

Uzasadnienie

Niniejsza ustawa zastępuje ustawę z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.). Celem przedmiotowej regulacji jest ułatwienie stosowania podpisu elektronicznego jako występującego w różnych postaciach i na różnych poziomach bezpieczeństwa mechanizmu uwierzytelnienia w elektronicznym obrocie prawnym. Ustawa przewiduje rozszerzenie listy usług certyfikacyjnych, a zwłaszcza katalogu dostępnych rodzajów podpisu elektronicznego, co umożliwi lepsze dostosowanie narzędzi oraz ich ceny do potrzeb administracji publicznej oraz przedsiębiorców. Podpisy elektroniczne będą mogły być składane zarówno przez osoby fizyczne, jak i osoby prawne lub jednostki organizacyjne, przy zastosowaniu lub bez zastosowania bezpiecznego urządzenia oraz w oparciu o certyfikat zwykły lub certyfikat kwalifikowany. Założeniem ustawodawcy jest zapewnienie ustawy o charakterze narzędziowym, która umożliwi elastyczne przyporządkowanie skutków prawnych dla poszczególnych rodzajów e-podpisu przez inne akty prawne z zakresu administracji lub gospodarki. W ustawie o podpisach elektronicznych skutki prawne nowych narzędzi powinny być uregulowane tylko w takim zakresie, w jakim jest to niezbędne z punktu widzenia dyrektywy lub nie budzi zasadniczych wątpliwości. Funkcjonowanie obecnie wielu z regulowanych przedmiotowymi przepisami usług certyfikacyjnych w obrocie prawnym przemawia za wprowadzeniem jedynie niezbędnych zmian w odniesieniu do narzędzi istniejących.

Względem uprzednio obowiązującej ustawy z dnia 18 września 2001 r. o podpisie elektronicznym rozszerzone zostało pojęcie „podpisującego”, które obecnie obejmuje zarówno osoby fizyczne jak i inne podmioty, w tym także podmioty świadczące usługi certyfikacyjne. Wprowadzenie nowego narzędzia w postaci podpisu zaawansowanego usprawni obrót gospodarczy oraz pracę administracji publicznej. Dotychczas jedynym prawnie uregulowanym rodzajem podpisu zaawansowanego w naszym kraju był bezpieczny podpis elektroniczny weryfikowany przy pomocy certyfikatu kwalifikowanego. Korzystanie z tej usługi jest dotychczas najbezpieczniejszym ale zarazem najdroższym rozwiązaniem ze względu na konieczność korzystania z bezpiecznych urządzeń do składania podpisu elektronicznego. Nowe definicje podpisującego, podpisu elektronicznego oraz podpisu zaawansowanego usuwają istniejące w obowiązującej ustawie zawężenia względem definicji zawartych w art. 2 ust. 1 i 2 Dyrektywy Parlamentu Europejskiego i Rady z dnia 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (99/93/WE). Analogiczne zmiany w styczniu 2008 r. wprowadziła Republika Austrii, której ustawa o podpisie elektronicznym przewidywała uprzednio jedynie tzw. „zwykły” podpis elektroniczny oraz bezpieczny podpis elektroniczny składany z wyłączeniem osób prawnych. W obecnej ustawie utrzymane zostały podstawowe rodzaje usług certyfikacyjnych przewidzianych obowiązującymi przepisami. W nowej ustawie o podpisach elektronicznych śladem rozwiązań austriackich odchodzi się od pojęcia bezpiecznego podpisu elektronicznego na rzecz jego odpowiednika w nomenklaturze wspólnotowej, którym jest podpis kwalifikowany.

