



Opinia Polskiego Towarzystwa Informatycznego

Dotycząca projektu Ustawy o podpisach elektronicznych, skierowanego do zaopiniowania przez Ministra Gospodarki.

Opinia została przygotowana przez Zespół Ekspertów PTI koordynowany przez wiceprezesa PTI kol. Wiesława Paluszyńskiego

5 grudnia 2008 roku

Uwagi ogólne:

Konieczność nowelizacji przepisów Ustawy o podpisie elektronicznym z dnia 16 sierpnia 2001 roku nie ulega wątpliwości. Ustawa ta zdezaktualizowała się technologicznie, w wyniku czego stała się praktycznie hamulcem w rozwoju e-administracji i e-gospodarki. Opiniując nową ustawę, która ma zastąpić dotychczasową, Polskie Towarzystwo Informatyczne kierowało się przede wszystkim następującymi przesłankami:

- Zapewnieniem pełnej zgodności ustawy z regulacjami UE i to zarówno z właściwą Dyrektywą, jak i wydaną na jej podstawie Decyzją Komisji Europejskiej oraz z dorobkiem prawnym i standaryzacyjnym UE;
- Stworzeniem aktu prawnego, który nie będzie służył wyłącznie podmiotom świadczącym usługi certyfikacyjne, ale osobom i podmiotom korzystającym z podpisu elektronicznego, podmiotom tworzącym rozwiązania informatyczne umożliwiające wykorzystywanie podpisu elektronicznego w jak najszerszych dziedzinach życia. Aktu jak najbardziej zrozumiałego dla użytkowników tej formy komunikacji elektronicznej, jak najbardziej neutralnego technologicznie, umożliwiającego nadążanie za zmieniającą się technologią;
- Uwzględnieniem prawie 6 letniej dyskusji w środowiskach technicznych i prawniczych, w trakcie których wskazywano na wady dotychczasowych rozwiązań.

Przesłany do zaopiniowania projekt ustawy nie zawiera niestety ani jednego projektu rozporządzenia wykonawczego (przewiduje się w nim delegacje do 7 obligatoryjnych i 2 opcjonalnych rozporządzeń). Biorąc pod uwagę charakter ustawy, gdzie większość spraw ważnych, z punktu widzenia techniki, będzie się znajdowała w rozporządzeniach, jest to poważna wada, która nie powinna mieć miejsca w opiniowaniu aktu o takim charakterze.

Osiągnięcie przejrzystości zapisów ustawy można zdecydowanie poprawić, eliminując zarzut powszechnie i słusznie podnoszony w stosunku do poprzedniej ustawy, że nie jest to ustawa o podpisie, ale oświadczeniu usług certyfikacyjnych, przenosząc do rozporządzeń sprawy organizacji i wymagań związanych z procesem wydawania danych do składania podpisu i związanych z nimi certyfikatów, a także funkcjonowaniem centrów certyfikacji. Brak projektów rozporządzeń niestety nie pozwolił na zaproponowanie w tym zakresie poprawek. Tym niemniej stoimy na stanowisku, że Minister Gospodarki powinien rozważyć taką możliwość przebudowania projektu.

Czytając zapisy proponowanej Ustawy i uzasadnienie do niej, w wielu punktach stwierdzaliśmy rozbieżności pomiędzy słusznymi zapisami uzasadnienia i zupełnie do nich nie przystającymi zapisami projektu. Nie wszystkie stwierdzenia zawarte w uzasadnieniu znalazły się też w projekcie. Siłą rzeczy opiniowaliśmy przesłany projekt, wydaje się jednak, że wskazane rozbieżności należy usunąć poprzez uzupełnienie projektu, lub zmianę uzasadnienia.



Kluczowym dla tej ustawy jest aparat pojęciowy, w tym definicje, a także problemy związane ze skutkami prawnymi składanych różnych rodzajów podpisów elektronicznych. Z tego względu nasza opinia składa się z trzech części.

- Pierwsza część stanowi propozycję całościowego i kompletnego uregulowania sfery definicji, wraz ze szczegółowymi uzasadnieniami propozycji.
- Druga część zawiera propozycję uporządkowania kwestii skutków prawnych.
- Trzecia część to tabela z propozycjami zmian i uwagami do proponowanych zapisów Ustawy.

Pragniemy podkreślić, że poprawianie zapisów bez rozstrzygnięcia dwóch pierwszych kwestii, czyli aparatu pojęciowego i skutków prawnych, może doprowadzić do zaakceptowania projektu niespójnego, zawierającego rozstrzygnięcia przypadkowe (jak to miało miejsce w poprzedniej Ustawie), niosącego w sobie kolejne zagrożenia dla stosowania podpisu elektronicznego.



Część pierwsza Opinii PTI dotycząca definicji.

Założenia dla zbioru Definicji

- A. Maksymalna prostota i precyzja;
- B. Neutralność technologiczna tam, gdzie jest to możliwe
- C. Definicje z Dyrektywy są podstawą, chyba że należy je doprecyzować w celu uzyskania zgodności z polskim systemem prawa
- D. Otwartość, transparentność, brak dyskryminacji
- E. Zgodność z aktualnym stanem rozwoju techniki

Definicje:

1. *"uwierzytelnienie" – uzyskanie pewności, że dana osoba fizyczna lub podmiot jest tym, za kogo się podaje*

Uzasadnienie: Definicja czym polega uwierzytelnienie ikogo wskazuje; nie ma sprzeczności z techniczną definicją : "**uwierzytelnienie**" – uzyskanie pewności, że dany podmiot jest tym, za kogo się podaje (ISO/IEC 10181-2)]

2. *„podpis elektroniczny” oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia*

Uzasadnienie – definicja z Dyrektywy¹; umożliwi stosowanie różnych rodzajów podpisów do różnych zastosowań, nie ogranicza podpisującego do osoby fizycznej i jest neutralna technologicznie

3. *„podpisujący” oznacza:*

1) osobę fizyczną, która działa w imieniu własnym albo w imieniu innych osób fizycznych lub podmiotu;

2) podmiot;

posiadające urządzenie do składania podpisu elektronicznego.

Uzasadnienie: Definicja taka sama, jak w projekcie Ustawy, z uwzględnieniem możliwości złożenia podpisu automatycznego przez podmiot (pieczęci).

¹ Dyrektywa 99/93/WE o wspólnotowych ramach dla podpisów elektronicznych



Uwagi dodatkowe

- a. W proponowanym brzmieniu podpisującym jest **osoba fizyczna** składająca podpis oraz **podmiot** składający pieczęć.
- b. W ten sposób podmiot świadczący usługi certyfikacyjne, pieczętuje certyfikaty (realizuje podpis cyfrowy)– właśnie automatycznie

4. *„zaawansowany podpis elektroniczny” oznacza podpis elektroniczny spełniający następujące wymogi:*

- a) *przyporządkowany jest wyłącznie podpisującemu;*
- b) *umożliwia zidentyfikowanie podpisującego;*
- c) *stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą;*
- d) *jest tak powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych jest wykrywalna*

Uzasadnienie – dokładna definicja z Dyrektywy

Uwagi dodatkowe

- a. Zostały skorygowane drobne błędy ustawy z Projektu

5. *„kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, złożony przez podpisującego będącego osobą fizyczną, za pomocą bezpiecznego urządzenia do składania podpisu elektronicznego i w okresie ważności certyfikatu kwalifikowanego, za pomocą którego można dokonać weryfikacji tego podpisu.*

Uzasadnienie: Jakkolwiek definicja kwalifikowanego podpisu elektronicznego nie pojawia się w dyrektywie, to z uwagi na konieczność usunięcia z polskiego prawa „bezpiecznego podpisu”, należy zachować definicję podpisu kwalifikowanego.

Uwagi dodatkowe

- a. Usunięto z definicji wadę przejściowości ważności podpisu elektronicznego i przywrócono konstrukcję prawną obowiązującą dla podpisu własnoręcznego: jeśli jest ważny w momencie składania, to jest ważny bezterminowo, chyba że zostanie przeprowadzony dowód jego nieważności; wygaśnięcie certyfikatu nie zmienia stanu prawnego złożonego podpisu
-
6. *„podpis urzędowy oznacza zaawansowany podpis elektroniczny składany przez podpisującego, będącego osobą fizyczną przy pomocy danych służących do składania podpisu elektronicznego zawartych w dokumencie tożsamości, spełniający wymagania określone przepisami odrębnymi.*



Uzasadnienie: Konieczne wprowadzenie koncepcji z uwagi na potrzebę rozwoju e-urzędu oraz projekt pl. ID.; przepisy odrębne to oczywiście ustawa dowodzie osobistym (projektowana) i informatyzacji (nowelizowana) oraz kpa

Uwagi dodatkowe

- a. W Ustawie należy oczywiście wpisać zasadę swobody stosowania podpisu kwalifikowanego tam, gdzie może być stosowany podpis urzędowy. Z drugiej strony, nie można ograniczać działania podpisu urzędowego wyłącznie do sfery publicznej, skoro z zasady niedyskryminacji wynika że może on być stosowany jako zaawansowany i być dowodem. Podpis urzędowy będzie miał ograniczony w ten sposób skutek względem kwalifikowanego, że będzie równoważny treści podpisanej formie pisemnej i podpisowi własnoręcznemu tylko wówczas gdy ustawa szczególna tak będzie stanowiła np. kpa.
- b. Definicja neutralna technologicznie

7. „pieczęć elektroniczna” – zaawansowany podpis elektroniczny uwierzytlniający podmiot.

