

OCENA SKUTKÓW REGULACJI

USTAWY O PODPISACH ELEKTRONICZNYCH

1. ANALIZA PROBLEMU

Podstawowym założeniem, które legło u podstaw opracowania ustawy o podpisach elektronicznych jest rozszerzenie katalogu nazwanych usług certyfikacyjnych, w tym zwłaszcza wprowadzenie nowych rodzajów podpisu elektronicznego. Dotychczasowe oparcie o bezpieczny podpis elektroniczny oraz tzw. „zwykły” podpis elektroniczny uznawane jest za niewystarczające i w niedostateczny sposób odwzorowujące siatkę pojęciową Dyrektywy Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. *w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego* (99/93/WE). Ze względu na konieczność zapewnienia ciągłości świadczenia usług projektowana ustawa o podpisach elektronicznych utrzymuje systematykę oraz znaczną część przepisów obowiązującej ustawy z dnia 18 września 2001 r. *o podpisie elektronicznym* (Dz. U. z dnia 15 listopada 2001 r.).

Wprowadzone liczne zmiany dokonywane były przy założeniu możliwie dokładnego odwzorowania terminologii dyrektywy wspólnotowej oraz wprowadzaniu nowych narzędzi z zapewnieniem ciągłości świadczenia usług dotychczas istniejących. W lutym 2009 r. było aktywnych ponad 202 tysiące certyfikatów kwalifikowanych do składania bezpiecznego podpisu elektronicznego. Wg danych z 2008 roku zrealizowanych zostało ok. 1.400.000 kwalifikowanych usług znakowania czasem. Dokładna liczba certyfikatów niekwalifikowanych nie jest możliwa do ustalenia ze względu na brak konieczności notyfikowania państwu tego rodzaju działalności certyfikacyjnej oraz brak danych statystycznych w tym zakresie. W związku z istnieniem systemów, które obsługują podpisy elektroniczne oraz koniecznością zapewnienia odbiorcom usług możliwości ich dalszego wykorzystywania w odniesieniu do funkcjonujących narzędzi wprowadzone zostaną wyłącznie niezbędne zmiany.

STAN OBECNY. W obowiązującej dotychczas ustawie o podpisie elektronicznym zdefiniowane były pojęcia **bezpieczny podpis elektroniczny** i **certyfikat kwalifikowany**. W treści tejże ustawy używa się określenia będącego połączeniem obu wcześniej zdefiniowanych pojęć: bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu. Na przykład art. 5 ust. 2 stanowi, że „dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej”. „Bezpečny podpis elektroniczny” to przede wszystkim spełnienie wymagań technologicznych określonych w przepisach wynikających z ustawy o podpisie elektronicznym. Są to m.in. określona struktura podpisu, użyte algorytmy kryptograficzne (skrót, szyfrowe) oraz tzw. podpisane atrybuty podpisu (ustawa wymaga minimum atrybutu jednoznacznie wskazującego na certyfikat służący do weryfikacji podpisu). Technologiczną poprawność podpisu bezpiecznego zapewnia „bezpieczne urządzenie do składania podpisu elektronicznego”. Certyfikat kwalifikowany można uzyskać w jednym z kwalifikowanych podmiotów świadczących usługi certyfikacyjne wpisanych do rejestru Ministra Gospodarki. W odniesieniu do tego rodzaju e-podpisu potocznie używana jest nazwa podpis kwalifikowany. Jakkolwiek w ustawie o podpisie elektronicznym nie było określenia „podpis kwalifikowany” to pojęcie takie występuje w licznych dokumentach wspólnotowych.

Bezpieczny podpis elektroniczny (podpis kwalifikowany) służy wyłącznie do podpisywania i może go złożyć wyłącznie osoba fizyczna.

Ustawa o podpisie elektronicznym dopuszczała również „zwykły” **podpis elektroniczny**, który nie jest wprawdzie równoważny własnoręcznemu, lecz nie można odmówić mu ważności i skuteczności wyłącznie ze względu na jego elektroniczną formę. Wykorzystanie podpisu elektronicznego opartego o niekwalifikowany certyfikat pozostaje w znacznej mierze ograniczone do określonych systemów informatycznych. Zwykły podpis elektroniczny oprócz podpisywania może być również wykorzystywany do autentykacji oraz szyfrowania. Z tego powodu karty służące do składania bezpiecznego podpisu elektronicznego zawierają z zasady również klucz prywatny zwykłego podpisu elektronicznego powiązany z certyfikatem niekwalifikowanym. Na przeszkodzie szerokiego wykorzystania tego rodzaju podpisu elektronicznego w procedurze administracyjnej stały przepisy Kodeksu Postępowania Administracyjnego, które uzależniały możliwość składania podań drogą elektroniczną od opatrzenia pisma bezpiecznym podpisem elektronicznym.

Oprócz wymienionych dwóch rodzajów podpisów elektronicznych inną nazwaną usługą certyfikacyjną funkcjonującą pod rządami obowiązującej obecnie ustawy jest **znakowanie czasem**, które wywołuje skutki prawne w postaci daty pewnej. Ponieważ bezpieczny podpis elektroniczny jest ważny tylko, jeśli został złożony w okresie ważności certyfikatu usługa ta posiada ważne znaczenie dowodowe oraz służy konserwacji mocy dowodowej podpisanych elektronicznie dokumentów.

