POLSKIE TOWARZYSTWO INFORMATYCZNE

ZARZĄD GŁÓWNY

02– 508 Warszawa, al. Puławska 39 lok. 4 tel: +48 22 838 47 05 fax: +48 22 636 89 87

Warszawa, 21 lipca 2009 r.

Szanowni Państwo,

przesyłam w załączeniu uwagi szczegółowe Polskiego Towarzystwa Informatycznego do projektu Ustawy o Podpisach elektronicznych w wersji przesłanej do uzgodnień międzyresortowych z 09.07.2009 roku.

Pragnę podkreślić, że uwagi o charakterze definicyjnym i ogólnym jakie przesłaliśmy w ramach poprzednich konsultacji nadal zachowały swą aktualność. Jednak w związku z przyjęciem przez MG innej koncepcji regulacji problematyki podpisu elektronicznego niż sugerowaliśmy, są one nie do uwzględnienia w sposób kompleksowy w przesłanym projekcie.

W tej sytuacji na etapie kolejnych uzgodnień międzyresortowych **zgłaszamy wyłącznie uwagi o charakterze szczegółowym, mając na względzie wyeliminowanie z ustawy najpoważniejszych dostrzeżonych uchybień.**

Deklarujemy też chęć uczestnictwa w konferencji uzgodnieniowej.

Z poważaniem

Wiesław Paluszyński

wiceprezes Polskiego Towarzystwa Informatycznego

Uwagi Polskiego Towarzystwa Informatycznego
do projektu Ustawy o podpisach elektronicznych z 09.07.2009r.

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 1	1. W zakresie przedmiotowym: Zwraca się uwagę, że podpis elektroniczny wcale nie musi być weryfikowany certyfikatem; ograniczenie zakresu zamyka ustawę na postęp technologiczny, ograniczając podpis elektroniczny jedynie do modelu podpisu opartego na PKI Należy przyjąć definicję usług certyfikacyjnych za Dyrektywą i nie wprowadzać do ustawy innych pojęć niż w Dyrektywie – w ten sposób zapewni się interoperacyjność z rozwiązaniami przyjętymi w innych krajach UE. Przyjęty zapis w projekcie narusza wyrażoną w dyrektywie zasadę niedyskryminacji tj iż nie można odmówić skuteczności podpisowi tylko na tej podstawie .. iż jest on np. weryfikowany w inny sposób niż na podstawie certyfikatu.	Przyjąć zapisy z Dyrektywy: 1. Ustawa określa warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi. 2.Ustawa nie dotyczy stosunków prawnych powstałych na podstawie zawartych umów regulujących zasady stosowania oświadczeń woli w postaci elektronicznej za wyjątkiem powszechnie obowiązujących przepisów dotyczących skutków prawnych odnoszących się do podpisu kwalifikowanego , zaawansowanego osobistego oraz usługi znakowania czasem
Brakujący artykuł	Ustawa powinna mieć też zakres podmiotowy tj wskazywać kogo dotyczy a kogo nie np. nie powinna odnosić się do stosunków wewnętrznych np wewnątrz przedsiębiorstwa, zakładu administracyjnego np. uczelni etc.. W starej ustawie należy jedynie dokonać drobnej korekty	Art. 2 Przepisy ustawy stosuje się do podmiotów świadczących usługi certyfikacyjne, mających siedzibę- na terytorium Rzeczypospolitej Polskiej, z zastrzeżeniem art. 4
Art. 2.3)	*podpis osobisty - zaawansowany podpis elektroniczny weryfikowany przy pomocy ważnego certyfikatu, składany przez podpisującego będącego osobą fizyczną, przy pomocy danych służących do składania podpisu elektronicznego zawartych w dokumencie tożsamości;*	Nie rozumiemy, dlaczego uope narzuca się metodę weryfikacji podpisu osobistego; nie należy przesądzać, że będzie do tego służyć certyfikat zwłaszcza, że już obowiązujące już. przepisy np. kpc przewidują inny sposób weryfikacji! Wprowadzenie definicji analogicznej jak dla podpisu kwalifikowanego powiela błąd zawarty w definicji podpisu kwalifikowanego (weryfikacja za pomocą ważnego certyfikatu kwalifikowanego), który to błąd z definicji podpisu kwalifikowanego już usunięto (zob. art. 2.5)) Propozycja PTI: *„podpis osobisty oznacza zaawansowany podpis elektroniczny składany przez podpisującego, będącego osobą fizyczną przy pomocy danych służących do składania podpisu elektronicznego zawartych w dowodzie osobistym”*
Art. 2.4)	*Pieczęć elektroniczna - dane w postaci elektronicznej, przyporządkowane danemu podmiotowi w taki sposób, że możliwa jest jego identyfikacja, dołączone do innych danych lub z nimi logicznie powiązane tak, że każda późniejsza zmiana tych danych jest wykrywalna;*	Dlaczego pieczęć nie ma być podpisem zaawansowanym? Propozycja PTI: *„pieczęć elektroniczna” – zaawansowany podpis elektroniczny uwierzytelniający podmiot.*
Art. 2 7)	weryfikacja podpisu elektronicznego – proces umożliwiający identyfikację podpisującego i stwierdzenie, że podpis został złożony za pomocą danych, o których mowa w ust. 7 oraz że podpisane dane nie uległy zmianie po jego złożeniu;	‘proces’ ma kontekst techniczny i jako pojęcie niezdefiniowane w ustawie nie powinien być używany, definicja sugeruje, żę proces ten może być wyłącznie pozytywny, co nie jest zgodne z prawdą Propozycja PTI - usunąć