Uzasadnienie: Niezbędne pojęcie dla e-faktury oraz innych zastosowań (składanie wniosków grupowych; wydawania zaświadczeń elektronicznych z rejestrów publicznych itp.) wymagających masowego przetwarzania. To zupełna nowość w ustawie i teoretycznie można sobie wyobrazić zastosowania pieczęci w sferze cywilnej i publicznej np. jako metoda zabezpieczania oficjalnych wiadomości publicznych, dokumentów etc.

Uwagi dodatkowe

- a. W Ustawie należy wpisać przepisy zmieniające wiele aktów prawnych, rzecz jasna w pierwszym rzędzie o e-fakturze, ale także o elektronicznej skrzynce podawczej.

8. „dane służące do składania podpisu” oznacza неповtarzalne dane, takie jak kody lub prywatne klucze kryptograficzne, które są używane przez podpisującego do składania podpisu elektronicznego;

Uzasadnienie: Definicja z Dyrektywy.

Uwagi dodatkowe

- a. Eliminacja błędów definicji w projekcie („przyporządkowane podpisującemu”)
 - b. Wprowadzenie przykładu oraz dosłowne przytoczenie definicji z Dyrektywy eliminuje wadę formalną definicji *idem per idem* (dane służące do składania podpisu są to dane, które służą do składania podpisu...)
9. *„dane służące do weryfikacji podpisu” oznacza dane, takie jak kody lub publiczne klucze kryptograficzne, używane do celów weryfikacji podpisu elektronicznego;*

Uzasadnienie: Definicja z Dyrektywy.



Uwagi dodatkowe – zob. pkt. 7

10. „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

Uzasadnienie: Doprecyzowana definicja z Dyrektywy [z niemieckiej ustawy o podpisie elektronicznym]

Uwagi dodatkowe

- a. Eliminacja błędu z poprzedniej ustawy, która definiowała urządzenia za szeroko – było to praktycznie całe środowisko składania podpisu, nad którym podpisujący miał UTRZYMAĆ wyłączną kontrolę

11. „bezpieczne urządzenie służące do składania podpisów” oznacza urządzenie służące do składania podpisów, które spełnia wymogi określone w Ustawie.

Uzasadnienie: Doprecyzowana definicja z Dyrektywy

Uwagi dodatkowe

- a. Korekta definicji w celu ujednolicenia z Dyrektywą oraz usunięcia błędu formalnego polegającego na wprowadzeniu wymagania jako atrybutu definiowanego pojęcia (urządzenie się tym wyróżnia, że ma certyfikat od ABW); zasady certyfikowania bezpiecznych urządzeń przez uprawnione organy powinny być umieszczone w tekście ustawy (w artykule dot. bezpiecznego urządzenia)
- b. Z uwagi na fakt, że definicja zawiera w sobie wymaganie, można rozważyć jej przesunięcie z części definicyjnej do przepisów szczegółowych w ustawie.

12. 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;

Uzasadnienie: Doprecyzowana definicja z Dyrektywy

Uwagi dodatkowe: zob. pkt . 9

13. „certyfikat” oznacza potwierdzenie elektroniczne, za pomocą którego dane służące do weryfikacji podpisu są przyporządkowane podpisującemu i potwierdzają jego tożsamość;



Uzasadnienie: Definicja z Dyrektywy z doprecyzowaniem; w oryginale jest: "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person"; "osoba" została zmieniona na „podpisującego” (w polskim systemie prawa mówiąc “osoba” mamy na myśli “osobę fizyczną lub prawną”, pozostają jeszcze jednostki organizacyjne nie posiadające osobowości prawnej)

Uwagi dodatkowe:

- a. Skorygowanie błąd definicji z projektu Ustawy: („potwierdza tożsamość” – dokonuje uwierzytelnienia podpisującego, a nie „umożliwia identyfikację”)

14. *„certyfikat kwalifikowany” oznacza certyfikat spełniający wymogi określone w art. i wydawany przez podmiot świadczący usługi certyfikacyjne, który spełnia wymogi z art...;*

Uzasadnienie: Definicja z Dyrektywy

Uwagi dodatkowe:

- a. Odnośne art. Ustawy można doprecyzować w momencie, gdy będą już ustalone
- b. Z uwagi na fakt, że definicja zawiera w sobie wymaganie, można rozważyć jej przesunięcie z części definicyjnej do przepisów szczegółowych w ustawie.

15. *„usługi certyfikacyjne” oznaczają usługi związane lub w których stosuje się podpisy elektroniczne, w szczególności polegające na wydawaniu i zarządzaniu certyfikatami.*

Uzasadnienie: Definicja nie występuje w Dyrektywie. Konieczna z punktu widzenia właściwego zdefiniowania zakresu Ustawy.

Uwagi dodatkowe

- a. poprzednia (ze starej ustawy) definicja usług certyfikacyjnych wprowadziła wiele niejasności, stąd propozycja szerokiej, otwartej definicji (niezamknięty katalog wielu usług, które mogą pojawić się w przyszłości) wynikająca z pkt. 9 Preambuły Dyrektywy jest bardziej odpowiednia.

16. *„produkt podpisu elektronicznego” oznacza oprogramowanie lub sprzęt, względnie ich istotne składniki, które są używane przez podmiot świadczący usługi certyfikacyjne do świadczenia usług podpisu elektronicznego lub służą do składania lub weryfikacji podpisów elektronicznych;*

Uzasadnienie: Definicja z Dyrektywy

Uwagi dodatkowe:



- a. Definicja w projekcie Ustawy wskazywała „ogólnie uznane normy”; z uwagi na bardzo nieprecyzyjne wskazanie, preferuje się przytoczenie dokładnej definicji, bez rozszerzeń dających pole do interpretacji.
- b. Należy w Ustawie określić mechanizm uznawania wymagań opisanych we wskazanych normach, jeśli są publikowane Decyzjami Komisji Europejskiej lub są wprowadzane do systemu prawnego na mocy innych aktów prawnych; jednakże zwraca się uwagę, że nawet bezpośrednio wskazanie normy w akcie prawnym nie powoduje przymusu zastosowania normy, jeśli podmiot wykaże, że spełnia wymagania, nie stosując danej normy (generalna zasada, że stosowanie norm jest dobrowolne!)



Pojęcia, które budzą zasadnicze wątpliwości w zaproponowanej redakcji (z art. 2 i 3):

Kwalifikowany podmiot świadczący usługi certyfikacyjne – powinno być „**podmiot świadczący usługi certyfikacyjne polegające na wydawaniu i zarządzaniu kwalifikowanymi certyfikatami**”, należy zmienić to sformułowanie w całej ustawie.

Podpis łączny - nie jest typem podpisu elektronicznego lecz konstrukcją prawną, dla której definiowanie skutków prawnych wykraczają poza zakres przedmiotowy ustawy. W obecnej formie definicja jest niezrozumiała.

Potwierdzanie ważności certyfikatów – można założyć, że chodzi o usługę OSCP - nie ma uzasadnienia, dla których ta akurat usługa miałaby być wyróżniona definicją, co nie oznacza, żeby tej usługi nie wprowadzić przepisem szczegółowym. Konieczne jest zaproponowanie redakcji tego przepisu.

Datownik elektroniczny – znacznik czasu stosowany w obiegu wewnętrznym jednostek administracji publicznej – brak uzasadnienia umieszczenia tego pojęcia w Ustawie. Ponadto, w części dotyczącej skutków prawnych należałoby określić skutki czynności polegającej na wystawianiu datowników elektronicznych, zaś w części dotyczącej świadczenia usług certyfikacyjnych obowiązki podmiotów wystawiających datowniki elektroniczne, co wykracza poza zakres przedmiotowy ustawy.