W art. 2 ust. 1 dokonana została zmiana w definicji tzw. podpisu zwykłego, która obecnie w ślad za dyrektywą odwołuje się w miejsce dotychczas stosowanego pojęcia „identyfikacji” do terminu „metody uwierzytelnienia”. Zmiana w definicji podpisu elektronicznego nie wpłynie na praktykę funkcjonowania tego narzędzia. Ustawa w ślad za dyrektywą nie definiuje pojęcia uwierzytelnienia, gdyż punktem odniesienia w tym zakresie są dokumenty standaryzacyjne oraz bieżący stan wiedzy informatycznej. Dążność do ścisłego

zdefiniowania wszystkich pojęć mogłaby prowadzić do usztywnienia przepisów i zmuszać w przyszłości do wielokrotnych zmian przepisów ustawowych. W świetle wiedzy informatycznej jedną z metod uwierzytelnienia jest podpis cyfrowy (digital signature), oparty na asymetrycznej technice kryptograficznej (para kluczy kryptograficznych: publiczny i prywatny). Dzięki matematycznej zależności między kluczami kryptograficznymi, weryfikacja podpisu cyfrowego umożliwia uwierzytelnienie, czyli potwierdzenie, że podpisujący jest tym, za kogo się podaje. Przełożeniem koncepcji podpisu cyfrowego opartego o zaufaną stronę trzecią na prawną terminologię dyrektywy 99/93/WE jest pojęcie zaawansowanego podpisu elektronicznego. Ten rodzaj podpisu elektronicznego stał się podstawą do zdefiniowania w ustawie jego pochodnych w postaci podpisu kwalifikowanego, podpisu urzędowego oraz pieczęci elektronicznej.

W art. 5 ust. 1 dyrektywy mowa jest o rodzaju podpisu, który w dyrektywie nie otrzymał własnej nazwy, a który w nomenklaturze wspólnotowej jest powszechnie określany jako „kwalifikowany podpis elektroniczny”. Chodzi o zaawansowany podpis elektroniczny oparty na kwalifikowanym certyfikacie i złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu. Mimo iż dyrektywa nie stanowi, że podpis elektroniczny musi dotyczyć osoby fizycznej, składającym kwalifikowany podpis elektroniczny może być tylko osoba fizyczna, ponieważ podpis taki uważany jest za równoważny z podpisem odręcznym.

Dla potrzeb elektronicznych dokumentów tożsamości ustawa wprowadza podpis urzędowy weryfikowany przy pomocy certyfikatów urzędowych. Jakkolwiek ten rodzaj zaawansowanego podpisu elektronicznego nie jest wymieniony w dyrektywie wspólnotowej to pamiętać należy, że dyrektywa wspólnotowa jako dyrektywa wymagań minimalnych nie zakazuje państwom członkowskim tworzenia funkcjonalnie wyodrębnionych rodzajów podpisu elektronicznego. Ogłoszony w ostatnim czasie przez Komisję Europejską Plan działań w zakresie e-Podpisu i e-Identyfikacji wskazuje jednoznacznie, że przyszłość podpisu elektronicznego jest ściśle związana z elektronicznymi dokumentami identyfikacyjnymi. Profil certyfikatów urzędowych określony zostanie przepisami ministra właściwego ds. informatyzacji. W świetle rozwiązań innych państw członkowskich podpisy składane przy pomocy elektronicznych dokumentów identyfikacyjnych mogą być weryfikowane zarówno przez certyfikaty zwykłe, jak i certyfikaty kwalifikowane. Bardzo często z dokumentem eID powiązany jest zarówno certyfikat zwykły jak i kwalifikowany, a w warstwie procesorowej dokumentu znajdują się klucze powiązane z oboma rodzajami certyfikatów. Dokument elektroniczny może zawierać klucze służące zarówno do identyfikacji w systemach e-government, jak i podpisywania dokumentów. Wykorzystanie w elektronicznych dokumentach identyfikacyjnych certyfikatów kwalifikowanych może pozwolić na zapewnienie uznawania podpisów złożonych przy pomocy krajowych dokumentów identyfikacyjnych w innych państwach. Uregulowania w zakresie certyfikatów urzędowych mogą umożliwić zastosowanie w dokumentach eID zarówno certyfikatów zwykłych, jak i kwalifikowanych. Szczegółowe skutki podpisów urzędowych określone zostaną w przepisach podległych ministrowi właściwemu ds. informatyzacji w trakcie prac nad elektronicznymi dowodami tożsamości.