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 2.9)	Dokładność synchronizacji – różnica czasu, który w dowolnie wybranej chwili nie różni się od czasu urzędowego lub czasu UTC(PL) o więcej niż ustaloną wartość	brak uzasadnienia dla umieszczenia tak technicznego pojęcia w uope ponadto, ostatnia zmiana pozbawiła tę definicję sensu (różnica czasu, która nie różni się) Propozycja PTI: Usunąć
Art. 2.10)	Urządzenie do składania podpisu elektronicznego jest to skonfigurowany sprzęt lub oprogramowanie stosowane w celu składania podpisu elektronicznego.	Definicja za szeroka. Jest to praktycznie całe środowisko składania podpisu, nad którym podpisujący miał UTRZYMAĆ wyłączną kontrolę . Istotą tego pojęcia jest zabezpieczenie nie całego procesu, a tych części procesu w których jest możliwy dostęp do danych do składania podpisu. Propozycja PTI: „urządzenie do składania podpisu elektronicznego" oznacza skonfigurowany sprzęt lub oprogramowanie, które jest przeznaczone do przechowywania, użycia i innych czynności z udziałem danych do składania podpisu elektronicznego
Art. 2.11)	bezpieczne urządzenie do składania podpisu elektronicznego - urządzenie do składania podpisu elektronicznego, spełniające wymagania określone w niniejszej ustawie oraz przepisach wydanych na podstawie art. 25 ust. 3 oraz uznane za takie przez właściwe krajowe lub zagraniczne jednostki notyfikowane w oparciu o przepisy o systemie oceny zgodności (bezpieczne urządzenie);	Definicja jest sprzeczna z zasadami tworzenia definicji (wyróżnikiem pojęcia są jego atrybuty, zatem definiować można jedynie przez określenie atrybutów, a nie wymagań) ; tu wyróżnikiem pojęcia „bezpiecznego urządzenia" jest fakt, że spełnia wymagania (?). Ponadto, niedopuszczalne jest definiowanie pojęcia odniesieniem do aktu prawnego niższego rzędu (art. 25 Ust. 3) **Rekomendacja: Bezpieczne urządzenie powinno zostać wprowadzone artykułem ustawy tak, jak dotychczas, tym bardziej, że w art. 25 ust. 1 te wymagania dot. bezpiecznego urządzenia są określone, zatem definicja jest nadmiarowa**.
Art. 2.12)	Urządzenie do weryfikacji podpisu elektronicznego jest to skonfigurowany sprzęt lub oprogramowanie służące do weryfikacji podpisu	Uzasadnienie jak dla propozycji 2.10) Propozycja PTI: urządzenie służące do weryfikacji podpisów" oznacza skonfigurowane oprogramowanie lub sprzęt które jest przeznaczone do przechowywania, użycia i innych czynności z udziałem danych służących do weryfikacji podpisu elektronicznego;
Art. 2.14)	Podmiot kwalifikowany (..)	Podkreślamy stanowczo, że zgodnie z Dyrektywą, kwalifikowane są USŁUGI, a nie podmioty, które je świadczą. Zapis w projekcie jest sprzeczny z Dyrektywą. **Propozycja PTI** Usunąć definicję i wszystkie odwołania do pojęcia „podmiotu kwalifikowanego w Ustawie
Art. 2.15)	certyfikat - zaświadczenie elektroniczne, za pomocą którego dane do weryfikacji podpisu elektronicznego są przypisywane podpisującemu, umożliwiając jego identyfikację; jeżeli podpisującym jest osoba fizyczna certyfikat może zawierać jej dane biometryczne.	Definicja w proponowanym brzmieniu jest niezgodna z Dyrektywą. Należy w szczególności podkreślić możliwe negatywne konsekwencje umieszczania danych WRAŻLIWYCH (w sensie społecznym i prawnym) w certyfikacie, który jest publikowany. **Rekomendacja: usunąć frazę „jeżeli podpisującym jest osoba fizyczna certyfikat może zawierać jej dane biometryczne**

