

## 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 do składania podpisu elektronicznego oraz w oparciu o certyfikat zwykły lub certyfikat kwalifikowany. Założeniem ustawodawcy jest przygotowanie 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.

Wychodząc na przeciw postulatom uproszczenia terminologii ustawowej, w tych przypadkach, kiedy było to możliwe, wprowadzono liczne skróty. W odniesieniu do pojęcia „bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu” wprowadzono przyjęte w nomenklaturze wspólnotowej pojęcie „podpis kwalifikowany”. W odniesieniu do przewidzianych obowiązującą dotychczas ustawą o podpisie elektronicznym i działających już na polskim rynku „kwalifikowanych podmiotów świadczących usługi certyfikacyjne w zakresie podpisu elektronicznego” wprowadzono skróconą nazwę „podmiot kwalifikowany”. Dopuszczono również skrót „bezpieczne urządzenie” w miejsce dotychczasowych „bezpiecznych urządzeń służących do składania podpisu elektronicznego”. 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. 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.

Względem uprzednio obowiązującej ustawy z dnia 18 września 2001 r. o podpisie elektronicznym rozszerzone zostało pojęcie „podpisującego” (art. 2 pkt. 13), które obecnie obejmuje zarówno osoby fizyczne jak i inne podmioty, w tym także podmioty świadczące usługi certyfikacyjne. Wprowadzenie nowego narzędzia w postaci podpisu zaawansowanego (art. 2 pkt 2) 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 najbezpieczniejszym, ale zarazem najdroższym rozwiązaniem ze

względu na konieczność korzystania z bezpiecznych urządzeń do składania podpisu elektronicznego. Cena zestawów do składania bezpiecznego podpisu elektronicznego spadła wprawdzie znacząco w ostatnim czasie, ale jest ona nadal znacząca dla użytkownika załatwiającego drogą elektroniczną niewielką ilość spraw.

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 odchodzi się od pojęcia „bezpieczny podpis elektroniczny” na rzecz pojęcia „podpis kwalifikowany”, które stanowi jego odpowiednik w nomenklaturze wspólnotowej.

W art. 2 ust. 1 dokonana została zgodnie z brzmieniem dyrektywy zmiana w definicji tzw. podpisu zwykłego, która obecnie odwołuje się w miejsce dotychczas stosowanego pojęcia „identyfikacji” do terminu „metody uwierzytelnienia”. Ustawa, podobnie jak dyrektywa, 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 oraz podpisu osobistego.

W ustawie (art. 2 ust. 5) mowa jest o podpisie kwalifikowanym, który w dyrektywie (art. 5.1) 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 e-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. Wydawanie kwalifikowanych certyfikatów jest działalnością regulowaną europejskimi dokumentami standaryzacyjnymi. Podmioty kwalifikowane, jako zaufana strona trzecia, wnoszą ważną wartość dodaną w zakresie zaufania w obrocie elektronicznym i odgrywają kluczową rolę na rynku usług certyfikacyjnych. W chwili obecnej w Europie działa ok. 90 podmiotów kwalifikowanych lub akredytowanych, które mogą wydawać certyfikaty kwalifikowane.

Dla potrzeb elektronicznych dokumentów tożsamości ustawa w art. 2 pkt 3 wprowadza podpis osobisty. Jakkolwiek ten rodzaj zaawansowanego podpisu elektronicznego

nie jest wymieniony w dyrektywie wspólnotowej to pamiętać należy, że dyrektywa wspólnotowa jako dyrektywa wymagań minimalnych nie zabrania państwom członkowskim tworzenia funkcjonalnie wyodrębnionych rodzajów podpisu elektronicznego lub nowych usług certyfikacyjnych. Ogłoszony przez Komisję Europejską „Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Plan działania na rzecz e-podpisu i e-identyfikacji w celu ułatwienia świadczenia transgranicznych usług publicznych na jednolitym rynku” (COM (2008) 798) wskazuje, że przyszłość podpisu elektronicznego jest związana z elektronicznymi dokumentami identyfikacyjnymi. Rodzaj certyfikatów przy pomocy których weryfikowany będzie podpis osobisty określony zostanie na etapie dalszych prac nad projektem pl.ID 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. Złożenie przez osobę fizyczną danych w postaci elektronicznej opatrzonej podpisem osobistym, skierowanych do podmiotu publicznego w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne wywołuje skutek prawny dokumentu z podpisem własnoręcznym (art. 5 ust. 4).

