje podpisany. Celem tej usługi jest wyeliminowanie sytuacji, w której ktoś próbuje czynić wielokrotny użytek z raz podpisanej wiadomości w taki sposób, jakby za każdym razem była to inna, nowa wiadomość. Przykładem może być tu wielokrotne przedstawianie do realizacji w banku tego samego elektronicznie podpisanego czeku w tygodniowych odstępach. Usługa ta ma duże znaczenie dla pewności obrotu.

## 1.6. Ekonomiczne koszty funkcjonowania podpisu dla banków i jego klientów

Instytucja podpisu elektronicznego znajduje szerokie zastosowanie w bankowości. Myślę, że nie jest przypadkiem fakt, iż rządowy projekt ustawy o podpisie elektronicznym powstawał w znacznej mierze w Narodowym Banku Polskim, a pracami kierowała Grażyna Rzymkowska z tegoż właśnie banku[36]. To bowiem banki będą jednymi z głównych beneficjentów wprowadzenia podpisu elektronicznego do polskiego systemu prawnego. Zresztą w polskim systemie certyfikacji w stosunku do banków szczególna rola przypadnie Narodowemu Bankowi Polskiemu. Funkcjonowanie instytucji podpisu elektronicznego będzie jednak pociągało za sobą określone koszty. Jak już wyjaśniono, sprawne i bezpieczne podpisy elektroniczne będą wymagały istnienia odpowiedniej Infrastruktury Klucza Publicznego. Nakłady potrzebne do jej zbudowania i przede wszystkim funkcjonowania są niemałe. Oznacza to, iż otrzymywanie certyfikatów nie jest i, najprawdopodobniej, nie będzie bezpłatne. Koszty poniosą zarówno banki, jak też i ich klienci.

Banki będą zmuszone ponosić koszty, które można ująć w dwóch grupach. Po pierwsze będą to te koszty, które można określić mianem zewnętrznych. Złożą się na nie wydatki związane przede wszystkim z kosztem wystawienia certyfikatów dla banku, a dokładniej dla personelu, który będzie się nimi posługiwał w imieniu banku. W obecnym stanie prawnym nie wydaje się bowiem

[36] Wstępny rządowy projekt ustawy o podpisie elektronicznym z dnia 29.11.1999.

możliwe, aby osoba prawna (czy jednostka organizacyjna nie posiadająca osobowości prawnej) mogła posługiwać się samodzielnie[37], w pełni skutecznie podpisem elektronicznym. Świadczy o tym brzmienie art. 4 pkt. 3 Ustawy o podpisie elektronicznym, który określa „osobę składająca podpis elektroniczny" jako osobę fizyczną, która, ewentualnie, może podpisać się „w imieniu innej osoby (..) prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej". Jest jednak możliwe to, iż certyfikat będzie wystawiony na osobę prawną, a posługiwać się nim będzie osoba fizyczna, działająca w charakterze organu osoby prawnej[38]. W związku z powyższym bank będzie potrzebował wielu certyfikatów, którymi będzie uwierzytelniał siebie wobec własnych klientów w trakcie przeprowadzania transakcji drogą elektroniczną. Zresztą podpis cyfrowy będzie stosowany nie tylko w relacjach bank-klient, ale również bank A – bank B, gdzie będzie dochodziło do wymiany między bankami informacji różnego typu, np. dokumentów, baz danych, propozycji zawarcia określonej umowy, itp. Koszt uzyskania takich certyfikatów to nie jedyny koszt w tej grupie. Ze względów bezpieczeństwa certyfikaty wydawane są zawsze tylko na czas określony, z reguły nie przekraczający dwóch lat.. Po tym czasie certyfikat wygasa. Istnieje jednak możliwość jego odnowienia przed upływem terminu jego ważności. Generowana jest wówczas nowa para kluczy, ale poza tym certyfikat pozostaje, w pewnym sensie, ten sam. Odnowienie certyfikatu związane jest jednak z opłatą. Kwota, którą trzeba zapłacić za certyfikat, bądź z jego odnowienie, zależna jest od poziomu bezpieczeństwa przezeń gwarantowanego. Tabela 1 zawiera stawki za poszczególne certyfikaty, stosowane przez firmę Unizeto sp. z o.o., prowadzącą Organ Certyfikacji - „Certum".

Tabela 1

Cennik uzyskania i odnowienia poszczególnych certyfikatów w „Certum"

| CERTYFIKAT | CENA (z VAT) |
|---|---|
| Certum Silver | 61 zł |
| Certum Silver – odnowienie | 30 zł |
| Certum Gold | 610 zł |
| Certum Gold – odnowienie | 305 zł |

*Źródło: http://www.certum.pl/pl/produkty/podpis/index.html.*

[37] W szczególności ze względu na wątpliwości, które nasuwają się w związku z art. 38 Kodeksu cywilnego.
[38] Nieco odmiennie P. Szyndzielorz „*Elektroniczna forma czynności prawnych*", „VaGla – Prawo i Internet", http://www.vagla.pl/, str. 87 i n.

W tabeli nie zawarto jeszcze jednego rodzaju certyfikatu. Jest on wydawany jedynie na podstawie samego adresu e-mail, charakteryzuje się on najmniejszym poziomem bezpieczeństwa i jest bezpłatny (stąd też jego brak w cenniku). Warto zaznaczyć, iż w powyższe ceny wliczono już koszt nośnika w postaci odpowiednich kart mikroprocesorowych, na których będą przechowywane klucze prywatne przynależące np. do banku. Jak widać, koszty zewnętrzne nie powinny się okazać zbyt uciążliwe dla banków. Nawet przy wykorzystaniu przez bank wielu najbezpieczniejszych certyfikatów Gold łączny wydatek, w skali bilansu choćby przeciętnego banku, będzie nieznaczny.

Drugą grupą kosztów są koszty wewnętrzne. Znajdą się w tej grupie wszystkie te wydatki, które są związane z wprowadzeniem w samym banku odpowiednich rozwiązań technologicznych, sprzętowych, proceduralnych i organizacyjnych. Oznacza to konieczność zainstalowania odpowiedniego oprogramowania, przeszkolenia personelu, stworzenia odpowiednich warunków technicznych (szybkie łącza z Internetem, szybkie komputery), lokalowych (np. pomieszczenie lub inne miejsce do przechowywania kart mikroprocesorowych, zawierających klucze prywatne), stworzenia procedur dostępu do kluczy i zasad posługiwania się podpisami cyfrowymi przez pracowników w określonych sytuacjach. Koszty te w dużej mierze zależą od rodzaju i skali podejmowanej przez bank działalności. Dlatego też trudno je w jakikolwiek sposób oszacować, czy podać ich wielkość. Można jednak zauważyć, że jeżeli już bank podjął decyzję o rozwoju bankowości elektronicznej, to koszty związane z funkcjonowaniem podpisu elektronicznego nie są duże. Poza tym większość wydatków ma charakter jednorazowy.

Koszty, które będzie musiał ponieść klient, są identyczne jak koszty zewnętrzne ponoszone przez bank. Musi on bowiem zaopatrzyć się w certyfikaty, przy pomocy których uwierzytelni się wobec banku. W przypadku „Certum" cena dla klientów indywidualnych i zbiorowych jest ta sama. Można jednak przypuszczać, iż banki będą w stanie wynegocjować korzystniejsze warunki finansowe niż przeciętni użytkownicy. Klient zasadniczo nie poniesie kosztów, które w przypadku banku określiliśmy mianem wewnętrznych, gdyż są to albo koszty typowe dla banku, albo też klient w chwili uzyskiwania podpisu już musi dysponować pewnym środkami i to niezależnie od chęci posiadania e-podpisu, np. komputerem. W praktyce najczęściej to bank na mocy umowy z Organem Certyfikacji przejmuje na siebie koszty związane z uzyskaniem przez swoich klientów podpisów elektronicznych. Takie działanie pozostaje w interesie banków, którym zależy na bezpiecznych metodach identyfikacji swoich klientów. Zresztą dzięki swej sile i pozycji rynkowej banki mogą wprowadzić do umowy z Organem Certyfikacji zapis, iż ten udostępnieni bezpłatnie ich klientom możliwość elektronicznego podpisywania dokumentów. Przykładem jest tu bank Powszechna Kasa Oszczędności Bank Polski S.A., którego klienci

„uzyskali możliwość nieodpłatnego pobrania identyfikatorów osobistych do zabezpieczania korespondencji prywatnej i służbowej (podpis cyfrowy i szyfrowanie)”[39].

## 1.7. Korzyści dla banków ze stosowania podpisu elektronicznego

Stosowanie podpisu elektronicznego niesie ze sobą szereg korzyści. Wynikają one przede wszystkim z faktu, iż instytucje e-podpisu umożliwia przyspieszenie rozwoju dochodowego działu bankowości – bankowości elektronicznej. Poza tym, podpis cyfrowy daje nawet lepsze uwierzytelnienie osoby niż podpis tradycyjny. Nie bez znaczenia jest też z pewnością fakt, że Organy Certyfikacji gotowe są ponosić odpowiedzialność materialną w określonych granicach za szkody powstałe z ich winy, np. niewłaściwego sprawdzenia tożsamości subskrybenta. Wszystko to sprawia, że ta nowa instytucja daje bankom wiele nowych możliwości, których wykorzystanie wymaga sprawnego i bezpiecznego funkcjonowania podpisu elektronicznego.

W warunkach zaostrzającej się konkurencji międzybankowej utrzymanie banku na możliwie najwyższej ścieżce wzrostu wymaga ograniczania kosztów. Nie ma już bowiem możliwości znaczącego zwiększenia zysków. Taką szansę daje bankowość elektroniczna, która pozwala znacznie ograniczyć koszty działalności detalicznej. Jej rozwój jest jednak uwarunkowany istnieniem odpowiednich metod, pozwalających na bezbłędną identyfikację klienta na odległość. Stosuje się różnorodne techniki zastępcze polegające np. na dostarczaniu klientowi co pewien czas tzw. karty kodów, na której znajdują się zdrapki zawierające poszczególne kody dostępu. Bank zakłada wówczas, iż ten, który się nimi posługuje, jest tym, któremu te kody wydano. Nie jest to ani bezpieczne, ani wygodne, a dodatkowo pociąga za sobą koszty związane z generowaniem i przesyłaniem nowych kodów do klienta. Tych niedogodności nie posiada podpis elektroniczny. Jego bezpieczne stosowanie staje się możliwe jednak dopiero z chwilą prawnego uregulowania skutków, które wywołuje. Dlatego wejście w życie Ustawy o podpisie elektronicznym pozwoli bankom na rozwijanie działalności w zakresie bankowości elektronicznej.

Podpis elektroniczny to bezpieczny sposób uwierzytelniania klienta. Wydaje się on być nawet bezpieczniejszy, niż podpis tradycyjny. Nawet jeżeli dany bank nie prowadzi na przykład oddziałów internetowych, to i tak w kontaktach z klientami stosowanie podpisu elektronicznego powinno ułatwić mu ich identyfikację. Nie będzie już konieczne przechowywanie wzorów

[39]PKO BP S.A., Referencja dla Unizeto Sp. z o.o., http://www.certum.pl/pl/programy_partnerskie/referencje/pkobp.html.

podpisów, wystarczy posłużenie się swoich podpisem (kluczem prywatnym) zapisanym na karcie mikroprocesorowej, choć na to przyjdzie pewnie jeszcze trochę poczekać.

Dla instytucji komercyjnych z pewnością ważna okaże się możliwość przerzucenia na Organ Certyfikacji kosztów związanych z błędną identyfikacją klienta, wynikłą z winy takiego organu. I tak np. „Certum zobowiązuje się do ponoszenia odpowiedzialności za bezpośrednie i pośrednie szkody, będące wynikiem niezgodności procesu weryfikacji tożsamości z deklarowanymi procedurami oraz braku dostępu do świadczonych usług, w tym w szczególności list certyfikatów unieważnionych”[40]. Oczywiście odpowiedzialność jest uzależniona od typu certyfikatu – im bezpieczniejszy, tym odpowiedzialność Organu jest większa. Określone są również maksymalne stawki odpowiedzialności. Przykładowo, „w przypadku wstąpienia szkód z winy Certum łączne gwarancje finansowe Certum w stosunku do wszystkich stron nie mogą przekroczyć jednorazowo sumy kwot dla wyszczególnionego niżej w tabeli zbioru certyfikatów. (...) odpowiedzialność Certum w stosunku do określonej osoby lub wszystkich osób, wynikająca z posługiwania się określonym typem certyfikatu przy realizacji podpisu cyfrowego lub transakcji, powinna być ograniczona do kwot nie przekraczających podanych w poniższej tabeli”. Kwoty, o któtych mowa znajdują się w tabeli 2.

Tabela 2

Kwoty maksymalnej odpowiedzialności „Certum" w zależności od używanych certyfikatów

| CERTYFIKAT | CENA (z VAT) |
|---|---:|
| Certum Level I | 0 zł |
| Certum Level II | 400 zł |
| Certum Level III | 20 000 zł |
| Certum Level IV | 100 000 zł |

*Źródło: http://www.certum.pl/pl/dokumentacja/kpc/index.htm.l*

Mówiąc o korzyściach i kosztach instytucji podpisu elektronicznego należy zdawać sobie sprawę, że staje się on wymogiem czasu i niezależnie od tego, czy jego wprowadzenie będzie bardziej lub mniej opłacalne dla banku, to po prostu nie da się nie zauważyć jego istnienia. Najważniejsze jest to, że Ustawa o podpisie elektronicznym zrównuje w skutkach tzw.

[40] Certum – http://www.certum.pl/pl/dokumentacja/kpc/index.html

kwalifikowany podpis elektroniczny z podpisem tradycyjnym. W praktyce oznacza to, że bank, który dostanie taki dokument będzie musiał uznać jego wiarygodność. Nie będzie się mógł tłumaczyć, iż nie prowadzi bankowości elektronicznej, i że nie uznaje takich dokumentów. Przykładowo, jeżeli wypowiedzenie umowy rachunku bankowego musi nastąpić na piśmie, to wystarczy, że nadawca wyśle wypowiedzenie w formie elektronicznej podpisane elektronicznie na oficjalny adres e-mailowy banku. Dlatego wprowadzenie instytucji podpisu elektronicznego do polskiego systemu prawnego zmusza banki (i nie tylko) do zaznajomienia się z zasadami jej działania[41].

[41] Ustawa o podpisie elektronicznym z dnia 18.09.2001 przewiduje w art. 58 ust. 2 okres przejściowy dla banków i organów władzy publicznej. Mają one czas do 31 grudnia 2002 roku na dostosowanie swojej działalności w zakresie świadczenia usług certyfikacyjnych oraz wykorzystania systemów teleinformatycznych do wymogów ustawy.

# Rozdział 2

# Wybrane prawne aspekty podpisu elektronicznego

## 2.1. Cywilnoprawna regulacja podpisu elektronicznego

### 2.1.1. Skutki podpisu elektronicznego

Instytucja podpisu elektronicznego wymaga istnienia odpowiedniej infrastruktury prawnej. Konieczne jest bowiem, ażeby miał on takie same znaczenie dla wszystkich podmiotów. Nie wystarczy by był on wzajemnie uznawany przez strony stosunku prawnego, gdyż w razie sporu, sąd nie uznałby jego doniosłości. Jego skuteczność powinna więc wynikać z przepisów prawa. Normy prawne powinny również wskazywać niezbędne zasady organizacji Infrastruktury Klucza Publicznego. Z tego względu tak ważne jest uchwalenie ustawy o podpisie elektronicznym, która tworzy niezbędne rozwiązania. Zadość temu czyni polska Ustawa o podpisie elektronicznym, która już w artykule 1 stwierdza, że „ustawa określa warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi".