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 2.18	Znakowanie czasem (..)	usługa czysto techniczna, brak przesłanek aby określać szczegółowo wymagania dla tej usługi oraz dla podmiotu, który świadczyłby taką usługę. Jeśli jednakże przeważyłaby opinia o potrzebie pozostawienia tej usługi w Ustawie, to definicja powinna być znacznie szersza niż dotychczasowa. Proponowana definicja jest oparta na koncepcji przyjętej w polskiej normie dot. usług znacznika czasu (PN ISO/IEC 18014-1): „usługa polegająca na dostarczaniu poświadczeń, że element danych istniał przed określonym punktem w czasie
Art. 4. 1)	Wprowadzono pojęcie „dobrowolnym systemie akredytacji	Dyrektywa nic nie mówi o systemie dobrowolnej akredytacji a jedynie o „dobrowolnej akredytacji”. Wykreślić słowo „system”
Art. 5.1		Nieprecyzyjny zapis może powodować wiele kontrowersji. Należy rozważyć następujące sytuacje a) w okresie zawieszenia podpis złożony jest ważny, zatem wywołuje skutki prawne (może to trwać kilka dni). b) popis złożony w czasie zawieszenia może zostać unieważniony w wyniku działania późniejszego, nawet jeśli wcześniej zawieszenie było anulowane. Dotychczasowa konstrukcja zapisu dotyczącego ważności podpisu złożonego w okresie zawieszenia była jasna i poparta praktyką międzynarodową. Niezrozumiała i nielogiczna jest zmiana zapisu.
Art. 5.3	„Dane w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym wywołują skutki dokumentu z podpisem własnoręcznym” – dane wywołują skutek prawny?? Podpis w odniesieniu do określonych danych wywołuje skutek prawny. Ustawa zgubiła fundamentalną zasadę równoważności podpisów!.	Zmienić na: *Złożenie(kwalifikowanego) podpisu elektronicznego na danych elektronicznych wywiera taki sam skutek prawny, jak złożenie podpisu własnoręcznego z zachowaniem formy pisemnej.*

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 7.1	Zapis w przyjętej formie daje tylko ograniczoną pewność co do czasu złożenia podpisu: „Uznaje się, że podpis elektroniczny znakowany czasem został złożony nie później, niż w chwili dokonywania tej usługi.”- ten zapis nie wnosi nic istotnego, co nie wynikałoby z definicji znacznika czasu. W szczególności, nie rozwiązuje problemu przypadku, jeśli podpis został złożony o wiele wcześniej niż wskazuje znacznik czasu. W takiej konstrukcji prawnej istnieje możliwość przeprowadzenia dowodu, że czynność prawna została dokonana wcześniej niż wskazuje znacznik czasu. Warto zwrócić uwagę, że istnieją konstrukcje usługi znacznika czasu, które umożliwiają wskazanie przedziału czasowego, w którym podpis został złożony. Ale wymaga rozszerzenia zakresu usługi znacznika czasu na dane (np. niepodpisane), a nie tylko na podpis. Usunięcie drugiego zdania z tego punktu znakomicie poszerza możliwości świadczenia usługi znakowania czasem!	Konsekwentnie, w całym projekcie usunąć odniesienie do znakowania czasem.
Art. 7.2	Przypisanie kwalifikowanemu znacznikowi czasu atrybutu daty pewnej w rozumieniu przepisów KC wzbudza w środowisku prawniczym wiele kontrowersji – w opinii autorów uwag przypisanie prostej czynności wstawienia znacznika czasu skutków równoważnych jednej z kwalifikowanych form pisemnych jest nieuprawnione. Daleko wykracza poza zakres wskazany w Dyrektywie.	Konsekwentnie, w całym projekcie usunąć odniesienie do kwalifikowanego znakowania czasem.
Art. 7.3	„Znakowanie czasem stanowi dowód tego, że usługa została wykonana w określonym czasie. Skutki prawne znakowania czasem określają przepisy odrębne. Jakie skutki prawne znakowania czasem określają przepisy odrębne? Zapis niezrozumiały	Rekomendujemy usunięcie zapisu.
Art. 8.2	zapis daje możliwość wystawiania certyfikatów kwalifikowanych przez MSWiA.. Prawo to może stanowić ogromny bodziec do realizacji własnych usług certyfikacyjnych i zaprzestania działania przez podmioty komercyjne	Rekomendujemy usunięcie zapisu wyłączenia dla MSWiA, ze względu na uzasadnione zagrożenie dla rozwoju wolnego rynku usług certyfikacyjnych
Art. 8.4 (usunięty)	z projektu usunięto zapis: „4. Podmiot kwalifikowany nie może wydawać certyfikatów kwalifikowanych w stosunkach prawnych, w których jest stroną, chyba że jest to niezbędne do wykonywania umowy z odbiorcą usług certyfikacyjnych.	Zapis ten zabezpieczał ustawowo przed konfliktem interesów. Niezrozumiałe jest jego usunięcie.
Art. 9.1	Pojęcie ‘odbiorcy usług certyfikacyjnych’ jest niepoprawne, ponieważ składa się z dwóch podmiotów, których relacja z podmiotem świadczącym usługi certyfikacyjne jest odmienna: subskrybenta, który zawiera umowę z dostawcą oraz tzw. strony ufającej, która umowy z dostawcą usługi nie ma, ale ufa certyfikatowi w oparciu o jego zawartość.	Usunąć pojęcie ‘odbiorcy usługi’ i wprowadzić do projektu w sposób opisowy osobę, dla której wydawany jest certyfikat (zawiera ona umowę o charakterze cywilnoprawnym z dostawcą usług, niezależnie czy w formie pisemnej czy nie – jest to fakt) oraz podmiotu (nie zawsze jest to osoba fizyczna), która ufa wynikowi weryfikacji podpisu dokonanej za pomocą certyfikatu (zob. uwagi do art. 22)