DYREKTYWA WSPÓLNOTOWA. W dyrektywie 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych mowa jest o trzech rodzajach podpisu cyfrowego¹. Pierwszym z nich jest najprostszy „**podpis elektroniczny**”, posiadający szerokie znaczenie. Podpis taki służy do weryfikacji tożsamości i uwierzytelniania danych. Może przy tym chodzić o tak prostą czynność jak podpisanie wiadomości elektronicznej nazwiskiem nadawcy lub przy użyciu kodu PIN. Aby stanowić podpis, uwierzytelnienie musi dotyczyć danych, a nie służyć tylko jako metoda lub technika uwierzytelniania dla podmiotu. Drugim zdefiniowanym w dyrektywie rodzajem podpisu elektronicznego jest „**zaawansowany podpis elektroniczny**”. Podpis taki musi spełniać wymagania określone w art. 2 ust. 2 dyrektywy. Dyrektywa nie preferuje żadnej technologii, ale w praktyce definicja ta dotyczy głównie podpisów elektronicznych opartych na infrastrukturze klucza publicznego (PKI). W rozwiązaniu tym dane podpisywane są z wykorzystaniem technik szyfrowania, które wymagają użycia klucza prywatnego. W art. 5 ust. 1 mowa jest o trzecim rodzaju podpisu cyfrowego, który w dyrektywie nie otrzymał własnej nazwy a w dokumentach wspólnotowych nazywany jest „**kwalifikowanym podpisem elektronicznym**”. Chodzi o zaawansowany podpis elektroniczny oparty na kwalifikowanym certyfikacie i złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu. Podpis taki musi spełniać wymagania określone w załącznikach I, II i III² do wymienionej dyrektywy. „**Podpisujący**” jest zdefiniowany w dyrektywie jako „osoba posiadająca urządzenie służące do składania podpisów, która działa w imieniu własnym lub w imieniu osób prawnych lub fizycznych, lub podmiotu, którego jest przedstawicielem”. Mimo iż

¹ Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania dyrektywy 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, COM(2006) 120 wersja ostateczna, Bruksela, 17 marca 2006.

² ZAŁĄCZNIK I Wymogi dotyczące certyfikatów kwalifikowanych, ZAŁĄCZNIK II Wymogi wobec podmiotów świadczących usługi certyfikacyjne, wystawiających certyfikaty Kwalifikowane, ZAŁĄCZNIK III Wymogi dotyczące bezpiecznych urządzeń służących do składania podpisu elektronicznego.

dyrektywa nie stanowi, że podpis elektroniczny może dotyczyć wyłącznie osoby fizycznej, to składającym „kwalifikowany” podpis elektroniczny (art. 5 ust. 1 dyrektywy) może być tylko osoba fizyczna ze względu na wymóg certyfikatu kwalifikowanego.

W świetle obecnych prac wspólnotowych nad wykorzystaniem podpisu elektronicznego, które prowadzone są w ramach implementacji dyrektywy usługowej tylko z certyfikatem kwalifikowanym wiązana jest możliwość osiągnięcia transgranicznej interoperacyjności procedur elektronicznych jeszcze przed utworzeniem europejskich mechanizmów walidacji e-podpisu. Wprowadzenie podpisu zaawansowanego, który nie wymaga stosowania tzw. bezpiecznego urządzenia powinno być zatem wdrażane z ostrożnością oraz bez szkody dla rozwiązań dotychczas istniejących. Podpis zaawansowany odmiennie do podpisu opartego o kwalifikowany certyfikat nie posiada wystandaryzowanego profilu w skali Unii Europejskiej i realizowany jest w ponad dwudziestu różnych modelach implementacji. Państwa członkowskie mają swobodę wyboru technologii zaawansowanych podpisów elektronicznych dla potrzeb krajowych zastosowań. Niemniej w chwili obecnej prowadzone są prace zmierzające do wybrania jednego formatu referencyjnego dla podpisu zaawansowanego, który powinien być uznawany przez wszystkie państwa członkowskie w procedurach transgranicznych.

Jako wzorcowy przykład wdrożenia podpisu zaawansowanego podawany jest częstokroć przykład Danii, gdzie certyfikaty OCES wykorzystane są we wszystkich systemach e-government. Kraj ten po nieudanych próbach upowszechnienia podpisu kwalifikowanego przeszedł na wyłączne stosowanie podpisów zaawansowanych. Certyfikaty dla osób fizycznych są udostępniane nieodpłatnie. Niemniej przygotowanie centrum certyfikacji kosztowało 5.7 mln EUR³ i wymaga co roku dalszych nakładów na podtrzymanie jego działalności. Podpis elektroniczny dla osób fizycznych dostępny jest nieodpłatnie, a podpisy osób prawnych oraz inne usługi certyfikacyjne udostępniane są na zasadach komercyjnych. Wadą tego rozwiązania jest brak certyfikatu kwalifikowanego. Przedsiębiorcy duńscy, którzy będą chcieli korzystać z procedur elektronicznych w innych państwach członkowskich będą zmuszeni do zakupu certyfikatu kwalifikowanego. Sama Dania obowiązana jest natomiast do uznawania kwalifikowanych certyfikatów na podstawie dyrektywy wspólnotowej.