Wprowadzenie definicji pieczęci elektronicznej (ang. „data stamping”- dosł. stemplowanie danych) może na celu zapewnienia nowego narzędzia opartego o podpis zaawansowany podmiotów innych aniżeli osoba fizyczna. Narzędzie to jest przeznaczone do składania w sposób zautomatyzowany i przeznaczone do podniesienia wiarygodności i integralności przesyłanych wiadomości. Pieczęć elektroniczna ma być generowana

automatycznie przez systemy informatyczne. W praktyce dotyczyć może takich czynności jak potwierdzanie faktu wpłynięcia dokumentów elektronicznych, potwierdzania przyjęcia zamówienia lub ewentualnie przy generowaniu faktur elektronicznych. Pod względem algorytmu kryptograficznego pieczęć elektroniczna nie musi niczym się różnić od podpisu elektronicznego. Pieczęć elektroniczna będzie weryfikowana przy pomocy zwykłego certyfikatu, gdyż w większości krajów Unii Europejskiej certyfikaty kwalifikowane wydawane są wyłącznie osobom fizycznym. W zależności od potrzeb administracji oraz gospodarki zastosowanie i skutki prawne tego narzędzia regulowane będą innymi ustawami.

Przyjęte w ustawie definicje podpisującego oraz pieczęci elektronicznej pozwolą zrezygnować z definicji „poświadczenie elektroniczne” i „zaświadczenie elektroniczne”, a także pozwolą zapewnić ciągłość funkcjonowania istniejącej obecnie krajowej infrastruktury klucza publicznego. Nowa definicja certyfikatu zawarta w art. 3 ust. 1 konsumuje dotychczasowe pojęcia zaświadczeń i poświadczeń certyfikacyjnych. Pojęcie certyfikatu w świetle europejskich dokumentów standaryzacyjnych obejmuje zarówno certyfikat wydawany podpisującym jak i zaświadczenie certyfikacyjne. W sensie wymogów technicznych oba pojęcia są tożsame. Pojęcia zaświadczenia certyfikacyjnego” i „poświadczenia elektronicznego” nie występują w dyrektywie wspólnotowej i zamieszczenie ich w ustawie jest nadmiarowe. Normy CWA także w odniesieniu do urzędów certyfikujących posługują się pojęciem „certificate CA”, czyli po prostu certyfikatu urzędu certyfikującego. Art. 3 ust. 1 zastępuje dotychczas stosowane pojęcie zaświadczenia certyfikacyjnego pojęciem certyfikatu. Podkreślić należy, że ustawa utrzymuje istniejącą architekturę krajowej infrastruktury klucza publicznego opartą o krajowy urząd certyfikujący i nie wprowadza crosscertyfikacji pomiędzy urzędami. Wiarygodność podmiotów kwalifikowanych będzie nadal ugruntowana na certyfikacie wydanym przez właściwy organ państwa. Dotychczas „zaświadczenie elektroniczne” będzie w świetle nowej nomenklatury certyfikatem ministra właściwego ds. gospodarki.

Kwalifikowana i zwykła usługa znakowania czasem oparta została o pojęcie czasu urzędowego i pozwala na jego wystawianie nie tylko podmiotom kwalifikowanym. Zwykła usługa znakowania czasem może być świadczona nie tylko przez podmioty kwalifikowane w oparciu o wybrane przez sam podmiot wiarygodne wzorce czasu. Kwalifikowana usługa znakowania czasem musi być świadczona wyłącznie przez podmioty kwalifikowane oraz w oparciu o wzorce czasu urzędowego. Wyłącznie kwalifikowana postać znakowania czasem wywoływać będzie jak dotychczas skutki daty pewnej w rozumieniu kodeksu cywilnego. Znakowanie czasem nie jest rozwiązaniem ujednoczonym we Wspólnocie i każde z państw we własnym zakresie decyduje o tym jakie usługi uznaje za kwalifikowane w zakresie znakowania czasem. W Polsce przyjęto rozwiązanie polegające na powiązaniu z czasem urzędowym i czasem UTC(PL) przy zachowaniu wymogów synchronizacji do tych czasów z określoną dokładnością. Wymagane dokładności synchronizacji oraz pozostałe warunki techniczne związane z zapewnieniem wiarygodności czasu stosowanego w tych usługach podane będą w rozporządzeniu wykonawczym do tej ustawy. W przypadku znakowania czasem utrzymany zostaje wymóg dokładności synchronizacji do jednej sekundy, przy czym wprowadzony zostaje obowiązek weryfikacji technicznej spełnienia tego wymogu.