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 9.2	Zapis „**Odbiorca usług certyfikacyjnych, w okresie ważności certyfikatu służącego do weryfikacji podpisu elektronicznego**, jest obowiązany przechowywać dane do składania tego podpisu w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem" – jest niepoprawny. W odniesieniu do odbiorcy – zob uwaga wyżej; ponadto należy przewidzieć obowiązek ochrony danych przed utratą w całym okresie życia. Inaczej po latach nie będzie możliwości przeprowadzenia dowodu na złożenie podpisu.	„Podpisujący jest obowiązany zapewnić ochronę danych do składania podpisu elektronicznego przed utratą lub nieuprawnionym wykorzystaniem"
Art. 10.3 i 4	Podmiot, o którym mowa w ust. 1, jest obowiązany stosować oprogramowanie, sprzęt lub ich istotne składniki, które są używane do udostępnienia usług podpisu elektronicznego lub do składania lub weryfikacji podpisów elektronicznych, spełniające wymagania ogólnie uznanych norm ustalonych na podstawie art. 10 dyrektywy 1999/93/WE. Minister właściwy ds. gospodarki w drodze obwieszczenia publikuje wykaz norm, o których mowa w ust. Nie ma podstaw do narzucania KAŻDEMU podmiotowi świadczącemu usługi certyfikacyjne obowiązku stosowania norm z listy MG!	Doprecyzować „Podmioty świadczące usługi wydawania i zarządzania certyfikatami **kwalifikowanymi**
Art. 10-15	Rozczłonkowano na art. 10-11 i 13-16 znacząco skracając listę wymagań w odniesieniu do podmiotów świadczących usługi kwalifikowane; Jednocześnie, z jednego artykułu zrobiono cztery, przedzielając 11 i 13 art. 12 o zakresach rozporządzeń Niezrozumiała jest niezgodność tego przepisu z Załącznikiem II Dyrektywy, co powoduje pogorszenie warunków konkurencji polskich podmiotów na rynku UE	Doprowadzić do zgodności wymagań dot. podmiotów świadczących usługi certyfikacyjne w postaci wydawania i zarządzania certyfikatami kwalifikowanymi z Załącznikiem II Dyrektywy. [Ekspertyza – ea/zo] str. 68-72 oraz 156 Zob. też uwagi szczegółowe dot. art. 10-15 poniżej
Art. 11.2	Ten sam zapis występuje w dwóch miejscach" Podmiot, o którym mowa w ust. 1 opracowuje i publikuje politykę certyfikacji, Art. 24: 2. Polityka certyfikacji to dokument określający szczegółowe rozwiązania techniczne i organizacyjne oraz zakres i warunki bezpieczeństwa tworzenia i stosowania certyfikatów. W Załączniku II do Dyrektywy nie jest używany termin 'polityka certyfikacji'. W akcie prawnym rangi ustawy nie powinny być używane nadmiarowo pojęcia techniczne.	Należy usunąć art. 11. 2