Z punktu widzenia osoby podpisującej się cyfrowo najważniejsze jest to, jakie skutki wywoła jej działanie. Czy podpis złożony na elektronicznym dokumencie w sposób elektroniczny będzie równorzędny z podpisem własnoręcznym? I czy będzie on spełniał wymóg formy pisemnej? Na te pytania Ustawa o podpisie elektronicznym, pod pewnymi warunkami, odpowiada twierdząco i to dwukrotnie. Po pierwsze, Ustawa o podpisie elektronicznym wprowadza do kodeksu cywilnego[42] nowy przepis w następującym brzmieniu:

> „Art. 78. §2. Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne formie pisemnej."

Po drugie, Ustawa już na początku wyraźnie stwierdza, że „dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom

[42] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (z 1964 r. Dz.U. Nr 16, poz. 93 z późn. zm.).

opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej”[43]. Jest to bardzo ważny przepis, przyjrzyjmy się mu więc dokładnie.

Przepis ten oznacza przede wszystkim to, że dane elektroniczne opatrzone podpisem elektronicznym będą traktowane tak samo jak dokument tradycyjny podpisany własnoręcznie. W szczególności dane podpisane elektronicznie będą spełniać zwykłej wymóg formy pisemnej. Ustawa w ten sposób zrównuje (chociaż nie całkowicie i nie w sposób bezwzględny) podpis tradycyjny z elektronicznym. Aby tak się stało podpis musi spełniać przynajmniej dwa warunki:

a) musi to być „bezpieczny podpis” – a więc taki, który spełnia wymogi określone przez art. 3 pkt 2 Ustawy definiujący taki podpis; zostały one już wskazane w pierwszym podrozdziale niniejszej pracy.
b) do weryfikacji takiego podpisu musi być używany tzw. certyfikat kwalifikowany.

Certyfikat kwalifikowany to taki certyfikat, który spełnia surowe warunki co do swojej zawartości. Musi on bowiem dawać gwarancję właściwej identyfikacji danej osoby. W takim certyfikacie powinny się znaleźć następujące elementy[44]:

a) numer certyfikatu,
b) wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji,
c) określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę oraz numer pozycji w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
d) imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone,
e) dane służące do weryfikacji podpisu elektronicznego,
f) oznaczenie początku i końca okresu ważności certyfikatu,
g) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat,
h) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji,
i) ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to polityka certyfikacji lub umowa z podmiotem świadczącym usługi certyfikacyjne,
j) ewentualnie inne dane, na wniosek osoby składającej podpis elektroniczny.

[43] Art. 5 ust. 2 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[44] Art. 20 ust. 1 i 2 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

Trzeba dodać, że kwalifikowany certyfikat powinien nie tylko spełniać wymogi określone powyżej, lecz również powinien być wystawiony przez tzw. kwalifikowany podmiot świadczący usługi certyfikacyjne. Jest to taki podmiot, który spełnił szereg warunków określonych w Ustawie[45] i został wpisany do odpowiedniego rejestru prowadzonego przez ministra właściwego do spraw gospodarki – obecnie jest to Minister Gospodarki.

Podpis elektroniczny, wywołujący skutki prawne przewidziane dla formy pisemnej, powinien zapewniać integralność danych opatrzonych takim podpisem i jednoznacznie wskazywać kwalifikowany certyfikat wykorzystywany do weryfikacji podpisu. Dodatkowo powinien to czynić w taki sposób, aby rozpoznawalne były wszelkie zmiany tych danych oraz zmiany wskazania certyfikatu, dokonane po złożeniu podpisu. Wymóg ten jest stawiany przez art. 5 ust. 3 Ustawy i można go traktować jako trzeci warunek niezbędny do tego, aby można było uznać dany dokument elektroniczny za równoważny dokumentowi tradycyjnemu.

Podpis elektroniczny może czynić również zadość jednej z tzw. kwalifikowanych form pisemnych, a dokładniej formie pisemnej z datą pewną. Umożliwia to omówiona wcześniej usługa znakowania czasem. Wystarczy, że podpis elektroniczny zostanie oznakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne. Wówczas, na mocy przepisów Ustawy, uważa się, że został on złożony nie później niż w chwili dokonywania tej usługi. Wywołuje to tym samym skutki prawne daty pewnej w rozumieniu kodeksu cywilnego[46].

Należy zadać pytanie, co w takim razie z podpisem, który nie będzie spełniał powyższych wymagań. Oczywiste jest to, że nie będzie czynił zadość wymogom formy pisemnej. Tym niemniej podpisowi elektronicznemu nie można odmówić ani ważności, ani skuteczności z tego względu, iż nie posiada on kwalifikowanego certyfikatu lub że nie jest podpisem bezpiecznym, lub też nie został złożony za pomocą bezpiecznego urządzenia[47]. Oznacza to, że jeżeli strony się tak umówią, to w ich stosunkach podpis będzie wywoływał takie skutki, jakie zgodnie ustanowią. Oczywiście nie mogą w ten sposób obchodzić bezwzględnie wiążących przepisów prawa, np. w zakresie formy czynności prawnej.

[45] Por. w szczególności art. 10 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[46] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (z 1964 r. Dz.U. Nr 16, poz. 93 z późn. zm.).
[47] Art. 8 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

### 2.1.2. Odpowiedzialność cywilna podmiotów świadczących usługi certyfikacyjne

Z punktu widzenia odbiorców usług certyfikacyjnych ważne jest uregulowanie w Ustawie o podpisie elektronicznym kwestii odpowiedzialności za szkody podmiotów świadczących usługi certyfikacyjne[48]. W myśl tych reguł wystawca certyfikatów będzie odpowiedzialny za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem obowiązków w zakresie świadczonych usług. Będzie mógł on jednak uwolnić się od odpowiedzialności, jeżeli wykaże, że nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które wystawca nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności. Odpowiedzialności nie poniesie również za te szkody, które wynikają z użycia certyfikatu poza zakresem określonym w polityce certyfikacji, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie. Wystawca nie odpowiada też za szkodę wynikła z nieprawdziwości danych zawartych w certyfikacie, a wpisanych na wniosek osoby składającej podpis.

Ciekawą kwestią jest stosunek tych regulowań do ogólnych zasad wynikających z kodeksu cywilnego. Powstaje wątpliwość, czy artykuł 11 Ustawy o podpisie elektronicznym należy traktować jako *lex specialis* wobec artykułu 471 kodeksu cywilnego[49]. Wydaje się, że odpowiedź powinna być twierdząca. W szczególności wskazuje na to fakt, że Ustawa wyraźnie rozszerza katalog okoliczności egzoneracyjnych, na które może powoływać się podmiot świadczący usługi certyfikacyjne. Dlatego też w zakresie odpowiedzialności wystawców certyfikatów z tytułu niewykonania lub nienależytego wykonania ich obowiązków w zakresie świadczonych prze nich usług właściwe wydaje się posługiwanie się zasadami określonymi w Ustawie o podpisie elektronicznym przed zastosowaniem zasad kodeksowych.

### 2.1.3. Oświadczenia woli a podpis elektroniczny

Ustawa o podpisie elektronicznym w zasadzie nie reguluje problematyki cywilnoprawnej. Wyjątki dotyczą tylko kwestii zrównania podpisu cyfrowego z podpisem tradycyjnym, które zostały omówione powyżej. W związku z tym właściwe wydaje się być stosowanie do kwestii nie unormowanych Ustawą reguł ogólnych prawa cywilnego, wynikających przede wszystkim z kodeksu cywilnego. Może powstać jednak szereg wątpliwości związanych ze specyfiką obrotu

[48] Art. 11 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[49] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (z 1964 r. Dz.U. Nr 16, poz. 93 z późn. zm.).

elektronicznego. Poniżej zostaną jedynie zasygnalizowane problemy, które będą wymagały rozwiązania bądź na drodze ustawowej, bądź na drodze orzecznictwa Sądu Najwyższego lub też poprzez przyjęte zwyczaje.

Pierwsza wątpliwość dotyczy chwili i miejsca złożenia oświadczenia woli podpisanego elektronicznego, a także chwili i miejsca zawarcia umowy. Istnieje tu szereg kwestii, które należy rozstrzygnąć. W myśl art. 61 KC[50] oświadczenie woli, które ma być złożone innej osobie, jest złożone z chwilą, gdy doszło do niej w taki sposób, że mogła zapoznać się z jego treścią. W przypadku złożenie oświadczenia woli przy użyciu sieci komputerowej nie bardzo wiadomo, czy będzie to chwila otrzymania wiadomości przez serwer na którym posiadamy skrzynkę pocztową, czy też będzie to chwila rzeczywistego spłynięcia informacji na nasz komputer. Wydaje się, iż w różnych sytuacjach odpowiedź będzie różna, a nie jest wykluczone, iż w grę będzie wchodzić jeszcze inny moment, np. chwila zapoznania się z wiadomością przy użyciu bezpośredniego dostępu do skrzynki na stronach WWW. Problemy może stwarzać również skuteczne odwołanie oświadczenia woli.

Ważna reguła interpretacyjna zawarta jest w art. 70 KC – według niej, w razie wątpliwości umowę poczytuje się za zawartą w chwili otrzymania przez składającego ofertę oświadczenia o jej przyjęciu lub też w chwili przystąpienia przez druga stronę do wykonania umowy. Ma to duże znaczenie, gdyż do zawarcia umowy za pomocą sieci będzie najczęściej dochodziło w trybie ofertowym. Mogą na tym tle powstać różne problemy dowodowe – przykładowo, jak oblat może wykazać, że jego oświadczenie o przyjęciu oferty w formie elektronicznej zostało rzeczywiście wysłane, nie wspominając już o udowodnieniu faktu dojścia tego oświadczenia do składającego ofertę. Trzeba też odpowiedzieć na pytanie, czy Internet (sieć komputerowa) jest środkiem bezpośredniego porozumiewania się na odległość. Wymaga tego art. 66 § 2 KC aby stwierdzić, czy oferta przestaje wiązać, gdy nie została przyjęta niezwłocznie, czy dopiero po upływie czasu, w którym składający ofertę mógł w zwykłym toku czynności otrzymać odpowiedź wysłaną bez nieuzasadnionego opóźnienia.

Miejsce złożenia oświadczenia woli i zawarcia umowy ma duże znaczenie przy zawieraniu transakcji przez Internet. Można się spodziewać, że przy takich umowach określenie, co jest jej miejscem zawarcia, napotka wiele trudności Kontrahenci znajdują się wówczas często na dwóch lub więcej obszarach prawnych, zatem powstaje fundamentalne pytanie, czyje prawo stosować. W Polsce określa to ustawa Prawo prywatne międzynarodowe[51]. Jednak wówczas, gdy nakazuje ona

[50] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (z 1964 r. Dz.U. Nr 16, poz. 93 z późn. zm.)
[51] Ustawa z dnia 12 listopada 1965 r. Prawo prywatne międzynarodowe (z 1965 r. Dz.U. Nr 46, poz. 290 z późn. zm.).

stosować prawo miejsca zawarcia umowy[52], pojawia się dylemat, co jest tym miejscem. Zgodnie z art. 70 § 2 KC w razie wątpliwości poczytuje się umowę za zawartą w miejscu otrzymania przez składającego ofertę oświadczenia o jej przyjęciu, a jeżeli dojście do składającego ofertę oświadczenia o jej przyjęciu nie jest potrzebne – w miejscu zamieszkania składającego ofertę. Nastręczać trudności może tu już choćby ustalenie, co jest miejscem otrzymania przez składającego ofertę oświadczenia o jej przyjęciu, w sytuacji, gdy ta odpowiedź zostanie przesłana elektronicznie[53].

Zastanowić się należy, czy jest możliwe udzielenie pełnomocnictwa do zawarcia umowy w drodze elektronicznej z użyciem podpisu elektronicznego. Wymaga to odpowiedzi na kolejne pytanie: czy w ogóle jest dopuszczalne użycie przez osobę trzecią cudzego podpisu elektronicznego za zgodą właściciela klucza prywatnego? A jakie przepisy należy stosować w sytuacji, gdy ktoś przez pomyłkę użyje naszego podpisu elektronicznego? Brak w tym zakresie jednoznacznych wskazań Ustawy. Naturalne w tej sytuacji stosowanie ogólnych reguł prawa cywilnego wydaje się być niemożliwe ze względu na art. 47 Ustawy o podpisie elektronicznym, który nakłada odpowiedzialność karną na osobę składającą bezpieczny podpis elektroniczny za pomocą danych przyporządkowanych do innej osoby.

Upowszechnianie się technologii podpisu elektronicznego niesie za sobą powstanie szeregu nowych zagadnień w zakresie wad oświadczeń woli. Wprawdzie nie będzie konieczne tworzenie żadnych nowych ich form, niemniej jednak powstaną z pewnością nowe sytuacje prawne, które nastręczać będą wątpliwości co do ich prawnej kwalifikacji. Wynikać to będzie przede wszystkim z technicznych ograniczeń związanych z elektroniczną postacią podpisu. Przykładowo, wysłanie podpisanej elektronicznie informacji może nastręczyć szereg trudności osobie, która bądź to nie jest wprawna w obsłudze komputera bądź nie posiada takiego edytora tekstu, przy którego użyciu zapisano oświadczenie woli. Czy osoba taka, która odczyta oświadczenie w formie zmodyfikowanej, a następnie złoży własne oświadczenie woli, będzie pozostawała w błędzie? Odpowiedź twierdząca może, w niektórych sytuacjach, okazać się zbyt pochopna, a to ze względu na stosunkową łatwość dowiedzenia okoliczności, które w rzeczywistości nie miały miejsca.

Niejasna pozostaje również kwestia odpowiedzialności cywilnej za szkody spowodowane udostępnieniem osobie trzeciej własnego podpisu (klucza prywatnego). Art. 15 Ustawy wspomina jedynie o obowiązku odbiorcy usług certyfikacyjnych polegającym na przechowywaniu danych służących do składania podpisu elektronicznego w sposób zapewniający ich ochronę przed

[52] Art. 27 § 2 Ustawy z dnia 12 listopada 1965 r. Prawo prywatne międzynarodowe (z 1965 r. Dz.U. Nr 46, poz. 290 z późn. zm.).

[53] Wskazane powyżej kwestie zostały szerzej omówione w pracy A. Króla „Zawarcie umowy w internecie według kodeksu cywilnego", opublikowanej pod adresem http://www.prometeus.com.pl/prawo/.

nieuprawnionym wykorzystaniem w okresie ważności certyfikatu. Nie ustanawia on jednak żadnej odpowiedzialności za naruszenie tego obowiązku.

## 2.2. Administracyjnoprawna regulacja podpisu elektronicznego

### 2.2.1. Świadczenie usług certyfikacyjnych

Usługi certyfikacyjne świadczone są przez podmioty zwane przez polską Ustawę „podmiotami świadczącymi usługi certyfikacyjne". W niniejszej pracy są one również nazywane wystawcami certyfikatów lub też Organami Certyfikacji. Ustawa wyróżnia:

a) „zwykłe" podmioty świadczące usługi certyfikacyjne,
b) kwalifikowane podmioty świadczące usługi certyfikacyjne.

Świadczenie usług certyfikacyjnych podlega zasadzie swobody podejmowania działalności gospodarczej. Prowadzenie takiej działalności nie będzie wymagać ani zezwolenia, ani tym bardziej koncesji. Działalność taką będzie mógł więc podjąć każdy przedsiębiorca bez względu na formę organizacyjną (osoba fizyczna, prawna czy jednostka organizacyjna). W szczególności usługi certyfikacyjne będą mogły świadczyć również banki komercyjne, gdyż ustawodawca w Ustawie o podpisie elektronicznym[54] zdecydował się na wprowadzenie zmian do Prawa bankowego[55]. Świadczenie takich usług zostało zaliczone do tak zwanych pozostałych czynności, które mogą być wykonywane przez banki. Nie będą mogły one jednak wydawać certyfikatów kwalifikowanych wykorzystywanych przy czynnościach, w których banki są stronami. Nie było tak jednak od początku, gdyż twórcy projektu Ustawy uznali, iż banki, jako instytucje zaufania społecznego, powołane są do wykonywania innych zadań – zauważyli oni bowiem, że wszystkie czynności bankowe związane są z operacjami finansowymi, do których świadczenia usług certyfikacyjnych nie należy[56]. Dopiero Senat zdecydował się na przyznanie bankom możliwości świadczenia usług certyfikacyjnych.