Między kwalifikowanym, a niekwalifikowanym znakowaniem czasu technicznie różnica polega na różnym obowiązkowi częstości weryfikacji wymaganej dokładności synchronizacji. Zakłada się wykorzystanie w tym celu wymiany pakietu NTP między serwerami czasu z zastosowaniem mechanizmów autoryzacji i autentyfikacji. Graniczny maksymalny okres siedmiu dni między kolejnymi weryfikacjami dokładności synchronizacji

w kwalifikowanym znakowaniu czasem, przy zastosowaniu odpowiednich pomocniczych wzorców czasu, zapewni w pełni dostępność tej usługi bez konieczności częstej weryfikacji wymaganej dokładności synchronizacji. Nie będzie to, zatem stanowiło utrudnienia dla świadczenia usług znakowania czasem, natomiast zdecydowanie zwiększy zaufanie do tych usług przez odejście od samodeklaracji w zakresie dokładności czasu stosowanego przez podmioty przy realizacji tych usług. Czas urzędowy jest jednoznacznie powiązany z czasem UTC(PL) – główną polską fizyczną realizacją międzynarodowego czasu UTC. Utrzymywanie dokładności synchronizacji czasu UTC(PL) do czasu UTC poniżej jednej dziesięciomilionowej części sekundy (poniżej 100 ns) w zupełności pozwala na wykorzystanie czasu urzędowego i czasu UTC (PL) do zagwarantowania rzetelności i wiarygodności czasu stosowanego w podpisie elektronicznym.

Zmieniona względem poprzedniej ustawy definicja „danych do weryfikacji podpisu elektronicznego” odzwierciedla okoliczność, że dane do weryfikacji podpisu elektronicznego pozwalają, oprócz identyfikacji podpisującego, zweryfikować inne istotne cechy podpisu (np. powiązanie podpisu z danymi do których został dołączony). Nowa definicja „urządzenia do składania podpisu elektronicznego” (art. 2 pkt 13) wprowadza zgodnie z analogiczną definicją zawartą w dyrektywie łącznik „lub” pomiędzy komponentem programistycznym i sprzętowym. Zniesiona zostaje zbędna definicja „bezpiecznego urządzenia służącego do weryfikacji podpisu elektronicznego”. Dyrektywa nie posługuje się pojęciem „bezpiecznych urządzeń do weryfikacji podpisu elektronicznego” odnosząc sformułowanie „bezpieczne urządzenia” jedynie do urządzeń generujących podpisy. Takie podejście posiada charakter zamierzony i wynika z technologii procesów generowania i weryfikacji. Poprawka zawarta w art. 2 pkt 15 nadaje pojęciu „urządzenie do weryfikacji podpisu” brzmienie zgodne z dyrektywą wspólnotową.

W dotychczasowej praktyce usług certyfikacyjnych pola rozszerzeń certyfikatu kwalifikowanego mają dostarczać dodatkowych informacji na temat funkcji i uprawnień właściciela certyfikatu. Rozwiązanie to okazuje się drogie: podmiot kwalifikowany odpowiada za dane umieszczane w certyfikacie, wobec czego musi wdrożyć procedury sprawdzania dokumentów na podstawie których dokonuje wpisów. Czynności te są obciążone ryzykiem, które pośrednio podnosi koszty działalności certyfikacyjnej. Osoba, która wystąpiła o certyfikat elektroniczny określając w nim dokładnie cechy i uprawnienia nie ma możliwości nieodpłatnej wymiany certyfikatu, gdy przestaną być aktualne zawarte w nim informacje. Należy stwierdzić, że znacznie tańszym rozwiązaniem w obrocie jest posługiwanie się certyfikatami atrybutów. Tego rodzaju *sui generis* certyfikat stanowi, że określona osoba (identyfikowana jako posiadacz pewnego klucza prywatnego) posiada określone uprawnienia. Certyfikaty atrybutów mogą być wydawane przez osoby uprawnione do nadawania uprawnień lub przez stronę trzecią jaką są podmioty certyfikacyjne. W sytuacji takiej uproszczeniu ulegają dokonywane czynności (np. Izba Adwokacka wydaje adwokatowi certyfikat atrybutu, zamiast wydawać mu zaświadczenie, na mocy którego adwokat uzyskuje odpowiedni wpis w certyfikacie kwalifikowanym), zmniejsza się liczba certyfikatów (ta sama osoba może być obecnie zmuszona do wyrabiania wielu certyfikatów ze względu na różne role, w jakich występuje), upraszcza się kwestie odpowiedzialności za dane umieszczane w certyfikacie. Tworząc repozytorium certyfikatów atrybutów można zapewnić funkcjonowanie swego rodzaju bazy danych o uprawnieniach lub udzielonych pełnomocnictwach. Certyfikaty atrybutów będą mogły być wydawane zarówno do certyfikatów zwykłych, jak i certyfikatów kwalifikowanych.