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 14.2	wyłączono z zachowania tajemnicy certyfikacyjnej kontrolerów i podmioty nadzorujące CC. Może to stanowić pole do naruszeń tej tajemnicy.	Uwzględnić kontrolerów i podmioty sprawujące nadzór nad podmiotami świadczącymi usługi certyfikacyjne
Art. 15	Zwraca się uwagę, ze kwestia odpowiedzialności podmiotu świadczącego usługi nie jest jednakowa w stosunku do osoby ubiegającej się o certyfikat (subskrybentem) oraz tzw. strony ufającej i nie można ich określić jednym terminem „odbiorca usług certyfikacyjnych". Z subskrybentem zawiera on umowę, gdzie można zawrzeć ograniczenia odpowiedzialności; strona ufająca nie jest związana umową i nie musi przestrzegać np. polityki certyfikacji, zatem odpowiedzialność podmiotu świadczącego usługi certyfikacyjne jest deliktowa. Stad warto rozdzielić warunki odpowiedzialności dla subskrybenta i strony ufającej.	Wprowadzić zapisy bazujące na art. 6.1 Dyrektywy. Należy rozważyć konkretne zapisy dot. odpowiedzialności w . [Ekspertyza – ea/zo] – str. 21-24 oraz str. 157-159
Art. 15.3.1	Wyrażenie nieprecyzyjne :" jeżeli wartość ta została wskazana w certyfikacie" – z uwagi na ryzyko, że rozszerzenie, w którym zwykle takie ograniczenie jest wpisywane, może nie być prawidłowo rozpoznane przez oprogramowanie; proponowane zastrzeżenie stanowi dla podmiotów świadczących usługi certyfikacyjne silną motywację do stosowania powszechnie uznanych standardów a nie własnych, wewnętrznych rozwiązań.	Sugeruje się zmianę frazy na następującą: „jeśli ograniczenie to mogło być rozpoznane"
Art. 15.4	Niepoprawna jest konstrukcja odpowiedzialności gwaranta za „wszelkie szkody"; ponadto, warto zauważyć, że w różnych jurysdykcjach nie musi być solidarnej odpowiedzialności wystawcy i gwaranta, dlatego warto to sprecyzować.	Proponuje się następujący zapis: " Podmiot świadczący usługi certyfikacyjne, który udzielił gwarancji za powszechnie dostępny certyfikat zgodnie z art. 4 pkt 4, odpowiada wobec osób, które w rozsądnych granicach polegają na zawartości certyfikatu na tych samych zasadach, jakby był jego wydawcą. Odpowiedzialność wydawcy certyfikatu i gwaranta tego certyfikatu jest solidarna.
Art. 18.2	. Podmiot o którym mowa w ust. 1 obowiązany jest stosować komponenty techniczne i procedury, które zapewnią, że czas używany w systemach do znakowania czasem jest zgodny, **pośrednio lub bezpośrednio**, z czasem urzędowym lub czasem UTC(PL) z wymaganą **dokładnością synchronizacji.** Skąd wiadomo jaka dokładność jest wymagana?	Zob. uwagę do art. 7 Konsekwentnie należy zastosować to samo rozwiązanie.
Art. 18.3-6	Jakie jest uzasadnienie szczegółowych zapisów technicznych dot. synchronizacji czasu?	Rekomendujemy usunięcie zapisu; właściwym miejscem jest rozporządzenie o czasie urzędowym, które przedmiotowo nie należy do ustawy o podpisach elektronicznych

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 19.1	Definicja usług certyfikacyjnych jest b. nieprecyzyjna dlaczego tylko wydawanie certyfikatów, a unieważnianie już nie? I co takiego szczególnego jest w znakowaniu czasem ponad to, ze można je zastosować w celu długoterminowego przechowywania danych podpisanych elektronicznie? Ponadto, definicja jest nieprawidłowo skonstruowana, ponieważ zamiast opisu cech, zawiera katalog usług i wszystko to, czego nie potrafimy opisać. Daje to olbrzymie pole do swobodnych interpretacji. Jedyną formą usługi certyfikacyjnej w formie kwalifikowanej powinno być wydawanie i zarządzanie certyfikatami kwalifikowanymi. Warto podkreślić, że Dyrektywa nie dopuszcza innych usług kwalifikowanych niż wydawanie i zarządzanie certyfikatami.	Należy przyjąć definicję z Dyrektywy (pkt. 9 Preambuły): **usługi certyfikacyjne - usługi związane lub stosujące podpisy elektroniczne, w szczególności polegające na wydawaniu i zarządzaniu certyfikatami** i wprowadzić ją przed art. 2.17

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 19.3	*Podmiot kwalifikowany podpisując:* *1) certyfikat lub certyfikat kwalifikowany wydany w wykonaniu umów o świadczenie usług certyfikacyjnych,* *2) informacje o statusie certyfikatów, w tym listę zawieszonych lub unieważnionych certyfikatów,* *3)* certyfikaty na potrzeby realizacji czynności lub usług certyfikacyjnych związanych z certyfikatami kwalifikowanymi wydanymi przez ten podmiot *posługuje się danymi do składania podpisu elektronicznego powiązanymi z certyfikatem wydanym przez ministra właściwego ds. gospodarki.* Zapis ten wprowadza usługi " roota krajowego", a jednocześnie nie ma żadnych wymagań dotyczących świadczenia tych usług przez ministra gospodarki! W starej ustawie takie warunki dla podmiotu świadczącego usługi Roota krajowego były. Należy szczególnie podkreślić, że wiarygodność całego systemu podpisów kwalifikowanych opiera się właśnie na bezpieczeństwie i wiarygodności certyfikatu root'a. Ponadto, brak uzasadnienia dla objęcia usługą wydawania certyfikatów przez Roota dla zabezpieczenia czynności związanych z wydawaniem certyfikatów kwalifikowanych . W niektórych przypadka może nie być nawet technicznej możliwości zastosowania certyfikatów zewnętrznych do tych czynności. Czy jest to sposób na zapewnienie przychodów dla root'a ?	Należy zredagować wymagania dotyczące kwestii krajowego punktu zaufania i Ew. Roota. Jest to zasadniczy błąd w Ustawie, nie zdefiniowanie podstawowego punktu zaufania w systemie.
Art. 20.	Potwierdzenie ważności certyfikatu jest to usługa, która stwierdza w szczególności ważność lub zawieszenie certyfikatu w czasie jej wykonania oraz datę i czas potwierdzenia i jest opatrzona zaawansowanym podpisem elektronicznym podmiotu świadczącego tę usługę	Nie jest zrozumiałe, dlaczego najpierw wprowadza się pojęcie pieczęci elektronicznej a potem się z tego pojęcia nie korzysta