Mimo niewątpliwie niższej ceny spowodowanej m.in. brakiem bezpiecznego urządzenia mankamentem podpisów zaawansowanych pozostaje brak jednolitego poziomu standardów technicznych i organizacyjnych w poszczególnych państwach, a przez to brak interoperacyjności w procedurach administracyjnych, które muszą obecnie dopuszczać uczestnictwo obywateli z innych państw członkowskich. Przewidziany w systemach prawnych przynajmniej piętnastu państw członkowskich podpis kwalifikowany, chociaż również wymaga dodatkowych prac dla zapewnienia paneuropejskiej interoperacyjności, stanowi obecnie podstawę wspólnotowych działań na rzecz transgranicznych procedur elektronicznych.

USTAWA O PODPISACH ELEKTRONICZNYCH. Wprowadzenie nowych usług certyfikacyjnych w zakresie podpisu elektronicznego pozwoli urzędowi i przedsiębiorcom na lepsze dostosowanie rodzaju i ceny stosowanych elektronicznych narzędzi podpisywania

³ Dane pochodzą z raportu “Study PKI and Certificate Usage in Europe 2006”, Fraunhofer Institute FOKUS, 31 Październik 2006, str. 24

i uwierzytelnienia. Ponieważ usługi certyfikacyjne posiadają co do zasady charakter komercyjnych nie jest wskazane, aby ustawowo wpływać na cenniki podmiotów komercyjnych. Podstawowym narzędziem dostępnym w tym zakresie pozostaje natomiast dywersyfikacja usług oraz podniesienie konkurencyjności rynku usług certyfikacyjnych.

Proponuje się wprowadzenie czterech rodzajów podpisu elektronicznego – „zwykłego”, „zaawansowanego” – czyli spełniającego dodatkowe wymogi dotyczące uwierzytelnienia składającego oraz bezpieczeństwa samej technologii podpisu, „urzędowego” – czyli szczególnej postaci podpisu zaawansowanego opartej o określoną specyfikację (m.in. w odniesieniu do certyfikatu i formatu e-podpisu) uznawanego przez wszystkie organy władzy publicznej, a także „kwalifikowanego” – czyli zaawansowanego podpisu weryfikowanego przez certyfikat kwalifikowany, złożonego za pomocą bezpiecznego urządzenia do składania podpisów pozostającego pod wyłączną kontrolą składającego podpis. Realizacja podpisu osoby prawnej zapewniona zostanie poprzez rozszerzenie definicji „podpisującego”. Podpis tego rodzaju (w tym jego szczególna postać pieczęć elektroniczna) będzie podpisem zaawansowanym powiązany z osobami prawnymi oraz jednostkami organizacyjnymi nie posiadającymi osobowości prawnej („pieczęć elektroniczna”). Propozycja Ministerstwa Gospodarki oparta zostanie na możliwie dokładnym odwzorowaniu terminologii zawartej w Dyrektywie 1999/93/WE z zastrzeżeniem, że konieczne będzie wprowadzenie również nowych usług certyfikacyjnych, które nie zostały przewidziane w dyrektywie.

PODPIS „ZWYKŁY”. Podpis niekwalifikowany zostanie w ustawie o podpisach elektronicznych utrzymany co do zasady w istniejącym dotychczas kształcie. Śladem wspólnotowej dyrektywy podkreślona została istota podpisu elektronicznego jako „metody uwierzytelnienia” („method of authentication”). W ślad za rozwiązaniami przyjętymi we wspólnotowej dyrektywie zostanie utrzymana podstawowa dla tego rodzaju podpisu elektronicznego zasada niedyskryminacji zawarta w art. 8, która stanowi że „Nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego”. Podkreślić należy, że ograniczone możliwości wykorzystania narzędzia jakim jest podpis niekwalifikowany wynikały częstokroć z ustaw innych niż ustawa o podpisie elektronicznym. Przykładem prawnych ograniczeń, które stanęły na przeszkodzie w wykorzystaniu samorządowych centrów certyfikacji świadczących usługi na poziomie niekwalifikowanym jest art. 63 § 3a KPA, który nakładał wymóg stosowania bezpiecznego podpisu elektronicznego przy składaniu podań. Podkreślić należy, że możliwość uznawania tego rodzaju podpisu elektronicznego w administracji publicznej zależeć będzie od dostępności w urzędach mechanizmów weryfikacji tego rodzaju podpisów elektronicznych. Problem ten zostanie rozwiązany w aspekcie prawnym stosowaną nowelizacją ustawy o informatyzacji, która przewiduje również zmiany w niektórych innych ustawach, w tym Kodeksie Postępowania Administracyjnego. Niezbędne jest jednak zniesienie wymogów, które stanowią zbędne obciążenia dla podmiotów świadczących ten rodzaj podpisu elektronicznego. Przykładem takich nadmiarowych wymogów znoszonych ustawą o podpisach elektronicznych jest m.in. obowiązek zawierania na piśmie umów z subskrybentem. Zniesiony zostaje również nadzór ministra nad świadczeniem usług niekwalifikowanych, gdyż podstawowym czynnikiem wymuszającym podnoszenie jakości w tym zakresie jest obecnie sam rynek wymuszający scertyfikowanie w międzynarodowych systemach akredytacji.