Nowe uregulowanie dotyczące uznawania certyfikatów z zagranicy precyzuje warunki jakie spełnione zostać muszą dla zrównania pod względem prawnym certyfikatów kwalifikowanych wydawanych przez podmiot zagraniczny z kwalifikowanymi certyfikatami wydawanymi przez krajowe centra certyfikacji. Art. 4 formułuje zasadę równoważności certyfikatów tego rodzaju wyłącznie w odniesieniu do certyfikatów kwalifikowanych. Jest to zgodne z dyrektywą, która nie wymaga uznawania certyfikatów zwykłych. Wprowadzenie wymogu uznawania certyfikatów zwykłych wyprzedzałoby obecny stan techniczny w zakresie walidacji przepisów we Wspólnocie. Nie bez znaczenia są prowadzone aktualnie przez Komisję Wspólnot Europejskich działania dotyczące uznawalności transgranicznej podpisów elektronicznych (Komunikat Komisji Wspólnot Europejskich do Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno – Społecznego, Komitetu Regionów z dnia 28 listopada 2008 „Plan działania dotyczący e-podpisów i e-identyfikacji, mający na celu ułatwienie świadczenia transgranicznych usług publicznych na jednolitym rynku” (COM (2008) 798). Zgodnie z komunikatem w 2009 roku zostają podjęte działania dotyczące ułatwienia w uznawalności przez państwa kwalifikowanych jak i zaawansowanych podpisów elektronicznych weryfikowanych kwalifikowanym certyfikatem (min. poprzez utworzenie wspólnej służby walidacyjnej) oraz ułatwień w stosowaniu zaawansowanych podpisów elektronicznych. Podkreślić należy, że walidacja dotyczyć będzie certyfikatów kwalifikowanych. Art. 4 rozróżnia obowiązek uznawania certyfikatów z państw Europejskiego Obszaru Gospodarczego wynikający z Dyrektywy 99/93/WE od uznawania certyfikatów z tzw. krajów trzecich. Uszczegółowione zostały skutki udzielenia gwarancji za certyfikat zagraniczny. Wprowadzenie precyzyjnych uregulowań w zakresie uznawania certyfikatów zagranicznych sprzyjać będzie rozwojowi konkurencji na krajowym rynku usług certyfikacyjnych, gdyż możliwe będzie wykorzystywanie przez obywateli certyfikatów kwalifikowanych wydanych w innych państwach europejskich.