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 24.1i 2	„zwraca się uwagę na niespójność pojęć: 1. Usługę świadczy się w oparciu o politykę certyfikacji 2. Polityka certyfikacji to (art. 25.2) dokument określający szczegółowe rozwiązania techniczne i organizacyjne oraz zakres i warunki bezpieczeństwa tworzenia i stosowania certyfikatów. 3. Usługi certyfikacyjne to (art. 20.1) wydawanie certyfikatów, znakowanie czasem, potwierdzanie ważności certyfikatów oraz inne usługi związane z podpisem elektronicznym. Zatem, w oparciu o jaki dokument należy świadczyć usługę znakowania czasem lub OCSP?	Rozważyć usunięcie ustępu 1 i 2 tym bardziej, że zgodnie z art. 6 ust. 4 Ustawy o świadczeniu usług drogą elektroniczną "Usługodawca jest zobowiązany do świadczenia usług drogą elektroniczną zgodnie z Regulaminem”.
Art. 24.3	Polityki certyfikacji i bezpieczeństwo urządzeń stanowią dwie różne delegacje i należy te przepisy rozłączyć. Delegacja powinna umożliwiać bezpośrednie wskazanie standardów ETSI w zakresie polityk certyfikacji.	W przypadku nieuwzględnienia powyższego komentarza, przeredagować przepis zgodnie z uwagą.
Art. 25.1	Niezrozumiałe jest, że w projekcie powtarza się niepoprawne brzmienie art. 18. 1 starej ustawy, a nie przytacza się treści załącznika III Dyrektywy. Uzasadnienie niepoprawności koncepcji bezpiecznego urządzenia do składania podpisu - zob. [Ekspertyza – ea/zo] str. 75-77	Wprowadzić do tego punktu treść załącznika III Dyrektywy
Art. 25.2	Wytyczne z Załącznika IV nie zostały precyzyjnie przytoczone	Wprowadzić do tego punktu treść załącznika IV Dyrektywy
Art. 26.1	Brak zgodności z Załącznikiem I Dyrektywy	Doprowadzić do zgodności
Art. 27.2 2)	Nie wiadomo, jakich obowiązków mógłby nie dopełnić podmiot i dlaczego z tego powodu druga strona umowy ma mieć unieważniony certyfikat	Usunąć pkt 2)
Art. 27.2 7)	Stoimy na stanowisku, że minister nie ma prawa zażądać unieważnienia certyfikatu w jakichkolwiek okolicznościach	Usunąć pkt 7)

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art. 28.1	Technika może wymagać publikacji więcej niż jednej listy certyfikatów unieważnionych lub nie zakładać publikowania żadnej listy certyfikatów unieważnionych – dla przykładu usługi certyfikacyjne dla czytników paszportów biometrycznych nie mają technologicznie list unieważnionych certyfikatów. e międzynarodowe przedsięwzięcie będzie w RP dziwnie uregulowane . Przepis powinien także umożliwiać zastosowanie innych niż publikowanie listy technik w szczególności, gdy warunki techniczne uniemożliwiają tego wykonanie (listy unieważnionych certyfikatów dla certyfikatów urzędowych w okresie 10 lat) Ponadto, Pozostawiono obowiązek publikowania list CRL przez wszystkie podmioty świadczące usługi certyfikacyjne - nawet, jeżeli te usługi nie polegają na wydawaniu certyfikatów. Należy także wspomnieć, że istnieją usługi certyfikacyjne, polegające na wydawaniu certyfikatów, dla których listy CRL są nierealizowalne technicznie, a zapewnienie ważności certyfikatu jest realizowane innymi technikami, tj. skrócenie okresu ważności certyfikatu lub weryfikacja online. Dla usług polegających na zarządzaniu wieloma milionami certyfikatów jednocześnie lista CRL nie może być publikowana ze względu na długi czas dostępu do listy.	Dostosować przepis do specyficznych warunków świadczenia różnych usług certyfikacyjnych. Lub ograniczyć przepis wyłącznie do usług wydawania certyfikatów kwalifikowanych
Art. 28.4	czas publikowania listy CRL może dotyczyć jedynie usługi polegającej na wydawaniu i zarządzaniu certyfikatami kwalifikowanymi.	Dopisać warunek „dla usługi polegającej na wydawaniu i zarządzaniu certyfikatami kwalifikowanymi
Art. 28.7	Zaawansowany podpis elektroniczny **podmiotu kwalifikowanego** podpisującego listę. Przepis dotyczy różnych podmiotów a nie podmiotów kwalifikowanych.	Wprowadzenie zmiany w art. 28.1 polegającej na ograniczeniu obowiązku publikowania list zawieszonych i unieważnionych certyfikatów tylko dla usług polegających na wydawaniu certyfikatów kwalifikowanych.
Art. 29.2	A (dodany w powiązaniu z art. 20 ust. 3): 2. Certyfikaty powiązane z danymi do składania podpisu elektronicznego służącymi do wykonania czynności określonych w art. 20 ust. 3 wydaje podmiotom kwalifikowanym minister właściwy do spraw gospodarki. Powtarza zapis art. 20 ust. 3, zatem jest nadmiarowy.	Usunąć ten artykuł