Czas urzędowy, czas zgodny z czasem urzędowym – zdecydowanie prezentowane jest stanowisko, że znakowanie czasem nie powinno być regulowane w takim zakresie jak w starej ustawie, gdzie opatrzeniu znacznikiem czasu podpisanych danych nadano, w sposób nieuzasadniony, rangę daty pewnej. Znakowanie czasem powinno mieć rangę czynności technicznej (zob. też poniżej punkt dot. znakowania czasem). W związku z tym nie ma potrzeby wprowadzania do tej ustawy bardzo wielu pojęć związanych z synchronizacją czasu (dokładność synchronizacji, techniczna weryfikacja synchronizacji). **Te pojęcia powinny się znaleźć w rozporządzeniu MG dotyczącym dystrybucji czasu urzędowego.**

Certyfikat urzędowy – jeśli podpis urzędowy będzie realizowany w oparciu o zaawansowany podpis elektroniczny, to ogólna definicja certyfikatu jest wystarczająca.

Certyfikat systemowy – przy przyjęciu rozwiązania pieczęci elektronicznej bazującej na zaawansowanym podpisie elektronicznym, definicja pojęcia ‘certyfikatu’ będzie wystarczająca.

Certyfikat atrybutów – brak uzasadnienia dla wprowadzania tej specyficznej usługi w formie zdefiniowanej w projekcie ustawy, dodatkowo opatrując ją właściwością kwalifikowanej dlatego, że świadczy ją podmiot wydający certyfikaty kwalifikowane; ponadto, zwraca się uwagę, że model biznesowy, w którym byłoby miejsce na wydawanie certyfikatów atrybutów nie musi zakładać, że podmiot wydający certyfikat klucza publicznego oraz certyfikaty atrybutów jest ten sam. Jeśli ta usługa miała by pozostać konieczne jest jej zdefiniowanie poprawne i uwzględniające powyższe uwagi.

Pojęcia, które budzą zasadnicze wątpliwości w zaproponowanej redakcji (wraz definicjami) z innych art. projektu

10.1 odbiorca usług certyfikacyjnych – pojecie niepoprawne, ponieważ składa się z dwóch podmiotów, których relacja z podmiotem świadczącym usługi certyfikacyjne jest odmienna: subskrybenta, który zawiera umowę z dostawcą usługi oraz tzw. strony ufającej, która umowy z dostawcą usługi nie ma, ale ufa certyfikatowi w oparciu o jego zawartość. W ustawie można te dwa podmioty określać opisowo.



21.1 znakowanie czasem - usługa czysto techniczna, brak przesłanek aby określać szczegółowo wymagania dla tej usługi oraz dla podmiotu, który świadczyłby taką usługę. Jeśli jednakże przeważałaby 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”

21.2 kwalifikowane znakowanie czasem – w definicji w projekcie zapisano, że do tego, aby świadczyć tę usługę potrzeba: a) być kwalifikowanym podmiotem i b) przeprowadzać ciągłą techniczną weryfikacją wymaganej dokładności synchronizacji do czasu urzędowego lub czasu UTC(PL) (nie określając, na czym to wymaganie mogłoby polegać). Ta definicja jest naruszeniem zasady równouprawnienia podmiotów (jeden ma przewagę nad drugim tylko dlatego, że jest kwalifikowany w zupełnie innym zakresie świadczonych usług), zatem jest niekonstytucyjny.

25.2 polityka certyfikacji – nie jest konieczna do określenia wymagań dla podmiotu świadczącego usługi certyfikacji (nie użyto jej w Załączniku II Dyrektywy). Zwraca się uwagę, że ustawie o świadczeniu usług drogą elektroniczną podmiot jest obowiązany świadczyć usługę w oparciu o Regulamin. Te dwa pojęcia można zintegrować dość łatwo, zatem polityka certyfikacji jest bytem mnożonym ponad potrzebę.



Część druga Opinii PTI dotycząca skutków prawnych.

Ustawa o podpisach elektronicznych – analiza skutków prawnych (art. 5 i 7 Projektu)

17. Art. 5.1 „Zaawansowany podpis elektroniczny, weryfikowany przy pomocy certyfikatu wywołuje skutek prawny, jeżeli został złożony w okresie ważności tego certyfikatu.(..)”

Proponuje się jego skreślenie

Uzasadnienie: W przepisie nie definiuje się jakiegokolwiek skutku prawnego, mówi się jedynie o tym, że podpis zaawansowany skutek wywołuje; w świetle art. 8 niniejszy przepis jest nadmiarowy.

18. Art. 5.2 „Podpis zaawansowany zapewnia integralność danych opatrzonych tym podpisem w ten sposób, że rozpoznawalne są wszelkie ich zmiany oraz jednoznacznie wskazuje na certyfikat wykorzystywany do weryfikacji tego podpisu.

Proponuje się skreślenie tego artykułu.

Uzasadnienie: [zbieżność z opinią M. Kutylowskiego – fragment przytoczony poniżej:

1. w Art. 5.2 dołączono nowy warunek [w stosunku do definicji przytoczonej w art. 2]:

jednoznacznie wskazuje certyfikat wykorzystywany do weryfikacji tego podpisu

Technicznie oznacza to zawarcie pola w podpisie zawierającego informacje o certyfikacie. Jest to zawężenie pojęcia zaawansowanego podpisu elektronicznego z Dyrektywy. Należy stwierdzić, że weryfikacja podpisu wymaga klucza publicznego a nie certyfikatu. Certyfikat może być jedną z form wskazania klucza publicznego osoby podpisującej.

Konsekwencje:

1. zaawansowany podpis elektroniczny według polskiej ustawy nie jest tym samym co „advanced electronic signature” z Dyrektywy. Pojęcie z projektu jest węższe. Dla uporządkowania dodam, że ściśle rzecz biorąc dotychczas stosowane techniki wymienione w rozporządzeniu Rady Ministrów 1094 nie spełniają warunku z art. 5.2.
2. Definicja zawęży możliwości technologiczne. Należy przypomnieć, że istnieją algorytmy podpisu („identity based signatures”), dla których klucz publiczny jest publicznym identyfikatorem podpisującego. W tej sytuacji użycie certyfikatu jest bezsensowne.

(..) Art. 5.2 nie wnosi on nic, oprócz niezgodności z Dyrektywą i problemów technicznych. Nie podnosi on bezpieczeństwa.

19. Art. 5.3. Dane w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym wywołują skutki złożenia oświadczenia woli w formie pisemnej.



Proponuje się wprowadzenie warunków równoważności podpisów, tak jak to jest wpisane w art. 5.1.a) Dyrektywy 99/93/WE o wspólnotowych ramach podpisów elektronicznych

[zbieżność z uwagą M. Kutylowskiego do art. 5.3]

złożenie(kwalifikowanego) podpisu elektronicznego na danych elektronicznych wywiera taki sam skutek prawny, jak złożenie podpisu własnoręcznego z zachowaniem formy pisemnej.

Uzasadnienie – usunięcie błędu w przepisie (dane same przez siebie nie wywołują skutków prawnych, tylko podpisana treść]

20. Art. 5. 4. Podpis łączny wywołuje skutki reprezentacji łącznej na zasadach określonych przez właściwe przepisy, umowę albo statut.

Proponuje się skreślenie przepisu

Uzasadnienie: wynika z propozycji usunięcia konstrukcji prawnej, jaką jest podpis łączny (nie stanowi on odrębnego rodzaju podpisu elektronicznego), mało tego w warunkach reprezentacji łącznej potrzebne jest złożenie nie jednego a wielu podpisów równoważnych odrębnym.

Art. 7. (dotyczy znakowania czasem i datownika elektronicznego)

Proponuje się skreślenie przepisu

Uzasadnienie:

[zbieżność z uwagą M. Kutylowskiego, przytoczona poniżej, ze zmianami edycyjnymi:

Skutki prawne kwalifikowanego znakowania czasem (skutki prawne daty pewnej) mogą być niebezpieczne dla porządku prawnego. Problem ten był wielokrotnie zgłaszany w wielu opiniach. Należy dodatkowo zwrócić uwagę na pewną niekonsekwencję: skutki prawne daty pewnej są wywoływane jedynie, gdy znakowanie czasem zostało dokonane w okresie ważności certyfikatu służącego do weryfikacji podpisu. Powstaje pytanie, jak wykazać, że dane znakowanie czasem zostało dokonane w okresie ważności certyfikatu? Przez znakowanie czasem znakowania czasem? Widać, że proponowane rozwiązanie wcale nie rozwiązuje problemu do końca.