Nowa ustawa znacząco liberalizuje nadzór nad świadczeniem usług certyfikacyjnych. Zniesiony zostaje nadzór nad podmiotami niekwalifikowanymi oraz pozwala w szerszym zakresie niż dotychczas świadczyć usługi kwalifikowane organom władzy publicznej. Podkreślić należy, że nie wszystkie kraje Unii Europejskiej przewidują nadzór nad podmiotami świadczącymi zwykłe usługi certyfikacyjne (Austria, Finlandia, Grecja, Włochy, Portugalia, Hiszpania, Węgry, Słowenia). W większości krajów nadzór sprawowany jest wyłącznie nad podmiotami kwalifikowanymi (Belgia, Dania, Francja, Niemcy, Irlandia, Luxemburg, Holandia, Szwecja, Wielka Brytania, Czechy, Estonia, Łotwa, Litwa, Malta). Szczegółowy nadzór nad zwykłymi podmiotami certyfikującymi nie był dotychczas możliwy ze względu na brak obowiązku notyfikacji tego rodzaju działalności ministrowi właściwemu ds. gospodarki. Zgodnie z art. 9 ust. 2 jedynie Narodowy Bank Polski oraz organy władzy publicznej sprawujące nadzór nad świadczeniem usług certyfikacyjnych nie mogą świadczyć usługi wydawania certyfikatów kwalifikowanych. Jest to w zgodzie pkt 12 preambuły Dyrektywy UE w którym stwierdza się, że usługi certyfikacyjne powinny świadczyć organy publiczne, osoby prawne lub fizyczne, jeżeli działają zgodnie z prawem krajowym. W odniesieniu do podmiotów ubiegających się o wpis do rejestru ministra właściwego ds. gospodarki zniesiona zostaje opłata za wpis do rejestru oraz kontrola wstępna. Zmiany w tym zakresie powinny przyczynić się do wzrostu liczby podmiotów oraz podnieść poziom konkurencyjności rynku. Wzorem prawa telekomunikacyjnego ustawa daje organowi nadzoru nowe skuteczne narzędzie w postaci uprawnienia do żądania informacji związanych z prowadzoną działalnością certyfikacyjną. Dotychczas wiele informacji związanych z działalnością podmiotów kwalifikowanych udostępnianych było na zasadzie dobrowolności.

Art. 20 otwiera możliwość świadczenia innych niż przewidziane w ustawie usług certyfikacyjnych - otwierając stosownie do rozwoju technologii i rynku - drogę do wprowadzania na rynek innowacji bez konieczności oczekiwania na uprzednią regulację prawną. Art. 16 ust. 2 pozwala na wydanie rozporządzenia, które określi warunki świadczenia innych usług związanych z podpisem elektronicznym, jeśli wymagać będzie tego względem bezpieczeństwa obrotu lub wykorzystanie tego rodzaju usług w administracji publicznej. Przepis ten stanowi delegację do fakultatywnego wydania rozporządzenia, jeśli w przyszłości powstaną nowe usługi związane z podpisem elektronicznym i w interesie odbiorców usług certyfikacyjnych będzie zachodziła konieczność ich ujednoczenia. Dopuszczenie usług nienazwanych zapewnia zwiększenie innowacyjności i konkurencyjności podmiotów, które funkcjonują pod jurysdykcją polską. Praktyka ostatnich lat wskazuje, że tzw. usługi nienazwane z ustawy o podpisie elektronicznym posłużyły do wprowadzenia potrzebnych rynkowi usług. Niektóre z tzw. usług nienazwanych zostały wprowadzone jako usługi nazwane (certyfikaty atrybutów, potwierdzenie ważności certyfikatów).

Projekt ustawy o podpisach elektronicznych został oparty na założeniu utrzymania krajowego urzędu certyfikacyjnego (czyli tzw. roota centralnego). Obowiązek posiadania roota nie wynika bezpośrednio z dyrektywy. Model krajowej infrastruktury klucza publicznego z centralnym rootem upraszcza rozpoznawanie zaufanych certyfikatów za granicą przez wskazanie tylko tego roota zamiast wielu lokalnych certyfikatów samopodpisanych. Oprócz rejestru wprowadzona zostanie czytelna maszynowo lista urzędów, która mogłaby być realizowana przy zastosowaniu standardu ETSI TS 102 204 (Trusted Services List). Konsekwencją wprowadzenia listy podmiotów świadczących usługi certyfikacyjne jest wprowadzenie delegacji do wydania aktu wykonawczego przewidzianego w art. 36 ust. 2. W chwili przygotowania projektu ustawy rozpoczęte zostały prace wspólnotowe zmierzające do zapewnienia jednolitych wymogów w zakresie sposobu publikacji i ochrony listy podmiotów kwalifikowanych lub akredytowanych. Brzmienie art. 38 jest konsekwencją uchwalenia nowej ustawy – Prawo upadłościowe i naprawcze.