Wprowadzenie definicji pieczęci elektronicznej (ang. „data stamping”- dosł. stemplowanie danych) ma na celu zapewnienie nowego narzędzia opartego o technologię zbliżoną do wykorzystywanej przy podpisie elektronicznym. Przyjęcie, że pieczęć elektroniczna nie jest podpisem elektronicznym pozwoli m.in. na pełną automatyzację jego stosowania. Narzędzie to jest przeznaczone do podniesienia wiarygodności i integralności przesyłanych wiadomości. Pieczęć elektroniczna może być generowana przez systemy informatyczne bez udziału człowieka. W praktyce zastosowanie pieczęci może dotyczyć takich czynności jak m.in. potwierdzanie faktu wpłynięcia dokumentów elektronicznych, potwierdzenie przyjęcia zamówienia lub ewentualnie przy generowaniu faktur elektronicznych. Pod względem technologicznym, w tym stosowanych algorytmów kryptograficznych, pieczęć elektroniczna nie musi niczym się różnić od podpisu elektronicznego. Ze względu na początkowy etap rozwoju tego narzędzia ustawa nie przesądza o rodzaju certyfikatów, które mogą być stosowane do weryfikacji pieczęci. Dla przykładu w rozwiązaniu czeskim przyjęto, że do weryfikacji pieczęci służy osobna kategoria certyfikatów systemowych, które różnią się nieznacznie swoim profilem od certyfikatów kwalifikowanych. Potrzeby praktyki obrotu gospodarczego i administracyjnego pozwolą w przyszłości wypełnić pieczęć elektroniczną pełniejszą treścią. Zakłada się, że zastosowanie i skutki prawne tego narzędzia regulowane będą innymi ustawami.

Przyjęte w ustawie definicje podpisującego oraz pieczęci elektronicznej umożliwią rezygnację z definicji „poświadczenie elektroniczne” i „zaświadczenie elektroniczne”, a także pozwolą zapewnić ciągłość funkcjonowania istniejącej obecnie krajowej infrastruktury klucza publicznego. Nowa definicja certyfikatu 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. Wydawane przez Europejski Komitet Standaryzacyjny CEN normy CWA także w odniesieniu do urzędów certyfikujących posługują się pojęciem „certificate CA”, czyli po prostu certyfikatu urzędu certyfikującego. Nie oznacza to zniesienia istniejących zaświadczeń i poświadczeń certyfikacyjnych, ale ich zastąpienie pojęciem certyfikatu. Podkreślić należy, że ustawa

utrzymuje istniejącą architekturę krajowej infrastruktury klucza publicznego opartą o krajowy urząd certyfikujący. Wiarygodność podmiotów świadczących kwalifikowane usługi certyfikacyjne będzie nadal ugruntowana na certyfikacie wydanym przez właściwy organ państwa. Dotychczasowe „zaświadczenie elektroniczne” będzie w świetle nowej nomenklatury certyfikatem ministra właściwego ds. gospodarki.

Nowe uregulowanie dotyczące uznawania certyfikatów z zagranicy (art. 3 i 4) 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. 3 i 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 e-podpisów we Wspólnocie. Nie bez znaczenia są prowadzone aktualnie przez Komisję Wspólnot Europejskich działania dotyczące transgranicznej uznawalności podpisów elektronicznych (por. 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*”). W 2009 roku zostają podjęte działania dotyczące walidacji kwalifikowanych jak i zaawansowanych podpisów elektronicznych weryfikowanych kwalifikowanym certyfikatem (m.in. poprzez utworzenie tzw. European Federated Validation Service) oraz ułatwień w stosowaniu zaawansowanych podpisów elektronicznych. Podkreślić należy, że w pierwszym okresie prace nad przyjazną dla użytkowników walidacją podpisów z innych krajów dotyczyć będą wyłącznie certyfikatów kwalifikowanych. Art. 3 i 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 bardziej 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. Podkreślić należy, że wzajemne uznawanie e-podpisu pozostaje w znacznej mierze problemem technicznym, a nie prawnym ze względu na brak krajowych platform walidacji. Zapewnienie wspólnej europejskiej przestrzeni zaufania nie jest możliwe bez rozwoju krajowych usług walidacji e-podpisu oraz ich integracji na poziomie wspólnotowym.

Kwalifikowana i zwykła usługa znakowania czasem oparta została o pojęcie czasu urzędowego i pozwala na jego wystawianie nie tylko podmiotom kwalifikowanym (art.7). Zwykła usługa znakowania czasem może być świadczona w oparciu o wybrane przez sam podmiot wiarygodne wzorce czasu. Kwalifikowana usługa znakowania czasem będzie świadczona 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 kwalifikowanego znakowania czasem utrzymany zostaje wymóg dokładności synchronizacji do jednej sekundy, przy czym wprowadzony zostaje obowiązek weryfikacji technicznej spełnienia tego wymogu.

Techniczna różnica między kwalifikowanym, a niekwalifikowanym znakowaniem czasem polega na różnym obowiązkowi częstości weryfikacji wymaganej dokładności synchronizacji (art.18). 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.

Art. 23 ustawy o podpisach elektronicznych wprowadza nowe uregulowania dotyczące certyfikatów atrybutów. 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 jest posługiwanie się w obrocie certyfikatami atrybutów. Tego rodzaju *sui generis* certyfikat stanowi, że określona osoba (identyfikowana jako posiadacz pewnego klucza prywatnego) posiada określone uprawnienia. Certyfikaty atrybutów nie są technologicznie tożsame z certyfikatami podpisu elektronicznego, gdyż zawarte w nich dane nie służą do weryfikacji e-podpisu. 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 kwalifikowanych (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.