]

I dalsze uzasadnienie:

(wyciąg z ekspertyzy dla MG Przegład krajowych uregulowań prawnych dotyczących podpisu elektronicznego pod kątem zbliżenia do rozwiązań funkcjonujących w krajach Unii Europejskiej, Elżbieta Andrukiewicz, Zdzisław Osada, grudzień 2003)

„Znakowanie czasem, o którym mowa w art. 7 ustawy, które poprawniej językowo można określać jako „oznaczanie czasu”, rozumiane jako czynność techniczna, nie powinno posiadać tak dużej rangi,



jaką nadała mu ustawa. Zgodnie z art. 7 ust. 2, znakowanie czasem, przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego.

Forma pisemna z poświadczeniem daty (art. 81 k.c.) należy do kwalifikowanych form pisemnych.

Przeniesienie jej w obszar oświadczeń woli przekazywanych w postaci elektronicznej wydaje się nieporozumieniem, nie znajdującym precedensu w innych ustawodawstwach europejskich [1]. Znakowanie czasem, choć w innej formule występuje w rozwiązaniach niemieckich i portugalskich podpisu elektronicznego. W obu tych systemach nie można znaleźć podstaw do uznania, że ich celem było nadanie podpisom waloru daty pewnej. W rozwiązaniu niemieckim data i czas wystawienia lub unieważnienia certyfikatu dzięki znakowaniu czasem mogą zostać dokładnie ustalone. Z kolei, w uregulowaniu portugalskim podmiot świadczący usługi certyfikacyjne wydaje oświadczenie określone jako ważność chronologiczna. Zaświadcza ono czas i datę wykreowania, wysłania albo otrzymania dokumentu elektronicznego. Dlatego też proponuje się skreślenie ust. 2 i 3 z art. 7 i wyeliminowanie równoważności znakowania czasem jako usługi ekwiwalentnej formie pisemnej z poświadczeniem daty. Za uchyceniem ust. 2 i 3 przemawia „przejściowość” domniemań wynikających z tych przepisów. Na domniemania wynikające z art. 7 ust. 2 i 3 można powoływać się tylko przez pewien czas i oba wygasają w tym samym momencie, tj. w chwili wygaśnięcia ważności zaświadczenia certyfikacyjnego, za pomocą którego jest weryfikowane poświadczenie elektroniczne na znaczniku czasu. Domniemanie wynikające z art. 7 ust. 2 dotyczące stwierdzenia istnienia określonych danych w postaci elektronicznej w chwili znakowania czasem jako ograniczone w czasie narusza istotę konstrukcji formy pisemnej z datą pewną. Także art. 7 ust. 3 stanowi, że domniemanie istnieje do utraty ważności zaświadczenia certyfikacyjnego. (Nie ma pewności, czy w przyszłości będzie możliwe – z różnych względów - ponowne oznaczenie czasu za pomocą konstrukcji wykorzystującej zaświadczenie certyfikacyjne....) Domniemanie to dotyczy wyłącznie określenia chwili przedstawienia podpisu elektronicznego kwalifikowanemu podmiotowi świadczącemu usługi certyfikacyjne. Możliwy jest dowód na fakt opatrzenia danych elektronicznych podpisem elektronicznym przed datą określoną usługą znakowania czasem. Wskazuje to na wzruszalność domniemania i możliwość przeprowadzenia dowodu na rzeczywistą datę złożenia podpisu elektronicznego.” [1] M. Drozdowicz, Błąd w elektronicznych czynnościach prawnych, Przegląd Prawa Handlowego z 2001r., nr 9.



Część trzecia Opinii PTI dotycząca zapisów projektu ustawy.

Oznaczenie	Uwaga	Propozycja
Uwagi ogólne do Projektu		
A.	<p>Projekt wprowadza wiele nowych pojęć, niekiedy zdefiniowanych bardzo nieprecyzyjnie (np. datownik elektroniczny, pieczęć elektroniczna, podpis urzędowy), nowe definicje dla terminów już znanych, wreszcie definicje są porozrzucane po całym projekcie. W kilku przypadkach przepisy szczegółowe odnoszą się do pojęć, które definiowane są w dalszych częściach projektu</p> <ul style="list-style-type: none"> • 20.1 usługi certyfikacyjne (regulowane począwszy od art. 2) • 21.1 znakowanie czasem i kwalifikowane znakowanie czasem (regulowane począwszy od art. 13.1) • 25.2 polityka certyfikacji (regulowane począwszy od art. 10.1) 	
B.	<p>Nie należy stosować pojęcia „kwalifikowany” w odniesieniu do podmiotów świadczących usługi certyfikacyjne. Przymiotnik „kwalifikowany” w odniesieniu do podmiotu sugeruje, że ktoś go zakwalifikował i w jakimś (bliżej niesprecyzowanym) sensie jest on lepszy od innych podmiotów. Narusza to zasadę równouprawnienia podmiotów a także może powodować podejrzenie, że jest formą „uprzedniej autoryzacji”, zabronionej przez Dyrektywę. W odniesieniu do usług świadczonych przymiotnik kwalifikowana jest prawidłowy (kwalifikowane usługi certyfikacyjne, usługa w formie kwalifikowanej itp.)</p>	
C.	<p>W wykonanej w grudniu 2003 roku, na zlecenie Ministra Gospodarki, Ekspertyzie , pt. „Przegląd krajowych uregulowań prawnych dotyczących podpisu elektronicznego pod kątem zbliżenia do rozwiązań funkcjonujących w krajach Unii Europejskiej” jest propozycja całościowej nowelizacji ustawy. W naszej opinii , kolejne propozycje z Ekspertyzy są w dalszym ciągu aktualne. Stąd w dalszych uwagach będziemy przywoływać poszczególne punkty tej ekspertyzy (oznaczanej jako [Ekspertyza_ea/zo] od inicjałów Autorów ekspertyzy).</p>	
Uwagi szczegółowe do projektu		
Art. 1	<p>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</p>	<p>Przyjąć zapisy z Dyrektywy:</p> <p>1. Ustawa określa warunki stosowania podpisu elektronicznego, skutki prawne jego stosowania, zasady świadczenia usług certyfikacyjnych oraz zasady nadzoru nad podmiotami świadczącymi te usługi.</p> <p>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 urzędowego oraz usługi znakowania czasem ².</p> <p>Uzasadnienie: zob [Ekspertyza – ea/zo], str. 148</p>

² Kwestie definicyjne zostały szczegółowo przedstawione w osobnym rozdziale opinii PTI



Oznaczenie	Uwaga	Propozycja
Brakujący artykuł	Ustawa musi mieć też zakres podmiotowy. W starej ustawie należy jedynie dokonać drobnej korekty	Art. 2 Przepisy ustawy stosuje się do podmiotów świadczących usługi certyfikacyjne, mających siedzibę lub świadczących usługi na terytorium Rzeczypospolitej Polskiej, z zastrzeżeniem art. 4. Uzasadnienie: zob [Ekspertyza – ea/zo], str. 148
Art. 2 brakująca definicja	Brakuje określenia, co rozumie się pod pojęciem „uwierzytelnienie”	<i>„uwierzytelnienie” – uzyskanie pewności, że dana osoba fizyczna lub podmiot jest tym, za kogo się podaje</i> Uzasadnienie: Definicja opisuje, na czym polega uwierzytelnienie i kogo wskazuje; nie ma sprzeczności z techniczną definicją : „uwierzytelnienie” – uzyskanie pewności, że dany podmiot jest tym, za kogo się podaje (ISO/IEC 10181-2)]; termin uwierzytelnienie jako pochodzący z języka informatycznego wymaga wyjaśnienia.
Art. 2.2	Nieprecyzyjne tłumaczenie definicji zaawansowanego podpisu elektronicznego	<i>„zaawansowany podpis elektroniczny” oznacza podpis elektroniczny spełniający następujące wymogi:</i> e) <i>przyporządkowany jest wyłącznie podpisującemu;</i> f) <i>umożliwia zidentyfikowanie podpisującego;</i> g) <i>stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą;</i> h) <i>jest tak powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych jest wykrywalna</i>
Art. 2.3	„weryfikowany przy pomocy <u>ważnego</u> kwalifikowanego certyfikatu” – taka konstrukcja zakłada przejściowość skuteczności podpisu, co powoduje jego ułomność prawną, jakiej nie ma zwykły podpis własnoręczny; istotne jest złożenie podpisu w okresie ważności certyfikatu i to powinno być kryterium równoważności tak złożonego podpisu elektronicznego z własnoręcznym, a podpis można zweryfikować także za pomocą certyfikatu poza okresem jego ważności (np. po wielu latach) ³	<i>„kwalifikowany podpis elektroniczny” oznacza zaawansowany podpis elektroniczny, złożony przez podpisującego będącego osobą fizyczną, za pomocą bezpiecznego urządzenia do składania podpisu elektronicznego i w okresie ważności certyfikatu kwalifikowanego, za pomocą którego można dokonać weryfikacji tego podpisu.</i> Uzasadnienie: Jakkolwiek definicja kwalifikowanego podpisu elektronicznego nie pojawia się w dyrektywie, to z uwagi na konieczność usunięcia z polskiego prawa „bezpiecznego podpisu”, należy zachować definicję podpisu kwalifikowanego.