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
art. 30 ust. 3 ppkt 7	(dodany): 7) plan finansowy oraz dokumenty przedstawiające sytuację finansową i majątkową składającego wniosek, w szczególności sprawozdanie finansowe za poprzedni rok prowadzenia działalności zweryfikowane przez biegłego rewidenta, a w przypadku podmiotów które nie prowadziły dotychczas działalności gospodarczej potwierdzenie posiadania lub możliwości pozyskania środków finansowych niezbędnych do prowadzenia tego rodzaju działalności: Brak uzasadnienia dla potrzeby pozyskania takich danych , które zwykle są tajemnicą przedsiębiorstwa. Należy podkreślić, że zawartość wniosku do ministra jest informacją publiczną, co daje możliwość łatwego uzyskania niezwykle wrażliwych informacji przez konkurencję.	– rekomenduje się usunięcie tego zapisu
Art. 40	W przypadku złożenia przez podmiot kwalifikowany podpisu elektronicznego lub pieczęci elektronicznej weryfikowanych certyfikatami ministra właściwego ds. gospodarki, z rażącym naruszeniem obowiązujących przepisów ustawy ,decyzja o wykreśleniu wpisu z rejestru podlega natychmiastowemu wykonaniu. Po wniesieniu skargi do sądu administracyjnego nie można wstrzymać wykonania decyzji” Co to są rażące naruszenia obowiązujących przepisów?	Przepis wymaga doprecyzowania
Art. 46. (usunięty)	W jednej z wcześniejszych wersji był przepis określający zasady wszczynania kontroli przez ministra gospodarki. Niezrozumiałe jest usunięcie tego zapisu.	Przywrócić ten przepis a ponadto: Dodać punkt 3) w wyniku skargi złożone przez osobę, która zawarła umowę na świadczenie usług certyfikacyjnych lub osobę, która weryfikując podpis elektroniczny, polega na zawartości certyfikatu.
Art. 58 2) 1)	Brzmienie zmian w KPA powinno uwzględniać propozycje nowelizacji KPA zawarta w znajdującej się w Sejmie nowelizacji Ustawy o informatyzacji podmiotów realizujących zadania publiczne. Niezależnie od powyższego, propozycja wprowadza nigdzie nie występujący i niezdefiniowany podpis elektroniczny weryfikowany kwalifikowanym certyfikatem. Jest to absolutnie niedopuszczalne, szczególnie ze względu bezpieczeństwa gdyż ta konstrukcja nie nakłada obowiązku zabezpieczenia danych do składania podpisu, i z tego powodu jest całkowicie niewiarygodna.	Dopasować brzmienie nowelizacji, usunąć podpis weryfikowany kwalifikowanym certyfikatem
Art. 59	Zmiany proponowane do art. 78 KC nie uwzględniają ustaleń dokonanych z Komisją Kodyfikacyjną Zapis „oświadczenie woli w postaci danych elektronicznych do których dołączono lub które logicznie powiązano z podpisem elektronicznym” jest bez sensu i niezgodny z definicją podpisu elektronicznego	propozycja: „ Dla zachowania formy elektronicznej wystarcza złożenie oświadczenia woli w postaci danych elektronicznych opatrzonych zaawansowanym podpisem elektronicznym”