Aby skorzystać z dobrodziejstw podpisu elektronicznego należy uzyskać certyfikat, dzięki któremu będzie możliwa weryfikacja osoby podpisującej. Ustawa celowo nie używa pojęć typu klucz prywatny, czy klucz publiczny – wspomina jedynie ogólnikowo o „weryfikacji". Realizuje tym samym postulat neutralności technologicznej. Nie precyzuje ona, jakich technik

[54] Art. 55 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[55] Ustawa z dnia 29 sierpnia 1997 roku Prawo bankowe (z 1997 r. Dz.U. Nr 140, poz. 939 z późn. zm.).
[56] Por. Sprawozdanie Sejmowej Komisji Transportu i Łączności z rozpatrzenia poselskiego i rządowego projektu ustawy o podpisie elektronicznym wygłoszone w Sejmie przez posła Karola Działoszyńskiego w dniu 19 lipca 2001 r.

kryptograficznych należy używać w procesie tworzenia i weryfikacji podpisu elektronicznego. Możliwa będzie więc przyszłości ewentualna zmiana (na bezpieczniejsze) metod wykorzystywanych na potrzeby tej instytucji. Ustawa pozostawia też uregulowanie szczegółowych kwestii technicznych przepisom szczególnych, co uelastycznia stosowanie samej ustawy[57].

Uzyskanie certyfikatu następuje na skutek zawarcia umowy pomiędzy podmiotem świadczącym usługi certyfikacyjne a odbiorcą tych usług (osobą chcącą używać podpisu elektronicznego). Zawarcie umowy powinno być poprzedzone poinformowaniem na piśmie lub za pomocą informacji trwale zapisanej na nośniku elektronicznym odbiorcy w sposób jasny i powszechnie zrozumiały o dokładnych warunkach używania certyfikatu. Świadczący usługi powinien uzyskać pisemne potwierdzenie zapoznania się z informacją jeszcze przed zawarciem umowy[58]. Umowa taka powinna być zawarta na piśmie. Nie spełnienie tego wymogu skutkuje nieważnością takiej umowy. Jeżeli jednak wszystkie pozostałe warunki zostaną spełnione, wówczas brak zachowania formy pisemnej nie powoduje nieważności certyfikatu[59].

Świadczenie usług certyfikacyjnych następuje na zasadach określonych w tzw. polityce certyfikacji. Prawny obowiązek opracowania i stosowania takiej polityki będą miały podmioty kwalifikowane, o których szerzej w następnym podrozdziale. Można się jednak spodziewać, że zdecydowana większość dostawców certyfikatów będzie posiadać opracowane i podane do powszechnej wiadomości stałe zasady, które będą wyznaczać sposób ich postępowania. Polityka certyfikacji określać powinna w szczególności[60]: zakres jej zastosowania, opis sposobu tworzenia i przesyłania kluczy publicznych (i ewentualnie generowania i przesyłania kluczy prywatnych), sposób identyfikacji osób ubiegających się o wydanie certyfikatu, rodzaje wydawanych certyfikatów i maksymalne okresy ich ważności, metody i tryb tworzenia certyfikatów oraz list unieważnionych i zawieszonych certyfikatów, opis elektronicznego zapisu struktur danych zawartych w certyfikatach, a także sposób zarządzania dokumentami związanymi ze świadczeniem usług certyfikacyjnych.

[57] Ibidem.
[58] Art. 14 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[59] Art. 16 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[60] Art. 17 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

### 2.2.2. Obowiązki podmiotów świadczących usługi certyfikacyjne

Ustawa o podpisie elektronicznym nakłada na wystawców certyfikatów określone obowiązki. Ich zakres zależy od tego, czy mamy do czynienia ze „zwykłym" podmiotem świadczącym takie usługi, czy z podmiotem kwalifikowanym. Oczywiście katalog obowiązków tego drugiego jest znacznie szerszy. Wynika to z faktu, że podmioty kwalifikowane mogą wystawiać certyfikaty, uwierzytelniające podpisy elektroniczne równorzędne z podpisami tradycyjnymi. Wiąże się to z koniecznością zapewnienia wyższego poziomu bezpieczeństwa, w tym również prawnego, dla osób chcących z nich korzystać. Poniżej zostaną wskazane najważniejsze obowiązki wystawców certyfikatów wynikające z samej Ustawy o podpisie elektronicznym.

Podmiot świadczący usługi certyfikacyjne jest obowiązany do zachowania w tajemnicy danych służących do składania tzw. poświadczeń elektronicznych[61]. Takie poświadczenie to nic innego, jak swego rodzaju podpis elektroniczny wystawcy certyfikatu. Zatem dane służące do jego tworzenia (swoisty klucz prywatny wystawcy) nie powinny być ujawniane, gdyż groziłoby to tym, iż każdy, kto wszedłby w posiadanie takich danych, mógłby podszyć się pod wystawcę.

Kolejnym obowiązkiem podmiotu świadczącego usługi certyfikacyjne jest bezpieczne przechowywanie i archiwizowanie dokumentów i danych w postaci elektronicznej bezpośrednio związanych z wykonywanymi usługami certyfikacyjnymi[62]. Nie dotyczy to jednak, co zrozumiałe, tych danych, które służą do składania podpisu elektronicznego, a więc generowanych przez taki podmiot kluczy prywatnych odbiorców. Dane te wręcz nie powinny być ani przechowywane, ani kopiowane przez wystawcę. Dla podmiotów kwalifikowanych czas trwania obowiązku przechowywania danych i dokumentów określony został na 20 lat.

Do podstawowych obowiązków podmiotów świadczących usługi certyfikacyjne należy unieważnianie i zawieszanie certyfikatów[63]. Podmioty kwalifikowane są do tego obowiązane, na mocy Ustawy, w określonych sytuacjach. Dotyczy to jedynie certyfikatów kwalifikowanych. Podmiot świadczący usługi certyfikacyjne musi unieważnić taki certyfikat przed upływem okresu jego ważności, jeżeli:

a) certyfikat ten został wydany na podstawie nieprawdziwych lub nieaktualnych danych,
b) podmiot nie dopełnił obowiązków określonych w Ustawie,

[61] Art. 12 ust. 1 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[62] Art. 13 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[63] Art. 21 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

c) osoba składająca podpis elektroniczny weryfikowany na podstawie tego certyfikatu nie utrzymała w tajemnicy danych służących do składania przez nią podpisu,
d) podmiot zaprzestaje świadczenia usług, a jego praw i obowiązków nie przejmuje inny kwalifikowany podmiot,
e) zażąda tego osoba składająca podpis elektroniczny lub osoba trzecia wskazana w certyfikacie,
f) zażąda tego minister właściwy do spraw gospodarki,
g) osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych.

Zawieszenie certyfikatu kwalifikowanego powinno nastąpić natomiast w przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia takiego certyfikatu. Zawieszenie certyfikatu może trwać najdłużej 7 dni. W tym czasie wystawca powinien podjąć kroki niezbędne do wyjaśnienia powstałych wątpliwości. Jeżeli okażą się one bezpodstawne podmiot świadczący usługi certyfikacyjne uchyli zawieszenie certyfikatu. Jeżeli jednak wątpliwości się potwierdzą, lub nie będzie możliwe ich wyjaśnienie w terminie 7 dni, wówczas wystawca zmuszony będzie unieważnić certyfikat. Raz unieważniony certyfikat nie będzie już mógł być uznany za ważny. Na wystawcy ciąży również obowiązek niezwłocznego powiadomienia osobę używającą danego podpisu elektronicznego o fakcie zawieszenia lub unieważnienia jej certyfikatu.

Podmiot świadczący usługi certyfikacyjne jest obowiązany publikować listę zawieszonych i unieważnionych certyfikatów. Ma to na celu umożliwienie sprawdzenia w procesie weryfikacji określonego podpisu elektronicznego, czy jest on nadal podpisem wiarygodnym. Ustawa określa szczegółowo[64], co powinna zawierać taka lista – najważniejszym jej elementem jest data i czas zawieszenia lub unieważnienia każdego certyfikatu. W tym bowiem momencie zawieszenia lub unieważnienie wywołuje odpowiednia skutki prawne.

Świadczyć usługi certyfikacyjne mogą, jak już wspomniano, wszyscy przedsiębiorcy. Jednak, aby uzyskać pełną skuteczność prawną należy posługiwać się certyfikatem wystawionym przez kwalifikowany podmiot świadczący takie usługi. Podmiot taki powinien uzyskać wpis do odpowiedniego rejestru. Musi on spełnić szereg wymagań, stawianych mu przez Ustawę. Kwalifikowany podmiot świadczący usługi certyfikacyjne wydający kwalifikowane certyfikaty jest obowiązany:

[64] Por. art. 22 ust. 3 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

a) zapewnić techniczne i organizacyjne możliwości szybkiego i niezawodnego wydawania, zawieszania i unieważniania certyfikatów oraz określania czasu dokonania tych czynności,
b) stwierdzić tożsamość osoby ubiegającej się o certyfikat,
c) zapewnić środki przeciwdziałające fałszerstwom certyfikatów i innych danych poświadczanych elektronicznie przez te podmioty, w szczególności przez ochronę urządzeń i danych wykorzystywanych przy świadczeniu usług certyfikacyjnych,
d) zawrzeć umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych,
e) poinformować osobę ubiegającą się o certyfikat, przed zawarciem z nią umowy, o warunkach uzyskania i używania certyfikatu, w tym o wszelkich ograniczeniach jego użycia,
f) używać systemów do tworzenia i przechowywania certyfikatów, w sposób zapewniający możliwość wprowadzania i zmiany danych jedynie osobom uprawnionym,
g) uzyskać uprzednią zgodę osoby, której wydano certyfikat, na jego publikację, jeżeli podmiot zapewnia publiczny dostęp do certyfikatów,
h) udostępniać odbiorcy usług certyfikacyjnych pełny wykaz bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych i warunki techniczne, jakim te urządzenia powinny odpowiadać,
i) zapewnić, w razie tworzenia przez niego danych służących do składania podpisu elektronicznego, poufność procesu ich tworzenia, a także nie przechowywać i nie kopiować tych danych ani innych danych, które mogłyby służyć do ich odtworzenia, oraz nie udostępniać ich nikomu innemu poza osobą, która będzie składała za ich pomocą podpis elektroniczny,
j) zapewnić, w razie tworzenia przez niego danych służących do składania podpisu elektronicznego, aby dane te z prawdopodobieństwem graniczącym z pewnością wystąpiły tylko raz,
k) publikować dane, które umożliwiają weryfikację, w tym również w sposób elektroniczny, autentyczności i ważności certyfikatów oraz innych danych poświadczanych elektronicznie przez ten podmiot oraz zapewnić nieodpłatny dostęp do tych danych odbiorcom usług certyfikacyjnych[65].

[65] Art. 10 ust. 1 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

Odrębne wymogi stawia Ustawa o podpisie elektronicznym osobom, które wykonują czynności związane ze świadczeniem usług certyfikacyjnych. Osoby takie powinny przede wszystkim posiadać pełną zdolność do czynności prawnych. Poza tym nie powinny być skazane prawomocnym wyrokiem za przestępstwa przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, przestępstwo skarbowe lub jakiekolwiek przestępstwo karane na podstawie Ustawy o podpisie elektronicznym. Od takich osób wymagane jest również posiadanie niezbędnej wiedzy i umiejętności w zakresie technologii tworzenia certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym[66].

### 2.2.3. Nadzór państwa

Państwo sprawuje nadzór nad podmiotami świadczącymi usługi certyfikacyjne poprzez ministra właściwego do spraw gospodarki – obecnie jest to Minister Gospodarki. Celem tego nadzoru jest zapewnienie ochrony interesów odbiorców usług certyfikacyjnych. Ma to zapewnić arsenał środków, którymi dysponuje minister. Należą do nich w szczególności:

a) prowadzenie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
b) wydawanie i unieważnianie zaświadczeń certyfikacyjnych,
c) kontrola działalności podmiotów świadczących usługi certyfikacyjne pod względem zgodności z Ustawą,
d) nakładanie kar przewidzianych w Ustawie.

Aby móc świadczyć usługi certyfikacyjne w charakterze kwalifikowanego podmiotu należy uzyskać wpis do rejestru prowadzonego przez ministra oraz uzyskać zaświadczenie certyfikacyjne, które stanowi swego rodzaju certyfikat przyznawany przez ministra podmiotowi kwalifikowanemu[67]. Dodatkowo podmiot taki nie może figurować w rejestrze dłużników niewypłacalnych. Aby uzyskać wpis należy złożyć wniosek do ministra, którego zawartość określa szczegółowo art. 24 ust. 2 Ustawy o podpisie elektronicznym. Spełnienie wymogów tam określonych jest podstawowym warunkiem koniecznym do uzyskania statusu podmiotu kwalifikowanego. Minister wpisując podmiot do rejestru, lub odmawiając go, ma możliwość sprawowania nadzoru nad systemem certyfikacji. Wydanie decyzji następuje po przeprowadzeniu kontroli zleconej przez ministra. Uzyskanie wpisu do rejestru oznacza potwierdzenie, że podmiot

[66] Art. 10 ust. 2 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[67] Por. rozdział VI Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

jest instytucją posiadającą wystarczający potencjał merytoryczny i techniczny dla wystawców certyfikatów kwalifikowanych i spełnia wymogi określone w Ustawie. Wpis jest dla podmiotu świadczącego usługi certyfikacyjne oficjalnym ministerialnym stwierdzeniem dobrego przygotowania do świadczenia usług, co jest z kolei ważnym elementem branym pod uwagę przez osoby chcące uzyskać certyfikat. Minister może odmówić dokonania wpisu do rejestru jeżeli:

a) wniosek i dołączone do niego dokumenty nie spełniają warunków określonych w Ustawie,
b) w dokumentach organizacyjnych podmiotu zamieszczone są postanowienia mogące zagrażać bezpieczeństwu albo w inny sposób naruszać interes odbiorców usług certyfikacyjnych,
c) podmiot został umieszczony w rejestrze dłużników niewypłacalnych,
d) wskazane we wniosku techniczne i organizacyjne możliwości wykonywania czynności w zakresie świadczenia usług certyfikacyjnych nie spełniają warunków określonych w Ustawie,
e) osoby wykonujące czynności związane ze świadczeniem usług certyfikacyjnych, zatrudniane przez podmiot świadczący takie usługi, nie spełniają wymogów określonych w Ustawie[68].

Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne jest prowadzony przez ministra właściwego do spraw gospodarki[69]. Rejestr taki jest jawny i publicznie dostępny. Co ciekawe, powinien być on prowadzony również w formie elektronicznej. Zmiany w nim powinny być dokonywane na bieżąco, stąd obowiązek nałożony na podmioty kwalifikowane niezwłocznego, najpóźniej w terminie 7 dni, zawiadamiania ministra o każdej zmianie danych zawartych we wniosku. Zawiadomić, najpóźniej 3 miesiące wcześniej, należy również o terminie zaprzestania świadczenia usług certyfikacyjnych.