PODPIS „ZAAWANSOWANY”. Zaawansowany podpis elektroniczny może występować zarówno w powiązaniu z kwalifikowanym certyfikatem, jak i innego rodzaju certyfikatami. Podpis tego rodzaju mógłby być składany zarówno z użyciem bezpiecznego urządzenia do składania e-podpisu jak i bez takiego urządzenia (np. w oparciu o rozwiązania wyłącznie softwareowe). Zgodnie ze zmienioną definicją urządzenia do składania podpisu będzie to skonfigurowany sprzęt lub oprogramowanie używane do wykorzystania danych służących do składania podpisu. Bezpieczne urządzenie służące do składania podpisów będzie wymagało spełnienia wymogów określonych w Załączniku III do wspólnotowej dyrektywy. Podpis zaawansowany będą mogły składać zarówno osoby fizyczne jak i prawne. Zaawansowany podpis elektroniczny zapewni integralność danych opatrzone tym podpisem i jednoznaczne wskazanie certyfikatu, w ten sposób, że rozpoznawalne są wszelkie zmiany tych danych oraz zmiany wskazania certyfikatu wykorzystywanego do weryfikacji e-podpisu. Dane w postaci elektronicznej opatrzone zaawansowanym podpisem elektronicznym będą umożliwiały ustalenie tożsamości podpisującego. Dane w postaci elektronicznej opatrzone zaawansowanym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu będą umożliwiały wywołanie skutków prawnych określonych w odrębnych przepisach. Przewiduje się, że zaawansowany podpis elektroniczny weryfikowany przy pomocy kwalifikowanego certyfikatu będzie wywoływał skutki prawne jeśli został złożony w okresie ważności tego certyfikatu.

Zaawansowany podpis elektroniczny może występować w szczególności bez certyfikatów kwalifikowanych. Opracowany przez Komisję Europejską „Plan działania na rzecz e-podpisu i e-identyfikacji ...” stwierdza m.in., że w przeciwieństwie do podpisów kwalifikowanych, zaawansowane e-podpisy nie otrzymały w dyrektywie w sprawie podpisów elektronicznych takiego samego jasnego statusu prawnego zakładającego ich równoważność z podpisem odręcznym. Państwa członkowskie mają jedynie obowiązek zapewnić, żeby zaawansowanemu e-podpisowi nie odmawiano skuteczności prawnej jedynie dlatego, że jest w formie elektronicznej. Oznacza to, że państwa członkowskie mają większą swobodę decyzji w sprawie akceptowania lub nieakceptowania określonych rodzajów zaawansowanego e-podpisu i przy podejmowaniu tej decyzji mogą się kierować własnymi wymogami dotyczącymi danego zastosowania podpisu. Dodatkowa trudność wiąże się z faktem, że wprawdzie zaawansowany e-podpis może być w teorii akceptowany w innym państwie członkowskim, ale w praktyce akceptacja taka następuje z trudnością ze względu na różnorodne rozwiązania techniczne, które są stosowane. W związku z tym walidacja zaawansowanego e-podpisu przez odbiorcę oraz ocena skuteczności prawnej czy poziomu bezpieczeństwa tego podpisu w kontekście danego zastosowania stanowią obecnie bardzo trudne zadania, które wymagają często szczegółowego badania każdego otrzymanego podpisu. Ponieważ definicja zaawansowanego podpisu elektronicznego zawarta w art. 2 ust. 2 dyrektywy w sprawie podpisów elektronicznych ma charakter ogólny, państwa członkowskie stosują bardzo różnorodne rozwiązania techniczne, które mają różne poziomy bezpieczeństwa. W przypadku niektórych zastosowań tych podpisów państwa członkowskie mogą również wymagać obowiązkowego stosowania określonych rozwiązań krajowych, co tworzy dodatkowe bariery dla transgranicznego stosowania podpisów zaawansowanych.

PODPIS URZĘDOWY. Ten rodzaj podpisu elektronicznego nie został przewidziany w dyrektywie wspólnotowej. Będzie to szczególny rodzaj podpisu zaawansowanego oparty o certyfikat urzędowy. Dane w postaci elektronicznej opatrzone podpisem urzędowym weryfikowanym za pomocą urzędowego certyfikatu będą równoważne pod względem skutków prawnych dokumentom opatrzonym podpisem własnoręcznym na zasadach, które

zostaną określone w KPA oraz przepisach odrębnych. Jego wprowadzenie do ustawy wynika z potrzeby zapewnienia jednego formatu podpisu dla potrzeb administracji publicznej przy równoległym zapewnieniu pluralizmu rozwiązań komercyjnych. Podpis tego rodzaju mógłby być wydawany przez podmiot spełniający wymogi specyfikacji zawartej w rozporządzeniu wydawanym przez ministra właściwego do spraw informatyzacji w uzgodnieniu z ministrem właściwym do spraw gospodarki. W szczególności wydawanie tego rodzaju podpisów elektronicznych mogłyby prowadzić organy władzy publicznej lub istniejące centra certyfikacji. Jednym z możliwych zastosowań tego rodzaju podpisu elektronicznego będzie wydawanie elektronicznych dokumentów identyfikacyjnych (kart municypalnych, dowodów tożsamości i innych). Zgodnie z koncepcją European Citizenship Card (ECC) podpis elektroniczny do kontaktów z administracją stanowi obowiązkową część składową dokumentów identyfikacyjnych. Mimo oparcia wspólnotowej dyrektywy (i w ślad za tym ustawy o podpisie elektronicznym) na założeniu, że usługi certyfikacyjne posiadają co do zasady charakter komercyjny brak jest zasadniczych przeszkód dla aktywności państwa w tej dziedzinie, w tym m.in. poprzez wydawanie elektronicznych dokumentów z kluczem do składania e-podpisu (eID) lub tworzenie urzędów certyfikujących w ramach poszczególnych projektów informatyzacji państwa.