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Art.60 ust 1	Zdjęto obowiązek stosowania kwalifikowanego podpisu z dużych podmiotów, zastępując go pieczęcią elektroniczną, ale zostawiono dla osób opłacających składki na własne ubezpieczenie!	Zapis powinien być zgodny z ogólna zasadą, że podpisem kwalifikowanym może się posługiwać Każdy podmiot w relacjach z ZUS. Poza tą forma można dopuścić inne, ale nie wolno zastąpić podpisu kwalifikowanego pieczęcią, bez możliwości stosowania podpisu kwalifikowanego. Przeredagować zapis w postulowanym kierunku.
Art. 60 ust. 2	Przepis wprowadza obowiązek stosowania w ZUS pieczęci elektronicznej wystawionej przez podmiot kwalifikowany. Nie ma uzasadnienia do „darowania" podmiotom świadczącym usługi wydawania certyfikatów kwalifikowanych nowego segmentu rynku. Przepis jest antykonstytucyjny!	Bezwzględnie usunąć warunek wydawania certyfikatów dla pieczęci przez podmioty „kwalifikowane"
Art. 64.1	Ilekroć przepisy odrębne przewidują złożenie bezpiecznego podpisu elektronicznego albo bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego certyfikatu kwalifikowanego, rozumie się przez to odpowiednio, obowiązek złożenia zaawansowanego podpisu elektronicznego albo podpisu kwalifikowanego. W ustawie z 18. Czerwca 2001 roku bezpieczny podpis obejmował bezpieczne urządzenie, aktualna definicja podpisu zaawansowanego nie obejmuje bezpiecznego urządzenia;- stąd pojęcia „bezpieczny podpis elektroniczny" i zaawansowany podpis elektroniczny nie są równoważne	Należy przejrzeć „przepisy odrębne" aby zdecydować, czy dana sytuacja wymaga zachowania formy pisemnej, czy nie. Odpowiednio zdecydować, czy zastąpić pojęciem podpisu zaawansowanego czy podpisu kwalifikowowanego
Art. 66	Przepis przewiduje funkcjonowanie NBP w zakresie ustawy, która zostaje zastąpiona niniejszą ustawą. W ust. 2 przewiduje się możliwość zmiany zakresu upoważnienia przez NBP, nie definiując, na czym mogłaby taka zmiana polegać. Oba zapisy nie mają podstaw prawnych.	Rozważyć prawidłowość zaproponowanej konstrukcji prawnej.
Art. 72	*Vacatio legis* ustawy jest za długie	Skrócić do 3 miesięcy.
Art. xx	Brak delegacji ministra do określenia formatu podpisu elektronicznego. Należy uszczegółowić obowiązki urzędów, pozostawiając sposoby udostępniania formularzy poza delegacją.	Minister właściwy do spraw informatyzacji w porozumieniu z ministrem właściwym do spraw administracji publicznej określi, w drodze rozporządzenia, warunki techniczne, wymagany format podpisu oraz warunki bezpieczeństwa udostępniania wzorów formularzy i dokumentów elektronicznych, o których mowa w ust.1
Art. xx	Brak określenia sposobu tworzenia punktu zaufania, umożliwiającego weryfikację certyfikatów kwalifikowanych wydawanych przez podmioty świadczące te usługi na obszarze Polski i Unii Europejskiej, realizowanego w postaci listy wskazanej w art. 32. ust.2 oraz warunków technicznych, jakie należy spełnić, aby ww. lista stała się takim punktem zaufania.	Należy zaproponować stosowne przepis, zgodnie z normami ETSI 102 030 i 102 231.

Przepis ustawy	*Uwagi PTI do treści oryginalnego przepisu*	*Sugestie zapisów ustawy (z komentarzem)*
Dobrowolna akredytacja - Nowy rozdział przed rozdziałem VIII,	Proponujemy zastosować funkcjonujący, rynkowy system oceny zgodności z Polską Normą PN ISO/IEC 27001:2007; podmiot świadczący usługi certyfikacyjne może uzyskać certyfikat zgodności systemu zarządzania bezpieczeństwem informacji dla zakresu usług certyfikacyjnych, jakie świadczy. Uzyskanie tego certyfikatu spełniałoby warunki przewidziane ustawą dla akredytowanego podmiotu świadczącego usługi certyfikacyjne.	Art. 44' (nowy artykuł) 1. Każdy podmiot świadczący usługi certyfikacyjne ma prawo ubiegania się o status akredytowanego podmiotu świadczącego usługi certyfikacyjne w systemie dobrowolnej akredytacji rozumianej zgodnie z art. 3 ust. 2 Dyrektywy o wspólnotowych ramach dla podpisów elektronicznych. 2. W celu uzyskania statusu podmiotu akredytowanego, podmiot świadczący usługi certyfikacyjne opracowuje system zarządzania bezpieczeństwem informacji dla zakresu usług, jakie świadczy. 3. Podmiot świadczący usługi certyfikacyjne poddaje system zarządzania bezpieczeństwem informacji ocenie zgodności z wymaganiami odnośnej polskiej normy, wykonywaną przez niezależny akredytowany podmiot działający w systemie akredytacji na podstawie ustawy o systemie oceny zgodności ((Dz. U. z 2004 r. Nr 204, poz. 2087, z późn. zm.) 4. Uzyskanie certyfikatu zgodności z polską normą wskazaną w ust. 3 jest równoważne uzyskaniu statusu akredytowanego podmiotu świadczącego usługi certyfikacyjne. 5. Podmiot świadczący usługi certyfikacyjne jest obowiązany niezwłocznie informować, za pomocą zwyczajowo przyjętych środków komunikacji, o wszelkich zmianach w certyfikacie zgodności, o którym mowa w ust. 4.