W rozdziale 6 i 7 nowa ustawa znacząco liberalizuje nadzór nad świadczeniem usług certyfikacyjnych oraz upraszcza procedurę wpisu do rejestru. Zgodnie z art. 3 ust 3 dyrektywy 99/93/WE nowa ustawa reguluje zasady nadzoru nad podmiotami świadczącymi usługi certyfikacyjne wydającymi certyfikaty kwalifikowane. Zniesiony zostaje natomiast nadzór nad podmiotami świadczącymi usługi niekwalifikowane. 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. W art. 9 dopuszczone zostało świadczenie usług certyfikacyjnych na poziomie kwalifikowanym przez ministra właściwego ds. administracji. Jest to w zgodzie pkt 12 preambuły Dyrektywy UE w którym stwierdza się, że usługi certyfikacyjne mogą świadczyć organy publiczne, osoby prawne lub fizyczne, jeżeli działają zgodnie z prawem krajowym. Centra kwalifikowane prowadzone przez administrację publiczną występują m.in. w Portugalii, Hiszpanii oraz na Słowacji. W odniesieniu do nowych 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. 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. W sposób bardziej precyzyjny niż dotychczas określono obowiązek archiwizacji danych w związku ze świadczeniem usług certyfikacyjnych oraz ograniczono okres przechowywania do lat 10. Jest to ważny krok w kierunku ograniczenia kosztów funkcjonowania podmiotów świadczących kwalifikowane usługi certyfikacyjne.

Przepisy ustawy wprowadzają 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. Dopuszczenie usług nienazwanych stanowi przesłankę zwiększenia 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. Oprócz rejestru wprowadzona zostanie czytelna maszynowo lista urzędów, która mogłaby być realizowana przy zastosowaniu standardu ETSI TS 102 231 (Trusted Services List). W tym zakresie nie zachodzi potrzeba zawarcia w ustawie upoważnienia do wydania aktów wykonawczych, gdyż listy TSL będą regulowane

decyzją Komisji Europejskiej w tym zakresie. W chwili przygotowania projektu ustawy rozpoczęte prowadzone są prace wspólnotowe zmierzające do zapewnienia jednolitych wymogów w zakresie sposobu publikacji i ochrony listy podmiotów kwalifikowanych lub akredytowanych w poszczególnych państwach.

Zawarta w art. 59 i przygotowana we współpracy z Komisją Kodyfikacyjną Prawa Cywilnego propozycja zmiany kodeksu cywilnego wprowadza modyfikację w zakresie elektronicznej formy oświadczenia woli. Przez wiele lat swojego obowiązywania, 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. W praktyce obrotu gospodarczego umowy zawierane są częstokroć z wykorzystaniem innych form uwierzytelnienia, opartych np. o odpowiednie loginy i hasła, w odpowiedni sposób zabezpieczające składane oświadczenia woli z równoczesną możliwością identyfikacji stron.

Podkreślić należy, że nie ma zasadniczych 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. 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 certyfikatem kwalifikowanym. 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. Niezależnie zatem od zastosowania przy składaniu e-podpisu tzw. bezpiecznego urządzenia wskazane będzie stosowanie certyfikatów kwalifikowanych. Dopuszczenie powyższych rodzajów podpisu elektronicznego posiada charakter wymagań minimalnych. Państwa członkowskie mogą zatem dopuścić również inne rodzaje podpisu elektronicznego lub krajowe mechanizmy uwierzytelnienia (taki jak np. zaufany profil).. Dotychczas obowiązujący przepis przewidywał wyłącznie możliwość zastosowania bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego certyfikatu kwalifikowanego. W związku z koniecznością zapewnienia możliwości udziału w procedurze administracyjnej podmiotom z innych krajów 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.

Zmiany w ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2007 r. Nr 11, poz. 74, z późn. zm.) umożliwią m.in. na wprowadzenie pierwszego obszaru zastosowań w administracji publicznej nowego narzędzia pieczęci elektronicznej. Uregulowania pozwolą na uwierzytelnienie podmiotu przekazującego dokumenty elektroniczne jako płatnika składek i udostępnienie mu zwrótnie w kanale Elektronicznej Wymiany Danych Kompleksowego Systemu Informatycznego ZUS przeznaczonych dla niego informacji zawierających dane osobowe ubezpieczonych i innych informacji o ograniczonym dostępie. Użycie pieczęci elektronicznej upraszcza postępowanie oraz obniża koszty ponoszone przez płatników składek związane z przekazywaniem elektronicznych dokumentów ubezpieczeniowych do Zakładu Ubezpieczeń Społecznych. ZUS zakłada również użycie w przyszłości innych rozwiązań w zakresie uwierzytelnienia oraz zapewnienia integralności i niezaprzeczalności przekazywanych dokumentów elektronicznych, co uwzględnione zostanie w innych ustawach i rozporządzeniach.

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.

Projekt ustawy podlega notyfikacji w trybie przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039, z późn. zm.).