Wśród arsenału środków, którymi dysponuje minister jest również wydawanie zaświadczeń certyfikacyjnych. Jego uzyskanie jest niezbędne do rozpoczęcia świadczenia usług certyfikacyjnych. Zaświadczenia certyfikacyjne to zaświadczenia elektroniczne, które służą do weryfikacji wystawców certyfikatów i są do nich przyporządkowane. Innymi słowy, są to swoiste certyfikaty, zawierające klucze publiczne podmiotów świadczących usługi certyfikacyjne, które służą do sprawdzania autentyczności kluczy prywatnych (poświadczeń certyfikacyjnych) tych podmiotów. Lista wydanych przez ministra zaświadczeń certyfikacyjnych również jest

[68] Art. 25 ust. 4 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[69] Art. 27 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

publikowana, i to w formie elektronicznej[70]. Na tej liście znajdują się również odpowiednie dane, które służą do weryfikacji wydawanych przez ministra zaświadczeń. Według projektu Ustawy o podpisie elektronicznym wspomnianej czynności mógł dokonywać jedynie minister właściwy do spraw gospodarki. Jednak Senat dokonał zmiany w Ustawie polegającej na tym, że minister może upoważnić Narodowy Bank Polski (lub podmiot od niego zależny) do wytwarzania i wydawania zaświadczeń certyfikacyjnych. Zmiana ta spotkała się z powszechną krytyką środowiska zarówno informatycznego, jak i prawniczego. Sejmowi nie udało się jednak odrzucić tej poprawki. Obecnie, na podstawie uchwalonych przepisów, NBP może zwrócić się z wnioskiem do ministra gospodarki o upoważnienie do dokonywania wspomnianych czynności, przy czym konstrukcja przepisu zdaje się wskazywać, iż minister nie może takiemu wnioskowi odmówić. Niejasne jest to, czy po upoważnieniu NBP sam minister będzie mógł nadal wydawać zaświadczenia certyfikacyjne – wydaje się, że nie. Szereg wątpliwości budzić może wówczas fakt, że jedynie NBP lub spółka od niego zależna będzie mogła świadczyć usługi, bez których nie może powstać kwalifikowany podmiot wystawiający certyfikaty. Według Urzędu Komitetu Integracji Europejskiej ten przepis narusza prawo UE, a według wielu prawników również i konstytucyjną zasadę równości podmiotów gospodarczych[71].

Minister sprawując nadzór nad wykonaniem przepisów Ustawy o podpisie elektronicznym może dokonywać kontroli działalności podmiotów świadczących usługi certyfikacyjne[72]. Minister może przeprowadzić taką kontrolę z urzędu albo na żądanie prokuratora, sądu, albo innych organów państwowych upoważnionych do tego na podstawie ustaw w związku z prowadzonymi przez nie postępowaniami w prawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne. Kontrolę przeprowadzają pracownicy ministerstwa na podstawie upoważnienia wydanego przez ministra, które określa jednocześnie zakres kontroli. Kontrola ma na celu ustalenie, czy działalność podmiotu jest zgodna z wymogami ustawy – jest to więc kontrola legalizmu prowadzonych działań. W swej zasadniczej części jest prowadzona na podstawie wybranych przepisów ustawy o Najwyższej Izbie Kontroli[73]. O wynikach kontroli powiadamiany jest podmiot skontrolowany i w przypadku stwierdzenia nieprawidłowości wyznaczany jest mu termin (nie krótszy niż 14 dni) do ich usunięcia.

W Ustawie zawarto również kompetencję dla ministra właściwego do spraw gospodarki do nakładania określonych kar, w szczególności kar pieniężnych. Karę taka może zostać nałożona na

[70] Art. 23 ust. 3 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[71] Tak np. Jarosław Mojsiejuk, prawnik HP Polska, w wywiadzie dla BiznesNet.pl zamieszczonym pod adresem http://www.biznesnet.pl/index.phtml?pg=wywiadownia&a=3400.
[72] Regulują to art. 30 oraz 35-41 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[73] Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (z 1995 r. Dz.U. Nr 13 , poz. 59 z późn. zm.).

podmiot, który prowadzi działalność niezgodnie z przepisami Ustawy w sposób zagrażający interesom odbiorców usług certyfikacyjnych, wówczas gdy nieprawidłowości są szczególnie rażące. Wysokość kary może wynieść do 50 000 złotych. Kara, w takich samych granicach może zostać nałożona również wówczas, gdy podmiot w wyznaczonym terminie nie usunie nieprawidłowości[74].

### 2.2.4. Uznawanie certyfikatów zagranicznych

Zadaniem podpisu elektronicznego jest sygnowanie dokumentów elektronicznych. Przesyłane są one następnie przy użyciu sieci informatycznych do ich odbiorców. Sposób przesyłania oznacza, że z taką samą łatwością możemy wysłać informację do osoby znajdującej się w sąsiednim pomieszczeniu, jak i do osoby znajdującej się na innym kontynencie. To samo dotyczy odbierania wiadomości od potencjalnych nadawców, którzy mogą być rozsiani po całym świecie. W związku z tym szczególnego znaczenia nabiera kwestia, czy dane podpisane elektronicznie przez nadawcę pochodzącego z poza Polski będą mogły być w świetle prawa uznane za podpisane takim podpisem, a w szczególności podpisem kwalifikowanym, spełniającym wymogi formy pisemnej. Oczywiście, nie będzie problemu, jeżeli taki podmiot będzie świadczył usługi w Polsce. Może on uzyskać wpis do polskiego rejestru podmiotów kwalifikowanych i działać jak każdy inny polski wystawca.

Odpowiednie uregulowanie zawiera Ustawa o podpisie elektronicznym[75]. Stwierdza ona, że certyfikat wydany przez podmiot, który nie ma siedziby w Polsce i nie świadczy tu usług zostaje, w określonych sytuacjach, zrównany pod względem prawnym z kwalifikowanym certyfikatem wydanym przez kwalifikowany podmiot polski. Ustawa wymienia okoliczności, w których takie zrównanie będzie mogło nastąpić. Jako pierwsza wymieniona jest sytuacja, w której podmiotowi świadczącemu usługi certyfikacyjne, który wydał ten certyfikat, została udzielona akredytacja. Jest to ewidentny błąd legislacyjny, gdyż akredytacja jest rozwiązaniem, które zostało w toku prac ustawodawczych całkowicie usunięte z Ustawy[76]. Artykuł 4 Ustawy odwołuje się wiec do pojęcia, które nie istnieje[77].

---

[74] Art. 30 i 32 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[75] Art. 4 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[76] Uczynił to Senat w stosowanych poprawkach, a Sejm poprawki przyjął na posiedzeniu w dniu 18 września 2001 roku.
[77] Niniejsza praca jest oddawana w chwili, gdy tekst Ustawy nie został jeszcze oficjalnie opublikowany, chociaż znany jest już numer Dziennika Ustaw, w którym się on ukaże. Pozostaje więc nadzieja, iż tekst Ustawy, którym posługuje się Autor, a opublikowany m.in. na stronach Sejmu RP, obarczony jest błędem, którego nie zawiera już wersja legalna.

Zrównanie pod względem prawnym zagranicznych certyfikatów z polskimi następuje również wtedy, gdy przewiduje to umowa międzynarodowa o wzajemnym uznawaniu certyfikatów, której stroną jest Polska. Przepis ten jednak traci moc z dniem wejścia naszego kraju do Unii Europejskiej. Z tą samą chwilą nowa grupa certyfikatów będzie mogła zostać uznana za równorzędne z certyfikatami wydanymi w Polsce. Będą to te certyfikaty, które będą spełniać jeden z poniższych warunków:

a) podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, został wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
b) podmiot świadczący usługi certyfikacyjne, mający siedzibę na terytorium Wspólnoty Europejskiej spełniający wymogi Ustawy, udzielił gwarancji za ten certyfikat,
c) certyfikat ten został uznany za kwalifikowany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi,
d) podmiot świadczący usługi certyfikacyjne, który wydal ten certyfikat, został uznany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi.

Na negatywną ocenę zasługuje fakt, iż Ustawa odwołuje się do pojęcia Wspólnoty Europejskiej, która została zastąpiona przez Unię Europejską na mocy traktatu z Maastricht z 7 lutego 1992 r.[78]. Jest to ewidentna pomyłka ustawodawcy, która powinna zostać poprawiona jeszcze przed wejściem ustawy w życie. Poza tym, wydaje się, że powyższe regulacje dobrze spełnią swoje zadanie. Jednak na czas ich rzeczywistej weryfikacji przyjdzie poczekać do dnia wejścia naszego kraju w struktury Unii Europejskiej.

## 2.3. Karnoprawna regulacja podpisu elektronicznego

Twórcy Ustawy o podpisie elektronicznym postanowili zawrzeć w jej treści katalog podstawowych przestępstw związanych ze stosowaniem podpisu i świadczeniem usług certyfikacyjnych. Pewna część czynów zabronionych będzie mogła być jednak karana na podstawie nowego kodeksu karnego[79], który rozszerza definicję dokumentu również na tzw. dokumenty elektroniczne. Stanowi on, iż „dokumentem jest każdy przedmiot lub zapis na komputerowym

[78] M. Łopaciński, „Analiza ustawy o podpisie elektronicznym", http://www.vagla.pl/skrypts/podpis_elektroniczny.htm.
[79] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (z 1997 r. Dz. U Nr 88, poz. 553 z późn. zm.).

nośniku informacji(...)”[80]. W ten sposób wszystkie czyny zabronione, w których ustawowym opisie występuje słowo „dokument” będą podstawą do karania przestępstw związanych z obrotem dokumentami elektronicznymi. Są to przestępstwa należące do grup przestępstw przeciwko wiarygodności dokumentów, obrotowi gospodarczemu i obrotowi pieniędzmi i papierami wartościowymi. Nie wszystkie jednak dokumenty elektroniczne będą podlegały ochronie na podstawie kodeksu karnego, a tylko te, które „ze względu na zawartą w nich treść stanowią dowód prawa, stosunku prawnego, lub okoliczności mogącej mieć znaczenie prawne”. Jest to jednak dosyć szerokie ujęcie „dokumentu” pozwalające ścigać szeroki katalog przestępstw[81].

W chwili uchwalania kodeksu karnego w 1997 roku instytucja podpisu elektronicznego, nie była ani znana polskiemu systemowi prawnemu, ani nawet jej uchwalenie nie było jeszcze projektowane. Dlatego też ustawa ta nie zawiera przepisów ściśle związanych z e-podpisem, nie pozwala też więc, w wielu przypadkach, na ich karanie. Ustawodawca, uznając konieczność unormowania tych kwestii, wprowadza do Ustawy o podpisie elektronicznym rozdział, zawierający katalog różnorodnych czynów zabronionych związanych zarówno z samym podpisem elektronicznym, jak i z system świadczenia usług certyfikacyjnych.

Pierwszym penalizowanym czynem jest brak zawarcia wymaganej umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom tych usług przez kwalifikowany podmiot świadczący usługi certyfikacyjne. Karę, przewidzianą w Ustawie w takim przypadku, stanowi kara grzywny w wysokości do 1 000 000 złotych[82]. Przepis ten ma na charakter przede wszystkim prewencyjny – ma zapobiegać unikaniu zawierania umów ubezpieczenia przez wystawców certyfikatów poprzez zagrożenie dotkliwą karą pieniężną. Polski system prawny nie przewiduje jednak, co do zasady, odpowiedzialności karnej osób prawnych. Niemożliwe jest więc nałożenie odpowiedzialności o charakterze karnym na jednostkę organizacyjną, odpowiedzialność może ponieść jedynie osoba fizyczna. Dlatego nasuwa się wątpliwość, czy nie mamy w tym przypadku do czynienia z karą o charakterze administracyjnym. Argumentem świadczącym przeciwko tej tezie wydaje się być brak wskazania w treści przepisu organu administracyjnego, który miałby taką karę nakładać. Jeżeli uznamy, że mamy do czynienia z normą prawnokarną, to może powstać na tym tle wątpliwość, kogo na podstawie powyższego przepisu należy ukarać – czy samą jednostkę organizacyjną, czy osobę odpowiedzialną w ramach tejże jednostki. Wskazówki udziela art. 53 Ustawy, który stanowi, że karę za większość opisanych w tym rozdziale czynów ponosi „także ten, kto dopuszcza się czynów (...), działając w imieniu lub interesie innej osoby

[80] Art. 115 § 14 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (z 1997 r. Dz. U Nr 88, poz. 553 z późn. zm.)
[81] A. Adamski „Prawo karne komputerowe”, Warszawa 2000, str. 80 i n.
[82] Art. 45 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

fizycznej, osoby prawnej lub jednostki organizacyjnej. TU Słowo „także" oznacza jednak, że ktoś jeszcze ponosi odpowiedzialność, a słowo „kto" sugeruje, że chodzi zdecydowanie o osobę fizyczną, a nie jakąkolwiek jednostkę organizacyjną. Problemu nie stwarza jedynie sytuacja, gdy podmiot świadczący usługi certyfikacyjne będzie to czynił jako osoba fizyczna. Zastrzeżenia budzi również wysokość grzywny, która wydaje się być zdecydowanie za wysoka. Rozwiązaniem dylematu byłoby stwierdzenie, że powyższy czyn stanowi po prostu wykroczenie.

Karze grzywny podlegał będzie również ten, kto świadcząc usługi certyfikacyjne, wbrew obowiązkowi określonemu w Ustawie nie informuje osoby ubiegającej się o certyfikat o warunkach uzyskania i używania certyfikatu. Kara ta jest jednak mniej dotkliwa – jej maksymalna wysokość wynosi 30 000 złotych[83]. Przepis ten umieszczono w interesie użytkowników certyfikatów, ma ich chronić przed brakiem informacji ze strony wystawcy certyfikatu. Trzeba jednak przyznać, że jest to bardzo duża dolegliwość w stosunku do wagi tego czynu.

Ustawa o podpisie elektronicznym przewiduje również surowsze kary, z karą pozbawienia wolności włącznie. Taką karę przewiduje przestępstwo polegające na składaniu bezpiecznego podpisu elektronicznego za pomocą danych służących do składania podpisu elektronicznego, które zostały przyporządkowane do innej osoby. W takim przypadku, oprócz kary grzywny, przepisy przewidują karę pozbawienia wolności do lat trzech. Możliwe jest też zastosowanie obu tych kar łącznie[84]. Problem, który się nasuwa w związku z tą regulacją, polega na odpowiedzi na pytanie, czy każde użycie cudzego podpisu powinno być karane, czy tylko to, dokonane wbrew woli właściciela podpisu. Brzmienie przepisu wyraźnie wskazuje na to, że każde użycie cudzego bezpiecznego podpisu będzie karane. Co jednak w sytuacji, gdy ktoś (np. osoba chwilowo sparaliżowana) zezwoli drugiej osobie na użycie swojego podpisu. Jest to możliwe na podstawie przepisów prawa cywilnego, jednak wydaje się, że prawo karne stoi temu na przeszkodzie, wyraźnie zabraniając używania cudzych danych służących do składania podpisu. Zakaz ten dotyczy jednak tylko bezpiecznego podpisu elektronicznego.

Taką samą karą zagrożone jest przestępstwo, które polega na kopiowaniu lub przechowywaniu danych służących do składania bezpiecznego podpisu lub poświadczenia elektronicznego lub innych dane, które mogłyby służyć do ich odtworzenia[85]. Ma to na celu zapewnienia bezpieczeństwa całego systemu przede wszystkim poprzez ochronę kluczy prywatnych tak, aby nikt, oprócz ich posiadaczy, nie mógł się nimi posługiwać. Nawet osoby tworzące te klucze

[83] Art. 46 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[84] Art. 47 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[85] Art. 48 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

w centrum certyfikacji nie mogą, po ich wytworzeniu, posiadać jakichkolwiek danych pozwalających im na ich odtworzenie.

Identyczne zagrożenie ustawowe przewidziane jest dla tego, kto, świadcząc usługi certyfikacyjne, wydaje certyfikat zawierający nieprawdziwe dane będące obligatoryjnym składnikiem certyfikatu kwalifikowanego, jak również i ten, kto umożliwia wydanie takiego certyfikatu w imieniu podmiotu świadczącego usługi certyfikacyjne. W ten sam sposób karane będzie posługiwanie się takim sfałszowanym certyfikatem. Istotą tych przepisów jest ochrona autentyczności certyfikatów[86]. Warto zwrócić uwagę na fakt, iż takiej ochronie podlegają wszystkie certyfikaty, a nie tylko kwalifikowane. Regulacja ta w znacznym stopniu pokrywa się z tą zawartą w art. 270 kodeksu karnego[87], ma jednak charakter szerszy, przede wszystkim dlatego, że nie przewiduje znamienia celu. Karane jest tu już samo wydanie, umożliwienie wydania lub posługiwanie się nieprawdziwym certyfikatem niezależnie od intencji jego wystawcy lub użytkownika.