BEZPIECZNY PODPIS ELEKTRONICZNY. Zgodnie z art. 5 ust. 1 wspólnotowej dyrektywy Państwa członkowskie obowiązane są zapewnić, że zaawansowane podpisy elektroniczne oparte o *kwalikowany certyfikat i złożone za pomocą bezpiecznego urządzenia do składania podpisu* „spełniają wymogi prawne podpisu w odniesieniu do danych w formie elektronicznej w ten sam sposób, co podpis odręczny w odniesieniu do danych znajdujących się na papierze” oraz „są dopuszczalne jako dowód w postępowaniu sądowym”. Ten rodzaj podpisu elektronicznego oparty o kwalifikowany certyfikat i bezpieczne urządzenie jest rozwiązaniem funkcjonującym pod rządami ustawy obecnie obowiązującej. W nomenklaturze wspólnotowej jest to tzw. **„podpis kwalifikowany”**. W ustawie o podpisach elektronicznych odchodzi się od pojęcia „bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu” na rzecz pojęcia „podpisu kwalifikowanego”. W chwili obecnej Polska jest jednym z ostatnich krajów w Europie, który używa określenia bezpieczny podpis elektroniczny. W styczniu br. nazwę bezpieczny podpis elektroniczny zastąpiła podpisem kwalifikowanym w nowelizacji swojej ustawy o podpisie elektronicznym Republika Austrii. Nazwa „bezpieczny podpis elektroniczny” była jedynie przyjętą nazwą kategorii podpisu elektronicznego, a nie bezwzględną gwarancją bezpieczeństwa tego narzędzia. W świetle nowej systematyki podpis kwalifikowany będzie to kwalifikowana postać podpisu zaawansowanego składana przy pomocy bezpiecznego urządzenia i weryfikowana przy pomocy certyfikatu kwalifikowanego. Tylko bezpieczny podpis elektroniczny (kwalifikowany wg. terminologii wspólnotowej) cechować będzie uniwersalność zastosowania oraz moc prawna równa w każdym przypadku podpisom własnoręcznym. Podpis tego rodzaju powiązany będzie wyłącznie z osobami fizycznymi, co wynika z wymogu podawania w certyfikacie kwalifikowanym imienia i nazwiska lub ewentualnie pseudonimu. Zgodnie z obowiązującymi standardami podpis tego rodzaju będzie służył wyłącznie do podpisywania oświadczeń wiedzy oraz woli (bez możliwości autentykacji lub szyfrowania). Przyjęcie takiego założenia służy zapewnieniu pewności interpretacji, czy użycie podpisu elektronicznego miało na celu podpisanie czy autentykację do systemu.

2. CELE WPROWADZENIA USTAWY:

- 1) Obniżenie ceny podpisów elektronicznych poprzez rozszerzenie katalogu dostępnych usług certyfikacyjnych, w tym zwłaszcza katalogu dostępnych rodzajów podpisu elektronicznego, co umożliwi lepsze dostosowanie narzędzi oraz ceny do potrzeb przedsiębiorców i administracji publicznej. Zmniejszenie obciążeń biurowatycznych.
- 2) Aktualizacja ustawodawstwa w zakresie podpisu elektronicznego do potrzeb w zakresie informatyzacji państwa.
- 3) Dostosowanie terminologii krajowych unormowań w zakresie podpisów elektronicznych do Dyrektywy Parlamentu Europejskiego i Rady z dnia 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (99/93/WE) oraz uwzględnienie prowadzonych obecnie prac nad interoperacyjnością podpisu elektronicznego we Wspólnocie.

Ad. pkt 1) obniżenie ceny podpisu elektronicznego poprzez rozszerzenie katalogu dostępnych usług certyfikacyjnych. W projekcie ustawy proponuje się:

- 1) Dopuszczenie nowych usług certyfikacyjnych w zakresie podpisu elektronicznego, co pozwoli urzędowi i przedsiębiorcom na lepsze dostosowanie rodzaju i ceny stosowanych elektronicznych narzędzi podpisywania i uwierzytelnienia. Wprowadzenie podpisu zaawansowanego pozwoli na składanie podpisów opartych także o kwalifikowany certyfikat ale bez konieczności posiadania bezpiecznego urządzenia do składania podpisu elektronicznego. Brak wykorzystania bezpiecznego urządzenia obniży wprawdzie wysoki poziom bezpieczeństwa ale pozwoli w zgodzie z dyrektywą wspólnotową wprowadzić nową kategorię podpisu elektronicznego, którego składanie będzie możliwe przy pomocy tańszych urządzeń do składania podpisu elektronicznego. Podpis tego rodzaju może zostać zastosowany np. przy składaniu faktur elektronicznych. W zgodzie z dyrektywą w nowej ustawie proponuje się trzy podstawowe kategorie podpisu elektronicznego: podpis zwykły, podpis zaawansowany oraz szczególną postać podpisu zaawansowanego, którą jest kwalifikowany podpis elektroniczny. Proponuje się wprowadzenie również podpisu urzędowego dodanego na wniosek MSWiA w związku z projektem elektronicznego dowodu tożsamości pl.ID.
- 2) Zgodnie z postulatami przedsiębiorców wprowadzony zostanie podpis osoby prawnej oraz pieczęć elektroniczna. Wprowadzenie nowej definicji „podpisującego”, która obejmuje również osoby prawne i jednostki organizacyjne pozwoli na powiązanie podpisu z podmiotem, stanowiąc znaczące ułatwienie i obniżenie kosztów w prowadzeniu działalności gospodarczej. Np., przedsiębiorcy zwracali uwagę, że składanie deklaracji ZUS wymaga częstokroć więcej niż jednego bezpiecznego podpisu elektronicznego, gdyż powiązanie tego rodzaju podpisu z konkretnymi osobami jest niedogodne w przypadku urlopu lub zmiany pracownika.
- 3) Uproszczono system rejestracji podmiotów świadczących usługi certyfikacyjne na poziomie kwalifikowanym poprzez zniesienie kontroli wstępnej i opłaty w wysokości 10000 Euro. Pozostałe wymogi dla centrów kwalifikowanych są określone międzynarodowymi standardami ETSI i nie mogą zostać obniżone poniżej poziomu określonego we wspólnotowych dokumentach standaryzacyjnych.