³ Kwestie związane ze skutkami prawnymi podpisów zostały przedstawione w osobnym rozdziale opinii PTI



Oznaczenie	Uwaga	Propozycja
Art. 2.4	<p>Zastosowanie łącznego podpisu elektronicznego (joint signature) budzi wątpliwości związane z przeniesieniem odpowiedzialności za składane podpisy i sposób reprezentacji z osób podpisujących na centrum certyfikacji. W praktyce, łączny podpis uzyskuje się przez złożenie wielu podpisów pojedynczych i określenie w konkretnym dokumencie regulacyjnym (np. polityce podpisu), w jakiej sytuacji zachodzą skutki podpisu łącznego.</p> <p>W projekcie ustawy wprowadzono podpis łączny bez wprowadzenia jakichkolwiek przepisów dotyczących realizacji podpisu łącznego – tj. wydawanie, kwalifikowalność. Nałożenie w innych przepisach wymagania stosowania podpisu łącznego może całkowicie wyeliminować podpis elektroniczny ze względu na częstość zmian w zakresie stosowania podpisu łącznego i koszty jego utrzymania.</p>	<p>Rekomendujemy usunięcie podpisu łącznego z tej ustawy, tym bardziej, że jest on potem używany jedynie w art. 5.5 do stwierdzenia rzeczy oczywistej. Podpis łączny nie może spełnić zakładanej funkcji w proponowanym kształcie tj. powiada się o nim w liczbie pojedynczej podczas gdy dot. sytuacji związanej w prawie z podpisami wielu osób. Nie ma mowy w projekcie o warunkach wydawania certyfikatów łącznych i danych do składania tego podpisu.</p>
Art. 2.5	Pojęcie podpisu urzędowego jest niejasne	<p><i>„podpis urzędowy oznacza zawansowany podpis elektroniczny składany przez podpisującego, będącego osobą fizyczną przy pomocy danych służących do składania podpisu elektronicznego zawartych w dokumencie tożsamości, spełniający wymagania określone przepisami odrębnymi.</i></p> <p><u>Uzasadnienie:</u> Konieczne wprowadzenie koncepcji z uwagi na potrzebę rozwoju e-urzędu oraz projekt pl. ID.; przepisy odrębne to oczywiście ustawa dowódzie osobistym (projektowana) i informatyzacji (nowelizowana) oraz kpa. Można założyć, że warunki dot. wydawania certyfikatów urzędowych określone byłyby w ustawie o dowódzie osobistym jako , że cykl życia tego certyfikatu związany jest z dokumentem tożsamości.</p>
Art. 2.6	Pojęcie pieczęci elektronicznej jest wprowadzeniem do polskiego systemu prawnego podpisu, który nie jest przypisany do osoby fizycznej, zatem powinno być jasne i zrozumiałe.	<p><i>„pieczęć elektroniczna” – zaawansowany podpis elektroniczny uwierzytelniający podmiot.</i></p> <p><u>Uzasadnienie:</u> Niezbędne pojęcie dla e-faktury oraz innych zastosowań (składanie wniosków grupowych; wydawania zaświadczeń elektronicznych z rejestrów publicznych itp.) wymagających masowego przetwarzania . To zupełne nowość w ustawie i teoretycznie można sobie wyobrazić zastosowania pieczęci w sferze cywilnej i publicznej np. jako metoda zabezpieczania oficjalnych</p>



Oznaczenie	Uwaga	Propozycja
		wiadomości publicznych, dokumentów etc.
Art. 2.7	Definicja (dane służące do składania podpisu) jest nieprecyzyjna	<p><i>„dane służące do składania podpisu” oznacza niepowtarzalne dane, takie jak kody lub prywatne klucze kryptograficzne, które są używane przez podpisującego do składania podpisu elektronicznego;</i></p> <p><u>Uzasadnienie:</u> Definicja z Dyrektywy.</p> <p>c. Eliminacja błędów definicji w projekcie („przyporządkowane podpisującemu”)</p> <p>d. Wprowadzenie przykładu oraz dosłowne przytoczenie definicji z Dyrektywy eliminuje wadę formalną definicji <i>idem per idem</i> (dane służące do składania podpisu są to dane, które służą do składania podpisu...)</p>
Art. 2.8	Definicja weryfikacji podpisu elektronicznego zawiera umożliwia identyfikację podpisującego i stwierdzenie, że podpis został złożony za pomocą danych, o których mowa w ust 7, oraz że dane te nie uległy zmianie po jego złożeniu. nie jest definicją i jest niepotrzebna;	Zasady weryfikacji podpisu elektronicznego należy zamieścić w przepisach szczegółowych ustawy (rozbudować art. 22 o zapisy załącznika IV Dyrektywy); w takiej sytuacji definicja stanie się zbędna
Art. 2.9	Definicja (dane służące do weryfikacji podpisu) jest nieprecyzyjna.	<p><i>dane służące do weryfikacji podpisu” oznacza dane, takie jak kody lub publiczne klucze kryptograficzne, używane do celów weryfikacji podpisu elektronicznego;</i></p> <p><u>Uzasadnienie:</u> Definicja z Dyrektywy.</p>
Art. 2.10	„Potwierdzenie ważności certyfikatu (..) – czynność jest definiowana przez mechanizm; definicja nieprecyzyjna, wprowadzająca zamieszanie i kompletnie niepotrzebna	Zasady potwierdzania ważności certyfikatu jako usługi certyfikacyjnej należy zamieścić w przepisach szczegółowych ustawy (zapisy w Rozdziale V ustawy); w takiej sytuacji definicja tej usługi jest zbędna



Oznaczenie	Uwaga	Propozycja
Art. 2.11	Definicja Datownika elektronicznego jest niezrozumiała. Brak wyraźnego rozróżnienia pomiędzy znakowaniem czasem a datownikiem elektronicznym. W uzasadnieniu wskazano, że jest to usługa wewnętrzna, analogiczna do znakowania czasem, w obiegu dokumentów w urzędzie – jaka jest zatem funkcja tej konstrukcji w odniesieniu do zakresu przedmiotowego ustawy o podpisie elektronicznym? Ponadto, jeżeli datownik elektroniczny ma stanowić realizację „time mark” to nie musi być opatrzony pieczęcią elektroniczną, a jedynie może być zabezpieczony zapisem w rejestrze.	W świetle wyrażonych wątpliwości należy rozważyć celowość utrzymywania tego pojęcia w ustawie. Być może powinna się znaleźć w ustawie o informatyzacji podmiotów realizujących zadania publiczne jako związana z e-administracją ?
Art. 2.12 i 2.13	Definicja czasu urzędowego jest nieprecyzyjna i nie należy do tej ustawy; ponadto, poziom bezpieczeństwa wzorca czasowego i sposobu jego dystrybucji nie zapewnia wystarczającej wiarygodności na potrzeby konstrukcji daty pewnej.	Należy przywołać odpowiednią ustawę wprowadzającą czas urzędowy (Ustawa z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej Dz.U. 04.56.548) i zaproponować nowelizację przepisów ustawy i wydanego na jej podstawie rozporządzenia w sposób zapewniający wiarygodny wzorzec czasu i sposób jego rozpowszechniania
Art. 2. 14	Definicja urządzenia do składania podpisu jest niepoprawna.	<i>„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</i> <u>Uzasadnienie:</u> Doprecyzowana definicja z Dyrektywy zmodyfikowana na podstawie niemieckiej ustawy o podpisie elektronicznym
Art. 2.15	(Bezpieczne urządzenie do składania podpisu elektronicznego) Zwraca się uwagę, że jedyną decyzją Komisji wskazującą odnośne normy jest 14/07/2003, która mówi o trzech normach: CWA 14167-1 (March 2003): security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements — CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP) — CWA 14169 (March 2002): secure signature-creation devices. z których tylko jedna odnosi się do SSCD	<i>„bezpieczne urządzenie służące do składania podpisów” oznacza urządzenie służące do składania podpisów, które spełnia wymogi określone w Ustawie.</i> Rekomendujemy wyeliminowanie definicji bezpiecznego urządzenia, ponieważ odnośne wymagania są zawarte w art. 26; który należy doprecyzować, przytaczając zapisy z Załącznika III Dyrektywy.