Zawarta w art. 69 i przygotowana we współpracy z Komisją Kodyfikacyjną Prawa Cywilnego propozycja zmiany kodeksu cywilnego uwzględnia wprowadzenie podpisu zaawansowanego poprzez odpowiednią modyfikację w zakresie formy oświadczenia woli. Przez wiele lat funkcjonowania, artykuł 78§2 k.c. w dotychczasowym brzmieniu, w praktyce nie miał większego znaczenia. Rynek bezpiecznego podpisu elektronicznego nie rozwinął się na tyle, aby jego wykorzystanie stało się standardem zawierania umów w postaci elektronicznej. Rynek odrzucił bezpieczny podpis elektroniczny akceptując inne formy dokonywania czynności w postaci elektronicznej, oparte o odpowiednie loginy i hasła, w odpowiedni sposób zabezpieczające integralność składanych oświadczeń z równoczesną możliwością identyfikacji podmiotu. W sferze bankowej, gdzie od wielu lat dla dokonywania czynności w formie równoważnej pisemnej wystarczające jest dokonanie czynności za pomocą elektronicznych nośników informacji, jeżeli dokumenty w których zawarte jest oświadczenie zostają w sposób należyty utrwalone i zabezpieczone, brak konieczności opatrywania ich bezpiecznym podpisem elektronicznym weryfikowanym ważnym kwalifikowanym certyfikatem. Nie bez znaczenia jest także rozwój techniki i kryptografii umożliwiający odpowiednie zabezpieczenie dokumentów elektronicznych zawierających oświadczenie woli, w sposób inny niż z użyciem bezpiecznego podpisu elektronicznego. Na uwagę zasługuje projekt Elektronicznego Postępowania Upominawczego gdzie w miejsce bezpiecznego podpisu elektronicznego pisma opatruje się podpisem elektronicznym spełniającym wymogi proponowanego art. 78¹ k.c. Wprawdzie dyrektywa 93/99/WE (zgodnie z art. 5 dyrektywy) nakazuje zrównanie formy pisemnej z opatrzeniem danych zaawansowanym podpisem elektronicznym weryfikowanym ważnym kwalifikowanym

certyfikatem złożonym za pomocą bezpiecznych urządzeń służących do składania podpisu, jednakże jest to tylko wymóg minimalny.

Nie ma przeszkód, aby zrównać formę pisemną z zaawansowanym podpisem elektronicznym. Proponowana zmiana nie ogranicza przy tym możliwości zastrzeżenia w przepisach ostrzejszego wymogu formy elektronicznej dla niektórych czynności tj. dokonywania czynności w postaci elektronicznej wyłącznie z użyciem podpisu elektronicznego weryfikowanego certyfikatem kwalifikowanym (kwalifikowana forma elektroniczna). Proponowana zmiana zrównuje formę pisemną z elektroniczną opartą wyłącznie o zaawansowany podpis elektroniczny bez użycia kwalifikowanego certyfikatu, nie oznacza to jednakże niedopuszczalności posługiwania się certyfikatem, w tym w związku z projektem wzajemnej uznawalności zagranicznym certyfikatem, czy też kwalifikowanym certyfikatem. Oczywiście, podmioty zamierzające dokonać czynności prawnej w formie elektronicznej równoważnej formie pisemnej za granicą, będą musiały wypełnić wymogi państwa według którego prawa dokonują czynności dla której nie zawsze będzie wystarczające użycie zaawansowanego podpisu elektronicznego, co jednakże nie jest argumentem za pozostawieniem aktualnej niepraktycznej regulacji. Proponowana zmiana wychodzi naprzeciw praktyce i postulowanym zmianom w doktrynie. A głównym jej celem jest dopasowanie przepisów prawa do istniejących i przyjętych zasad obrotu w Internecie.