- 4) Wprowadzone zostały nowe usługi, takie jak m.in. certyfikaty atrybutów. Usługa ta pozwoli na wprowadzanie części danych zawartych dotychczas w certyfikacie kwalifikowanym do dodatkowego certyfikatu związanego z certyfikatem kwalifikowanym. Wprowadzone rozwiązanie pozwala na możliwość zmiany dodatkowych danych bez konieczności zakupu nowego certyfikatu kwalifikowanego.
- 5) W ramach znoszenia obciążeń administracyjnych zasady kontroli podmiotów świadczących usługi certyfikacyjne zostaną dostosowane do zmian wprowadzanych ustawą o swobodzie działalności gospodarczej.

Ad. pkt 2) – aktualizacja ustawy do potrzeb w zakresie informatyzacji państwa:

1. Przeprowadzono aktualizację rozwiązań prawnych przyjętych w ustawie do potrzeb oraz działań związanych z informatyzacją urzędów administracji publicznej. Kwalifikowana i zwykła usługa znakowania czasem powiązana została z czasem urzędowym.
2. Na wniosek MSWiA wprowadzono nową kategorię podpisu urzędowego weryfikowanego przy pomocy certyfikatu urzędowego. Postulat ten został zgłoszony w związku z prowadzonymi pracami nad elektronicznym dowodem tożsamości pl.ID. Ponieważ sama ustawa nie reguluje okresu ważności certyfikatów dostosowanie w tym względzie dla potrzeb certyfikatów powiązanych z dowodem osobistym nastąpi w drodze aktów wykonawczych.
3. Wprowadzona zostanie lista zaufania kwalifikowanych podmiotów świadczących usługi certyfikacyjne, która może być wykorzystana zarówno w mechanizmach weryfikacji zawartych na ePUAP, jak i stanowi ważny element budowy europejskiej listy zaufania lub wymiany danych w tym zakresie pomiędzy systemami z różnych państw. Zmiany w tym zakresie wynikają z kierunków prowadzonych obecnie prac wspólnotowych w zakresie wzajemnego uznawania podpisu elektronicznego.
4. Zmiana przepisów dotyczących uznawania certyfikatów z zagranicy pozwoli na włączenie w obrót prawny certyfikatów zwykłych i kwalifikowanych wydanych w innych krajach Unii Europejskiej. Rozwiązanie to zastępuje anachroniczne uregulowania przyjęte w dotychczas obowiązującej ustawie przyjętej przed przystąpieniem do Unii Europejskiej. Oczekiwać należy, że w miarę poprawy dostępności produktów podpisu elektronicznego z innych państw podniesiona zostanie konkurencyjność krajowych usług certyfikacyjnych.
5. Z nadzoru sprawowanego przez ministra właściwego do spraw gospodarki wyłączono świadczenie usług certyfikacyjnych, które nie mają charakteru usług kwalifikowanych. Liberalizacja w tym zakresie jest zgodna z rozwiązaniami w zakresie modelu nadzoru przyjętymi w wielu innych państwach Unii Europejskiej.

Ad. pkt 3) – Dostosowanie do terminologii Dyrektywy Parlamentu Europejskiego i Rady z dnia 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (99/93/WE)

Obowiązująca ustawa o podpisie elektronicznym zapewniła ramy prawne dla dwóch rodzajów podpisu elektronicznego: tzw. podpisu "zwykłego" oraz bezpiecznego podpisu

elektronicznego weryfikowanego ważnym certyfikatem kwalifikowanym. W dyrektywie 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych mowa jest o trzech rodzajach podpisu cyfrowego. Pierwszym z nich jest najprostszy „podpis elektroniczny”, posiadający szerokie znaczenie. Podpis taki służy do weryfikacji tożsamości i uwierzytelniania danych. Drugim zdefiniowanym w dyrektywie rodzajem podpisu elektronicznego jest „zaawansowany podpis elektroniczny”. Podpis taki musi spełniać wymagania określone w art. 2 ust. 2 dyrektywy. Dyrektywa nie preferuje żadnej technologii, ale w praktyce definicja ta dotyczy głównie podpisów elektronicznych opartych na infrastrukturze klucza publicznego (PKI). W rozwiązaniu tym dane podpisywane są z wykorzystaniem technik szyfrowania, które wymagają użycia klucza prywatnego. W art. 5 ust. 1 dyrektywy mowa jest o trzecim rodzaju podpisu cyfrowego, który w dyrektywie nie otrzymał własnej nazwy a w dokumentach wspólnotowych nazywany jest „kwalifikowanym podpisem elektronicznym”. Podkreślając znaczenie konieczności korzystania z wielu rodzajów podpisu elektronicznego ustawa, w ślad za nazwą dyrektywy wspólnotowej, została nazwana ustawą o podpisach elektronicznych. Podpisy te posiadają zróżnicowany poziom bezpieczeństwa i mogą być stosowane do zastosowań o różnych poziomach ryzyka. Oznacza to, że najdroższa kategoria bezpiecznego podpisu elektronicznego nie musi być stosowana na wyłączność i może współwystępować z różnymi rodzajami e-podpisu, w tym takimi które weryfikowane będą przez certyfikaty zwykłe (wydawane na przykład przez samorządowe urzędy certyfikacji).