Do naruszenia zaufania do systemu certyfikacji o podobnym charakterze dochodzi również wtedy, gdy podmiot dokonujący znakowania danych czasem „przystawia" inną datę niż rzeczywista. Podmiot świadczący usługi certyfikacyjne, który, świadcząc usługę znakowania czasem, umożliwia oznaczenie danych czasem innym niż z chwili wykonywania tej usługi oraz poświadcza elektronicznie tak powstałe dane podlega grzywnie lub karze pozbawienia wolności do lat trzech lub obu tym karom łącznie. Odpowiedzialność taką, w myśl przepisów Ustawy, poniesie jednak tylko kwalifikowany wystawca certyfikatów[88].

Jak już wcześniej wspomniano podmiot świadczący usługi certyfikacyjne ma obowiązek unieważnić certyfikat wówczas między innymi wówczas, gdy zażąda tego osoba składająca podpis elektroniczny, osoba trzecia wskazana w certyfikacie lub minister właściwy do spraw gospodarki. Ten, kto zaniecha unieważnienia certyfikatu w takich okolicznościach podlega grzywnie lub karze pozbawienia wolności do lat trzech lub obu tym karom łącznie. Obowiązek ten ciąży na podmiocie świadczącym usługi certyfikacyjne również w wielu innych sytuacjach, nie podlegają one jednak ochronie o charakterze karnym. Wydaje się, że jest to wynikiem szczególnej dbałości autorów ustawy o interesy przede wszystkim ministra do spraw gospodarki, chcących w ten sposób wzmocnić jego kompetencje.

[86] Art. 49 i art. 50 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[87] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (z 1997 r. Dz. U Nr 88, poz. 553 z późn. zm.). Art. 270 ma następującą treść: „Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa, podlega (...).".
[88] Art. 51 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

Ustawa o podpisie elektronicznym przewiduje odpowiedzialność karną za ujawnienie lub niezgodne z Ustawą wykorzystywanie informacji objętych tajemnicą, związaną ze świadczeniem usług certyfikacyjnych, przez osoby, które są zobowiązane do zachowania tej tajemnicy. Czyn taki podlega karze grzywny do 1 000 000 złotych lub karze pozbawienia wolności do lat trzech albo obu tym karom łącznie. Jeżeli jednak sprawca dopuszcza tego czynu jako podmiot świadczący usługi certyfikacyjne lub jako kontroler albo w celu osiągnięcia korzyści majątkowej lub osobistej ustawowe zagrożenie karą jest wyższe – sprawca może zostać ukarany grzywną do 5 000 000 złotych albo karą pozbawienia wolności do lat pięciu albo obu tym karom łącznie[89]. Wymiar kary, w szczególności grzywny, wydaje się być i w tym przypadku zdecydowanie za surowy. Dla porównania ten, kto ujawnia lub wykorzystuje tajemnicę bankową podlega grzywnie do 1 000 000 złotych i karze pozbawienia wolności do lat trzech[90]. Prawo bankowe nie przewiduje już formy kwalifikowanej tego przestępstwa. Porównując ustawowe zagrożenia należy dodatkowo wziąć pod uwagę, że zakres danych podlegających tajemnicy bankowej jest o wiele szerszy niż zakres danych objętych tajemnicą związaną ze świadczeniem usług certyfikacyjnych. Banki, oprócz danych osobowych, mają również dostęp do informacji o charakterze majątkowym. Ustawa o podpisie elektronicznym nie precyzuje dokładnie zakresu tajemnicy „certyfikacyjnej" – wspomina jedynie ogólnikowo o poufności danych służących do tworzenia i składania podpisu elektronicznego.

Wydaje się, iż zawarte w Ustawie przepisy o charakterze karnym będą dobrze chronić interesy odbiorców usług certyfikacyjnych. Tym niemniej nie są jednak pozbawione usterek, a niektóre z nich budzą zastrzeżenia co do surowości przewidywanych zagrożeń ustawowych. Właściwą drogą budowania zaufania do podpisów elektronicznych i zapewnienia ich bezpieczeństwa wydaje się być nie tylko drakońskie karanie tych, którzy naruszą reguły prawa, lecz również, a właściwie przede wszystkim, zbudowanie takiego systemu certyfikacji opartego na grze wolnorynkowej, który będzie samoczynnie eliminował z rynku podmiot nieuczciwe. Nie do przecenienia jest też skuteczny nadzór ze strony administracji państwowej, który nie powinien jednak przerodzić się w próby kontroli całego systemu.

[89] Art. 52 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[90] Art. 170 ust. 5 ustawy z dnia 29 sierpnia 1997 roku Prawo bankowe (z 1997 r. Dz.U. Nr 140, poz. 939 z późn. zm.).

# Rozdział 3

# Charakterystyka rozwiązań polskich na tle międzynarodowym

## 3.1. Kształtowanie się instytucji podpisu elektronicznego na świecie

Na początku lat 90-tych doszło do gwałtownego rozwoju Internetu. Medium to daje możliwość szybkiego przesyłania informacji na dowolną odległość. Początkowo źródło pochodzenia informacji nie miało dużego znaczenia. Fascynowano się ogromem zebranych wiadomości oraz ich dostępnością z każdego miejsca na Ziemi posiadającego linię telefoniczną. Stopniowo jednak okazywało się, jak ważne jest właściwe uwierzytelnianie osób przesyłających dane poprzez sieć elektroniczną. Wpływ na powstanie różnych sposobów identyfikacji podmiotów korzystających z sieci miał fakt, iż dość szybko zauważono możliwość gospodarczego wykorzystania Internetu. Dla dalszego rozwoju usług elektronicznych niezbędne okazało się stworzenie metod pozwalających zarówno na zabezpieczenie przesyłanych danych (szyfrowanie), jak też i na uwiarygodnienie ich pochodzenia. Temu ostatniemu celowi służą na przykład różnego rodzaju hasła, które otrzymujemy po zarejestrowaniu się jako użytkownicy określonych usług internetowych. Za pomocą hasła pośrednio informujemy, przykładowo, dostawcę usług o naszej tożsamości – trudno będzie innej osobie podszyć się pod nas, gdyż wówczas musiałaby wykazać się znajomością naszego hasła. Jego zgadnięcie lub przechwycenie nie jest jednak niemożliwe. Poza tym w takim przypadku nie istnieje praktyczna możliwość potwierdzenia dokładnych danych personalnych danej osoby przez drugą stronę. Brak odpowiednich sposobów uwierzytelniania kontrahenta na odległość hamował rozwój handlu elektronicznego.

Pojawiła się więc potrzeba znalezienia stosownych rozwiązań. Odpowiedzią okazał się właśnie podpis elektroniczny. Oprócz opracowania potrzebnych koncepcji konieczne stało się również stworzenie ram prawnych dla funkcjonowania tej instytucji. Stało się to oczywiście tam, gdzie wykorzystanie sieci komputerowych było największe – w Stanach Zjednoczonych Ameryki. Pierwszym stanem, który wprowadził odpowiednie regulacje był stan Utah. W 1995 roku powstała tam pierwsza na świecie ustawa o podpisie elektronicznym – *Utah Digital Signature Act*. Zawierała ona, co zrozumiałe, wiele niedociągnięć, mimo to stała się impulsem do opracowania kompleksowych rozwiązań prawnych. W ślad za nią kolejne stany USA wprowadzały do swojego ustawodawstwa instytucję podpisu elektronicznego. Ostatecznie kwestię tę postanowiono

uregulować na szczeblu federalnym. Prezydent Clinton 30 czerwca 2000 roku podpisał ustawę "Electronic Signatures in Global and National Commerce Act", która 1 października weszła w życie w Stanach Zjednoczonych[91].

Sprawą podpisu elektronicznego zajęła się również Komisja Narodów Zjednoczonych ds. Międzynarodowego Prawa Handlowego. Opracowała ona w 1996 roku Prawo Modelowe o Handlu Elektronicznym**.** Europa również nie pozostawała długo w tyle. Pierwsze regulacje wprowadzono w Niemczech – miało to miejsce 13 czerwca 1997 roku. Jej zapisy wywarły silny wpływ na ustawodawstwo innych państw europejskich, które już wkrótce rozpoczęły wprowadzanie instytucji podpisu elektronicznego do własnego ustawodawstwa. Ustawy o podpisie elektronicznym przyjęto już m.in. w Hiszpanii, Szwecji, Finlandii, Wielkiej Brytanii, Włoszech, Francji, Węgrzech, Słowacji i Czechach[92]. Duże znaczenie dla procesu legislacji w Europie miało opracowanie przez Parlament Europejski i Radę Unii Europejskiej Dyrektywy w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego[93]. Nastąpiło to 13 grudnia 1999 roku. Dyrektywa ta ustanawia ogólne warunki, którym odpowiadać powinno ustawodawstwo członków Unii tym zakresie. To przede wszystkim na jej postanowieniach wzorowane są rozwiązania dotyczące podpisu elektronicznego w krajach europejskich.

## 3.2. Regulacje Komisji Narodów Zjednoczonych ds. Międzynarodowego Prawa Handlowego

Komisja Narodów Zjednoczonych ds. Międzynarodowego Prawa Handlowego (UNCITRAL) jest organem ONZ, którego zadaniem jest opracowywanie międzynarodowych regulacji prawnych dotyczących handlu. Regulacje te nie mają wprawdzie mocy powszechnie obowiązującej, cieszą się jednak dużym autorytetem, stając się przez to ogólnie akceptowanym wzorcem rozwiązań w danej dziedzinie. Dość wcześnie UCITRAL zajął się problematyką obrotu elektronicznego. Już w 1996 roku uchwalono Prawo Modelowe o Handlu Elektronicznym. Zawiera ono wzorcowe regulacje dotyczące różnych jego aspektów, w tym również podpisu elektronicznego.

[91] *Digital Signature Law Survey*, http://rechten.kub.nl/simone/ds-lawsu.htm.
[92] *DIGITAL SIGNATURE : Inventory of international regulatory, standardisation and commercial activities*, http://europa.eu.int/ISPO/ecommerce/interaction/issues.html.
[93] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronical signature*, opublikowany w: *Official Journal of the European Communities* z 19.01.2000.

W Prawie Modelowym znajduje się tylko jeden przepis odnoszący się bezpośrednio do podpisu elektronicznego. Jest to artykuł 7, który zawiera postanowienia, które możemy uznać za definicję podpisu elektronicznego. Artykuł ten ma następujące brzmienie:

> „Kiedy prawo wymaga podpisu osoby, ten wymóg jest spełniony odnośnie do danych wiadomości jeżeli:
>
> a) jest użyta metoda do identyfikacji osoby i wskazania zgody tej osoby na informacje zawarte w danych wiadomości oraz
> b) metoda była w takim stopniu wiarygodna, w jakim jest to właściwe na potrzeby, na które dane wiadomości zostały wygenerowane lub komunikowane, w świetle wszystkich okoliczności, włączając w to stosowną umowę."

Jak wyraźnie widać regulacja ta dopuszcza każdą technikę podpisu, byleby była ona wiarygodna w takim stopniu, w jakim jest to potrzebne ze względu cel podpisu. Ocena wiarygodności zastosowanej metody, o jakiej mowa w powyższym przepisie, będzie dokonywana *ex post*, najczęściej przez organ sądowy rozstrzygający powstały spór. Jest to oczywiście bardzo ogólna, zatem i bardzo szeroka definicja podpisu elektronicznego. Jej mankamentem jest to, iż o istnieniu bądź nieistnieniu podpisu decydują w danym przypadku przesłanki o charakterze ocennym.

Zdając sobie sprawę z potrzeby szerszego uregulowania omawianej problematyki, a także z niedoskonałości dotychczasowych rozwiązań, w 1997 roku rozpoczęto pracę nad tzw. Jednolitymi Regułami dotyczącymi Podpisów Elektronicznych. Do dziś nie została opracowana ostateczna wersja, dostępny jest natomiast projekt Jednolitych Reguł[94]. Początkowo planowano dokonać odpowiednich zmian i uzupełnień w Prawie Modelowym, stwierdzono jednak, że część państw już przyjęła do swoich porządków prawnych Prawo Modelowe, a część państw była w trakcie przyjmowania, a więc jego zmiana mogłaby wywołać niepotrzebne trudności w krajach, które już przyjęły model UNCITRAL[95].

Najważniejszą zasadą ustalaną przez Jednolite Reguły jest zasada neutralności technologicznej, która jest zawarta w artykule trzecim. Jest to ogólna zasada, która w odniesieniu do podpisu elektronicznego oznacza, że żaden podpis nie może być dyskryminowany ze względu na stosowaną metodę identyfikacji elektronicznej. Oczywiście, każdy podpis powinien spełniać pewne podstawowe wymagania stawianie tej instytucji. Oznacza to również, iż przepisy prawne powinny być formułowane w taki sposób, aby jednoznacznie nie przesądzały rodzaju technologii używanej

[94] *UNCITRAL*, http://www.uncitral.org.
[95] *HOGA - Serwis prawny „Prawo komputerowe"*, Adam Tocha, http://prawo.hoga.pl/tematyczne/pr_komp_podp_uncitral.asp.

na potrzeby tej instytucji. Zasada ta ma fundamentalne znaczenie dla swobodnego rozwoju e-podpisu. Jej przejawem jest już brzmienie wspomnianego wcześniej artykułu 7 Prawa Modelowego. Wyraz swój znajduje również w wielu postanowieniach Jednolitych Reguł.

Cechą charakterystyczną Jednolitych Reguł jest to, iż w odniesieniu do podpisu elektronicznego stosują one tzw. podejście dwupoziomowe. Polega ono na tym, że na pierwszym poziomie przyznaje się niektóre skutki prawne wszystkim technikom podpisu elektronicznego, na drugim poziomie przyznaje się szerokie skutki prawne tylko technikom bardziej bezpiecznym[96]. Pierwszy poziom można odnaleźć już w artykule 7 Prawa Modelowego. Jego postanowienia zostały też inkorporowane do artykułu 6 Jednolitych Reguł, który stwierdza w paragrafie (1): „Kiedy prawo wymaga podpisu osoby, ten wymóg jest spełniony odnośnie danych wiadomości, jeżeli użyty podpis elektroniczny jest w takim stopniu wiarygodny w jakim jest to właściwe na potrzeby, na które dane wiadomości zostały wygenerowane lub komunikowane, w świetle wszystkich okoliczności, włączając w to stosowną umowę". Jest to praktycznie powtórzenie regulacji Prawa Modelowego. Paragraf (2) stwierdza natomiast, że „Paragraf (1) stosuje się, jeżeli wymóg tam zawarty jest w formie obowiązkowej lub jeżeli prawo wymienia skutki braku podpisu".

Wyodrębnienie drugiego poziomu oparte jest na brzmieniu dalszej części artykułu 6. Najbardziej istotny jest tu paragraf (4), który posiada następujące brzmienie:

> „(3) Podpis elektroniczny jest uważany za wiarygodny w celu spełnienia wymogu z paragrafu (1) jeżeli:
>
> (a) środki do tworzenia podpisu elektronicznego są, w kontekście w jakim są używane, połączone tylko z osobą podpisującego i z żadną inną osobą;
>
> (b) środki do tworzenia podpisu elektronicznego były, w czasie podpisywania, pod wyłączną kontrolą podpisującego i żadnej innej osoby;
>
> (c) jakakolwiek zmiana podpisu elektronicznego, dokonana po czasie podpisania, jest wykrywalna; oraz
>
> (d) jeżeli celem wymogu prawnego dla podpisu jest zapewnienie integralności informacji do której się odnosi, każda zmiana tej informacji jest wykrywalna."

Określa się w ten sposób wymagania stawiane podpisowi elektronicznemu. Są to: unikalność, wyłączna kontrola oraz integralność podpisu i informacji. Jeżeli zostaną spełnione powyższe warunki skutek będzie taki, że dane czynności zostaną uznane *ex ante* jako wiarygodne i jednocześnie wywołają skutki prawne takie, jak podpis ręczny.