Nowelizacja Kodeksu postępowania administracyjnego dopuszczająca składanie podań z użyciem podpisów elektronicznych weryfikowanych przy pomocy certyfikatu kwalifikowanego wynika z konieczności dostosowania postępowania administracyjnego ogólnego do prac związanych z implementacją dyrektywy o usługach na rynku wewnętrznym. W świetle prowadzonych przez Komisję Europejską prac nad procedurami elektronicznymi przewidzianymi w art. 8 dyrektywy konieczne będzie zapewnienie uznawania zaawansowanego podpisu elektronicznego weryfikowanego przy pomocy certyfikatu kwalifikowanego oraz kwalifikowanego podpisu elektronicznego. Dotychczas obowiązujący przepis przewidywał wyłącznie możliwość zastosowania bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego certyfikatu kwalifikowanego. W związku z koniecznością zapewnienia możliwości elektronicznego udziału w procedurze administracyjnej podmiotom z krajów, gdzie dominuje podpis zaawansowany weryfikowany przy pomocy certyfikatu kwalifikowanego niezbędne jest rozszerzenie zakresu dopuszczonych rodzajów podpisu elektronicznego. Podkreślić należy, że Komisja Europejska nie przewiduje wymogu uznawania podpisów zaawansowanych weryfikowanych przy pomocy certyfikatów innych niż kwalifikowany.

Proponowana zmiana ustawy o świadczeniach rodzinnych z dnia 28 listopada 2003 r. (Dz.U. z 2006 r. Nr 139, poz. 992, z późn. zm.) ułatwi przesyłanie informacji pomiędzy systemami informatycznymi urzędów skarbowych i urzędów gmin w zakresie pozyskiwania zaświadczeń o dochodach dla osób – wnioskodawców ubiegających się o świadczenia rodzinne. Zapis pozwoli na rezygnację z obecnego systemu dostarczania zaświadczenia o dochodzie z urzędu skarbowego wraz z wnioskiem o świadczenia rodzinne. Wnioskodawca będzie składał wniosek o świadczenia rodzinne w gminie, natomiast gmina pozyska od urzędu skarbowego informację o dochodzie osoby, na zasadzie wymiany informacji pomiędzy systemami.

Proponowana zmiana ustawy o pomocy osobom uprawnionym do alimentów z dnia 7 września 2007 r. (Dz.U. Nr 192, poz. 1378, z późn. zm.) ułatwi przesyłanie informacji pomiędzy systemami informatycznymi urzędów skarbowych i urzędów gmin w zakresie

pozyskiwania zaświadczeń o dochodach dla osób – wnioskodawców ubiegających się o świadczenia z funduszu alimentacyjnego. Zapis pozwoli na rezygnację z obecnego systemu dostarczania zaświadczenia o dochodzie z urzędu skarbowego wraz z wnioskiem o świadczenia z funduszu alimentacyjnego. Wnioskodawca będzie składał wniosek o świadczenia z funduszu alimentacyjnego w gminie, natomiast gmina pozyska od urzędu skarbowego informację o dochodzie osoby, na zasadzie wymiany informacji pomiędzy systemami.

Proponowane zmiany w ustawie z dnia o promocji zatrudnienia i instytucjach rynku pracy z dnia 20 kwietnia 2004 r. (Dz. U. z 2008 r. Nr 69, poz. 415, Nr 70, poz. 416 i Nr 171, poz. 1056) ułatwią przesyłanie informacji pomiędzy systemami informatycznymi Publicznych Służb Zatrudnienia oraz podmiotów realizujących zadania publiczne poprzez uwierzytelnienie przekazywanych informacji oraz zagwarantowanie ich integralności.

Wychodząc na przeciw postulatowi uproszczenia terminologii ustawowej w tych przypadkach, kiedy jest to możliwe wprowadzone zostały liczne skróty. W odniesieniu do przyjętego w nomenklaturze wspólnotowej pojęcia „zaawansowany podpis elektroniczny” wprowadzony został skrót „podpis zaawansowany” oraz „podpis kwalifikowany”. W odniesieniu do kwalifikowanych podmiotów świadczących usługi certyfikacyjne w zakresie podpisu elektronicznego, które stanowią szczególny przypadek podmiotu świadczącego usługi certyfikacyjne dopuszczalne będzie użycie stosowanego w dokumentach i standardach wspólnotowych terminu „podmiot kwalifikowany”. Dopuszczono również skrót „bezpieczne urządzenie”.

Projekt ustawy, jako dotyczący usług społeczeństwa informacyjnego podlegać będzie notyfikacji w ramach systemu przewidzianego dyrektywą wspólnotową 98/34/WE.