Wprowadzone zostały inne postulowane w opiniach ekspertów zmiany. W szczególności usunięta została definicja bezpiecznego urządzenia do weryfikacji podpisu elektronicznego, która nie występuje w dyrektywie wspólnotowej. Zmieniona została definicja urządzenia do składania podpisu elektronicznego, które obecnie może być złożone z komponentu programistycznego lub sprzętowego. Upřednio urządzenie do składania podpisu elektronicznego zawsze musiało zawierać komponent techniczny. W miejsce zaświadczenia elektronicznego wprowadzono zgodnie z nomenklaturą wspólnotową termin certyfikat.

3. KONSULTACJE SPOŁECZNE:

Projekt ustawy został przedstawiony do zaopiniowania kwalifikowanym podmiotom świadczącym usługi certyfikacyjne, producentom oprogramowania do składania i weryfikacji podpisu elektronicznego oraz producentom urządzeń do identyfikacji biometrycznej. W konsultacjach włączone zostały następujące organizacje przedsiębiorców: Polskie Towarzystwo Informatyczne (PTI), Polska Izba Informatyki i Telekomunikacji (PIIT), Krajową Izbą Gospodarczą (KIG), Krajową Izbą Gospodarczą Elektroniki i Telekomunikacji (KIGEiT), Związek Banków Polskich, Stowarzyszenie Internet Society Polska (ISOC), Stowarzyszenie „Miasta w Internecie”, Stowarzyszenie „Podpis Elektroniczny – Mobilny Internet”, PKPP Lewiatan oraz Business Center Club. Projekt przedstawiony został również Komisji Wspólnej Rządu i Samorządu Terytorialnego oraz Komisji Kodyfikacyjnej Prawa Cywilnego.

W toku przeprowadzonych konsultacji społecznych oraz uzgodnień międzyresortowych wprowadzono szereg zmian w projekcie ustawy. Wynik uzgodnień wskazywał w szczególności na konieczność dokonania zmian w ustawach innych, niż ustawa o podpisie elektronicznym. Zdecydowano się zatem na wydłużenie terminu uzgodnień

międzyresortowych oraz zgłoszenie przez ministerstwa propozycji zmian w przepisach podległych danemu resortowi. W następstwie projekt został uzupełniony m.in. o propozycję zmian w Kodeksie cywilnym oraz w Kodeksie postępowania administracyjnego. Ze względu na niewielką ilość otrzymanych propozycji wprowadzono w ustawie dodatkowy termin dla Rady Ministrów na dostosowanie innych ustaw. W odniesieniu do usługi certyfikatów atrybutów wprowadzono możliwość świadczenia tego rodzaju usługi certyfikacyjnej zarówno w odniesieniu do certyfikatów zwykłych, jak i kwalifikowanych. Zdecydowano się odstąpić od narzucenia podmiotom kwalifikowanym obowiązku dostarczania aplikacji na główne systemy operacyjne. Jak wskazywano w uzgodnieniach podmioty kwalifikowane nie są jedynym deweloperem tego rodzaju oprogramowania i w znacznej mierze pozostają zależne od aplikacji dostępnych na rynku. Wymóg tego rodzaju stanowiłby dodatkowe obciążenie dla podmiotów chcących uczestniczyć na tym rynku oraz nie znajduje uzasadnienia w europejskich standardach dotyczących świadczenia usług na poziomie kwalifikowanym. Wydaje się, że rozwiązanie problemu wieloplatfornowości aplikacji podpisujących i weryfikujących należy upatrywać w podniesieniu konkurencyjności rynku usług certyfikacyjnych, w tym m.in. szerszemu niż dotychczas dopuszczeniu korzystania z usług certyfikacyjnych dostawców zagranicznych.

W odniesieniu do podmiotów kwalifikowanych wprowadzono pewne ułatwienia dotyczące sposobu prowadzenia działalności dotyczące możliwości przechowywania w postaci elektronicznej dokumentów związanych z prowadzeniem działalności certyfikacyjnej. Biorąc pod uwagę długi okres przechowywania tego rodzaju dokumentów jest to istotne udogodnienie dla podmiotów prowadzących lub przewidujących rozpoczęcie tego rodzaju działalności. Ze względu na brak zainteresowania instytucją datownika elektronicznego (time marking) zdecydowano się na rezygnację z tej usługi. Wydaje się, że ze względu na brak związku ze świadczeniem usług certyfikacyjnych tego rodzaju narzędzie mogłoby być ewentualnie regulowane przepisami dotyczącymi informatyzacji. Odstąpiono również od propozycji tzw. podpisu identyfikacyjnego i łącznego, które krytykowane były jako nadmiarowe w stosunku do zwykłego podpisu elektronicznego lub wielokrotnego podpisywania podpisem zaawansowanym.