---

[96] *HOGA - Serwis prawny „Prawo komputerowe"*, Adam Tocha, http://prawo.hoga.pl/tematyczne/pr_komp_podp_uncitral.asp

Jak widać z powyższego, zasada jest taka, że każda technologia podpisu elektronicznego użyta w celu podpisania danych wiadomości, według artykułu 6 paragraf (1) Jednolitych Reguł oraz artykułu 7 Prawa Modelowego, wywołuje skutki prawne, pod warunkiem, że była wystarczająco wiarygodna w świetle wszystkich okoliczności. To podejście nazywamy podejściem pierwszego poziomu. Tym niemniej, w Jednolitych Regułach istnieje także drugie założenie, które uprzywilejowuje techniki uznawane za szczególnie wiarygodne, bez względu na okoliczności w jakich są używane. Taki jest cel artykułu 6 paragraf (3), który ma stworzyć pewność, w czasie lub przed czasem użycia technologii podpisu cyfrowego, że użycie określonej technologii wywoła skutek prawny równoznaczny ze skutkiem podpisu ręcznego. Z tych względów paragraf (3) artykułu 6 jest kluczową regulacją Jednolitych Reguł, dostarczając więcej pewności co do skutku prawnego, niż art. 7 Prawa Modelowego o Handlu Elektronicznym[97].

Projekt Jednolitych Reguł dotyczących Podpisów Elektronicznych normuje również kwestie dotyczące odpowiedzialności podpisujących, dostawców usług certyfikacyjnych, a także osób polegających na podpisie.

### 3.3. Zgodność rozwiązań polskich z normami Unii Europejskiej w sprawie podpisu elektronicznego

Polska wkrótce ma szansę stać się jednym z członków Unii Europejskiej. Jednym z warunków przystąpienia do Unii jest harmonizacja polskiego systemu prawnego z unijnym[98]. Dotyczy to oczywiście również regulacji w dziedzinie podpisu elektronicznego. Jest to jednak niezbędne nie tylko w kontekście wstąpienia do Wspólnoty, lecz przede wszystkim ze względu na fakt, iż wymiana handlowa naszego kraju przypada w większości na kraje unijne. Zbliżenie polskich regulacji do tych, które powszechnie obowiązują w Europie Zachodniej umożliwi polskim przedsiębiorstwom sprawne funkcjonowanie w gospodarce, w której wiedza jest najważniejszym dobrem, a szybki przepływ informacji decyduje o sukcesie na rynku.

Problematykę podpisu elektronicznego w poszczególnych krajach Unii Europejskiej regulują ustawodawstwa państw członkowskich. Aby jednak zapewnić jednolitość stosowanych rozwiązań postanowiono na szczeblu unijnym sformułować ogólne warunki, którym powinny odpowiadać przepisy we wszystkich krajach. W założeniach ma to umożliwić bezpośrednią,

[97] *HOGA - Serwis prawny „Prawo komputerowe”*, Adam Tocha, http://prawo.hoga.pl/tematyczne/pr_komp_podp_uncitral.asp.

[98] Art. 68 Układu Europejskiego ustanawiającego stowarzyszenie między Rzecząpospolitą Polską, z jednej strony, a Wspólnotami Europejskimi i ich Państwami Członkowskimi, z drugiej strony, sporządzonego w Brukseli dnia 16 grudnia 1991 r. (z 1994 r. Dz.U. Nr 11, poz. 38 z późn. zm.).

wzajemną uznawalność podpisów pochodzących z różnych państw Eurolandu, w szczególności poprzez wzajemne akceptowanie certyfikatów wydanych w poszczególnych państwach. Środkiem do realizacji tych celów stała się Dyrektywa Parlamentu Europejskiego i Rady w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego (dalej: Dyrektywa)[99]. Dyrektywa ta harmonizuje przepisy prawne państw członkowskich UE w zakresie stosowania podpisu elektronicznego w obrocie prawnym. Ustanawia wspólnotowe ramy prawne dla podpisów elektronicznych i niektórych usług certyfikacyjnych. Twórcy dyrektywy mają na celu stymulowanie rozwoju w Europie handlu elektronicznego, wymiany informacji w sektorze publicznym, pomiędzy administracjami krajów członkowskich, pomiędzy administracjami a instytucjami i obywatelami w takich między innymi obszarach jak zamówienia publiczne, podatki, ubezpieczenia społeczne, ochrona zdrowia czy sądownictwo[100]. Na mocy Dyrektywy kraje członkowskie otrzymały 18 miesięcy na przystosowanie jej zaleceń do prawa narodowego. Czas na dokonanie zmian i wprowadzenie stosownych regulacji upłynął 19 lipca 2001 roku.

W świetle powyższych uwag ważne jest więc stwierdzenie, czy polska Ustawa o podpisie elektronicznym jest zgodna z unijną Dyrektywą. Istotne jest przede wszystkim to, czy regulacje w poszczególnych systemach prawnych są na tyle podobne, by można było odnaleźć ich wzajemne odpowiedniki. Twórcy polskiej Ustawy o podpisie elektronicznym już w fazie tworzenia projektu mieli na względzie przyszłe członkostwo naszego kraju w Unii Europejskiej. Mogli więc od podstaw zbudować odpowiedni system certyfikacji, zapewniający zgodność ze standardami zachodnimi. Znane bowiem już były i Dyrektywa, i stosowne ustawy obowiązujące w innych państwach, w tym również w krajach Europy Środkowo-Wschodniej. Szczegółowa analiza tej problematyki znacznie wykracza poza ramy niniejszego opracowania, dlatego też rozważania zostaną ograniczone do rozstrzygnięcia podstawowej kwestii.

Odpowiadając na powyższe pytanie od razu należy zauważyć, że już pobieżna lektura Ustawy o podpisie elektronicznym uwidacznia, że polski ustawodawca garściami czerpał z postanowień Dyrektywy. Wiele przepisów jest niemal dosłownie i w całości przeniesionych do polskiej regulacji. Dobrym przykładem jest sama definicja podpisu elektronicznego, której wersja z Ustawy została przytoczona w pierwszym rozdziale niniejszej pracy. Podpis elektroniczny według Dyrektywy to: „dane w formie elektronicznej, które dodane są do innych danych elektronicznych lub są z nimi logicznie powiązane i służą do autoryzacji”[101]. Zbieżność obu regulacji jest tu wyraźnie widoczna. Podobnie jest w szeregu innych przepisów – w szczególności dotyczących

[99] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronical signature*, opublikowany w: *Official Journal of the European Communities* z 19.01.2000.
[100] W. Marciński, *Prawo i podpis*, TELEINFO, 2000, Nr 1, http://www.teleinfo.com.pl/ti/2000/01/t09.html
[101] Ibidem, art. 2 ust. 1.

kwestii definicyjnych. Niemal cały art. 3 Ustawy o podpisie elektronicznym, w którym znajduje się tzw. słowniczek ustawy, stanowi odpowiednie tłumaczenie artykułu 2 Dyrektywy, zatytułowanego „Definicje". Fakt ten należy ocenić pozytywnie. Korzystanie z gotowych, sprawdzonych rozwiązań wydaje się być właściwsze, niż szukanie własnych, oryginalnych, które nawet gdyby okazały się pod jakimś względem lepsze, to mogłyby narazić nasz kraj na „blokadę elektroniczną" z powodu ich niezgodności z międzynarodowymi standardami.

Podobieństwa nie dotyczą tylko kwestii definicyjnych. Przepisy Ustawy nadające kształt całemu systemowi certyfikacji są wzorowane na rozwiązaniach unijnych. W Dyrektywie zapisano bodaj najważniejszą zasadę dotyczącą organizacji infrastruktury klucza publicznego, a mianowicie zasadę swobody świadczenia usług certyfikacyjnych[102]. Stanowi ona, iż państwa członkowskie Unii nie mogą uzależniać możliwości świadczenia tych usług od uzyskania wcześniejszego zezwolenia. Można jedynie wprowadzić system dobrowolnej akredytacji, czyli swego rodzaju urzędowego potwierdzenia wysokiego standardu usług. Postanowiono też, że wszelkie wymagania muszą być obiektywne, transparentne, proporcjonalne i nie dyskryminujące. Na państwa nakłada się obowiązek nadzoru. Polska Ustawa niemal w całości stosuje się do powyższej zasady, stanowiąc, że prowadzenie działalności w zakresie świadczenia usług certyfikacyjnych nie wymaga uzyskania zezwolenia, ani koncesji. Przewiduje się jedynie procedury ogólnego nadzoru nad podmiotami świadczącymi usługi certyfikacyjne[103]. Wątpliwości budzi jednak szczególnie uprzywilejowana rola Narodowego Banku Polskiego i podmiotów od niego zależnych w zakresie wydawania zaświadczeń certyfikacyjnych, co może naruszać europejskie normy dotyczące wolnej konkurencji i wspomniane postanowienia Dyrektywy.

Dyrektywa zwraca uwagę na to, aby ze względu na szybki rozwój technologiczny i globalny charakter Internetu stanowić takie regulacje, które pozostaną otwarte na różne technologie i usługi weryfikacji danych elektronicznych[104]. Sama stosuje się do własnych zaleceń świadomie unikając używania pojęcia „podpis cyfrowy", a stosując „podpis elektroniczny". Jak to już wyjaśniono w pierwszym rozdziale niniejszej pracy, nie zawęża to pojęcia e-podpisu jedynie do technik opartych o system klucza asymetrycznego, a pozwala na objęcie nim również i innych istniejących już, jak i przyszłych, sposobów elektronicznego podpisywania się. Również Ustawa posługuje się tylko pojęciem podpisu elektronicznego, czyniąc to i tak z wielką ostrożnością. Jej twórcy wręcz wolą posługiwać się takimi pojęciami jak dane, poświadczenia czy zaświadczenia elektroniczne, które

[102] Ibidem, art. 3 ust. 1.
[103] Por. art. 9 ust. 1, art. 23 oraz rozdział VII Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
[104] Por. w szczególności punkt (8) i (9) we wstępie dokumentu: *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronical signature*, opublikowanego w: *Official Journal of the European Communities* z 19.01.2000.

mają opisywać całe zjawisko, umożliwiając w ten sposób stosowanie ustawy do przyszłych, nieznanych dziś jeszcze sytuacji.

Sporo zamieszania mogłaby wprowadzić sytuacja, w której systemy certyfikacyjne poszczególnych państw przewidywałyby różne rodzaje podpisów elektronicznych, i dodatkowo, wiązałyby z nimi różne skutki prawne. Między innymi zapobieganiu takim sytuacjom ma służyć Dyrektywa, która pośrednio określa rodzaje podpisów elektronicznych. Stanowi ona, że nie są potrzebne żadne ustawowe warunki ramowe dla podpisów elektronicznych, które są używane wyłącznie w systemach opierających się na dobrowolnych cywilnoprawnych porozumieniach między określoną liczbą uczestników[105]. Tak więc można mówić o podpisie elektronicznym *sui generis*, którego istnienie jest niezależne od norm prawa, a skutki jego są takie, jakie nada mu zgodna wola umawiających się stron. Poza tym, zgodnie z Dyrektywą, normy prawne krajów Unii Europejskiej powinny zasadniczo wyróżniać dwie postacie podpisów elektronicznych:

a) podpis elektroniczny (zwykły)[106] – jego definicja została podana powyżej. Tylko podpis spełniający określone tam warunki będzie wywoływał skutki określone prawem, a więc przede wszystkim będzie on uznany przez normy prawne za podpis, chociaż nie oznacza to, że będzie równorzędny podpisowi tradycyjnemu, ani że będzie spełniał warunek formy pisemnej. Powinien być on jednak dopuszczony jako dowód w postępowaniu sądowym[107],
b) zaawansowany podpis elektroniczny[108] – jest to taki podpis, który łącznie spełnia następujące kryteria:

— jest połączony z osobą podpisującą w sposób unikalny,
— jest zdatny do identyfikacji osoby podpisującej,
— jest stworzony za pomocą środków, które znajdują się pod wyłączną kontrolą podpisującego,
— jest związany z danymi, do których się odnosi w taki sposób, że pozwala na wykrycie jakiejkolwiek zmiany treści tych danych po złożeniu podpisu.

Dyrektywa wskazuje, że zaawansowany podpis elektroniczny, aby wywoływał pełne skutki prawne powinien opierać się na kwalifikowanym certyfikacie i powinien być kreowany za pomocą bezpiecznego urządzenia tworzącego podpis. W odniesieniu do takich sygnatur państwa członkowskie powinny w swych ustawodawstwach zapewnić, aby:

[105] Ibidem, punkt (16) wstępu.
[106] Ibidem, art. 2 ust. 1.
[107] Ibidem, art. 5 ust. 2.
[108] Ibidem, art. 5 ust. 1.

a) spełniały kryteria prawne podpisu w stosunku do danych w formie elektronicznej, tak samo jak podpis ręczny spełnia kryteria w stosunku do danych umieszczanych na papierze,
b) były dopuszczalne jako dowód w postępowaniu prawnym[109].

Można stwierdzić, że pod względem rodzajów kreowanych podpisów elektronicznych polska Ustawa jest zgodna z europejską Dyrektywą. Ustawa również przewiduje podpisy zwykłe i kwalifikowane. Projekt Ustawy przewidywał pośrednio trzeci rodzaj podpisu, mianowicie taki, który miał być wydawany przez autoryzowane kwalifikowane podmioty świadczące usługi certyfikacyjne. Jednakże Senat wprowadził poprawki usuwające tę niezgodność[110].

Odpowiadając na zadane na wstępie pytanie wydaje się, że polska Ustawa o podpisie elektronicznym jest zgodna z uregulowaniami Dyrektywy Parlamentu Europejskiego i Rady w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego. Potwierdzeniem tego faktu jest opinia wydana przez Zespół Integracji Europejskiej Biura Studiów i Ekspertyz Kancelarii Sejmu w sprawie zgodności projektu Ustawy o podpisie elektronicznym z prawem Unii Europejskiej[111]. Dotyczy ona wprawdzie projektu poselskiego ustawy, a nie jej wersji końcowej, ale to właśnie na tym projekcie opiera się dzisiejszy kształt Ustawy. Opinia ta w konkluzjach stwierdza, że „(…) projekt ustawy o podpisie elektronicznym jest zgodny z obowiązującym prawem Unii Europejskiej oraz postanowieniami Układu Europejskiego". Harmonizacja obu regulacji zostanie potwierdzona w rzeczywistości po wejściu w życie polskiej Ustawy, w szczególności już po wstąpieniu Polski do Unii Europejskiej.

### 3.4. Analiza na tle rozwiązań niemieckich

Niemcy są pierwszym krajem europejskim, w którym przyjęto regulacje prawne dotyczące podpisu elektronicznego. Stało się tak dzięki uchwaleniu 22 lipca 1997 roku ustawy o usługach informacyjnych i komunikacyjnych[112]. Jej artykuł trzeci, składający się z 16 paragrafów, stanowi ustawę o podpisie elektronicznym (cyfrowym)[113]. Ustawa ta wyprzedziła nawet Dyrektywę Unii

[109] Ibidem, art. 5 ust. 1.
[110] W odniesieniu do projektu rządowego ustawy o podpisie elektronicznym zwracali na to uwagę Andrzej M. Borzyszkowski, M. Srebrny w: *Uwagi do projektów poselskiego i rządowego ustawy o podpisie elektronicznym (17.III.2001)*, http://www.ipipan.waw.pl/~marians/e-podpis/opiniaBS10319.html
[111] *Opinia w sprawie zgodności projektu Ustawy o podpisie elektronicznym z prawem Unii Europejskiej*, Biuro Studiów i Ekspertyz Kancelarii Sejmu, Zespół Integracji Europejskiej, 24.01.2001 r.

[112] *Gesetz zur Regelung Rahmenbedingungen für Informations- und Kommunikationsdienste*, 22.07.1997.
[113] ibidem, *Gesetz zur digitalen Signatur*.