Oznaczenie	Uwaga	Propozycja
Art. 2.16	Definicja niezgodna z Dyrektywą	<p><i>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;</i></p> <p><u>Uzasadnienie:</u> Doprecyzowana definicja z Dyrektywy</p>
Art. 2.17	Definicja wiąże produkt podpisu elektronicznego z podmiotem świadczącym usługi certyfikacyjne, co jest niezgodne z definicją dyrektywy, która nazywa produktem także te rzeczy, które są przeznaczone do użycia przy tworzeniu bądź weryfikacji podpisów elektronicznych.	<p><i>Produkt podpisu elektronicznego jest to oprogramowanie, sprzęt lub ich istotne składniki, które są używane przez podmioty świadczące usługi certyfikacyjne do udostępnienia usług podpisu elektronicznego lub są przeznaczone do składania lub weryfikacji podpisów elektronicznych.</i></p> <p><u>Uzasadnienie:</u> Doprecyzowana definicja z Dyrektywy</p>
Art. 2.18	Definicja ‘podpisującego’ zawęży zakres stosowania podpisów elektronicznych Uwaga redakcyjna: definicja ‘podpisującego’, jako pojęcie fundamentalne dla zrozumienia ustawy, powinna następować bezpośrednio za definicją podpisu elektronicznego	<p><i>21. „podpisujący” oznacza:</i></p> <p><i>1) osobę fizyczną, która działa w imieniu własnym albo w imieniu innych osób fizycznych lub podmiotu;</i></p> <p><i>3) podmiot;</i></p> <p><i>posiadające urządzenie do składania podpisu elektronicznego.</i></p> <p><u>Uzasadnienie:</u> Definicja taka sama, jak w projekcie Ustawy, z uwzględnieniem możliwości złożenia podpisu automatycznego przez podmiot (pieczęci).</p>
Art. 3	Dalszy ciąg definicji, zwykle wszystkie definicje zawierają się w jednym artykule ustawy	Połączyć art. 2 i 3 w jeden



Oznaczenie	Uwaga	Propozycja
Art. 3.1	Definicja niezgodna z definicją z Dyrektywy Z uwagi na logikę definiowania pojęć na podstawie już zdefiniowanych, pojęcie ‘certyfikatu’ powinno następować po ‘urządzeniu do weryfikacji podpisu’.	<p>„certyfikat” oznacza potwierdzenie elektroniczne, za pomocą którego dane służące do weryfikacji podpisu są przyporządkowane podpisującemu i potwierdzają jego tożsamość;</p> <p><u>Uzasadnienie:</u> Definicja z Dyrektywy z doprecyzowaniem; w oryginale jest: "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person" ; “osoba” została zmieniona na „podpisującego” (w polskim systemie prawa mówiąc “osoba” mamy na myśli “osobę fizyczną lub prawną”, pozostają jeszcze jednostki organizacyjne nie posiadające osobowości prawnej)</p> <p><u>Uwagi dodatkowe:</u></p> <p>b. Skorygowanie błąd definicji z projektu Ustawy: („potwierdza tożsamość” – dokonuje uwierzytelnienia podpisującego, a nie „umożliwia identyfikację”)</p>
Art. 3.3	Definicja (certyfikatu kwalifikowanego) proponowana w ustawie nie jest definicją, ponieważ zawiera wymagania (opisane w przepisach szczegółowych Ustawy), a nie opisuje cech wyróżniających	<p>Rekomenduje się usunąć definicję, a wymagania na certyfikat kwalifikowany doprecyzować w art. 27 lub zmienić definicję na:</p> <p>„certyfikat kwalifikowany” oznacza certyfikat spełniający wymogi określone w art. i wydawany przez podmiot świadczący usługi certyfikacyjne, który spełnia wymogi z art...;</p> <p><u>Uzasadnienie:</u> Definicja z Dyrektywy z dostosowaniem do realiów polskiej ustawy</p>
Art. 3.4	Sprzeczność definicji: pieczęć elektroniczna nie jest realizowana przez osobę fizyczną, ale podpisujący jest osobą fizyczną, która używa pieczęci! W przypadku zastosowania mechanizmu podpisu zaawansowanego do realizacji pieczęci elektronicznej ogólne pojęcie certyfikatu jest wystarczające.	W świetle uwag należy rozważyć brzmienie tego przepisu
Art. 3.5	Definicja nieprawidłowa – certyfikat kwalifikowany NIE JEST certyfikatem urzędowym; zasada, że wszędzie tam, gdzie można stosować certyfikat urzędowy, można też stosować certyfikat kwalifikowany, nie należy do definicji, a jest określona w art. 5. W przypadku zastosowania mechanizmu podpisu zaawansowanego do realizacji	W świetle uwag należy rozważyć brzmienie tego przepisu.



Oznaczenie	Uwaga	Propozycja
	podpisu urzędowego ogólne pojęcie certyfikatu jest wystarczające.	
Art. 3.6	Definicja Certyfikatu atrybutów nie odnosi się do zakresu przedmiotowego ustawy, ponieważ nie ma bezpośredniego związku z certyfikatem klucza publicznego. Wykorzystanie certyfikatów atrybutów może być elementem modelu biznesowego w konkretnym zastosowaniu podpisu elektronicznego .	W świetle uwag należy rozważyć brzmienie tego przepisu, albo poprzez rezygnację albo rozbudowę o przepisy określające odpowiednio, wystawiającego certyfikat atrybutów i warunki jego wydawania.
Art. 4.1	Zapis nieprecyzyjny i za szeroki – Dyrektywa określa jedynie zasadę, że certyfikat uznany za kwalifikowany w jednym z krajów EOG musi być uznany przez pozostałe kraje członkowskie jako kwalifikowany.	Zmienić na: Certyfikat wydany jako kwalifikowany przez podmiot świadczący usługi certyfikacyjne i mający siedzibę na terytorium Wspólnoty Europejskiej zrównuje się pod względem prawnym z certyfikatem kwalifikowanym wydanym przez podmiot świadczący usługi certyfikacyjne i mający siedzibę na terytorium Rzeczypospolitej Polskiej pod warunkiem, że pierwszy podmiot spełnia wymagania Dyrektywy 1999/93/WE
Art. 4.1. 1)	Pominięto słowo dobrowolnej w opisie ‘systemu akredytacji’ – jest ono użyte w art. 7 pkt 1a) Dyrektywy	Wprowadzić słowa „systemu dobrowolnej akredytacji”, o którym mowa w art. (zob. propozycja. zapisów dotyczących dobrowolnej akredytacji)
Art. 5.1	„Zaawansowany podpis elektroniczny, weryfikowany przy pomocy certyfikatu wywołuje skutek prawny, jeżeli został złożony w okresie ważności tego certyfikatu” – w świetle art. 8 niniejszy art. jest nadmiarowy	W świetle uzasadnienia zawartego w osobnym rozdziale dołączonym do opinii, należy rozważyć całościowo rozwiązanie skutków prawny podpisów innych niż kwalifikowany
Art. 5.2	Art. 5.2 powtarza definicję zaawansowanego podpisu, dodając warunek zawężający :jednoznacznie wskazuje certyfikat wykorzystywany do weryfikacji tego podpisu” Wprowadzenie tego przepisu powoduje niezgodność z definicją zaawansowanego podpisu elektronicznego zawartą w Dyrektywie. Należy stwierdzić, że w najogólniejszym sensie weryfikacja zaawansowanego podpisu elektronicznego wymaga klucza publicznego (danych służących o weryfikacji podpisu) a nie certyfikatu.	W świetle uzasadnienia zawartego w osobnym rozdziale dołączonym do opinii, należy rozważyć całościowo rozwiązanie skutków prawny podpisów innych niż kwalifikowany



Oznaczenie	Uwaga	Propozycja
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!. Dalsze uzasadnienie – zob. [Ekspertyza – ea/zo] str. 152	Zmienić na: <i>Złożenie(kwalifikowanego) podpisu elektronicznego na danych elektronicznych wywiera taki sam skutek prawny, jak złożenie podpisu własnoręcznego z zachowaniem formy pisemnej.</i>
Art. 5.4	Zob. komentarz do art. 2.4	Rozważyć celowość pozostawienia instytucji podpisu łącznego
Art. 6.1	Problem artykułu 6.1 został rozwiązany poprzez zaproponowanie definicji w ustawie eliminujących występowanie problemu uwierzytelnienia podpisującego	Rozważyć celowość usunięcia art. 6.1
Art. 6.2	Kompletnie niezrozumiałe zastrzeżenie – jeśli dane są z PESEL, to nie można użyć ich do weryfikacji podpisu elektronicznego? Proponowana konstrukcja jest niezgodna z definicją podpisu elektronicznego. Ponadto, jakie to czynności podpisującego nie rodzą skutków prawnych?	Usunąć art. 6.2 - proste formy uwierzytelniania oparte na innych technologiach niż PKI zawiera projekt ustawy o Informatyzacji podmiotów realizujących zadania publiczne.
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. Zob. rozdział opinii PTI dot. skutków prawnych



Oznaczenie	Uwaga	Propozycja
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. Szczegółowe uzasadnienie – zob. [Ekspertyza – ea/zo] str. 61	Konsekwentnie, w całym projekcie usunąć odniesienie do kwalifikowanego znakowania czasem. Zob. rozdział opinii PTI dot. skutków prawnych
Art. 7.3	Konsekwencja wykreślenia datownika elektronicznego	Konsekwentnie, w całym projekcie usunąć odniesienie do datownika elektronicznego. Zob. rozdział opinii PTI dot. skutków prawnych
Art.10.1 i 2	Tematycznie nie należą do rozdziału 3 (obowiązki podmiotów świadczących usługi certyfikacyjne)	Utworzyć nowy rozdział dot. praw i obowiązków osoby zawierającej umowę z podmiotem świadczącym usługi certyfikacyjne oraz zasad weryfikacji ważności certyfikatów kwalifikowanych w odniesieniu do osoby lub podmiotu polegających na zawartości certyfikatu lub dołączyć odpowiednio do art. 22 i 23.
Art. 10.1	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. Dalsze uzasadnienie – zob. [Ekspertyza – ea/zo] str. 55	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)
Art. 10.2	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. 11-16	Rozczłonkowano na art. 11-12 i 14-16 znacząco skracając listę wymagań w odniesieniu do podmiotów świadczących usługi kwalifikowane; Jednocześnie, z jednego artykułu zrobiono cztery, przedzielając 12 i 14 art. 13 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. 11-16 poniżej



Oznaczenie	Uwaga	Propozycja
Art. 12.1	<p>Ten sam zapis występuje w dwóch miejscach”</p> <p>Podmiot, o którym mowa w ust. 1 opracowuje i publikuje politykę certyfikacji, określającą szczegółowe rozwiązania techniczne i organizacyjne oraz zakres i warunki bezpieczeństwa tworzenia i stosowania certyfikatów</p> <p>Art. 25: 2. Polityka certyfikacji to dokument określający szczegółowe rozwiązania techniczne i organizacyjne oraz zakres i warunki bezpieczeństwa tworzenia i stosowania certyfikatów.</p> <p>W Załączniku II do Dyrektywy nie jest używany termin ‘polityka certyfikacji’. W akcie prawnym rangi ustawy nie powinny być używane nadmiarowo pojęcia techniczne.</p>	Należy usunąć art. 12. 1
Art. 13.1	<p>Art. 13. 1. Rada Ministrów określi, w drodze rozporządzenia:</p> <ol style="list-style-type: none"> 1) szczegółowe warunki techniczne i organizacyjne, które muszą spełniać kwalifikowane podmioty świadczące usługi certyfikacyjne; 2) warunki techniczne i organizacyjne znakowania czasem oraz wydawania certyfikatu atrybutów; 3) wymagania z zakresu ochrony fizycznej pomieszczeń; <p>- uwzględniając konieczność zapewnienia ochrony interesów odbiorców usług certyfikacyjnych, bezpieczeństwo przechowywania danych oraz konieczność zapewnienia, że czas używany do realizacji usług certyfikacyjnych nie różni się od czasu urzędowego lub czasu UTC(PL).</p> <p>Wynika z tego, że zakres rozporządzenia tzw. technicznego jest w zamiarze znacznie szerszy niż do tej pory – a powinien być znacznie mniejszy, jeśli w ogóle jakkolwiek</p> <p>Umieszczenie w jednym rozporządzeniu trzech różnych usług (sugeruje otwarcie</p>	<p>Ograniczyć zakres Rozporządzenia jedynie do:</p> <p>‘warunków organizacyjnych i technicznych, jakie muszą spełniać podmioty świadczące usługi certyfikacyjne polegające na wydawaniu i zarządzaniu certyfikatami kwalifikowanymi, uwzględniając konieczność zapewnienia ochrony interesów podpisujących, osób lub podmiotów polegających na zawartości certyfikatów, bezpieczeństwo przechowywania danych oraz konieczność zapewnienia zgodności z wymogami dyrektywy 1999/93/WE i ogólnie uznanymi normami ustalonymi na podstawie art. 10 tej dyrektywy”.</p>



Oznaczenie	Uwaga	Propozycja
	<p>katalogu usług kwalifikowanych dla znakowania czasem oraz certyfikacji atrybutów) powoduje, że ustawodawca ingeruje w sposób świadczenia usług elektronicznych zupełnie niespotykany w innych obszarach (np. usług telekomunikacyjnych).</p> <p>Dla części usług ustawodawca określi szczegółowe warunki organizacyjne i techniczne, dla innych tylko 'warunki techniczne'. Ponadto, jak zapewnić, że czas używany nie różni się od czasu urzędowego, a jednocześnie wprowadzać pojęcie dokładności synchronizacji (art. 14.2)?</p>	
Art. 14.1	<p>Podmiot świadczący usługę znakowania czasem udostępnia politykę certyfikacji i informacje na temat bezpieczeństwa usługi.</p> <p>Na podstawie tego przepisu można żądać informacji nt. konfiguracji firewalli systemu służącego do wydawania certyfikatów</p>	Zob. uwagę do art. 7 Konsekwentnie należy zastosować to samo rozwiązanie.
Art. 14.2	<p>. 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.</p> <p>Skąd wiadomo jaka dokładność jest wymagana?</p>	Zob. uwagę do art. 7 Konsekwentnie należy zastosować to samo rozwiązanie.
Art. 15.2	<p>2. Potwierdzenie tożsamości może nastąpić, w szczególności z wykorzystaniem danych biometrycznych osoby ubiegającej się o certyfikat.</p> <p>Zapis jest niezrozumiały</p>	Problematyka ta powinna być regulowana w przepisach dot. dokumentów identyfikacyjnych; wyrażamy zaniepokojenie, że przepis ten mógłby stanowić zachętę do nieusprawiedliwionego zbierania danych sensytywnych przez Państwo.
Art. 16.2	<p>Delegacja zawarta w przepisie nie jest zrozumiała i częściowo („warunki techniczne i organizacyjne) pokrywa się z delegacją zawartą w art. 13.1 (..) warunki świadczenia usług, ze szczególnym uwzględnieniem czynności, które mogą wykonywać kwalifikowane podmioty świadczące usługi certyfikacyjne w związku z wykorzystaniem elektronicznych środków komunikacji w administracji publicznej oraz warunki techniczne i organizacyjne ich wykonywania, (..)</p> <p>Nie można określać w rozporządzeniu przedmiotu, który nie jest określony w ustawie</p>	Usunąć art. 16.2



Oznaczenie	Uwaga	Propozycja
Art. 17	Zwraca się uwagę, że 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. Stąd 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. 17.4	Wyrażenie nieprecyzyjne :” jeżeli wartość ta została ujawniona 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. 17.6	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. 19.2	Podmiot świadczący usługi certyfikacyjne jest obowiązany używać systemów do tworzenia, przechowywania lub określania ważności certyfikatów oraz systemów do tworzenia podpisów elektronicznych , w sposób zapewniający prawdziwość danych oraz możliwość wprowadzania zmiany tych danych jedynie osobom uprawnionym, Ten punkt logicznie przynależy do art. 12.4, z zastrzeżeniem, że podmiot świadczący usługi certyfikacyjne nie tworzy podpisów.	Rozważyć scalenie treści art. 19.2 z 12.4 lub usunąć art. 19.2
Art. 20.1	Definicja usług certyfikacyjnych jest b. nieprecyzyjna dlaczego tylko wydawanie certyfikatów, a unieważnianie już nie? I co takiego szczególnego jest w znakowaniu czasem ponad to, że 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



Oznaczenie	Uwaga	Propozycja
Art. 20.2	<p>„Kwalifikowany podmiot może świadczyć inne usługi związane z podpisem elektronicznym, jeżeli uwzględni właściwe normy i standardy wspólnotowe lub międzynarodowe.</p> <p>Które normy są właściwe? Czym różni się standard od normy w sensie prawnym? Po co zapisywać oczywistość, że podmiot może świadczyć usługi?</p>	Proponowane rozwiązanie wychodzi poza zakres ustawy; jest oczywiste, że jeśli ustawa nie zabrania, to podmioty mogą świadczyć dowolne usługi certyfikacyjne; rozważyć usunięcie art. 20.2
Art. 21.1	Znakowanie czasem jest to usługa certyfikacyjna, polegająca na dołączeniu do danych logicznie powiązanych z podpisem elektronicznym lub innymi danymi w postaci elektronicznej informacji o czasie wykonania tej usługi, zgodnym z czasem urzędowym lub czasem UTC(PL) przy okresowej technicznej weryfikacji synchronizacji do czasu urzędowego lub czasu UTC(PL) oraz opatrzeniu danych pieczęcią elektroniczną.	Z uwagi na postulat usunięcia znakowania czasem i skutków prawnych jego stosowania (zob. art. 7), należy usunąć art. 21.1
Art. 21.2	<p>Kwalifikowane znakowanie czasem jest to znakowanie czasem przez podmiot kwalifikowany, z ciągłą techniczną weryfikacją wymaganej dokładności synchronizacji do czasu urzędowego lub czasu UTC(PL)</p> <p>Aby świadczyć kwalifikowaną usługę wystarczy być kwalifikowanym podmiotem (!) oraz zapewnić ciągłą techniczną weryfikację wymaganej dokładności! (nie wiadomo, co znaczy ten termin)</p> <p>To jest ukryta autoryzacja i nierówne traktowanie podmiotów.</p>	Usunąć art. 21.2
Art. 22.	<p>Potwierdzenie ważności certyfikatu jest to usługa, która stwierdza w szczególności ważność lub zawieszenie certyfikatu w czasie jej wykonania oraz datę i czas potwierdzenia.</p> <p>Należy potwierdzenie ważności wprowadzić do art. 31 i uogólnić.</p>	Zintegrować z treścią art. 31.1



Oznaczenie	Uwaga	Propozycja
Art. 25.1	<p>„Kwalifikowany podmiot świadczy usługi certyfikacyjne w oparciu o politykę certyfikacji”.</p> <p>Ponadto, zwraca się uwagę na niespójność pojęć:</p> <ol style="list-style-type: none"> 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. <p>Zatem, w oparciu o jaki dokument należy świadczyć usługę znakowania czasem lub OCSP?</p>	<p>Rozważyć usunięcie całego przepisu 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”.</p> <p>Potraktować konsekwentnie pozostałe punkty art. 25;</p>
Art. 25.2	<p>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.</p>	<p>W przypadku nieuwzględnienia powyższego komentarza, przereklamować przepis zgodnie z uwagą.</p>
Art. 26.1	<p>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</p>	<p>Wprowadzić do tego punktu treść załącznika III Dyrektywy</p>
Art. 26.2	<p>Wytyczne z Załącznika IV nie zostały precyzyjnie przytoczone</p>	<p>Wprowadzić do tego punktu treść załącznika IV z zamianą 'rekomendacji' na 'wymagania' (w akcie prawnym nie mogą być zawarte rekomendacje)</p>
Art. 26.4	<p>„Badania zgodności urządzeń i procesów, o których mowa w ust. 1 i 2 z wymaganiami Unii Europejskiej i międzynarodowych organizacji standaryzacyjnych odbywają się zgodnie z odrębnymi przepisami” – jakich procesów? Dyrektywa w art. 3.4 mówi jedynie o „zgodności bezpiecznych urządzeń do składania podpisów z wymogami ustanowionymi w załączniku III,</p>	<p>Propozycja następującego zapisu: Badania zgodności urządzeń i procesów, o których mowa w ust. 1 i 2 z wymaganiami określonymi w ust. 1 Unii Europejskiej i międzynarodowych organizacji standaryzacyjnych odbywają się zgodnie z odrębnymi przepisami.</p>



Oznaczenie	Uwaga	Propozycja
Art. 26.5	„Służby ochrony państwa, w rozumieniu przepisów o ochronie informacji niejawnych, dokonują oceny przydatności urządzeń, o których mowa w ust. 1, do ochrony informacji niejawnych i wydają stosowne certyfikaty bezpieczeństwa.” – wykracza poza zakres przedmiotowy ustawy, działania takie wynikają wprost z ustawy o ochronie informacji niejawnych.	Rozważyć usunięcie art.26.5-7
Art. 27.1	Brak zgodności z Załącznikiem I Dyrektywy Szczegółowe uzasadnienie – zob. {Ekspertyza – ea/zo} str. 65-66	Doprowadzić do zgodności
Art. 29	„Podmiot kwalifikowany wydając certyfikat potwierdza prawdziwość danych zawartych w tym certyfikacie” Jakie uzasadnienie wprowadzenia informacji o potwierdzeniu prawdziwości danych tego w rozdziale o ważności certyfikatów? Na ten temat jest mowa w art. 15.	Usunąć art. 29
Art.30.2 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. 30.2 7)	Stoimy na stanowisku, że minister nie ma prawa zażądać unieważnienia certyfikatu w jakichkolwiek okolicznościach	Usunąć pkt 7)
Art. 31.1	Technika może wymagać publikacji więcej niż jednej listy certyfikatów unieważnionych. 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) – zob. uwaga do art. 22.	Art. 31.1. Podmiot świadczący usługi certyfikacyjne publikuje listy zawieszonych i unieważnionych certyfikatów kwalifikowanych oraz świadczy usługę potwierdzania ich ważności. Zmiana także w ust. 6.
Art. 31.4	Zgodnie z dokumentem ETSI TS 101 456 (punkt 7.3.6 Uwaga 2) zawieszanie certyfikatów jest opcjonalne	Zamienić „jest obowiązany” na „może”
Art. 32	„Świadczenie usług w formie kwalifikowanej wymaga uzyskania wpisu (..)” – uważamy, że to działanie ma charakter uprzedniej autoryzacji, zabronionej przez Dyrektywę, ponieważ uzależnia świadczenie usług od decyzji administracyjnej (wniosek można przyjąć lub odrzucić);	Należy zmienić zapisy o wniosku w szeregu dalszych punktach (par. 32-48) tak, aby dopasować do nowej treści punktu 23.1: „Podmiot świadczący usługi certyfikacyjne polegające na wydawaniu certyfikatów kwalifikowanych lub zamierzający podjąć taką działalność powiadamia Ministra właściwego do spraw gospodarki.” Szczegółowe zapisy dla formuły powiadomienia w kolejnych artykułach ustawy można znaleźć w [Ekspertyzie – ea/zo] str. 168-170
Art. 45.1	Kontrola powinna być wszczynana także w wyniku skargi obywatela; należy zwrócić uwagę, że punkt ten daje Ministrowi możliwość kontroli także w podmiotach nie świadczących usług w formule kwalifikowanej	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.



Oznaczenie	Uwaga	Propozycja
Art. 59	„Kto, świadcząc usługę znakowania czasem umożliwi oznaczenie danych czasem innym niż z chwili wykonywania tej usługi (..)” – art. skutecznie odstraszaający od świadczenia usługi znakowania czasem w oparciu o czas urzędowy Z uwagi na postulat usunięcia regulacji dot. znakowania czasem proponuje się usunięcie tego artykułu.	Przyjąć rozwiązanie wynikające z wcześniejszych rozstrzygnięć dot. znakowania czasem
Art. 62.1	Ilekróć przepisy odrębne przewidują złożenie bezpiecznego podpisu elektronicznego lub bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu rozumie się przez to obowiązek złożenia kwalifikowanego podpisu elektronicznego. Ta automatyczna zamiana może nie objąć wszystkich istotnych przypadków zastosowania podpisów elektronicznych uregulowanych w przepisach prawa – np. automatyzm zadziała i w rozporządzeniu o e-fakturze (gdzie wystarczający jest podpis zaawansowany), i w podobnych przypadkach - w KPA.	Należy uwzględnić nowe rodzaje podpisów elektronicznych. Minister właściwy do spraw gospodarki powinien zaproponować zmiany przepisów odrębnych w taki sposób, aby konstrukcję bezpiecznego podpisu zamienić na odpowiedni rodzaj podpisu elektronicznego
Art. 64	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. 66	„(..) dostosują polityki certyfikacji (..)” Zapis zbyt zawężający	Zamienić na „dostosują warunki świadczenia usług certyfikacyjnych”
Art. 68	Termin 18 miesięcy na wprowadzenie przepisów wykonawczych jest stanowczo zbyt długi – zob. uwaga ogólna C opinii PTI.	Rozważyć skrócenie terminu do 3 miesięcy
Art. 70	<i>Vacatio legis</i> ustawy jest za długie	Skrócić do 3 miesięcy.



Oznaczenie	Uwaga	Propozycja
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 przepisy, zgodnie z normami ETSI 102 030 i 102 231.
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) <ol style="list-style-type: none"> 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.