Maciej Łopaciński

Analiza ustawy o podpisie elektronicznym

Dokument ten jest oparty na wersji ustawy uchwalonej przez Sejm RP w dniu 27 lipca 2001 i skierowanym do rozpatrzenia do Senatu.

Ustawa o podpisie elektronicznym wprowadza pojęcie podpisu elektronicznego i definiuje warunki w których jest on równoważny pod względem prawym z podpisem własnoręcznym.

W obecnej wersji ustawa jest bublem legislacyjnym i wymaga poprawek w Senacie. Do drobnych błędów należy odwoływanie się w art. 3 do pojęcia Wspólnoty Europejskiej (art. 3.4, 3.5, 3.6) która została zastąpiona przez Unię Europejską na mocy traktatu z Maastricht z 7 lutego 1992 r.

Dużo poważniejsze mogą być konsekwencje zapisów definiujących podpis i warunki jego uznawania:

Art. 4.1: "podpis elektroniczny - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny"

oraz Art. 8: "Nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu lub kwalifikowanego certyfikatu wydanego przez akredytowany podmiot świadczący usługi certyfikacyjne, lub nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego."

W konsekwencji: każde dane, które są w postaci elektronicznej i które są dołączone do innych danych i służą do identyfikacji osoby są podpisem elektronicznym. W szczególności sygnatura pod mailem o teści "Jan Nowak, ul. Puławska 1001, Warszawa" jest na mocy obecnej wersji ustawy podpisem elektronicznym. Sygnatura taka jest w postaci elektronicznej, jest dołączona do innych danych i służy do identyfikacji osoby, a więc wypełnia art. 4.1 i art. 8.

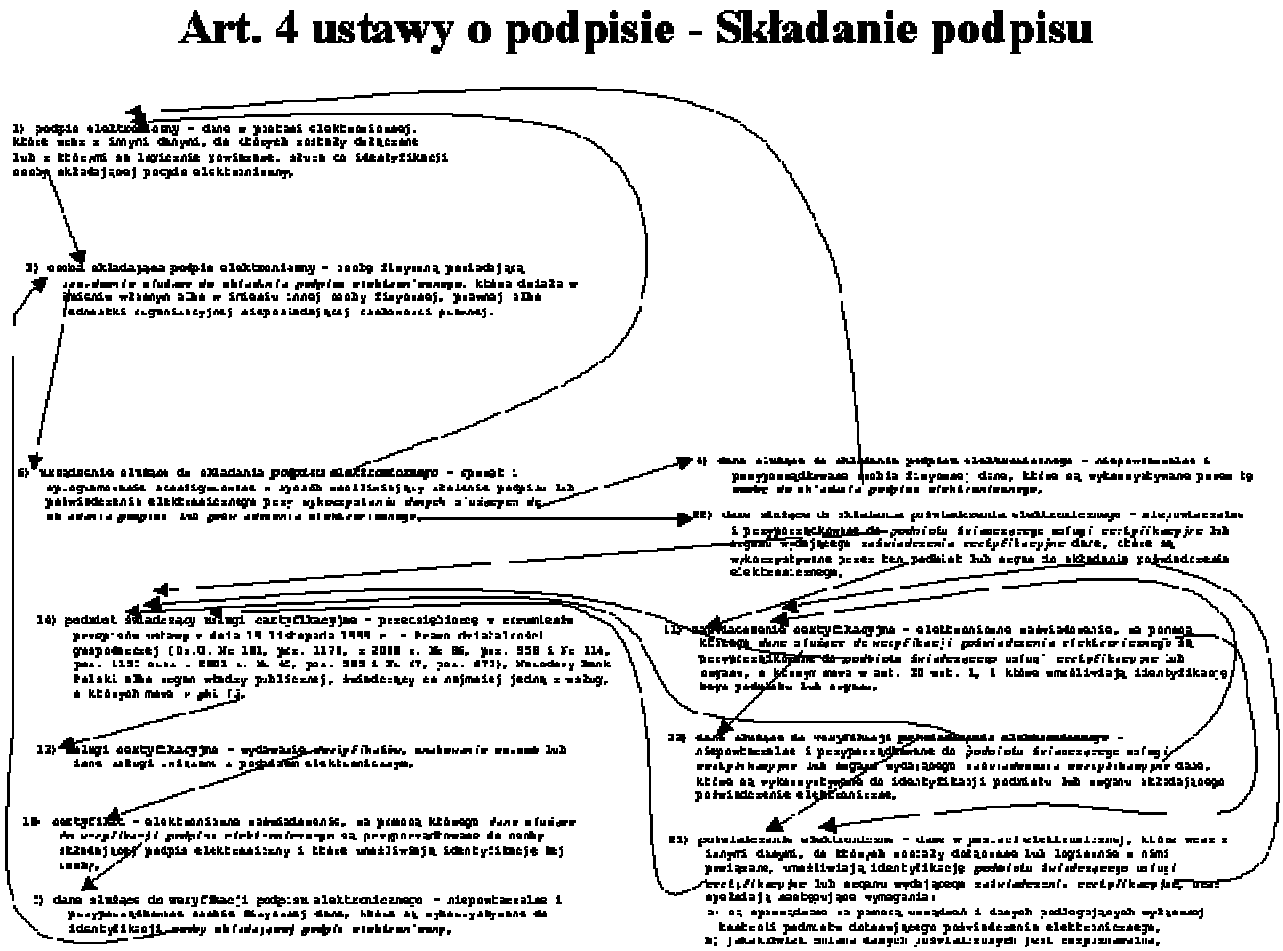
Do braków ustawy należy zaliczyć brak definicji "weryfikacji podpisu elektronicznego" przy jednoczesnym zdefiniowaniu pojęcia "weryfikacji bezpiecznego podpisu elektronicznego" (art. 4.24). Do niezdefiniowanego pojęcia " weryfikacji podpisu elektronicznego" odwołują się definicje np. "urządzenia służącego do weryfikacji podpisu elektronicznego" (art. 4.8).

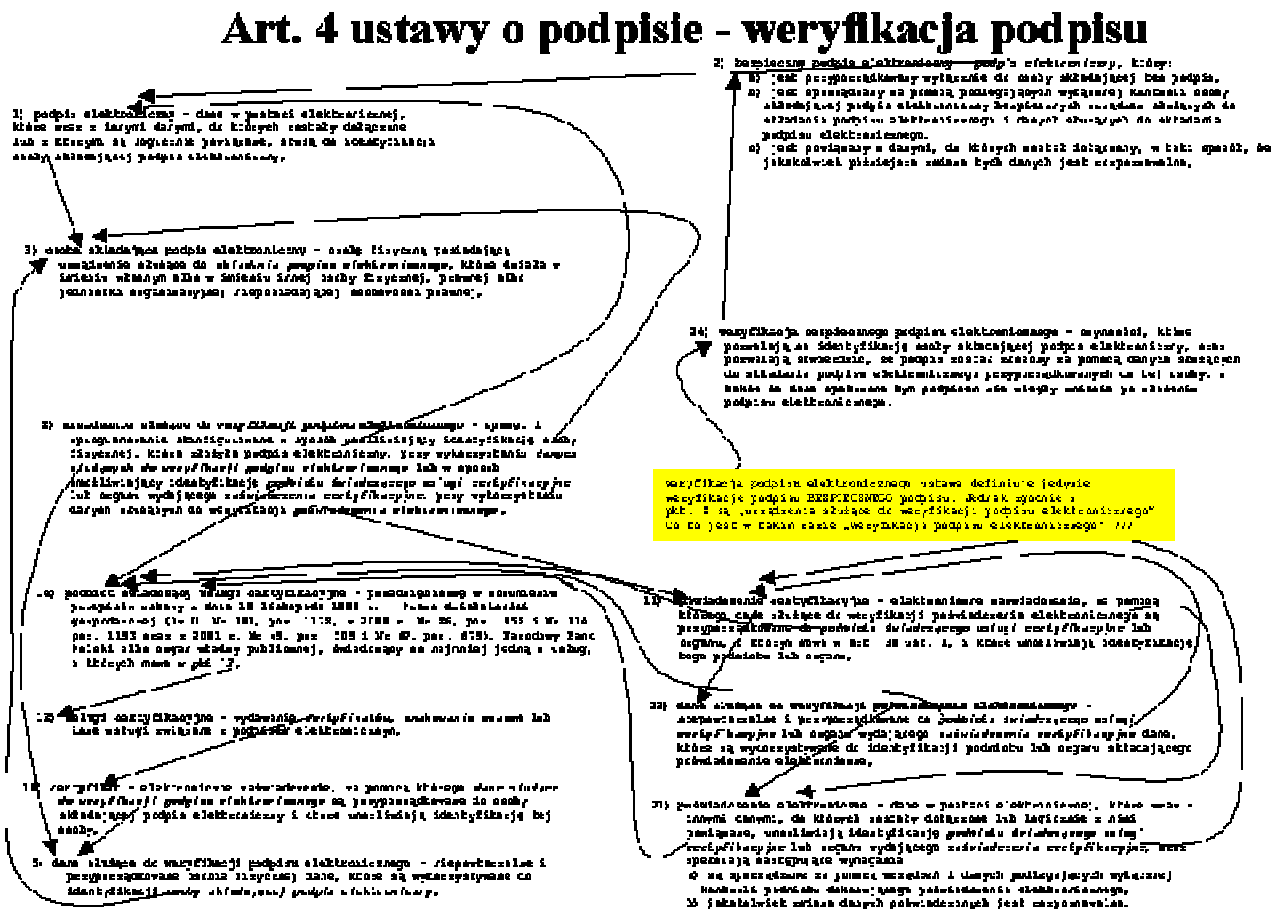
Jako przykład niekonsekwencji ustawodawcy można podać art. 14. Stawia on wymóg poinformowania przed zawarciem umowy o świadczenie usług certyfikacyjnych (nawet nie kwalifikowanych) "... na piśmie lub za pomocą informacji trwale zapisanej na nośniku elektronicznym..." oraz "...pisemnego poświadczania zapoznania się z...". Ponieważ ustawa zrównuje bezpieczny podpis elektroniczny z własnoręcznym, można oczekiwać, że do uzyskania certyfikatu niekwalifikowanego wystarczy posiadanie certyfikatu kwalifikowanego, połączenie z internetem i złożenie odpowiedniego bezpiecznego podpisu elektronicznego. Jednak zapisy ustawy oznaczają, że nawet jeśli mamy możliwość składania bezpiecznego podpisu, chcąc uzyskać niekwalifikowany certyfikat to musimy po zgłoszeniu

przez np. internet poczekać, aż wystawca przyśle tradycyjną pocztą CD-ROM (trwały zapis na nośniku elektronicznym) z informacjami, zapoznać się z nimi i dopiero w tym momencie możemy posłużyć się posiadanym kwalifikowanym certyfikatem do potwierdzenia, że przeczytaliśmy informacje z CD.-ROMu.

Niektóre zapisy ustawy należałoby poddać brzytwie Okhama. Przykładowo: ustawa rozróżnia "kwalifikowany podmiot świadczący usługi certyfikacyjne" od "akredytowanego podmiotu świadczącego usługi certyfikacyjne". Podmiot "kwalifikowany" to taki podmiot który jest wpisany przez ministra do rejestru podmiotów kwalifikowanych. Podmiot akredytowany to podmiot kwalifikowany (czyli wpisany do rejestru) który posiada decyzje ministra potwierdzającą wpis do tego rejestru (akredytację). Zgodnie z art. 26 minister najpierw udziela akredytacji, czyli wydaje decyzję potwierdzającą wpis, a następnie niezwłocznie wpisuje podmiot do rejestru podmiotów kwalifikowanych.

Przejrzystość sformułowań ustawy obrazują dwa grafy na których usiłowałem zrozumieć zawarte w art. 4 definicje podpisywania i weryfikowania podpisu elektronicznego.





Co racjonalny ustawodawca miał na myśli

Ustawa wprowadza pojęcia "podpisu elektronicznego" oraz "bezpiecznego podpisu elektronicznego". Jak pisałem we wstępie pojęcie "podpisu elektronicznego" jest jakąś niedoróbką legislacyjną w której nie bardzo wiem o co autorowi chodzi, pomimo, że znaczna część ustawy jest jemu poświęcona. Rozwiązaniem zagadki tego niebezpiecznego "podpisu elektronicznego" może być chęć objęcia przez ustawodawcę podpisów takich jak wydawane przez np. Verisign. Tylko po co taki podpis wprowadzać do ustawy jeśli nie rodzi skutków prawnych, a więc nic nie znaczy?

"Bezpieczny podpis elektroniczny" to taki który (art. 4.2)
a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,
b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Jeśli "bezpieczny podpis elektroniczny" jest weryfikowany przy pomocy kwalifikowanego certyfikatu to jest równoważny z podpisem własnoręcznym. (art. 5.2)

Certyfikat jest to zgodnie z art. 4.10 "elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej

podpis elektroniczny i które umożliwiają identyfikację tej osoby". Najczęściej danymi tymi będzie to klucz publiczny.

Certyfikat może być "kwalifikowanym certyfikatem" (art. 4.12) lub "certyfikatem" (art.4.10). Różnica pomiędzy nimi sprowadza się do tego, że certyfikat kwalifikowany spełnia warunki określone w ustawie i jest wydawany przez podmiot świadczący usługi certyfikacyjne i spełniający warunki ustawy.

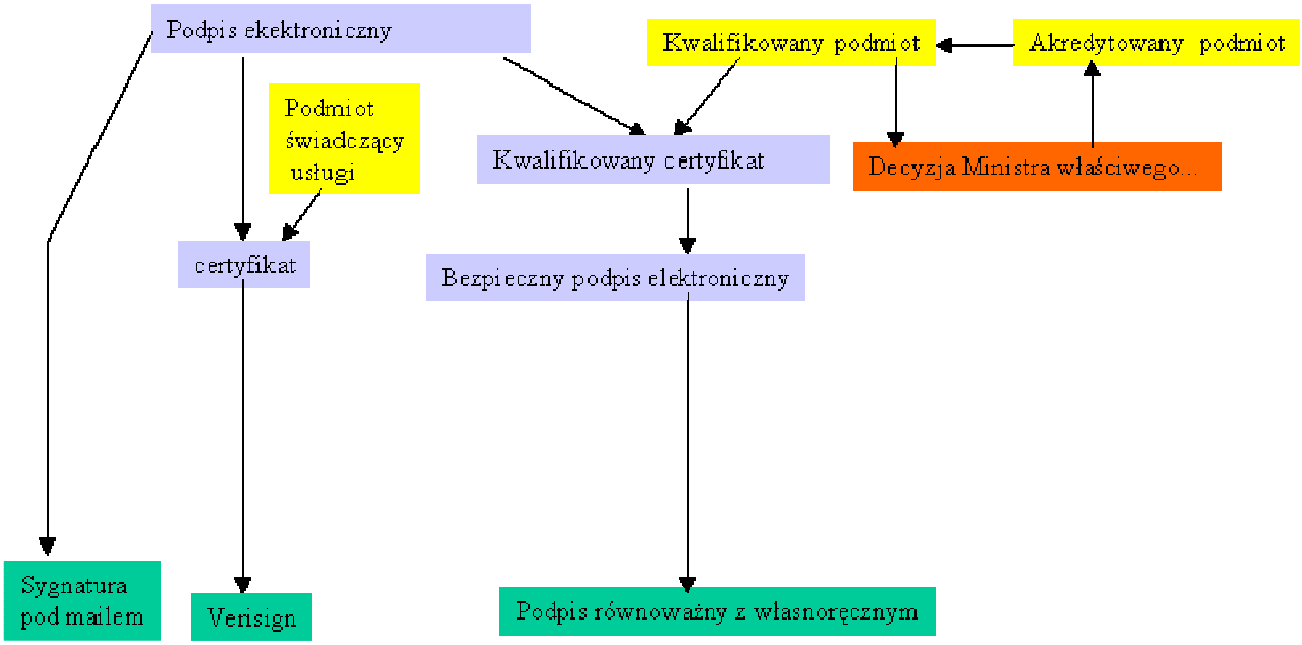
"Certyfikat" nie będący certyfikatem kwalifikowanym może wydać każdy. Jednak wydając taki certyfikat trzeba pamiętać o art. 11 który, wprowadza odpowiedzialność za szkody "spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych usług".

Certyfikat kwalifikowany zgodnie z art. 20.1 musi zawierać:
1) numer certyfikatu,
2) wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany do stosowania zgodnie z określoną polityką certyfikacji,
3) określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę oraz numer akredytacji lub pozycji w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
4) imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone,
5) dane służące do weryfikacji podpisu elektronicznego,
6) oznaczenie początku i końca okresu ważności certyfikatu,
7) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat,
8) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji,
9) ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany, jeżeli przewiduje to polityka certyfikacji lub umowa, o której mowa w art. 14 ust. 1.

Oraz na żądanie osoby składającej podpis elektroniczny inne dane niż wymienione w ust. 1 na wniosek osoby składającej podpis elektroniczny, a w szczególności wskazanie czy osoba ta działa: 1) we własnym imieniu, albo
2) jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo
3) w charakterze członka organu albo organu osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo
4) jako organ władzy publicznej.

Podpis elektroniczny będzie składany przy pomocy "urządzeń służących do składania podpisu elektronicznego" (art. 4.6) lub "bezpiecznych urządzeń służących do składania podpisu elektronicznego" (art. 4.7). "Bezpieczne urządzenie" to takie które spełnia wymagania ustawy określone w art. 18. Autorom ustawy można pogratulować rozumienia słowa bezpieczene jako równoważnika "spełniającego wymogi ustawy".

Podstawowe pojęcia ustawy o podpisie elektronicznym



Podsumowując wszelkie formy podpisu elektronicznego, nawet sygnatury pod mailami, są podpisem elektronicznym.

Podmioty świadczące usługi certyfikacyjne

Ustawa rozróżnia "podmioty świadczące usługi certyfikacyjne" i "kwalifikowane podmioty świadczące usługi certyfikacyjne". Rozróżnienie pomiędzy tymi dwoma rodzajami podmiotów i ich usługami zajmuje znaczną część ustawy i jest przedstawione w tabelce.

Podmioty świadczące usługi certyfikacyjne	**Kwalifikowane podmioty świadczące usługi certyfikacyjne**
Przedsiębiorstwo, NBP, organ władzy publicznej	Przedsiębiorstwo, NBP, organ władzy publicznej
Nie wymaga zezwolenia, koncesji	Wpis do rejestru kwalifikowanych podmiotów
Wydaje certyfikaty	Wydaje kwalifikowane certyfikaty
Znakowanie czasem nie ma skutków prawnych	Znakowanie czasem wywołuje skutki daty pewnej w rozumieniu KC
----------	Uważa się, że bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu został złożony przez osobę określoną w tym certyfikacie, jako osoba składająca podpis

	elektroniczny
	Ma obowiązek: 1) zapewnić techniczne i organizacyjne możliwości szybkiego i niezawodnego wydawania, zawieszania i unieważniania certyfikatów oraz określenia czasu dokonania tych czynności, 2) stwierdzić tożsamość osoby ubiegającej się o certyfikat, 3) zapewnić środki przeciwdziałające fałszerstwom certyfikatów i innych danych poświadczanych elektronicznie przez te podmioty, w szczególności przez ochronę urządzeń i danych wykorzystywanych przy świadczeniu usług certyfikacyjnych, 4) zawrzeć umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych, 5) poinformować osobę ubiegającą się o certyfikat, przed zawarciem z nią umowy, o warunkach uzyskania i używania certyfikatu, w tym o wszelkich ograniczeniach jego użycia, 6) używać systemów do tworzenia i przechowywania certyfikatów, w sposób zapewniający możliwość wprowadzania i zmiany danych jedynie osobom uprawnionym, 7) jeżeli podmiot zapewnia publiczny dostęp do certyfikatów to ich publikacja wymaga uprzedniej zgody osoby, której wydano ten certyfikat, 8) udostępniać odbiorcy usług certyfikacyjnych pełny wykaz bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych i warunki techniczne, jakim te

	urządzenia powinny odpowiadać, 9) zapewnić, w razie tworzenia przez niego danych służących do składania podpisu elektronicznego, poufność procesu ich tworzenia, a także nie przechowywać i nie kopiować tych danych ani innych danych, które mogłyby służyć do ich odtworzenia, oraz nie udostępniać ich nikomu innemu poza osobą, która będzie składała za ich pomocą podpis elektroniczny, 10) zapewnić, w razie tworzenia przez niego danych służących do składania podpisu elektronicznego, aby dane te z prawdopodobieństwem graniczącym z pewnością wystąpiły tylko raz, 11) publikować dane, które umożliwią weryfikację, w tym również w sposób elektroniczny, autentyczności i ważności certyfikatów oraz innych danych poświadczanych elektronicznie przez ten podmiot oraz zapewnić nieodpłatny dostęp do tych danych odbiorcom usług certyfikacyjnych.
Odpowiada za szkody	Odpowiada za szkody
Przechowuje i archiwizuje dokumenty	Przechowuje i archiwizuje dokumenty przez 20 lat
	W przypadku zaprzestania działalności dokumenty będzie odpłatnie przechowywał minister
Ma obowiązek poinformować przed zawarciem umowy o różnicach pomiędzy certyfikatem nie będącym certyfikatem kwalifikowanym a certyfikatem kwalifikowanym	
Ma obowiązek poinformować przed zawarciem umowy na wydanie certyfikatu o: 1) zakres i ograniczenia jego stosowania,	Ma obowiązek poinformować przed zawarciem umowy na wydanie certyfikatu o: 1) zakres i ograniczenia jego stosowania,

2) skutki prawne składania podpisów elektronicznyc h weryfikowanych przy pomocy tego certyfikatu, 3) informację o systemie dobrowolnej akredytacji i rejestracji podmiotów kwalifikowanych i ich znaczeniu.	2) skutki prawne składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu, 3) informację o systemie dobrowolnej akredytacji i rejestracji podmiotów kwalifikowanych i ich znaczeniu.
Ma obowiązek poinformować przed zawarciem umowy o tym, że podpis elektroniczny weryfikowany certyfikatem nie będącym certyfikatem kwalifikowanym nie wywołuje skutków rónożędnych z podpisem własnoręcznym	
	Ma obowiązek opracować politykę certyfikacji
Może korzystać z poświadczenia notarialnego danych osoby ubiegającej się o certyfikat	
	jest obowiązany stosować takie procedury ich wydawania certyfikatów kwalifikowanych, aby uzyskać od osoby ubiegającej się o certyfikat pisemną zgodę na stosowanie danych służących do weryfikacji jej podpisu elektronicznego, które są zawarte w wydany certyfikacie
	Powiadomić zainteresowanego o wydaniu certyfikatu dla osoby działającej w jego imieniu
	Unieważnić lub zawiesić certyfikat w przypadkach określonych w art. 21
Publikować listę zawieszonych certyfikatów	Publikować listę zawieszonych certyfikatów
Podlega kontroli ministra	Podlega kontroli ministra
	Informuje ministra o upadłości

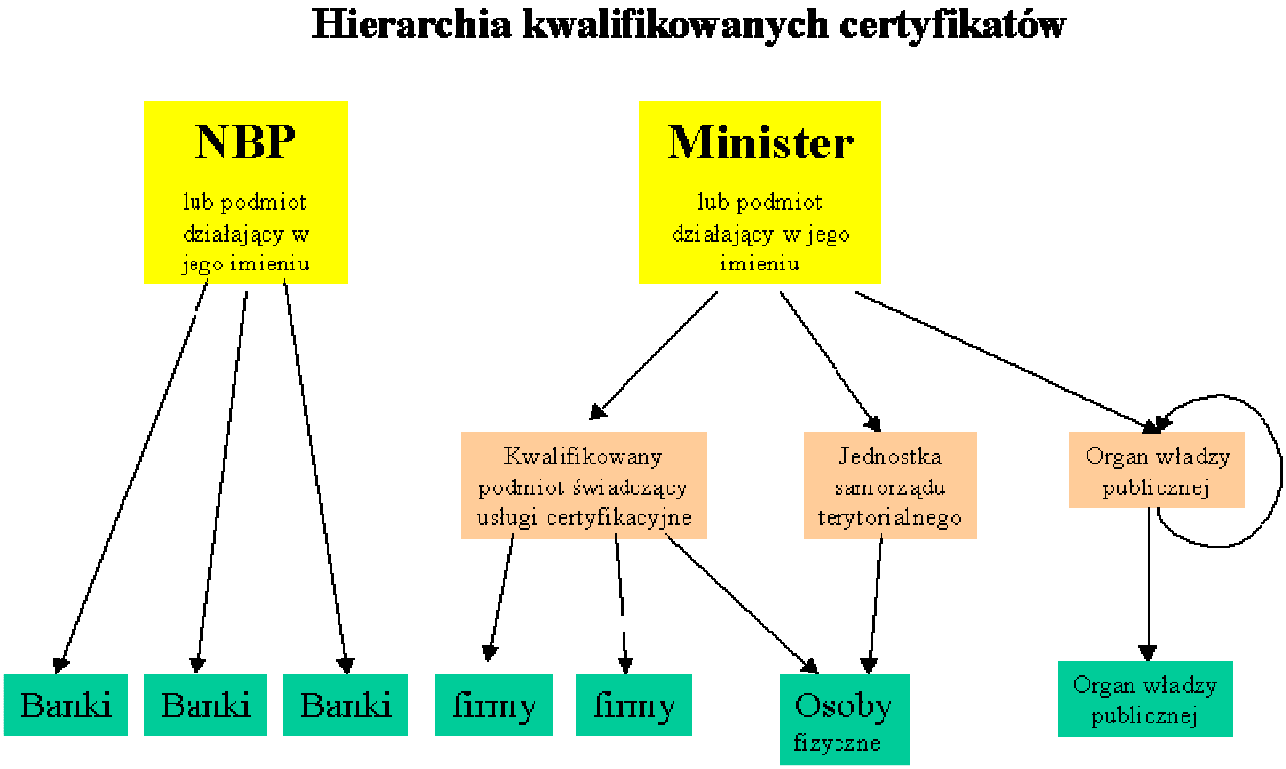
Ograniczenia świadczenia usług certyfikacyjnych:

Art. 9.2 "Organy władzy państwowej i NBP mogą świadczyć usługi certyfikacyjne wyłącznie na użytek własny lub innych organów władzy publicznej."
Art. 9.3 "Jednostka samorządu terytorialnego może świadczyć usługi certyfikacyjne także na potrzeby mieszkańców ją zamieszkujących, tylko w celach niezarobkowych"

Hierarchia certyfikacji

Nadrzędnymi podmiotami w hierarchii certyfikacyjnymi określonymi w ustawie są minister właściwy do spraw gospodarki oraz Narodowy Bank Polski (art. 23). NBP jest nadrzędny dla

banków, minister w pozostałych przypadkach. Zarówno NBP jak i minister może zlecić prowadzenie tego nadrzędnego rejestru wybranemu podmiotowi - ministra obowiązuje w tym przypadku ustawa o zamówieniach publicznych.



Pozostałe prace legislacyjne

Ustawa wchodzi w życie w 6 miesięcy od dnia ogłoszenia. Do tego czasu ministrowie mają:

Art. 10. 4. Rada Ministrów może określić, w drodze rozporządzenia, szczegółowe warunki techniczne i organizacyjne, które muszą spełniać kwalifikowane podmioty świadczące usługi certyfikacyjne, w tym wymagania z zakresu ochrony fizycznej pomieszczeń, w których znajdują się informacje, o których mowa w art. 12 ust.1, uwzględniając zakres stosowania wydawanych przez nie certyfikatów, wymagania ich ochrony oraz konieczność zapewnienia ochrony interesów odbiorców usług certyfikacyjnych.

Art. 10.5. Minister właściwy do spraw instytucji finansowych, w porozumieniu z ministrem właściwym do spraw gospodarki, po zasięgnięciu opinii Polskiej Izby Ubezpieczeń, określi, w drodze rozporządzenia, sposób i szczegółowe warunki spełnienia obowiązku ubezpieczenia, o którym mowa w ust. 1 pkt 4, w tym w szczególności termin powstania obowiązku zawarcia umowy ubezpieczenia oraz minimalne sumy gwarancyjne, z uwzględnieniem konieczności zapewnienia gwarancji spełnienia obowiązku zawarcia umowy ubezpieczenia.

Art. 17.2. Rada Ministrów określa, po zasięgnięciu opinii Prezesa Narodowego Banku Polskiego, w drodze rozporządzenia, podstawowe wymagania organizacyjne i techniczne dotyczące polityk certyfikacji dla kwalifikowanych certyfikatów, uwzględniając zakres zastosowania tych certyfikatów oraz okresy ich ważności, konieczność zapewnienia współdziałania różnych urządzeń do składania i weryfikacji podpisów elektronicznych,

zapewnienie bezpieczeństwa obrotu prawnego oraz uwzględniając standardy Unii Europejskiej.

Art. 18.3. Rada Ministrów, określi, w drodze rozporządzenia, szczegółowe warunki techniczne, jakim powinny odpowiadać bezpieczne urządzenia do składania podpisów elektronicznych oraz bezpieczne urządzenia do weryfikacji podpisów elektronicznych, uwzględniając potrzebę zapewnienia nienaruszalności i poufności danych opatrzonych takim podpisem.

Art. 18.5. Służby ochrony państwa, w rozumieniu przepisów o ochronie informacji niejawnych, dokonują oceny przydatności urządzeń, o których mowa w ust. 1 i 2, do ochrony informacji niejawnych i wydają stosowne certyfikaty bezpieczeństwa.

Art. 23.5 5. Minister właściwy do spraw gospodarki może, w trybie przepisów o zamówieniach publicznych, powierzyć podmiotowi świadczącemu usługi certyfikacyjne wytwarzanie i wydawanie zaświadczeń certyfikacyjnych, o których mowa w ust. 2 i 3, publikację listy, o której mowa w ust. 4, oraz danych służących do weryfikacji wydanych zaświadczeń certyfikacyjnych.

Art. 24.8 Minister właściwy do spraw gospodarki określi, w drodze rozporządzenia:
1) wzór i szczegółowy zakres wniosku, uwzględniając możliwość elektronicznego przetwarzania danych zawartych w formularzach,
2) szczegółowy tryb tworzenia i wydawania zaświadczenia certyfikacyjnego, w tym przez podmioty upoważnione na podstawie art. 23 ust. 5 lub 6, biorąc pod uwagę konieczność zapewnienia poufności tworzenia i wydawania zaświadczenia certyfikacyjnego,
3) wysokość opłat za rozpatrzenie wniosku o udzielenie akredytacji oraz dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, uwzględniając uzasadnione koszty ponoszone w związku z postępowaniem akredytacyjnym i prowadzeniem rejestru.

Inne ważne zapisy

Kluczowymi zapisami ustawy są zapisy pozwalające na:

składanie oświadczeń woli w formie elektronicznej. Art. 54 zobowiązanie organów władzy publicznej do umożliwienia wnoszenia podań, wniosków i innych czynności w formie elektronicznej. Art. 58 - Niestety są na to 4 lata.