Europejskiej w tej sprawie. Z tego właśnie względu wprowadzone przez nią normy nie mogły być zsynchronizowane z regulacjami ogólnoeuropejskimi. Jest to widoczne w niektórych postanowieniach tejże ustawy. Nie oznacza to oczywiście niezgodności z późniejszą Dyrektywą, niemniej jednak niemiecka ustawa jest nieco odmienna od regulacji przyjmowanych w innych krajach europejskich już po uchwaleniu Dyrektywy. Regulacje te bowiem są do siebie bardzo podobne, a nawet są w znacznej mierze identyczne. Na tym tle zauważalna jest odmienność prawa niemieckiego. Warto się więc im przyjrzeć, gdyż próby choćby lekko odmiennego ukształtowania systemu certyfikacji zasługują na uwagę. Poza tym, przepisy obowiązujące w Niemczech mają duże znaczenie dla przedsiębiorstw rozwijających handel z naszym sąsiadem.

Pierwsza różnica jest widoczna już w samym pojęciu podpisu – niemiecka ustawa posługuje się pojęciem podpisu cyfrowego, podczas gdy ustawodawstwa innych państw posługują się raczej pojęciem podpisu elektronicznego. Przez podpis cyfrowy rozumie się taki podpis, który został stworzony przy użyciu asymetrycznej pary kluczy kryptograficznych. Pojęcie to definiuje §2 pkt (1) niemieckiej ustawy. Według niej podpis cyfrowy jest pieczęcią na danych cyfrowych, który został postawiony za pomocą klucza prywatnego, i który umożliwia ustalenie posiadacza klucza podpisu i zapewnia integralność danych. Dokonuje się tego za pomocą odpowiednio powiązanego klucza publicznego zaopatrzonego w certyfikat organu certyfikacji. Jak widać, definicja ta wyraźnie ogranicza podpis w formie danych elektronicznych jedynie do takich sygnatur, które zostały stworzone i mogą zostać uwierzytelnione za pomocą pary: klucz prywatny – klucz publiczny. Podpisywanie się z użyciem innych metod nie byłoby więc uznane za podpis elektroniczny. Przykładem jest metoda biometryczna (antropometryczna), której istota sprowadza się do użycia niepowtarzalnych cech każdego człowieka, takich jak linie papilarne, obraz tęczówki oka, kształt dłoni, do identyfikacji danej osoby, a także do identyfikacji wysłanych przez nią dokumentów. W takim przypadku, w myśl definicji z niemieckiej ustawy, zależnie od sposobu wykorzystania tych cech, taki podpis nie zawsze będzie mógł być uznany za podpis cyfrowy. Może mieć to implikacje dla uznawania w Niemczech certyfikatów zagranicznych, w tym też i polskich, gdyż nasza Ustawa za podpis elektroniczny uznaje znacznie szerszy krąg zjawisk.

Kolejna różnica dotyczy budowy sytemu certyfikacji. Niemiecka ustawa wymaga tzw. licencji na świadczenie usług certyfikacyjnych. Oznacza to koncesjonowanie przez państwo działalności na tym polu. Nie jest to zgodne z wymogami Dyrektywy Unii Europejskiej, jest to również odmienne w stosunku do rozwiązań przyjętych w Polsce. W obu właśnie wymienionych przypadkach świadczenie usług certyfikacyjnych podlega zasadzie swobody podejmowania i prowadzenia działalności gospodarczej. Niemiecki system przewiduje swobodę działania podmiotów certyfikacyjnych, która ma podlegać przede wszystkim zasadom wolnej konkurencji.

Niemniej jednak samo podjęcie takiej działalności wymaga uprzedniego uzyskania odpowiedniej licencji wydawanej przez stosowny organ państwowy. Rozbieżność ta jest dość istotna, gdyż godzi ona w podstawową, ogólnie przyjętą zasadę organizacji systemu certyfikacji, jaką jest minimalizacja ingerencji organów państwowych w system certyfikacji. Dążenie do wzmocnienia roli państwa widoczne jest również już w procesie świadczenia usług. Przykładowo, uzyskanie certyfikatu możliwe jest jedynie na podstawie danych osobowych, nie można posługiwać się pseudonimem przy jego uzyskaniu. Wprawdzie można używać pseudonimu w kontaktach z innymi osobami, ale organ certyfikacyjny zawsze posiada dokładne dane użytkownika. Dodatkowo, wystawca certyfikatu jest obowiązany, na żądanie odpowiednich władz, przekazać dane dotyczące tożsamości osoby posługującej się pseudonimem, jeśli jest to konieczne w ściganiu przestępstw lub wykroczeń[114]. Takich regulacji nie zawiera polska Ustawa o podpisie elektronicznym. Nie znajdziemy w niej również tak szerokiego, jak w ustawie niemieckiej, katalogu okoliczności, które uprawniają władze do żądania zablokowania określonych certyfikatów.

Trzeba powiedzieć, że niemiecka ustawa o podpisie cyfrowym, określa skutki podpisu cyfrowego właśnie. Trudno więc orzec, co z pozostałymi sygnaturami, które wykraczają poza ramy podpisu cyfrowego, czy nawet podpisu elektronicznego. Ustawa wspomina jedynie o tym, iż „zastosowanie innej procedury podpisu cyfrowego jest możliwe, o ile podpisy cyfrowe zgodne z niniejszą ustawą nie są wymagane przez klauzule prawne”[115]. Można się domyślać, że przez „inną procedurę podpisu cyfrowego” rozumie się m.in. podpis elektroniczny. Skutki takiego podpisu nie są jednak bliżej określone. Zresztą celem ustawy nie jest szczegółowe określanie skutków prawnych, lecz „zapewnienie ogólnych warunków, w których podpisy cyfrowe będą uważane za bezpieczne, a ich fałszerstwa, a także manipulowanie podpisanymi danymi będzie możliwe w sposób pewny do stwierdzenia”[116]. Niemiecka ustawa wprowadza podpis zdigitalizowany do powszechnego obrotu, pozostawiając określenie jego znaczenia partnerom handlowym lub przepisom szczególnym. Upoważnia ona rząd federalny do wydania szeregu aktów, które mają szczegółowo określić kwestie takie jak: procedury przyznania, cofnięcia lub unieważnienia licencji organom certyfikacji, obowiązki wystawców certyfikatów, okres ważności certyfikatów czy dalsze uszczegółowienie warunków kontroli wystawców certyfikatów.

[114] J. Stokłosa, *Podpis elektroniczny można przyrównać o pieczęci*, Rzeczpospolita, 2.03.1998.
[115] § 1 pkt (2) Gesetz zur digitalen Signatur, w: Gesetz zur Regelung Rahmenbedingungen für Informations- und Kommunikationsdienste, 22.07.1997
[116] ibidem, § 1 pkt (1).

## 3.5. Inne regulacje podpisu elektronicznego

Podpis elektroniczny jest instytucją powszechnie wprowadzaną do użytku w wielu państwach na świecie. W procesie tym nie uczestniczą jedynie kraje słabo, lub w wcale nie skomputeryzowane. Instytucja ta umożliwia swobodny rozwój kontaktów, w tym przede wszystkim handlowych, z wykorzystaniem sieci komputerowych. Umożliwia to zniesienie takich barier jak granica państwowa czy odległość między kontrahentami. E-podpis zyskuje swoje miejsce właśnie w dziedzinie wymiany międzynarodowej, gdzie mocno utrudniona jest fizyczna identyfikacja kontrahenta i wysyłanych przez niego wiadomości. Dlatego też, tak ważne jest to, aby regulacje konstytuujące system podpisu elektronicznego w poszczególnych krajach były do siebie zbliżone, bowiem nie wystarczy podpisać wiadomość elektronicznie. Istotne jest i to, jakie skutki wiąże z tym podpisem zgodnie ze swoim ustawodawstwem nasz kontrahent, od którego otrzymaliśmy dane w formie zdigitalizowanej. Czy są one takie, jakie wiążą się z tą instytucją w naszym kraju? Warto na początku zadać sobie jeszcze bardziej podstawowe pytanie, a mianowicie, czy zapis elektroniczny widniejący pod dokumentem w ogóle jest podpisem elektronicznym według prawa naszego partnera? Odpowiedź na to pytanie uchronić może przed niepotrzebnymi komplikacjami. Przydatne wydaje się więc przytoczenie regulacji niektórych państw, w szczególności po to, by sprawdzić, czy różnią się one mocno od siebie. Ze względu na ograniczone ramy niniejszej pracy, za przedmiot analizy posłużą nam same definicje podpisu elektronicznego obowiązujące w wybranych krajach. Mają one podstawowe znaczenie dla rozstrzygnięcia, czy podobieństwo regulacji pozwala na zaufanie określonym podpisom[117].

Przegląd podpisów elektronicznych trzeba zacząć od Stanów Zjednoczonych Ameryki. Jest to nie tylko najbardziej skomputeryzowane państwo na świecie, ale także i miejsce powstania pierwszych przepisów dotyczących podpisu elektronicznego. Znalazły się one w ustawie stanu Utah z 1995 roku. Niezależnie od regulacji stanowych postanowiono ujednolicić stosowanie e-podpisów na szczeblu federalnym. W tym celu 24 stycznia 2000 roku uchwalono ustawę "Electronic Signatures in Global and National Commerce Act". Zaczęła ona obowiązywać 1 października 2000 roku. Ze względu na swój ponadstanowy charakter dotyczy ona kwestii, które nie występują w innych krajach. Przede wszystkim określa ona minimalne wymagania stawiane wszystkim podpisom i wystawcom certyfikatów w określonych sytuacjach niezależnie od stanu USA, a także stosunek regulacji stanowych do regulacji ogólno amerykańskich. Ustawa zawiera oczywiście

[117] Definicje przytoczone w niniejszym podrozdziale podane zostały w tłumaczeniu pochodzącym ze strony *HOGA - Serwis prawny „Prawo komputerowe”*, http://prawo.hoga.pl/tematyczne/pr_komp_podp_swiat.asp, której autorem jest Adam Tocha. Wyjątkiem są definicje z ustawy amerykańskiej oraz irlandzkiej, podane w tłumaczeniu własnym.

definicję podpisu elektronicznego. Według niej, „podpis elektroniczny oznacza elektroniczny dźwięk, symbol lub proces, dołączony lub logicznie powiązany z umową lub zapisem danych i stworzony lub użyty przez osobę z zamiarem podpisania zapisanych danych”[118]. Widać wyraźnie podobieństwo z polską definicją, która w praktyce różni się jedynie tym, iż nie ogranicza tego pojęcia do „dźwięku, symbolu lub procesu”, mówiąc szerzej o „danych w postaci elektronicznej”. Niektórzy autorzy zwracają jednak uwagę, iż polska definicja jest za szeroka – zapis amerykański może stanowić wzór do jej ograniczenia[119].

Podobne do polskiego podejście, jeśli chodzi o definicję, prezentuje irlandzka ustawa o handlu elektronicznym z 2000 roku. Według niej, „podpis elektroniczny oznacza dane w formie elektronicznej dołączone, inkorporowane lub logicznie powiązane z innymi danymi elektronicznymi, które służą jako metoda potwierdzenia autentyczności osoby od której pochodzą i które zawierają zaawansowany podpis elektroniczny.”[120]. Irlandzka ustawa używa szerokiego pojęcia e-podpisu, w którym mieści się również podpis cyfrowy. Ten ostatni nie jest tam zdefiniowany. Wprawdzie definicja podpisu elektronicznego zawarta w ustawie irlandzkiej popełnia klasyczny błąd logiczny *idem per idem*, poza tym jednak jest mocno zbliżona do polskiej, pozostając wyraźnie pod wpływem Dyrektywy Unii Europejskiej dotyczącej omawianej problematyki.

Inaczej tę kwestię normuje singapurska ustawa z 1998 roku o transakcjach elektronicznych. Osobno określa znaczenie pojęcia podpis elektroniczny, a osobno znaczenie pojęcia podpis cyfrowy. W tej ustawie podpis elektroniczny definiuje się jako litery, znaki, cyfry oraz inne symbole w formie cyfrowej dołączone lub logicznie powiązane z zapisem elektronicznym, oraz wykonywane lub przyjmowane na potrzeby potwierdzenia autentyczności lub zatwierdzenia zapisu elektronicznego[121]. Jest to szerokie określenie e-podpisu, dość zresztą zbliżone do zapisów polskich. Singapur wprowadził jednak pewne *novum* w tej dziedzinie. Ustawa o transakcjach elektronicznych konstytuuje bowiem przynajmniej cztery rodzaje podpisów. Są to:

a) podpis elektroniczny, którego definicja została przytoczona powyżej,
b) bezpieczny podpis elektroniczny, który powinien być unikalny, zdatny do identyfikacji osoby posługującej się nim, tworzony za pomocą środków pozostających pod wyłączną kontrolą takiej osoby, powinien też zapewniać integralność podpisanego dokumentu,

[118] Section 106 (5), *Electronic Signatures in Global and National Commerce Act*, 24.01.2000.
[119] Por. np. M. Łopaciński, *Analiza ustawy o podpisie elektronicznym*, http://www.vagla.pl/skrypts/podpis_elektroniczny.htm.
[120] Art. 2 pkt (1) *Electronic Commerce Bill*, Irlandia, 2000, http://prawo.hoga.pl/tematyczne/irlandia_ecommercebill2000.pdf.
[121] Art. 2 *Electronic Transactions Act*, Singapur, 1998, http://www.cca.gov.sg/eta/index.html.

c) podpis cyfrowy, który jest definiowany jako podpis elektroniczny składający się z transformacji zapisu elektronicznego przy użyciu kryptosystemu asymetrycznego oraz funkcji hash'ującej *(tworzącej jednokierunkowy skrót wiadomości – przyp. aut.)* w ten sposób, że osoba, która posiada początkowy przetransformowany w odwrotną stronę zapis elektroniczny oraz klucz publiczny osoby podpisującej, może dokładnie określić:

— czy transformacja była wytworzona przy użyciu klucza prywatnego zgodnego z kluczem publicznym osoby podpisującej, i

— czy początkowy zapis elektroniczny był zmieniany od czasu wytworzenia transformacji,

d) bezpieczny podpis cyfrowy, czyli taki, który został postawiony w czasie swojej ważności, został prawidłowo zweryfikowany przez klucz publiczny zawarty w certyfikacie, i przede wszystkim został wydany na podstawie godnego zaufania certyfikatu, któremu stawia się szereg dodatkowych wymogów.

Rozwiązanie przyjęte przez Singapur mnoży byty, określając zarówno czym jest podpis cyfrowy, a czym elektroniczny. To niespotykane rozwiązanie jest o tyle ważne, iż pozwala na lepsze zrozumienie różnić pomiędzy obu rodzajami podpisów. Niemniej jednak praktyczne zastosowanie takich zapisów może okazać się dość skomplikowane, choć z drugiej strony zapewnia aktualność takiej ustawy na wiele lat, bez potrzeby nadmiernego rozszerzania pojęcia podpisu elektronicznego, jak ma to miejsce w Polsce.

Stosunkowo odmienne podejście do podpisu elektronicznego zaprezentowali Brytyjczycy w swojej ustawie o komunikacji elektronicznej z 2000 roku. Według niej podpisem elektronicznym jest wszystko w formie elektronicznej, jeżeli:

a) jest inkorporowane lub w inny sposób logicznie związane z komunikacją elektroniczną lub elektronicznymi danymi, oraz

b) inkorporacja lub związanie wyraża się w celu ustalenia autentyczności komunikacji lub danych, lub integralności komunikacji lub danych, lub jednego i drugiego.

W ustawie brytyjskiej widać oryginalne rozwiązania w zakresie definicji e-podpisu, mimo że wciąż chodzi o to samo, i sens nadal jest zbliżony. Niewątpliwie jest to jedna z najszerszych, spotykanych definicji podpisu elektronicznego, którym jest „wszystko w formie elektronicznej", jeżeli spełnia powyższe, mocno ogólne warunki. Wydaje się, iż nawet zwykły podpis pod e-mailem, typu „John Smith", według tej regulacji powinien być uznany za podpis elektroniczny. Na tym tle trzeba zaznaczyć, iż ten sam zarzut można postawić i polskiej Ustawie, która wykazuje dużą zgodność, nawet w tym negatywnym sensie, z ustawą brytyjską.

Z dosyć pobieżnego przeglądu sposobów określenia podpisu elektronicznego wyraźnie wynika, że regulacje poszczególnych państw są do siebie mocno zbliżone, przynajmniej jeśli chodzi o kwestie definicyjne. Nieco większe różnice można zaobserwować, jeśli chodzi o skutki prawne przyznawane poszczególnym podpisom. Znaczące rozbieżności pojawiają się dopiero na etapie organizacji systemu certyfikacji. Rozwiązania wahają się tu od pozostawienia bardzo dużej swobody podmiotom świadczącym usługi certyfikacyjne i ograniczeniem roli państwa jedynie do nadzoru nad całym systemem, do bardzo silnej reglamentacji ze strony państwa, które czasem wręcz przejmuje w swoje ręce wystawianie certyfikatów.

# ZAKOŃCZENIE

Uczestnictwo w nowoczesnej gospodarce wymaga sprawnych narzędzi. Jednym z nich jest podpis elektroniczny. Funkcjonuje on w określonych uwarunkowaniach ekonomicznych i w danej infrastrukturze prawnej. Dlatego też tematem niniejszej pracy są ekonomiczne i prawne aspekty podpisu elektronicznego. Jej celem było omówienie i zestawienie w jednej pracy technicznych i prawnych zasad działania podpisu elektronicznego oraz wskazanie korzyści, kosztów oraz możliwych problemów z nim związanych.

Przy pisaniu niniejszej pracy wykorzystano możliwie szeroki materiał źródłowy. Oparto się zarówno na opracowaniach książkowych czy prasowych, jak też i na informacjach elektronicznych pochodzących z Internetu. Wiele istotnych wiadomości zaczerpnięto z internetowych materiałów i serwisów obcojęzycznych. Medium to zostało wykorzystane także przy zbieraniu danych źródłowych pochodzących od wystawców certyfikatów. Wszystkie zebrane w powyższy sposób informacje poddano krytycznej analizie, a następnie uporządkowano i zestawiono w sposób umożliwiający zrozumienie tej istotnej, a zarazem dość skomplikowanej problematyki.

W pierwszym rozdziale omówiono szczegółowo zasady działania podpisu elektronicznego oraz całego systemu certyfikacji. Wskazano również korzyści i koszty stosowania podpisu dla banków. Rozdział drugi pozwolił na opisanie ram prawnych stworzonych przez Ustawę o podpisie elektronicznym. Zawarto w nim przede wszystkim opis skutków prawnych stosowania podpisu elektronicznego oraz prawne zasady świadczenia usług certyfikacyjnych. W ostatnim rozdziale zawarto analizę polskiego sposobu ukształtowania instytucji podpisu elektronicznego na tle rozwiązań międzynarodowych. Omówiono w nim kwestię zgodności polskiego ustawodawstwa z wytycznymi Unii Europejskiej oraz wskazana na podobieństwa i różnice w regulacjach innych krajów i organizacji międzynarodowych w stosunku do regulacji polskiej.

Najtrudniejszym zadaniem niniejszej pracy było zdecydowanie jasne i zwięzłe przedstawienie zasad działania podpisu elektronicznego z uwzględnieniem rygorów stawianych pracy naukowej. Podstawowa trudność polegała bowiem na konieczności zdefiniowania i wyjaśnienia już na samym początku pojęć, których stopniowe przybliżanie dokonywane było na przestrzeni całego rozdziału pierwszego. Podanie precyzyjnej definicji zupełnie jeszcze nie znanej w Polsce instytucji podpisu elektronicznego mógł spowodować zupełny brak zrozumienia ze strony czytelnika. Z drugiej strony rezygnacja z precyzyjnej definicji na rzecz przybliżonego opisu narażała pracę na zarzut braku naukowej ścisłości. Zdaniem Autora, udało się, podając precyzyjną definicję, uniknąć związanego z tym niezrozumienia, dzięki jednoczesnym przybliżonym

wyjaśnieniom dotyczącym istoty podpisu elektronicznego. Wadą przyjętego rozwiązania jest zaburzenie przyjętej konstrukcji pierwszego rozdziału, ze względu na wprowadzenie już na początku pojęć, które w całości są omówione dopiero w przynależnym im miejscu.

Powstanie pierwszych w Polsce podmiotów świadczących usługi certyfikacyjne pozwoliło na przeprowadzenie analizy kosztów stosowania podpisu elektronicznego. Jednak ze względu na początkową fazę ich działalności oraz tajemnicę handlową przeprowadzanych transakcji nie można było dokonanie dokładnych całościowych wyliczeń. Oparto się więc na danych podawanych przez wystawców do publicznej wiadomości. Przyspieszenie prac legislacyjnych nad Ustawą o podpisie elektronicznym sprawiło, iż możliwe stało się włączenie do niniejszej pracy omówienia reguł prawnych, według których podpis elektroniczny będzie funkcjonował w Polsce. Ustawa zacznie obowiązywać dopiero w 2002 roku, dlatego też analiza prawna ma charakter czysto teoretyczny.

Należy stwierdzić, iż wiele z problemów, w tym w szczególności prawnych, jedynie zasygnalizowano, a niektóre całkowicie pominięto. Stało się tak ze względu na konieczność utrzymania w przyzwoitych ramach rozmiaru niniejszej pracy. Dlatego trzeba podkreślić, iż praca ta nie pretenduje do miana całościowego ujęcia omawianej problematyki.

# BIBLIOGRAFIA

## WYKAZ WYKORZYSTANYCH PUBLIKACJI


1) Adamski, A., *Prawo karne komputerowe*, Warszawa 2000.
2) Ahuja, V., *Bezpieczeństwo w sieciach – Internet, Intranet, Firewall*, Warszawa 1997.
3) Barta, J., Markiewicz, R., *Internet a Prawo*, Kraków 1998.
4) Bartosiewicz, M., *Bity Twojego podpisu*, ENTER, 2001, Nr 5.
5) Grzeszak A., *Podpisel*, Polityka, 2001, Nr 7.
6) McFredries, P., *E-mail nie tylko dla orłów*, Warszawa 1996.
7) Schneider, B., *Kryptografia dla praktyków*, Warszawa 1995.
8) Sitnicki, I., Srebrny M., *Błądzenie w pomysłach*, Rzeczpospolita, 10.02.2001.
9) Sitnicki, I., Srebrny M., *Jak podpisuje się świat*, Rzeczpospolita, 9.02.2001.
10) Sitnicki, I., Srebrny M., *Nie taki diabeł straszny, jak go malują*, Rzeczpospolita, 8.02.2001.
11) Stokłosa, J., *Podpis elektroniczny można przyrównać o pieczęci*, Rzeczpospolita, 2.03.1998.
12) Zombirt, J., (oprac.), *E-zakupy za odciski palców*, BANK, 2000, Nr 2.

# WYKAZ WYKORZYSTANYCH MATERIAŁÓW INTERNETOWYCH


13) *DIGITAL SIGNATURE : Inventory of international regulatory, standardisation and commercial activities*, http://europa.eu.int/ISPO/ecommerce/interaction/issues.html
14) *Digital Signature Law Survey*, http://rechten.kub.nl/simone/ds-lawsu.htm
15) *ICRI: Projects: DigiSig Links*, *Interdisciplinary Centre for Law & Information Technology*, http://www.law.kuleuven.ac.be/icri/projects/digisig_lb_eng.htm
16) *BiznesNet.pl – Centrum Polskiego eBiznesu*, http://www.biznesnet.pl/index.phtml?pg=wywiadownia&a=3400
17) *Certum*, http://www.certum.pl
18) *HOGA - Serwis prawny „Prawo komputerowe”*, Adam Tocha, http://prawo.hoga.pl/tematyczne/pr_komp_podp_uncitral.asp
19) *HOGA - Serwis prawny „Prawo komputerowe”*, Adam Tocha, http://prawo.hoga.pl/tematyczne/pr_komp_podp_swiat.asp
20) *NETLAW.PL: wortal prawniczy Radosława Chmury*, http://www.netlaw.pl/e-podpis/index.html
21) *Signet*, http://www.signet.pl
22) *UNCITRAL*, http://www.uncitral.org
23) *VaGla – Prawo i Internet*, http://www.vagla.pl/podpis/
24) *Wielka Internetowa Encyklopedia Multimedialna*, http://www.wiem.onet.pl
25) Borzyszkowski, A. M., Srebrny M., *Uwagi do projektów poselskiego i rządowego ustawy o podpisie elektronicznym (17.III.2001)*, http://www.ipipan.waw.pl/~marians/e-podpis/opiniaBS10319.html
26) Król, A., *Zawarcie umowy w internecie według kodeksu cywilnego*, http://www.prometeus.com.pl/prawo/
27) Łopaciński, M., *Analiza ustawy o podpisie elektronicznym*, http://www.vagla.pl/skrypts/podpis_elektroniczny.htm
28) Marciński, W., *Prawo i podpis*, TELEINFO, 2000, Nr 1, http://www.teleinfo.com.pl/ti/2000/01/t09.html
29) PKO BP S.A., *Referencja dla Unizeto Sp. z o.o.*, http://www.certum.pl/pl/programy_partnerskie/referencje/pkobp.html

30) Szyndzielorz, P., *Elektroniczna forma czynności prawnych*, VaGla – Prawo i Internet, http://www.vagla.pl/podpis/

## WYKAZ ŹRÓDEŁ PRAWA


1) Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).
2) Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (z 1964 r. Dz.U. Nr 16, poz. 93; zm. z 1971 r. Dz. U. Nr 27, poz. 252; z 1976 r. Dz. U. Nr 19, poz. 122; z 1982r. Dz. U. Nr 11, poz. 81; z 1982 r. Dz. U. Nr 19, poz. 147; z 1982 r. Dz. U. Nr 30, poz. 210; z 1984 r. Dz. U. Nr 45, poz. 242; z 1985 r. Dz. U. Nr 22, poz. 99; z 1989 r. Dz. U. Nr 3, poz. 11; z 1989 r. Dz. U. Nr 33, poz. 175; z 1990 r. Dz. U. Nr 34, poz. 198; z 1990 r. Dz. U. Nr 55, poz. 321; z 1990 r. Dz. U. Nr 79, poz. 464; z 1991 r. Dz. U. Nr 107, poz. 464; z 1991 r. Dz. U. Nr 115, poz. 496; z 1993r. Dz. U. Nr 17, poz. 78; z 1994 r. Dz. U. Nr 27, poz. 96; z 1994 r. Dz. U. Nr 85, poz. 388; z 1994 r. Dz. U. Nr 105, poz. 509; z 1995 r. Dz. U. Nr 83, poz. 417; z 1995 r. Dz. U. Nr 141, poz. 692; z 1996 r. Dz. U. Nr 114, poz 542; z 1996 r. Dz. U. Nr 114, poz. 542; z 1996 r. Dz. U. Nr 139, poz. 646; z 1996 r. Dz. U. Nr 149, poz. 703; z 1997 r. Dz. U. Nr 43, poz. 272; z 1997 r. Dz. U. Nr 115, poz. 741; z 1997 r. Dz. U. Nr 117, poz. 751; z 1997 r. Dz. U. Nr 157, poz. 1040; z 1998 r. Dz. U. Nr 117, poz. 758; z 1998 r. Dz. U. Nr 106, poz. 668; z 1999 r. Dz. U. Nr 52 poz. 532; z 2000 r. Dz. U. Nr 22, poz. 271; z 2000 r. Dz. U. Nr 74, poz. 855; z 2000 r. Dz. U. Nr 74, poz. 857; z 2000 r. Dz. U. Nr 88, poz. 983; z 2000 r. Dz. U. Nr 114, poz. 1191; z 2001 r. Dz. U. Nr 11, poz. 91)
3) Ustawa z dnia 29 sierpnia 1997 roku Prawo bankowe (z 1997 r. Dz.U. Nr 140, poz. 939; zm. z 1998 r. Dz. U. Nr 162, poz. 1118; z 1998 r. Dz. U. Nr 160, poz. 1063; z 1999r. Dz. U. Nr 11, poz. 95; z 1999 r. Dz. U. Nr 40, poz. 399; z 2000 r. Dz. U. Nr 94, poz. 1037; z 2000 r. Dz. U. Nr 122, poz. 1316; z 2000 r. Dz. U. Nr 114, poz. 1191; z 2000 r. Dz. U. Nr 93, poz. 1027; z 2000 r. Dz. U. Nr 116, poz. 1216; z 2000 r. Dz. U. Nr 119, poz. 1252; z 2001 r. Dz. U. Nr 8, poz. 64)
4) Układ Europejski ustanawiający stowarzyszenie między Rzecząpospolitą Polską, z jednej strony, a Wspólnotami Europejskimi i ich Państwami Członkowskimi, z drugiej strony, sporządzony w Brukseli dnia 16 grudnia 1991 r. (z 1994 r. Dz.U. Nr 11, poz. 38; zm. z 1995 r. Dz. U. Nr 63, poz. 326; z 1995 r. Dz. U. Nr 63, poz. 324; z 1997r. M.P. Nr 10, poz. 74; z 1997 r. Dz. U. Nr 104, poz. 662; z 1999 r. Dz. U. Nr 30, poz. 288; z 2000 r. Dz. U. Nr 21, poz. 263)
5) Ustawa z dnia 23 grudnia 1994 roku o Najwyższej Izbie Kontroli (z 1995 r. Dz.U. Nr 13, poz. 59; zm. z 1996 r. Dz. U. Nr 64, poz. 315; z 1996 r. Dz. U. Nr 89, poz. 402; z 1997r. Dz. U. Nr 79, poz. 484; z 1997 r. Dz. U. Nr 96, poz. 589; z 1997 r. Dz. U. Nr 121, poz. 770; z 1997 r.

Dz. U. Nr 133, poz. 883; z 1997 r. Dz. U. Nr 28, poz. 153; z 1998 r. Dz. U. Nr 148, poz. 966; z 1998 r. Dz. U. Nr 162, poz. 1116; z 1998 r. Dz. U. Nr 162, poz. 1126; z 1998 r. Dz. U. Nr 155, poz. 1016; z 2000 r. Dz. U. Nr 60, poz. 704)

# WYKAZ POZOSTAŁYCH ŹRÓDEŁ


1) *Opinia w sprawie zgodności projektu Ustawy o podpisie elektronicznym z prawem Unii Europejskiej*, Biuro Studiów i Ekspertyz Kancelarii Sejmu, Zespół Integracji Europejskiej, 24.01.2001 r.
2) *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronical signature*, opublikowany w: *Official Journal of the European Communities* z 19.01.2000.
3) *Electronic Commerce Bill*, Irlandia, 2000, http://prawo.hoga.pl/tematyczne/irlandia_ecommercebill2000.pdf
4) *Electronic Signatures in Global and National Commerce Act*, USA, 24.01.2000
5) *Electronic Transactions Act*, Singapur, 1998, http://www.cca.gov.sg/eta/index.html
6) *Gesetz zur digitalen Signatur*, w: *Gesetz zur Regelung Rahmenbedingungen für Informations- und Kommunikationsdienste*, 22.07.1997
7) *Gesetz zur Regelung Rahmenbedingungen für Informations- und Kommunikationsdienste*, 22.07.1997
8) Poselski projekt ustawy o podpisie elektronicznym, złożony przez posłów dnia 21.12.2000
9) Sprawozdanie Sejmowej Komisji Transportu i Łączności z rozpatrzenia poselskiego i rządowego projektu ustawy o podpisie elektronicznym wygłoszone w Sejmie przez posła Karola Działoszyńskiego w dniu 19 lipca 2001 r.
10) Uzasadnienie do poselskiego projektu ustawy o podpisie elektronicznym złożonego przez posłów dnia 21.12.2000
11) Wstępny rządowy projekt ustawy o podpisie elektronicznym z dnia 29.11.1999

# SPIS SCHEMATÓW

# SPIS TABEL