Zgłaszana w trakcie konsultacji społecznych konieczność uwzględnienia prowadzonych obecnie prac wspólnotowych wymagała wprowadzenia długiego okresu *vacatio legis* dla przedmiotowej regulacji. Harmonogram prac wspólnotowych przewidziany w „Planie działań na rzecz e-podpisu i e-identyfikacji ...” zakłada, że w III kwartale br. prowadzone będą m.in. prace w zakresie opracowania nowych standardów referencyjnych dla podpisu elektronicznego. Prowadzone obecnie prace wspólnotowe, w tym w szczególności ustalenia w sprawie standardów referencyjnych, będą mieć istotny wpływ na treść aktów wykonawczych do ustawy o podpisach elektronicznych.

Projekt ustawy o podpisach elektronicznych został zamieszczony na stronie internetowej Ministerstwa Gospodarki, zgodnie z ustawą z dn. 7 lipca 2005 o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414). W toku prowadzonych prac nie wpłynęło żadne prawidłowe zgłoszenie działalności lobbingowej w przedmiocie procedowanego projektu ustawy.

4. ZAKRES OCENY SKUTKÓW REGULACJI:

Podmioty na które bezpośrednio oddziałuje projekt aktu prawnego to Ministerstwo Gospodarki, Narodowy Bank Polski oraz podmioty świadczące usługi certyfikacyjne.

Pośrednio projekt wpłynie na funkcjonowanie administracji publicznej oraz przedsiębiorców, poprzez m.in. umożliwienie korzystania z szerokiego katalogu podpisów elektronicznych oraz usług certyfikacyjnych związanych elektronicznymi podpisami. Przepisy ustawy wpływają na kwalifikowane podmioty świadczące usługi certyfikacyjne poprzez umożliwienie świadczenia nowych usług certyfikacyjnych, a zwłaszcza nowych rodzajów podpisu elektronicznego. W odniesieniu do prowadzenia listy podmiotów kwalifikowanych oraz zniesienia zaświadczeń i poświadczeń przepisy ustawy wpłyną na funkcjonowanie krajowego urzędu certyfikującego. Przepisy projektu ustawy wpływają też bezpośrednio na organ nadzoru, którym jest minister właściwy do spraw gospodarki poprzez uproszczenie systemu rejestracji i ograniczenie nadzoru wyłącznie do podmiotów kwalifikowanych.

5. SKUTKI WPROWADZENIA USTAWY:

• wpływ regulacji na dochody i wydatki sektora finansów publicznych (w tym budżetu państwa i budżetów jednostek samorządu terytorialnego)

Zniesiona zostanie opłata za wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne w zakresie podpisu elektronicznego. Opłata za wpis do rejestru posiadała charakter zryczałtowany i wynosiła 10.000 Euro. Przez cały okres obowiązywania ustawy od dnia 16 sierpnia 2006 opłata taka została uiszczona czterokrotnie. Uszczuplenie budżetu państwa w tym zakresie nie jest możliwe do oszacowania, gdyż trudno przewidzieć przyszłą liczbę podmiotów zainteresowanych wpisem do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Koszt wdrożenia projektowanej regulacji będzie związany z koniecznością modernizacji krajowego urzędu certyfikującego, poprzez m.in. nałożenie obowiązku prowadzenia listy podmiotów kwalifikowanych. Koszty te będą nieznaczące i obciążą budżet Narodowego Banku Polskiego, który w chwili obecnej prowadzi krajowy urząd certyfikujący. Ustawa nie wpłynie na budżety jednostek samorządu terytorialnego.

• wpływ regulacji na rynek pracy

W odniesieniu do nowych rodzajów usług certyfikacyjnych (takich jak m.in. podpis zaawansowany) podkreślić należy, że istnieją już standardy i rozwiązania techniczne, których przeniesienie do Polski poprzez opracowanie krajowych aplikacji podpisujących i weryfikujących oparte jest o dobrowolne działania podmiotów funkcjonujących na konkurencyjnym rynku. Niektóre usługi (takie jak certyfikaty atrybutów, potwierdzenie ważności certyfikatów), były uprzednio świadczone jako usługi nienazwane i obecnie zyskują jedynie wyraźne uregulowanie ustawowe. Wprowadzenie nowych usług certyfikacyjnych, w tym w szczególności nowych rodzajów podpisu elektronicznego pozytywnie wpłynie na konkurencyjność gospodarki. Oddziaływanie na sytuację i rozwój regionów nie będzie znaczne, chociaż upowszechnienie podpisu elektronicznego może pośrednio wpłynąć na ułatwienie dostępu do elektronicznej administracji w obszarach wiejskich oraz z zagranicy. W tym ostatnim przypadku szczególnie ważne jest zapewnienie niezawodnych mechanizmów uznawania podpisów wspólnotowych, co pozwoli na korzystanie z usług przedsiębiorców z innych krajów Europejskiego Obszaru Gospodarczego. Przyjęcie projektu sprawi, że polska administracja publiczna będzie bardziej przyjazna obywatelom i przedsiębiorcom. Zawarte w ustawie rozwiązania mające na celu zmniejszenie obciążeń regulacyjnych dla podmiotów kwalifikowanych skłonią większą grupę przedsiębiorców do podejmowania tego rodzaju działalności usługowej.

- ***zgodność z prawem Unii Europejskiej***

W zakresie swojej regulacji ustawa implementuje Dyrektywę Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych.