SEJM
RZECZYPOSPOLITEJ POLSKIEJ

III kadencja

Prezes Rady Ministrów
RM 10-15-01

**Druk nr 2651**
Warszawa, 22 lutego 2001 r.

Pan
Maciej Płażyński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku.

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o **podpisie elektronicznym** wraz z projektami podstawowych aktów wykonawczych,

co do którego Rada Ministrów zadeklarowała, że ma na celu dostosowanie polskiego ustawodawstwa do prawa Unii Europejskiej.

Jednocześnie, zgodnie z wymogami art. 31 ust.3b Regulaminu Sejmu, przekazuję przetłumaczone na język polski, teksty przepisów Unii Europejskiej, do których ma być dostosowane prawo polskie.

Ponadto uprzejmie informuję, że do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Spraw Wewnętrznych i Administracji.

Z wyrazami szacunku

(-) Jerzy Buzek

**Projekt**

# USTAWA
# O PODPISIE ELEKTRONICZNYM

## ROZDZIAŁ I
## PRZEPISY OGÓLNE

Art. 1.

Ustawa określa warunki i skutki prawne stosowania podpisu elektronicznego, zasady świadczenia usług związanych z podpisem elektronicznym i nadzoru nad podmiotami świadczącymi te usługi.

Art. 2.

Przepisy niniejszej ustawy stosuje się do podmiotów świadczących usługi certyfikacyjne, mających siedzibę lub świadczących usługi na terytorium Rzeczypospolitej Polskiej.

Art. 3.

Certyfikaty wydane przez podmiot świadczący usługi certyfikacyjne, nie mający siedziby na terytorium Rzeczypospolitej Polskiej i nie świadczący usług na jej terytorium, zrównuje się pod względem prawnym z kwalifikowanymi certyfikatami wydanymi przez akredytowany lub kwalifikowany podmiot świadczący usługi certyfikacyjne, mający siedzibę lub świadczący usługi na terytorium Rzeczypospolitej Polskiej, jeżeli:

1) podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, spełnia wymagania niniejszej ustawy i została mu udzielona akredytacja,
2) podmiot świadczący usługi certyfikacyjne, mający siedzibę na terytorium Rzeczypospolitej Polskiej lub świadczący usługi na jej terytorium, udzielił gwarancji za ten certyfikat,
3) przewiduje to umowa międzynarodowa o wzajemnym uznaniu certyfikatów,
4) podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, spełnia wymagania niniejszej ustawy i została mu udzielona akredytacja w państwie członkowskim Unii Europejskiej,
5) podmiot świadczący usługi certyfikacyjne, mający siedzibę na terytorium Wspólnoty Europejskiej spełniający wymogi niniejszej ustawy, udzielił gwarancji za ten certyfikat,
6) certyfikat ten został uznany za kwalifikowany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi lub
7) podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, został uznany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi.

Art. 4.

Użyte w niniejszej ustawie wyrażenia oznaczają:

1) „podpis elektroniczny” – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację osoby fizycznej składającej podpis, oraz spełniają następujące wymagania:
   a) są przyporządkowane wyłącznie do osoby fizycznej składającej podpis,
   b) pozwalają stwierdzić, czy osoba fizyczna składająca podpis działa:
      – we własnym imieniu,
      – jako przedstawiciel innej określonej osoby fizycznej lub osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej,
      – w charakterze członka organu lub organu określonej osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej albo
      – jako określony organ władzy publicznej,
   c) są sporządzane za pomocą urządzeń i danych, podlegających wyłącznej kontroli osoby fizycznej składającej podpis,
   d) jakakolwiek zmiana danych podpisanych jest rozpoznawalna,
2) „osoba składająca podpis elektroniczny” – osoba fizyczna, której tożsamość jest określana za pomocą złożonego podpisu elektronicznego,
3) „dane służące do składania podpisu elektronicznego” – niepowtarzalne i przyporządkowane określonej osobie fizycznej dane, które są wykorzystywane przez tę osobę do złożenia podpisu elektronicznego,
4) „dane służące do weryfikacji podpisu elektronicznego” – niepowtarzalne i przyporządkowane określonej osobie fizycznej dane, które są wykorzystywane do potwierdzenia tożsamości osoby składającej podpis elektroniczny,
5) „urządzenie do składania podpisu elektronicznego” – sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający złożenie podpisu elektronicznego przy wykorzystaniu danych służących do składania podpisu elektronicznego,
6) „bezpieczne urządzenie do składania podpisu elektronicznego” – urządzenie do składania podpisu elektronicznego, spełniające wymagania określone w niniejszej ustawie,
7) „urządzenie do weryfikacji podpisu elektronicznego” – sprzęt i oprogramowanie skonfigurowane w sposób umożliwiający potwierdzenie, przy wykorzystaniu danych służących do weryfikacji podpisu elektronicznego, tożsamości osoby fizycznej, która złożyła podpis elektroniczny,
8) „bezpieczne urządzenie do weryfikacji podpisu elektronicznego” – urządzenie do weryfikacji podpisu elektronicznego, spełniające wymagania określone w niniejszej ustawie,
9) „certyfikat” – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do określonej osoby składającej podpis elektroniczny i które umożliwiają potwierdzenie tożsamości tej osoby,
10) „zaświadczenie certyfikacyjne” – elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do określonego podmiotu świadczącego usługi certyfikacyjne i które umożliwiają potwierdzenie tożsamości tego podmiotu,
11) „kwalifikowany certyfikat” – certyfikat spełniający warunki, określone w art. 19 niniejszej ustawy i wydany przez akredytowany lub kwalifikowany podmiot świadczący usługi certyfikacyjne,
12) „usługi certyfikacyjne” – wydawanie certyfikatów, znakowanie czasem lub inne usługi związane z podpisem elektronicznym,
13) „podmiot świadczący usługi certyfikacyjne” – przedsiębiorca w rozumieniu przepisów ustawy z dnia 19 listopada 1999 r. Prawo działalności gospodarczej (Dz. U. Nr 101, poz. 1178 oraz z 2000 r. Nr 86,poz. 958 i Nr 114, poz. 1193) albo organ władzy publicznej, świadczący usługi, o których mowa w pkt 12,

14) „akredytacja” – decyzja administracyjna potwierdzająca, że podmiot świadczący usługi certyfikacyjne spełnia wymagania określone w niniejszej ustawie,
15) „akredytowany podmiot świadczący usługi certyfikacyjne” – podmiot świadczący usługi certyfikacyjne posiadający akredytację,
16) „kwalifikowany podmiot świadczący usługi certyfikacyjne” – podmiot świadczący usługi certyfikacyjne wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
17) "znakowanie czasem" – usługa polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem i poświadczeniem elektronicznym, oznaczenia rzeczywistego czasu wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę,
18) „polityka certyfikacji” – szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób tworzenia oraz zakres i sposób stosowania certyfikatu w warunkach jednolitych wymagań bezpieczeństwa,
19) "odbiorca usług certyfikacyjnych" – osoba fizyczna, osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która zawarła z podmiotem świadczącym usługi certyfikacyjne umowę o świadczenie usług certyfikacyjnych lub która w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub inne dane, elektronicznie poświadczone przez podmiot świadczący usługi certyfikacyjne,
20) "jednostki sektora publicznego" – jednostki organizacyjne, o których mowa w art. 4 ust. 1 ustawy z dnia 10 czerwca 1994 r. o zamówieniach publicznych (Dz. U. z 1998 r. Nr 119, poz. 773, z 1999 r. Nr 45, poz. 437 oraz z 2000 r. Nr 12, poz. 136, Nr 93, poz. 1027 i Nr 110, poz. 1167),
21) "poświadczenie elektroniczne" – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne, oraz spełniają następujące wymagania:
    a) są sporządzane za pomocą urządzeń i danych podlegających wyłącznej kontroli podmiotu dokonującego poświadczenia elektronicznego,
    b) jakakolwiek zmiana danych poświadczonych jest rozpoznawalna.

## ROZDZIAŁ II
## SKUTKI PRAWNE PODPISU ELEKTRONICZNEGO

### Art. 5.

1. Podpis elektroniczny weryfikowany przy pomocy certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu. Podpis elektroniczny złożony w okresie zawieszenia certyfikatu wykorzystywanego do jego weryfikacji wywołuje skutki prawne z chwilą uchylenia tego zawieszenia.
2. Dane w postaci elektronicznej opatrzone podpisem elektronicznym weryfikowanym na podstawie ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi.
3. Podpis elektroniczny weryfikowany na podstawie kwalifikowanego certyfikatu zapewnia integralność danych opatrzonych podpisem i jednoznaczne wskazanie kwalifikowanego certyfikatu, w ten sposób, że rozpoznawalne są wszelkie próby zmiany tych danych lub zmiany wskazania kwalifikowanego certyfikatu wykorzystywanego do weryfikacji tego podpisu.

4. Domniemywa się, że podpis elektroniczny weryfikowany na podstawie ważnego kwalifikowanego certyfikatu został złożony przez osobę określoną w tym certyfikacie, jako osoba składająca podpis elektroniczny.
5. Po upływie terminu ważności certyfikatu lub od dnia jego unieważnienia oraz w okresie jego zawieszenia domniemanie, o którym mowa w ust. 4, nie istnieje, chyba że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu lub przed dniem jego unieważnienia albo zawieszenia.
6. Spełnienie wymogu, o którym mowa w art. 4 pkt 1 lit. c), domniemywa się.
7. Podpis elektroniczny może być znakowany czasem.
8. Domniemywa się, że podpis elektroniczny znakowany czasem przez akredytowany lub kwalifikowany podmiot świadczących usługi certyfikacyjne został złożony nie później niż w czasie rzeczywistym wskazanym za pomocą tej usługi. Domniemanie to istnieje do dnia utraty ważności certyfikatu wykorzystywanego do weryfikacji tego znakowania. Przedłużenie istnienia domniemania wymaga kolejnego znakowania czasem podpisu elektronicznego wraz z danymi służącymi do poprzedniej weryfikacji przez akredytowany lub kwalifikowany podmiot świadczący tę usługę.
9. 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 do składania podpisu elektronicznego.

Art. 6.

Do skutków prawnych podpisu elektronicznego, w zakresie nie uregulowanym w niniejszej ustawie, stosuje się przepisy dotyczące podpisów własnoręcznych.

Art. 7.

1. Strony stosunku prawnego mogą, w drodze umowy, uznać za prawnie skuteczny podpis elektroniczny weryfikowany na podstawie certyfikatu wydanego przez podmiot nie mający siedziby na terytorium Rzeczypospolitej Polskiej i nie świadczący usług certyfikacyjnych na jej terytorium.
2. Przepisu ust. 1 nie stosuje się do podpisu elektronicznego weryfikowanego na podstawie certyfikatu wydanego przez podmiot świadczący usługi certyfikacyjne, mający siedzibę na terytorium państw członkowskich Unii Europejskiej i pod względem prawnym zrównanego z certyfikatami wydawanymi przez podmiot świadczący usługi certyfikacyjne, mający siedzibę na terytorium Rzeczypospolitej Polskiej.

## ROZDZIAŁ III
## OBOWIĄZKI PODMIOTÓW ŚWIADCZĄCYCH USŁUGI CERTYFIKACYJNE

Art. 8.

1. Prowadzenie działalności w zakresie świadczenia usług certyfikacyjnych, z zastrzeżeniem ust. 2, nie wymaga uzyskania zezwolenia, ani koncesji.
2. Świadczenie usług certyfikacyjnych na rzecz lub przez organy władzy publicznej i jednostki sektora publicznego, z wyjątkiem Narodowego Banku Polskiego, wymaga akredytacji udzielonej przez ministra właściwego do spraw wewnętrznych.

Art. 9.

1. Podmioty świadczące usługi certyfikacyjne są obowiązane:
   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 uzyskanie certyfikatu, w sposób określony w polityce certyfikacji,
   3) uzyskać dodatkowe dane, które mają być zawarte w certyfikacie,
   4) 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,
   5) zawrzeć umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych, w przypadku gdy usługi są świadczone przez akredytowane lub kwalifikowane podmioty świadczące usługi certyfikacyjne,
   6) poinformować osobę, która występuje o certyfikat, przed zawarciem z nią umowy o warunkach uzyskania i używania certyfikatu, w tym o wszelkich ograniczeniach jego użycia oraz - w przypadku gdy podmiot nie posiada akredytacji – również o istnieniu możliwości uzyskania certyfikatu od podmiotu akredytowanego,
   7) używać systemów do znakowania czasem, tworzenia i przechowywania certyfikatów, w sposób zapewniający możliwość wprowadzania i zmiany danych jedynie osobom uprawnionym oraz gwarantujący publiczny dostęp do certyfikatów, jeżeli osoby, którym wydano te certyfikaty wyraziły zgodę na taki dostęp,
   8) udostępniać, na wniosek odbiorcy usług certyfikacyjnych, wykaz bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych,
   9) zapewnić, w razie tworzenia przez nie danych służących do składania podpisu elektronicznego, poufność procesu ich tworzenia, a także nie przechowywać i nie kopiować tych danych oraz nie udostępniać ich nikomu innemu poza osobą, która będzie składała za ich pomocą podpis elektroniczny,
   10) zapewnić za pomocą środków technicznych, aby dane służące do składania podpisów elektronicznych, po zakończeniu procesu ich tworzenia, wystąpiły tylko raz,
   11) zapewnić weryfikację, w tym również w sposób elektroniczny, autentyczności i ważności certyfikatów oraz innych danych poświadczanych elektronicznie przez te podmioty.
2. Osoba wykonująca czynności związane ze świadczeniem usług certyfikacyjnych powinna:
   1) posiadać pełną zdolność do czynności prawnych,
   2) nie być skazana prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, przestępstwo skarbowe lub przestępstwo, o którym mowa w rozdziale X ustawy,
   3) posiadać wyższe wykształcenie,

4) posiadać niezbędną wiedzę w zakresie technologii tworzenia certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym.

3. Minister właściwy do spraw wewnętrznych może określić, w drodze rozporządzenia, szczegółowe warunki techniczne i organizacyjne, które muszą spełniać akredytowane lub kwalifikowane podmioty świadczące usługi certyfikacyjne wykorzystywane do ochrony informacji prawnie chronionych, uwzględniając rodzaj tych informacji, wymagania ich ochrony oraz konieczność zapewnienia ochrony interesów odbiorców usług certyfikacyjnych.
4. Minister właściwy do spraw instytucji finansowych, w porozumieniu z ministrem właściwym do spraw wewnętrznych, po zasięgnięciu opinii Polskiej Izby Ubezpieczeń, określi, w drodze rozporządzenia, sposób i szczegółowe warunki spełnienia obowiązku ubezpieczenia, o którym mowa w ust. 1 pkt 5, w tym w szczególności termin powstania obowiązku zawarcia umowy ubezpieczenia oraz minimalne sumy gwarancyjne, z uwzględnieniem konieczność zapewnienia gwarancji spełnienia obowiązku zawarcia umowy ubezpieczenia.

Art. 10.

1. Podmiot świadczący usługi certyfikacyjne odpowiada wobec odbiorców usług certyfikacyjnych, z zastrzeżeniem ust. 2, za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych usług, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które podmiot świadczący usługi certyfikacyjne nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności.
2. Podmiot świadczący usługi certyfikacyjne nie odpowiada wobec odbiorców usług certyfikacyjnych za szkody wynikające z użycia certyfikatu poza zakresem określonym w polityce certyfikacji, która została wskazana w certyfikacie, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie.
3. Podmiot świadczący usługi certyfikacyjne, który udzielił gwarancji za certyfikat, odpowiada wobec odbiorców usług certyfikacyjnych za wszelkie szkody spowodowane użyciem tego certyfikatu.

Art. 11.

1. Informacje dotyczące działalności podmiotu świadczącego usługi certyfikacyjne, których nieuprawnione ujawnienie mogłoby narazić na szkodę interes tego podmiotu lub odbiorców usług certyfikacyjnych, a w szczególności dane służące do składania poświadczeń elektronicznych i dane osobowe osób, które złożyły wniosek o wydanie certyfikatu, są objęte tajemnicą.
2. Zakazane jest ujawnianie informacji, o których mowa w ust. 1.
3. Do zachowania tajemnicy, o której mowa w ust. 1, są obowiązani:
   1) osoby reprezentujące podmiot świadczący usługi certyfikacyjne,
   2) osoby pozostające z podmiotem świadczącym usługi certyfikacyjne w stosunku pracy, w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze,
   3) pracownicy, osoby pozostające w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze z podmiotami świadczącymi usługi na rzecz podmiotu świadczącego usługi certyfikacyjne.
4. Osoby, o których mowa w ust. 3, mają obowiązek udzielenia informacji, o których mowa w ust. 1, wyłącznie na żądanie:

1) sądu lub prokuratora w związku z toczącym się postępowaniem karnym lub karnym skarbowym,
2) ministra właściwego do spraw wewnętrznych w związku ze sprawowaniem przez niego nadzoru nad działalnością podmiotów świadczących usługi certyfikacyjne,
3) innych organów państwowych upoważnionych do tego na podstawie ustaw w związku z prowadzonymi przez nie postępowaniami w sprawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne.

5. Obowiązek zachowania tajemnicy, o której mowa w ust. 1, trwa przez okres 5 lat od ustania stosunków prawnych określonych w ust. 3.

Art. 12.

1. Podmiot świadczący usługi certyfikacyjne, z zastrzeżeniem art. 9 ust. 1 pkt 9, przechowuje i archiwizuje dokumenty i dane w postaci elektronicznej bezpośrednio związane z wykonywanymi usługami certyfikacyjnymi w sposób zapewniający bezpieczeństwo przechowywanych danych.
2. Obowiązek przechowania trwa przez okres 50 lat od chwili powstania danego dokumentu.
3. W przypadku likwidacji podmiotu świadczącego usługi certyfikacyjne, dokumenty i dane w postaci elektronicznej, o których mowa w ust. 1, przechowuje likwidator tego podmiotu lub jeden ze wspólników spółki cywilnej.
4. Przepis art. 476 § 3 Kodeksu spółek handlowych stosuje się odpowiednio. Właściwy sąd niezwłocznie zawiadamia ministra właściwego do spraw wewnętrznych o wyznaczonym przechowawcy.
5. Minister właściwy do spraw wewnętrznych może określić, w drodze rozporządzenia, krótszy minimalny okres przechowywania, o którym mowa w ust. 2, jednak nie krótszy niż 20 lat, uwzględniając konieczność zapewnienia ochrony interesów odbiorców usług certyfikacyjnych.

## ROZDZIAŁ IV
## ŚWIADCZENIE USŁUG CERTYFIKACYJNYCH

Art. 13.

1. Podmiot świadczący usługi certyfikacyjne wydaje certyfikat na wniosek osoby zainteresowanej składaniem podpisów elektronicznych i na podstawie umowy określającej co najmniej:
   1) zakres stosowania certyfikatu,
   2) okres ważności certyfikatu,
   3) zakres świadczonych usług certyfikacyjnych,
   4) koszty świadczonych usług certyfikacyjnych.
2. Podmiot świadczący usługi certyfikacyjne przed zawarciem umowy, o której mowa w ust. 1, powinien uzyskać pisemne potwierdzenie zapoznania się przez osobę zainteresowaną z warunkami uzyskania i używania certyfikatu, o których mowa w art. 9 ust. 1 pkt 6.
3. Podmioty, które wydają certyfikaty inne niż kwalifikowane, określają w załączniku do umowy, o której mowa w ust. 1, politykę certyfikacji wskazaną w wydanym certyfikacie.

Art. 14.

Odbiorca usług certyfikacyjnych jest obowiązany:

1) przechowywać dane służące do składania podpisów elektronicznych w sposób zapewniający ich ochronę przed nieuprawnionym wykorzystaniem przez okres ważności certyfikatu,
2) niezwłocznie powiadamiać podmiot świadczący usługi certyfikacyjne o niebezpieczeństwie lub próbach nieuprawnionego wykorzystania urządzeń służących do składania lub weryfikacji podpisów elektronicznych i danych służących do składania tych podpisów.

Art. 15.

1. Umowy o świadczenie usług certyfikacyjnych powinny być sporządzane w formie pisemnej pod rygorem nieważności.
2. Nieważność umowy o świadczenie usług certyfikacyjnych nie powoduje nieważności certyfikatu, jeżeli został on wydany na wniosek osoby zainteresowanej i spełnia pozostałe wymogi określone niniejszą ustawą.

Art. 16.

1. W celu zapewnienia interesów odbiorców usług certyfikacyjnych i umożliwienia współdziałania różnych urządzeń do składania i weryfikacji podpisów elektronicznych rozwiązania zawarte w polityce certyfikacji obejmują w szczególności:
   1) zakres zastosowania danej polityki certyfikacji,
   2) szczegóły dotyczące sposobu tworzenia i przesyłania danych elektronicznych, które zostaną opatrzone poświadczeniami elektronicznymi przez podmiot świadczący usługi certyfikacyjne,
   3) maksymalne okresy ważności certyfikatów,
   4) sposób identyfikacji i uwierzytelnienia osób, którym wydano certyfikat i podmiotów świadczących usługi certyfikacyjne,
   5) wymagania w zakresie metod i trybu tworzenia oraz udostępniania certyfikatów, list unieważnionych i zawieszonych certyfikatów oraz innych poświadczonych elektronicznie danych,
   6) wymagania z zakresu ochrony fizycznej pomieszczeń, w których znajdują się informacje, o których mowa w art. 11 ust. 1,
   7) szczegóły elektronicznego zapisu struktur danych zawartych w certyfikatach i innych danych poświadczanych elektronicznie,
   8) wymagania w zakresie zarządzania dokumentami związanymi z wykonywaniem usług certyfikacyjnych.
2. Minister właściwy do spraw wewnętrznych, z zastrzeżeniem ust. 3 i 4, określa, w drodze rozporządzenia, polityki certyfikacji, dotyczące kwalifikowanych certyfikatów, uwzględniając w szczególności rodzaje i zakres czynności prawnych, przy których dokonywaniu będą wykorzystywane kwalifikowane certyfikaty.
3. Rada Ministrów określa, w drodze rozporządzenia, polityki certyfikacji wykorzystywane do ochrony informacji niejawnych i innych informacji prawnie chronionych, uwzględniając rodzaj informacji i konieczność zapewnienia skutecznej ochrony tych informacji.
4. Rozporządzenia określające polityki certyfikacji, o których mowa w ust. 2, wykorzystywane przy dokonywaniu czynności, o których mowa w art. 5 i 6 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. Nr 140, poz. 939, z 1998 r. Nr 160, poz. 1063 i Nr 162,

poz. 1118, z 1999 r. Nr 11, poz. 95 i Nr 40, poz. 399 oraz z 2000 r. Nr 93,poz. 1027, Nr 94, poz. 1037, Nr 114, poz. 1191, Nr 116, poz. 1216, Nr 119, poz. 1252 i Nr 122, poz. 1316) przez banki, a także przez inne pomioty w związku z tymi czynnościami, są wydawane w porozumieniu z Prezesem Narodowego Banku Polskiego.

Art. 17.

1. Wraz z wydaniem kwalifikowanego certyfikatu, podmiot świadczący usługi certyfikacyjne jest obowiązany, na wniosek osoby składającej podpis elektroniczny, udostępnić jej warunki techniczne jakim powinny odpowiadać bezpieczne urządzenia do składania oraz do weryfikacji podpisów elektronicznych.
2. Bezpieczne urządzenia do składania podpisów elektronicznych powinny co najmniej:
   1) uniemożliwiać pozyskiwanie danych służących do składania podpisów elektronicznych przez osoby trzecie,
   2) nie zmieniać danych, które mają zostać podpisane oraz umożliwiać przedstawienie tych danych osobie składającej podpis elektroniczny przed momentem jego złożenia,
   3) gwarantować, że złożenie podpisu będzie poprzedzone wyraźnym ostrzeżeniem, że kontynuacja operacji będzie równoznaczna ze złożeniem podpisu elektronicznego,
   4) zapewniać łatwe rozpoznawanie istotnych dla bezpieczeństwa zmian w urządzeniu do składania podpisu elektronicznego.
3. Bezpieczne urządzenia służące do weryfikacji podpisu elektronicznego powinny spełniać następujące wymagania:
   1) dane używane do weryfikacji podpisu elektronicznego odpowiadają danym, które są uwidaczniane osobie weryfikującej ten podpis,
   2) podpis elektroniczny jest weryfikowany rzetelnie, a wynik weryfikacji prawidłowo wykazany,
   3) osoba weryfikująca może w sposób nie budzący wątpliwości ustalić zawartość podpisanych danych,
   4) autentyczność i ważność certyfikatów lub innych danych poświadczonych elektronicznie jest rzetelnie weryfikowana,
   5) wynik weryfikacji i tożsamość osoby składającej podpis elektroniczny są poprawnie uwidaczniane,
   6) użycie pseudonimu jest jednoznacznie wskazane,
   7) istotne dla bezpieczeństwa zmiany w urządzeniu do weryfikacji podpisu elektronicznego są łatwo rozpoznawalne.
4. Minister właściwy do spraw wewnętrznych, z zastrzeżeniem ust. 5, 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.
5. Prezes Rady Ministrów może określić, w drodze rozporządzenia, szczegółowe warunki techniczne, jakim powinny odpowiadać bezpieczne urządzenia do składania podpisów elektronicznych oraz bezpieczne urządzenia do weryfikacji podpisów elektronicznych służące do ochrony informacji niejawnych, uwzględniając potrzebę zapewnienia nienaruszalności i poufności danych opatrzonych takim podpisem.
6. Minister właściwy do spraw wewnętrznych, z zastrzeżeniem ust. 7, ocenia zgodność danego typu urządzeń, o których mowa w ust.2 i 3, z obowiązującymi przepisami.

7. Służby ochrony państwa, w rozumieniu przepisów o ochronie informacji niejawnych, dokonują oceny przydatności urządzeń, o których mowa w ust. 2 i 3, do ochrony informacji niejawnych i wydają stosowne certyfikaty bezpieczeństwa.

Art. 18.

1. Za czynności, o których mowa w art. 17 ust. 6 i 7, pobiera się opłatę.
2. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wysokość opłat za czynności, o których mowa w art. 17 ust. 6, uwzględniając uzasadnione koszty ponoszone w związku z ich wykonaniem.
3. Opłaty, o których mowa w art. 17 ust. 7, określają odrębne przepisy.

Art. 19.

1. Kwalifikowane certyfikaty muszą zawierać następujące dane:
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 odpowiednim rejestrze akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
4) imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny; użycie pseudonimu musi być wyraźnie zaznaczone,
5) wskazanie czy osoba składająca podpis elektroniczny działa:
a) we własnym imieniu,
b) jako przedstawiciel innej określonej osoby fizycznej lub osoby prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej,
c) w charakterze członka organu lub organu określonej osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej,
d) jako określony organ władzy publicznej,
6) dane służące do weryfikacji podpisu elektronicznego,
7) oznaczenie początku i końca okresu ważności certyfikatu,
8) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat,
9) ograniczenia zakresu ważności certyfikatu, jeżeli przewiduje to określona polityka certyfikacji,
10) ograniczenie najwyższej wartości granicznej transakcji, w której certyfikat może być wykorzystywany jeżeli przewiduje to określona polityka certyfikacji lub umowa, o której mowa w art. 13 ust. 1.
2. Jeżeli polityka certyfikacji nie przewiduje ograniczenia najwyższej wartości granicznej transakcji, przepisu ust. 1 pkt 10 nie stosuje się.
3. Minister właściwy do spraw wewnętrznych, może określić, w drodze rozporządzenia, szczegółowe warunki ochrony kwalifikowanych certyfikatów wykorzystywanych do ochrony informacji prawnie chronionych, uwzględniając konieczność zapewnienia bezpieczeństwa tych informacji oraz biorąc pod uwagę zmiany wynikające z postępu technicznego.

## ROZDZIAŁ V

## WAŻNOŚĆ CERTYFIKATÓW

Art. 20.

1. Certyfikat jest ważny w okresie w nim wskazanym.
2. Certyfikat może zostać zawieszony przez podmiot świadczący usługi certyfikacyjne, jeżeli osoba składająca podpisy elektroniczne weryfikowane na jego podstawie nie wywiązuje się z obowiązków określonych w umowie, o której mowa w art. 13 ust.1, lub w przepisach niniejszej ustawy.
3. Podmiot świadczący usługi certyfikacyjne zawiesza certyfikat na wniosek osoby składającej podpis elektroniczny lub podmiotu upoważnionego przez tę osobę w umowie, o której mowa w art. 13 ust. 1.
4. Podmiot świadczący usługi certyfikacyjne może zawiesić certyfikat także w przypadkach innych niż wskazane w ust. 2 i 3, w szczególności jeżeli nie dopełnił obowiązków nałożonych na niego niniejszą ustawą lub umową, o której mowa w art. 13 ust. 1. Art. 10 ust. 1 stosuje się odpowiednio.
5. Certyfikat może zostać unieważniony przez podmiot świadczący usługi certyfikacyjne przed upływem jego ważności, jeżeli mimo wcześniejszego zawieszenia certyfikatu, osoba składająca podpisy elektroniczne weryfikowane na jego podstawie nadal nie wywiązuje się z obowiązków określonych w umowie, o której mowa w art. 13 ust.1, lub w przepisach niniejszej ustawy.
6. Podmiot świadczący usługi certyfikacyjne unieważnia certyfikat przed upływem jego ważności:
   1) na wniosek osoby składającej podpis elektroniczny weryfikowany na podstawie tego certyfikatu,
   2) na wniosek podmiotu upoważnionego przez osobę, o której mowa w pkt 1, w umowie, o której mowa w art. 13 ust.1,
   3) jeżeli został wydany na podstawie danych, o których mowa w art. 9 ust. 1 pkt 2 i 3, a które okazały się nieprawdziwe lub stały się nieaktualne.
7. Certyfikat, który został zawieszony, może zostać następnie unieważniony lub jego zawieszenie może zostać uchylone.
8. Certyfikat, który został unieważniony, nie może być następnie uznany za ważny.
9. W przypadku unieważniania lub zawieszania certyfikatu, podmiot świadczący usługi certyfikacyjne zawiadamia niezwłocznie osobę składającą podpisy elektroniczne weryfikowane na jego podstawie.
10. Zawieszenie lub unieważnienie certyfikatu nie może następować z mocą wsteczną.

Art. 21.

1. Podmiot świadczący usługi certyfikacyjne publikuje listę zawieszonych i unieważnionych certyfikatów osób składających podpis elektroniczny, z którymi zawarł umowę, o której mowa w art. 13 ust. 1.
2. Zawieszone lub unieważnione certyfikaty umieszcza się na każdej liście zawieszonych i unieważnionych certyfikatów publikowanej przed dniem upływu okresu ważności certyfikatu oraz na pierwszej liście publikowanej po upływie tego okresu.
3. Lista zawieszonych i unieważnionych kwalifikowanych certyfikatów powinna zawierać w szczególności:

1) numer kolejny listy i wskazanie, że lista została opublikowana zgodnie z określoną polityką certyfikacji i dotyczy certyfikatów wydanych zgodnie z tą polityką,
2) datę i czas opublikowania listy z dokładnością określoną w polityce certyfikacji,
3) datę przewidywanego opublikowania kolejnej listy,
4) określenie podmiotu świadczącego usługi certyfikacyjne wydającego listę i państwa, w którym ma on siedzibę, oraz w przypadku akredytowanego podmiotu świadczącego usługi certyfikacyjne - numer akredytacji, a w przypadku kwalifikowanego podmiotu świadczącego usługi certyfikacyjne - numer wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
5) numer każdego zawieszonego lub unieważnionego certyfikatu oraz wskazanie, czy został on unieważniony czy zawieszony,
6) datę i czas, z dokładnością określoną w polityce certyfikacji, zawieszenia lub unieważnienia poszczególnego certyfikatu,
7) poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, publikującego listę.

## ROZDZIAŁ VI
## UDZIELANIE AREDYTACJI I DOKONYWANIE WPISU DO REJESTRU AKREDYTOWANYCH LUB KWALIFIKOWANYCH PODMIOTÓW ŚWIADCZĄCYCH USŁUGI CERTYFIKACYJNE

Art. 22.

1. Podmiot świadczący usługi certyfikacyjne może wystąpić o udzielenie akredytacji lub o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.
2. Świadczenie usług certyfikacyjnych w charakterze akredytowanego podmiotu świadczącego usługi certyfikacyjne wymaga akredytacji udzielonej przez ministra właściwego do spraw wewnętrznych, wpisania do rejestru akredytowanych podmiotów świadczących usługi certyfikacyjne i uzyskania zaświadczenia certyfikacyjnego wykorzystywanego do weryfikowania poświadczeń elektronicznych tego podmiotu, wydanego przez ministra właściwego do spraw wewnętrznych, z zastrzeżeniem ust. 4.
3. Świadczenie usług certyfikacyjnych w charakterze kwalifikowanego podmiotu świadczącego usługi certyfikacyjne wymaga uzyskania wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne i uzyskania zaświadczenia certyfikacyjnego wykorzystywanego do weryfikowania poświadczeń elektronicznych tego podmiotu, wydanego przez ministra właściwego do spraw wewnętrznych, z zastrzeżeniem ust. 4.
4. Minister właściwy do spraw wewnętrznych może upoważnić określony podmiot, w tym Narodowy Bank Polski, na jego wniosek, do wytwarzania i wydawania zaświadczeń certyfikacyjnych, o których mowa w ust. 2 i 3.
5. W wypadku, o którym mowa w ust. 4, minister właściwy do spraw wewnętrznych, udzielając akredytacji lub dokonując wpisu do rejestru, o którym mowa w ust. 1, wskazuje podmiotowi świadczącemu usługi certyfikacyjne nazwę i siedzibę podmiotu upoważnionego do wytwarzania i wydawania zaświadczeń certyfikacyjnych.

Art. 23.

1. Akredytacji udziela się oraz wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne dokonuje się na wniosek podmiotu, który zamierza świadczyć lub świadczy usługi certyfikacyjne.
2. Wniosek o udzielenie akredytacji lub o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne powinien zawierać:
   1) imię i nazwisko lub nazwę (firmę) wnioskodawcy,
   2) wskazanie polityki certyfikacji, zgodnie z którą mają być tworzone i stosowane kwalifikowane certyfikaty lub świadczone inne usługi związane z podpisem elektronicznym,
   3) miejsce zamieszkania lub siedzibę oraz adres wnioskodawcy,
   4) aktualny wypis z krajowego rejestru sądowego,
   5) imię i nazwisko osób, o których mowa w art. 9 ust. 2, które podmiot ten zatrudnia lub zamierza zatrudnić,
   6) informacje o kwalifikacjach i doświadczeniu zawodowym oraz zaświadczenia o niekaralności osób, o których mowa w pkt 5,
   7) wskazanie technicznych i organizacyjnych możliwości wykonywania czynności w zakresie świadczenia usług certyfikacyjnych,
   8) zobowiązanie do nieużywania danych służących do składania poświadczeń elektronicznych do wydawania zaświadczeń certyfikacyjnych innym podmiotom świadczącym usługi certyfikacyjne,
   9) regulamin organizacyjny określający w szczególności sposób zapobiegania ujawnianiu informacji, których wykorzystanie mogłoby naruszać interes odbiorców usług certyfikacyjnych,
   10) dokumenty przedstawiające sytuację finansową wnioskodawcy w okresie ostatnich 3 lat poprzedzających datę złożenia wniosku, w tym dokumenty potwierdzające brak zaległości podatkowych i brak zaległości w odprowadzaniu składek na ubezpieczenie społeczne; jeśli wnioskodawca istnieje krócej niż 3 lata, należy przedstawić dokumenty przedstawiające sytuację finansową wnioskodawcy przez cały okres istnienia wnioskodawcy,
   11) plan organizacyjny i finansowy działalności wnioskodawcy na najbliższe 3 lata,
   12) dowód uiszczenia opłaty za rozpatrzenie wniosku o udzielenie akredytacji lub o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
   13) dane służące do weryfikacji poświadczeń elektronicznych składanych przez podmiot w ramach świadczonych przez niego usług certyfikacyjnych,
   14) numer identyfikacji podatkowej wnioskodawcy,
   15) numer identyfikacyjny REGON wnioskodawcy.
3. Przepisu ust. 2 pkt 4, 10, 11 i 15 nie stosuje się do wniosku składanego przez organ władzy publicznej.
4. W przypadku braków we wniosku, minister właściwy do spraw wewnętrznych wzywa wnioskodawcę do jego uzupełnienia, wyznaczając termin nie krótszy niż 7 dni.
5. Termin, o którym mowa w ust. 4, może zostać przedłużony na umotywowany wniosek wnioskodawcy złożony przed upływem tego terminu.
6. Nie uzupełnienie wniosku w wyznaczonym terminie skutkuje odrzuceniem wniosku.
7. Za rozpatrzenie wniosku o udzielenie akredytacji lub o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne pobiera się opłatę. Uiszczona opłata nie podlega zwrotowi.
8. Minister właściwy do spraw wewnętrznych 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. 22 ust. 4, biorąc pod uwagę konieczność zapewnienia poufności tworzenia i wydawania zaświadczenia certyfikacyjnego,
3) wysokość opłat za udzielenie akredytacji oraz dokonanie wpisu do rejestru akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne, uwzględniając uzasadnione koszty ponoszone w związku z postępowaniem akredytacyjnym i prowadzeniem rejestrów.

Art. 24.

1. Minister właściwy do spraw wewnętrznych wydaje decyzję o udzieleniu bądź odmowie udzielenia akredytacji w terminie 2 miesięcy od dnia złożenia kompletnego wniosku.
2. Decyzja o udzieleniu akredytacji powinna w szczególności określać nazwę polityki certyfikacji, w ramach której dany podmiot może wydawać kwalifikowane certyfikaty lub świadczyć inne usługi związane z podpisem elektronicznym.
3. Minister właściwy do spraw wewnętrznych dokonuje wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne lub wydaje decyzję o odmowie dokonania wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne w terminie 1 miesiąca od dnia złożenia kompletnego wniosku.
4. Minister właściwy do spraw wewnętrznych odmawia udzielenia akredytacji, jeżeli:
   1) wniosek i dołączone do niego dokumenty nie spełniają warunków określonych w ustawie,
   2) w dokumentach organizacyjnych podmiotu są zamieszczone postanowienia mogące zagrażać bezpieczeństwu albo w inny sposób naruszać interes odbiorców usług certyfikacyjnych,
   3) przedstawiony przez podmiot plan organizacyjny i finansowy działalności na najbliższe 3 lata nie zabezpiecza w należyty sposób interesów odbiorców usług certyfikacyjnych,
   4) z dokumentów, o których mowa w art. 23 ust. 2 pkt 10, wynika, że podmiot posiada zaległości podatkowe lub zaległości w odprowadzaniu składek na ubezpieczenie społeczne,
   5) wskazane we wniosku techniczne i organizacyjne możliwości wykonywania czynności w zakresie świadczenia usług certyfikacyjnych nie zabezpieczają należycie interesów odbiorców usług certyfikacyjnych,
   6) osoby, o których mowa w art. 23 ust. 2 pkt 5, nie dają rękojmi należytego wykonywania powierzonych czynności w zakresie świadczenia usług certyfikacyjnych.
5. Minister właściwy do spraw wewnętrznych wydaje decyzję o odmowie dokonania wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, jeżeli wniosek i dołączone do niego dokumenty nie spełniają warunków określonych w niniejszej ustawie.

Art. 25.

1. Po udzieleniu akredytacji, minister właściwy do spraw wewnętrznych niezwłocznie wpisuje podmiot świadczący usługi certyfikacyjne do rejestru akredytowanych podmiotów świadczących usługi certyfikacyjne.

2. Wpis do rejestru akredytowanych podmiotów świadczących usługi certyfikacyjne obejmuje:
   1) imię i nazwisko lub nazwę (firmę) akredytowanego podmiotu świadczącego usługi certyfikacyjne,
   2) sposób reprezentacji akredytowanego podmiotu świadczącego usługi certyfikacyjne oraz numer wpisu do krajowego rejestru sądowego i oznaczenie sądu prowadzącego ten rejestr,
   3) imiona i nazwiska osób reprezentujących akredytowany podmiot świadczący usługi certyfikacyjne,
   4) nazwę polityki certyfikacji, w ramach której dany podmiot może wydawać kwalifikowane certyfikaty lub świadczyć inne usługi związane z podpisem elektronicznym,
   5) numer i datę wydania decyzji o udzieleniu akredytacji lub o cofnięciu akredytacji,
   6) informacje o sumie ubezpieczenia i warunkach umowy, o której mowa w art. 9 ust. 1 pkt 5, oraz nazwę zakładu ubezpieczeń.
3. Wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne obejmuje:
   1) imię i nazwisko lub nazwę (firmę) kwalifikowanego podmiotu świadczącego usługi certyfikacyjne,
   2) sposób reprezentacji kwalifikowanego podmiotu świadczącego usługi certyfikacyjne oraz numer wpisu do krajowego rejestru sądowego i oznaczenie sądu prowadzącego ten rejestr,
   3) imiona i nazwiska osób reprezentujących kwalifikowany podmiot świadczący usługi certyfikacyjne,
   4) nazwę polityki certyfikacji, w ramach której dany podmiot może wydawać kwalifikowane certyfikaty lub świadczyć inne usługi związane z podpisem elektronicznym,
   5) informacje o sumie ubezpieczenia i warunkach umowy, o której mowa w art. 9 ust. 1 pkt 5, oraz nazwę zakładu ubezpieczeń,
   6) datę dokonania wpisu lub wydania decyzji o wykreśleniu wpisu.
4. Podmiot, któremu akredytacja została udzielona lub który uzyskał wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, ma obowiązek, w terminie 30 dni od dnia doręczenia decyzji o udzieleniu akredytacji lub zawiadomieniu o dokonaniu wpisu, doręczyć dowód zawarcia umowy, o której mowa w art. 9 ust. 1 pkt 5, oraz przedstawić informacje, o których mowa w ust. 2 pkt 6 i ust. 3 pkt 5. Minister właściwy do spraw wewnętrznych niezwłocznie po uzyskaniu informacji, o których mowa w ust. 2 pkt 6 i ust. 3 pkt 5, uzupełnia o nie wpis do rejestru akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne.
5. Jeżeli podmiot, któremu akredytacja została udzielona lub który uzyskał wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, nie wywiąże się w terminie z obowiązku, o którym mowa w ust. 4, minister właściwy do spraw wewnętrznych wydaje decyzję o cofnięciu akredytacji lub o wykreśleniu wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne.
6. Po dokonaniu wpisu do rejestru akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne minister właściwy do spraw wewnętrznych niezwłocznie, jednak nie wcześniej niż w dniu wywiązania się przez podmiot świadczący usługi certyfikacyjne z obowiązku, o którym mowa w ust. 4, wydaje zaświadczenie certyfikacyjne, o którym mowa w art. 22 ust. 2 i 3.

Art. 26.

1. Rejestry akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne prowadzi minister właściwy do spraw wewnętrznych.
2. Rejestry, o których mowa w ust. 1, i zaświadczenia certyfikacyjne, o których mowa w art. 22 ust. 2 i 3, są jawne i dostępne dla osób trzecich.
3. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób prowadzenia rejestrów akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne, wzór tych rejestrów oraz szczegółowy tryb postępowania w sprawach o wpis do rejestru, uwzględniając konieczność zapewnienia dostępności do rejestrów osób trzecich oraz możliwość wpisywania wszystkich danych uzyskanych w toku postępowania w sprawie udzielenia akredytacji lub dokonania wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, w tym informacji o likwidacji lub upadłości podmiotu świadczącego usługi certyfikacyjne.

Art. 27.

Akredytowany lub kwalifikowany podmiot świadczący usługi certyfikacyjne jest obowiązany zawiadamiać niezwłocznie ministra właściwego do spraw wewnętrznych o każdej zmianie danych zawartych we wniosku, o którym mowa w art. 23 ust. 2.

Art. 28.

1. W przypadku otwarcia likwidacji akredytowanego lub kwalifikowanego podmiotu świadczącego usługi certyfikacyjne minister właściwy do spraw wewnętrznych wydaje decyzję o cofnięciu akredytacji lub wykreśleniu wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Decyzja staje się wykonalna z dniem zakończenia likwidacji.
2. W przypadku ogłoszenia upadłości akredytowanego lub kwalifikowanego podmiotu świadczącego usługi certyfikacyjne cofnięcie akredytacji lub wykreślenie wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne następuje z mocy prawa.
3. Jeżeli odrębne przepisy nie przewidują likwidacji podmiotu świadczącego usługi certyfikacyjne, minister właściwy do spraw wewnętrznych wydaje decyzję o cofnięciu akredytacji lub wykreśleniu wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne w przypadku zaprzestania działalności przez ten podmiot.
4. Obowiązek poinformowania ministra właściwego do spraw wewnętrznych o ogłoszeniu upadłości lub zamknięciu likwidacji ciąży na syndyku lub likwidatorze.
5. W przypadku oddalenia wniosku o ogłoszenie upadłości z przyczyn wskazanych w art. 13 rozporządzenia Prezydenta Rzeczypospolitej z dnia 24 października 1934 r. - Prawo upadłościowe (Dz. U. z 1991 r. Nr 118, poz. 512, z 1994 r. Nr 1, poz. 1, z 1995 r. Nr 85, poz. 426, z 1996 r. Nr 6, poz. 43, Nr 43, poz. 189, Nr 106, poz. 496 i Nr 149, poz. 703, z 1997 r. Nr 28, poz. 153, Nr 54, poz. 349, Nr 117, poz. 751, Nr 121, poz. 770 i Nr 140, poz. 940, z 1998 Nr 117, poz. 756 oraz z 2000 r. Nr 26, poz. 306, Nr 84, poz. 948, Nr 94, poz. 1037 i Nr 114, poz. 1193) ust. 2 stosuje się odpowiednio. Obowiązek poinformowania ministra właściwego do spraw wewnętrznych ciąży na członkach organu osoby prawnej, komplementariuszach spółki osobowej prawa handlowego lub wspólnikach spółki jawnej.

## ROZDZIAŁ VII
## NADZÓR NAD DZIAŁALNOŚCIĄ PODMIOTÓW ŚWIADCZĄCYCH USŁUGI CERTYFIKACYJNE

Art. 29.

1. Minister właściwy do spraw wewnętrznych sprawuje nadzór nad przestrzeganiem przepisów niniejszej ustawy, zapewniając ochronę interesów odbiorców usług certyfikacyjnych.
2. Zadanie, o którym mowa w ust. 1, minister właściwy do spraw wewnętrznych realizuje poprzez:
   1) akredytację podmiotów świadczących usługi certyfikacyjne,
   2) prowadzenie rejestrów akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
   3) wydawanie i unieważnianie zaświadczeń certyfikacyjnych, o których mowa w art. 22 ust. 2 i 3,
   4) kontrolę działalności podmiotów świadczących usługi certyfikacyjne pod względem zgodności z niniejszą ustawą,
   5) nakładanie kar przewidzianych w niniejszej ustawie,
   6) podejmowanie innych działań przewidzianych przepisami niniejszej ustawy.

Art. 30.

1. Minister właściwy do spraw wewnętrznych wydaje decyzję o cofnięciu akredytacji lub wykreśleniu wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, jeżeli stwierdzi, że podmiot świadczący usługi certyfikacyjne prowadzi działalność niezgodnie z przepisami niniejszej ustawy w sposób zagrażający interesom odbiorców usług certyfikacyjnych. Wydanie decyzji o cofnięciu akredytacji skutkuje wykreśleniem wpisu w rejestrze akredytowanych podmiotów świadczących usługi certyfikacyjne.
2. Przed wydaniem decyzji, o której mowa w ust. 1, minister właściwy do spraw wewnętrznych może wezwać podmiot świadczący usługi certyfikacyjne, aby w określonym terminie usunął stwierdzone niezgodności i doprowadził swoją działalność do stanu zgodnego z przepisami niniejszej ustawy.
3. Wydając decyzję, o której mowa w ust. 1, lub dokonując wezwania, o którym mowa w ust. 2, minister właściwy do spraw wewnętrznych może unieważnić zaświadczenie certyfikacyjne, o którym mowa w art. 22 ust. 2 lub ust. 3, i umieścić je na liście unieważnionych certyfikatów akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Przepisy dotyczące listy unieważnionych certyfikatów, o której mowa w art. 21, stosuje się odpowiednio.
4. Unieważnienie zaświadczenia certyfikacyjnego, o którym mowa w art. 22 ust. 2 lub ust. 3, wykorzystywanego do weryfikacji poświadczeń elektronicznych składanych odpowiednio przez akredytowane lub kwalifikowane podmioty świadczące usługi certyfikacyjne, powoduje nieważność tych poświadczeń, chyba, że zostanie udowodnione, że poświadczenie zostało złożone przed unieważnieniem zaświadczenia certyfikacyjnego.
5. Unieważnienie poświadczenia elektronicznego, o którym mowa w ust. 4, wykorzystywanego do weryfikacji ważności certyfikatów wydanych przez akredytowany lub kwalifikowany podmiot świadczący usługi certyfikacyjne, powoduje nieważność tych certyfikatów.
6. Unieważnienie poświadczenia elektronicznego, o którym mowa w ust. 4, wykorzystywanego do weryfikacji ważności usługi znakowania czasem świadczonej przez akredytowany

lub kwalifikowany podmiot świadczący usługi certyfikacyjne pozbawia skutków prawnych tę usługę.

Art. 31.

1. Wydając decyzję, o której mowa w art. 30 ust. 1 lub dokonując wezwania, o którym mowa w art. 30 ust. 2, minister właściwy do spraw wewnętrznych może nałożyć na podmiot świadczący usługi certyfikacyjne karę pieniężną do wysokości 250.000 złotych, jeżeli stwierdzone nieprawidłowości były szczególnie rażące.
2. W razie nie usunięcia nieprawidłowości w wyznaczonym terminie, minister właściwy do spraw wewnętrznych może nałożyć na podmiot świadczący usługi certyfikacyjne karę pieniężną wysokości 250.000 złotych.
3. Przy ustalaniu wysokości kar pieniężnych, o których mowa w ust. 1 i 2, minister właściwy do spraw wewnętrznych jest obowiązany uwzględnić stopień szkodliwości czynu oraz rodzaj i wagę stwierdzonych nieprawidłowości.
4. Kara pieniężna podlega egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji.

Art. 32.

1. Decyzja o cofnięciu akredytacji lub wykreśleniu wpisu w rejestrze akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne jest natychmiast wykonalna.
2. Jeżeli jest to uzasadnione koniecznością zapewnienia ochrony interesów odbiorców usług certyfikacyjnych, minister właściwy do spraw wewnętrznych może wstrzymać natychmiastowe wykonanie decyzji o cofnięciu akredytacji lub skreśleniu wpisu z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, jednak na okres nie dłuższy niż 1 miesiąc.
3. Wniesienie skargi do Naczelnego Sądu Administracyjnego nie wstrzymuje wykonalności decyzji, o której mowa w ust. 1. Przepisu art. 40 ustawy z dnia 11 maja 1995 r. o Naczelnym Sądzie Administracyjnym (Dz. U. Nr 74, poz. 368 i Nr 104, poz. 515, z 1997 r. Nr 75, poz. 471, Nr 106, poz. 679, Nr 114, poz. 739 i Nr 144, poz. 971, z 1998 r. Nr 162, poz. 1126, z 1999 r. Nr 75, poz. 853 oraz z 2000 r. Nr 2, poz. 5, Nr 48, poz. 552, Nr 60, poz. 704 i Nr 91, poz. 1008) nie stosuje się.

Art. 33.

Od dnia doręczenia decyzji o cofnięciu akredytacji lub wykreśleniu wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne podmiot świadczący usługi certyfikacyjne nie może zawierać umów o świadczenie usług certyfikacyjnych.

Art. 34.

Jeżeli decyzja o cofnięciu akredytacji lub wykreśleniu wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne, zostanie zaskarżona do Naczelnego Sądu Administracyjnego, rozpoznanie skargi powinno nastąpić w terminie 2 miesięcy od daty jej wniesienia.

Art. 35.

W przypadku jakiejkolwiek zmiany danych zawartych we wniosku, o którym mowa w art. 23 ust. 1, minister właściwy do spraw wewnętrznych może przeprowadzić kontrolę akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne pod względem spełniania wymagań niezbędnych do uzyskania akredytacji lub wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Art. 36.

Minister właściwy do spraw wewnętrznych kontroluje zgodność działalności podmiotów świadczących usługi certyfikacyjne, w tym ich jednostek organizacyjnych, z wymaganiami niniejszej ustawy.

Art. 37.

1. Kontrolę przeprowadzają pracownicy komórki organizacyjnej ministerstwa obsługującego ministra właściwego do spraw wewnętrznych w zakresie akredytacji podmiotów świadczących usługi certyfikacyjne, zwani dalej "kontrolerami", na podstawie legitymacji służbowej i imiennego upoważnienia określającego kontrolowaną jednostkę organizacyjną i podstawę prawną podjęcia kontroli.
2. Imienne upoważnienia do przeprowadzenia kontroli wydają: minister właściwy do spraw wewnętrznych albo z jego upoważnienia dyrektor komórki organizacyjnej ministerstwa obsługującego ministra właściwego do spraw wewnętrznych w zakresie akredytacji podmiotów świadczących usługi certyfikacyjne, zwanej dalej „komórką kontrolującą”.
3. Kontrolę materiałów zawierających informacje niejawne przeprowadza się z zachowaniem przepisów o ochronie informacji niejawnych na podstawie legitymacji służbowej i odrębnego upoważnienia wydanego przez ministra właściwego do spraw wewnętrznych.
4. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, wzór legitymacji służbowej kontrolera oraz sposób jej wydania i wymiany, uwzględniając konieczność zapewnienia jednoznacznej identyfikacji kontrolera oraz sprawności funkcjonowania komórki kontrolującej.

Art. 38.

Minister właściwy do spraw wewnętrznych przeprowadza kontrolę:

1) z urzędu, nie rzadziej jednak niż raz na rok,
2) na żądanie prokuratora lub sądu, albo innych organów państwowych upoważnionych do tego na podstawie ustaw w związku z prowadzonymi przez nie postępowaniami w sprawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne.

Art. 39.

Kontrola ma na celu ustalenie, czy działalność podmiotu świadczącego usługi certyfikacyjne jest zgodna z wymaganiami niniejszej ustawy. Zakres kontroli określa upoważnienie, o którym mowa w art. 37 ust. 1.

Art. 40.

W celu prawidłowego przeprowadzenia kontroli:

1) kierownicy kontrolowanych jednostek organizacyjnych mają obowiązek przedkładać na żądanie kontrolera wszelkie dokumenty i materiały niezbędne do przygotowania i przeprowadzenia kontroli, z zachowaniem przepisów o ochronie informacji prawnie chronionych,
2) kontrolerzy mają prawo do:
   a) swobodnego wstępu do obiektów i pomieszczeń kontrolowanych jednostek organizacyjnych,
   b) wglądu do wszelkich dokumentów i innych nośników informacji, bezpośrednio związanych z kontrolowaną działalnością oraz zabezpieczania dokumentów i innych materiałów dowodowych, z zachowaniem przepisów o ochronie informacji prawnie chronionych,
   c) przeprowadzania oględzin obiektów i innych składników majątkowych oraz przebiegu określonych czynności,
   d) wzywania i przesłuchiwania świadków,
   e) żądania od pracowników kontrolowanych jednostek organizacyjnych udzielenia ustnych lub pisemnych wyjaśnień,
   f) korzystania z pomocy biegłych i specjalistów.

Art. 41.

1. Kontroler podlega wyłączeniu, na wniosek lub z urzędu, z postępowania kontrolnego, jeżeli wyniki kontroli mogłyby oddziaływać na jego prawa lub obowiązki, na prawa lub obowiązki jego małżonka albo osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnych i powinowatych do drugiego stopnia albo osób związanych z nim z tytułu przysposobienia, opieki lub kurateli. Powody wyłączenia kontrolera trwają także po ustaniu małżeństwa, przysposobienia, opieki lub kurateli.
2. Kontroler może być wyłączony, na wniosek lub z urzędu, z postępowania kontrolnego w każdym czasie, jeżeli zachodzą uzasadnione wątpliwości co do jego bezstronności.
3. O przyczynach powodujących wyłączenie kontroler lub kierownik kontrolowanej jednostki organizacyjnej niezwłocznie zawiadamia dyrektora komórki kontrolującej.
4. O wyłączeniu kontrolera postanawia minister właściwy do spraw wewnętrznych; postanowienie ministra jest ostateczne.
5. Do czasu wydania postanowienia, o którym mowa w ust. 4, kontroler podejmuje jedynie czynności nie cierpiące zwłoki.

Art. 42.

Kontrola jest prowadzona w siedzibie kontrolowanej jednostki organizacyjnej oraz w miejscach i czasie wykonywania jej zadań, a jeżeli tego wymaga dobro kontroli - również w dniach wolnych od pracy i poza godzinami pracy.

Art. 43.

1. Kontroler ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli.
2. Dowodami są w szczególności dokumenty, zabezpieczone rzeczy, wyniki oględzin, zeznania świadków, opinie biegłych oraz pisemne wyjaśnienia i oświadczenia.

Art. 44.

1. Kontroler może sporządzać, a w razie potrzeby może zażądać od kierownika kontrolowa-

nej jednostki organizacyjnej sporządzenia niezbędnych dla kontroli odpisów lub wyciągów z dokumentów, jak również zestawień i obliczeń na podstawie dokumentów.
2. Zgodność odpisów i wyciągów oraz zestawień i obliczeń z oryginalnymi dokumentami potwierdza kierownik kontrolowanej jednostki organizacyjnej, w której dokumenty się znajdują, lub osoba przez niego upoważniona.

Art. 45.

1. Kontroler dokonuje pobrania rzeczy w obecności kierownika kontrolowanej jednostki organizacyjnej, w której rzecz się znajduje, a w razie jego nieobecności - pracownika wyznaczonego przez tego kierownika. Pobrana rzecz powinna być zaopatrzona przez uczestników pobrania w trwałe cechy lub znaki uniemożliwiające zastąpienie jej inną.
2. Z pobrania rzeczy sporządza się protokół, który podpisuje kontroler i osoba uczestnicząca w pobraniu.

Art. 46.

1. W razie potrzeby ustalenia stanu faktycznego obiektów lub innych składników majątkowych albo przebiegu określonych czynności, kontroler może przeprowadzić oględziny.
2. Oględziny przeprowadza się w obecności kierownika kontrolowanej jednostki organizacyjnej, a w razie jego nieobecności - pracownika wyznaczonego przez tego kierownika.
3. Z przebiegu i wyniku oględzin sporządza się niezwłocznie protokół, który podpisuje kontroler i osoba wymieniona w ust. 2.
4. Przebieg i wyniki oględzin mogą być ponadto utrwalone:
    1) przez sporządzenie stenogramu; stenogram przekłada się na pismo zwykłe z zaznaczeniem zastosowanego systemu stenografii, dołączając pierwopis stenogramu do protokołu,
    2) za pomocą aparatury i środków technicznych służących do utrwalania obrazu lub dźwięku; utrwalony obraz lub dźwięk stanowi załącznik do protokołu.

Art. 47.

1. Kontroler może żądać od pracowników kontrolowanej jednostki organizacyjnej udzielenia mu, w terminie przez niego wyznaczonym, ustnych lub pisemnych wyjaśnień w sprawach dotyczących przedmiotu kontroli.
2. Odmowa udzielenia wyjaśnień może nastąpić jedynie w przypadkach, gdy wyjaśnienia mają dotyczyć:
    1) tajemnicy prawnie chronionej innej niż tajemnica służbowa, a kontroler nie posiada właściwego upoważnienia,
    2) faktów i okoliczności, których ujawnienie mogłoby narazić na odpowiedzialność karną lub majątkową osoby wezwanej do złożenia wyjaśnień, a także jego małżonka albo osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnych i powinowatych do drugiego stopnia bądź osób związanych z nim z tytułu przysposobienia, opieki lub kurateli.
3. Prawo odmowy udzielenia wyjaśnień w przypadkach, o których mowa w ust. 2 pkt 2, trwa mimo ustania małżeństwa lub przysposobienia.
4. Osoba udzielająca wyjaśnień może uchylić się od odpowiedzi na pytania, jeżeli zachodzą okoliczności, o których mowa w ust. 2.

Art. 48.

1. Każdy może złożyć kontrolerowi ustne lub pisemne oświadczenie dotyczące przedmiotu kontroli.
2. Kontroler nie może odmówić przyjęcia oświadczenia, jeżeli ma ono związek z przedmiotem kontroli.

Art. 49.

1. Wyniki przeprowadzonej kontroli kontroler przedstawia w protokole kontroli.
2. Protokół kontroli zawiera opis stanu faktycznego stwierdzonego w toku kontroli działalności podmiotu świadczącego usługi certyfikacyjne, w tym ustalonych nieprawidłowości, z uwzględnieniem przyczyn powstania, zakresu i skutków tych nieprawidłowości oraz osób za nie odpowiedzialnych.

Art. 50.

Protokół kontroli podpisują kontroler i osoba reprezentująca kontrolowany podmiot świadczący usługi certyfikacyjne.

Art. 51.

1. Osobie reprezentującej kontrolowany podmiot świadczący usługi certyfikacyjne przysługuje prawo zgłoszenia, przed podpisaniem protokołu kontroli, umotywowanych zastrzeżeń, co do ustaleń zawartych w protokole.
2. Zastrzeżenia należy zgłosić na piśmie w terminie 14 dni od dnia otrzymania protokołu kontroli. W szczególnych przypadkach dyrektor komórki kontrolującej może przedłużyć ten termin.
3. W razie zgłoszenia zastrzeżeń, o których mowa w ust. 1, kontroler jest obowiązany dokonać ich analizy i w miarę potrzeby podjąć dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienić lub uzupełnić odpowiednią część protokołu kontroli.
4. W razie nieuwzględnienia zastrzeżeń w całości lub w części kontroler przekazuje na piśmie swoje stanowisko zgłaszającemu zastrzeżenia.

Art. 52.

1. Osoba reprezentująca kontrolowany podmiot świadczący usługi certyfikacyjne może odmówić podpisania protokołu kontroli, składając w terminie 7 dni od dnia jego otrzymania pisemne wyjaśnienie tej odmowy.
2. W razie zgłoszenia zastrzeżeń, o których mowa w art. 51 ust. 1, termin do złożenia wyjaśnienia odmowy podpisania protokołu liczy się od dnia otrzymania stanowiska co do tych zastrzeżeń, o którym mowa w art. 51 ust. 4..
3. O odmowie podpisania protokołu kontroli i złożeniu wyjaśnienia kontroler czyni wzmiankę w protokole.
4. Odmowa podpisania protokołu kontroli przez osobę reprezentującą kontrolowany podmiot świadczący usługi certyfikacyjne nie stanowi przeszkody do podpisania protokołu przez kontrolera i realizacji ustaleń kontroli.

Art. 53.

1. Przed sporządzeniem przez kontrolera wystąpienia pokontrolnego kontroler może zwrócić się do osoby reprezentującej kontrolowany podmiot świadczący usługi certyfikacyjne o złożenie w wyznaczonym terminie dodatkowych wyjaśnień na piśmie dotyczących przyczyn i okoliczności powstania nieprawidłowości przedstawionych w protokole kontroli.
2. Osoba reprezentująca kontrolowany podmiot świadczący usługi certyfikacyjne może z własnej inicjatywy złożyć kontrolerowi w terminie z nim uzgodnionym pisemne wyjaśnienia, o których mowa w ust. 1.

Art. 54.

Minister właściwy do spraw wewnętrznych po zapoznaniu się z protokołem i zastrzeżeniami, o których mowa w art. 51 ust. 1, oraz wyjaśnieniami, o których mowa w art. 52 ust. 1 i art. 53 ust. 1, powiadamia kontrolowany podmiot świadczący usługi certyfikacyjne o wynikach kontroli i w razie stwierdzenia nieprawidłowości wyznacza termin ich usunięcia, nie krótszy niż 14 dni. W przypadku stwierdzenia rażących nieprawidłowości, minister właściwy do spraw wewnętrznych może nałożyć karę pieniężną, o której mowa w art. 31 ust. 1, bezpośrednio po ich stwierdzeniu.

Art. 55.

Do obowiązków kontrolera należy w szczególności:

1) należyte, bezstronne i terminowe wykonywanie zadań,
2) obiektywne ustalanie i rzetelne dokumentowanie wyników kontroli,
3) przestrzeganie tajemnicy prawnie chronionej,
4) godne zachowanie się.

Art. 56.

1. Pracownik komórki kontrolnej jest obowiązany zachować w tajemnicy informacje, które uzyskał w związku z wykonywaniem czynności służbowych.
2. Obowiązek zachowania tajemnicy trwa również po ustaniu zatrudnienia.

Art. 57.

Minister właściwy do spraw wewnętrznych rozpatruje skargi na podmioty świadczące usługi certyfikacyjne, stosując odpowiednio przepisy Kodeksu postępowania administracyjnego.

Art. 58.

1. Pracownicy zatrudnieni w komórkach organizacyjnych ministerstwa zapewniającego obsługę ministra właściwego do spraw wewnętrznych wykonujący zadania określone w niniejszej ustawie nie mogą prowadzić działalności gospodarczej, być wspólnikami lub akcjonariuszami, ani wykonywać obowiązków osoby reprezentującej lub członka rady nadzorczej i komisji rewizyjnej podmiotu świadczącego usługi certyfikacyjne, a także pozostawać z podmiotem świadczącym usługi certyfikacyjne w stosunku pracy, stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze.
2. Przepis ust. 1 nie narusza przepisów o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne.

Art. 59.

Pracownicy zatrudnieni w komórkach organizacyjnych ministerstwa zapewniającego obsługę ministra właściwego do spraw wewnętrznych wykonujący zadania określone w niniejszej ustawie, a także osoby wykonujące określone w niej czynności na rzecz tych komórek organizacyjnych na podstawie umowy zlecenia lub innego stosunku prawnego o podobnym charakterze, są obowiązani do zachowania w tajemnicy informacji uzyskanych w związku z wykonywaniem tych czynności.

## ROZDZIAŁ VIII
## RADA AKREDYTACYJNA

Art. 60.

1. Tworzy się Radę Akredytacyjną przy ministrze właściwym do spraw wewnętrznych, jako organ doradczy i opiniodawczy w sprawach związanych z działalnością podmiotów świadczących usługi certyfikacyjne.
2. Do zadań Rady Akredytacyjnej należy:
   1) opiniowanie projektów aktów normatywnych dotyczących działalności podmiotów świadczących usługi certyfikacyjne,
   2) opiniowanie sprawozdań ministra właściwego do spraw wewnętrznych z działalności akredytacyjnej,
   3) przedstawianie opinii w sprawach związanych z działalnością podmiotów świadczących usługi certyfikacyjne.

Art. 61.

1. Rada Akredytacyjna składa się z 12 osób.
2. Członków Rady Akredytacyjnej, w tym przewodniczącego i wiceprzewodniczącego, powołuje minister właściwy do spraw wewnętrznych spośród osób posiadających wiedzę i doświadczenie w sprawach związanych z zadaniami określonymi w niniejszej ustawie, z tym że dwóch spośród osób reprezentujących podmioty świadczące usługi certyfikacyjne oraz po jednej osobie rekomendowanej przez:
   1) ministra właściwego do spraw łączności,
   2) ministra właściwego do spraw instytucji finansowych,
   3) ministra właściwego do spraw gospodarki,
   4) Szefa Urzędu Ochrony Państwa,
   5) Szefa Wojskowych Służb Informacyjnych,
   6) Prezesa Narodowego Banku Polskiego,
   7) Przewodniczącego Komisji Papierów Wartościowych i Giełd.
3. Kadencja członków Rady Akredytacyjnej trwa 6 lat, licząc od dnia powołania, z tym że co 3 lata kończy się kadencja połowy członków. Członkowie Rady Akredytacyjnej pełnią swoje funkcje do czasu powołania ich następców.
4. Powołanie przewodniczącego i wiceprzewodniczącego Rady Akredytacyjnej następuje na 3 lata.
5. Powołanie sześciu członków pierwszej Rady Akredytacyjnej następuje na 3 lata.
6. Do członków Rady Akredytacyjnej stosuje się odpowiednio przepisy dotyczące obowiązku zachowania tajemnic prawnie chronionych.

7. Minister właściwy do spraw wewnętrznych określa, w drodze rozporządzenia, wysokość i sposób wynagradzania członków Rady Akredytacyjnej, uwzględniając wysokość przeciętnego wynagrodzenia miesięcznego w gospodarce narodowej.

Art. 62.

Zasady i tryb działania Rady Akredytacyjnej określa regulamin uchwalany przez Radę Akredytacyjną i zatwierdzany przez ministra właściwego do spraw wewnętrznych.

## ROZDZIAŁ IX
## ŁĄCZENIE PODMIOTÓW ŚWIADCZĄCYCH USŁUGI CERTYFIKACYJNE

Art. 63.

1. Połączenie podmiotów świadczących usługi certyfikacyjne, z których przynajmniej jeden jest podmiotem akredytowanym lub kwalifikowanym, wymaga zezwolenia ministra właściwego do spraw wewnętrznych.
2. Wniosek o wydanie zezwolenia, o którym mowa w ust. 1, składa każdy z łączących się podmiotów świadczących usługi certyfikacyjne.
3. Wniosek o wydanie zezwolenia, o którym mowa w ust. 1, powinien zawierać:
   1) imię i nazwisko lub nazwę (firmę) wnioskodawcy,
   2) wskazanie polityki certyfikacji, w ramach której wnioskodawca wydaje kwalifikowane certyfikaty lub świadczy inne usługi związane z podpisem elektronicznym,
   3) wskazanie polityki certyfikacji, zgodnie z którą podmiot przejmujący lub mający powstać w wyniku połączenia ma tworzyć kwalifikowane certyfikaty lub świadczyć inne usługi związane z podpisem elektronicznym,
   4) miejsce zamieszkania lub siedzibę oraz adres wnioskodawcy,
   5) aktualny wypis z krajowego rejestru sądowego,
   6) imię i nazwisko osób, o których mowa w art. 9 ust. 2, które podmiot przejmujący lub mający powstać w wyniku połączenia zamierza zatrudnić,
   7) informacje o kwalifikacjach i doświadczeniu zawodowym oraz zaświadczenia o niekaralności osób, o których mowa w pkt 6,
   8) wskazanie technicznych i organizacyjnych możliwości wykonywania czynności w zakresie świadczenia usług certyfikacyjnych przez podmiot przejmujący lub mający powstać w wyniku połączenia,
   9) zobowiązanie do nieużywania, przez podmiot przejmujący lub mający powstać w wyniku połączenia, danych służących do składania poświadczeń elektronicznych do wydawania zaświadczeń certyfikacyjnych innym podmiotom świadczącym usługi certyfikacyjne,
   10) regulamin organizacyjny podmiotu przejmującego lub mającego powstać w wyniku połączenia, określający w szczególności sposób zapobiegania ujawnianiu informacji, których wykorzystanie mogłoby naruszać interes odbiorców usług certyfikacyjnych,
   11) plan organizacyjny i finansowy działalności podmiotu przejmującego lub mającego powstać w wyniku połączenia na najbliższe 3 lata,
   12) numer identyfikacji podatkowej wnioskodawcy,
   13) numer identyfikacyjny REGON wnioskodawcy.

4. Zezwolenie, o którym mowa w ust. 1, powinno określać nazwę polityki lub polityk certyfikacji, w ramach których podmiot przejmujący lub mający powstać w wyniku połączenia ma wydawać kwalifikowane certyfikaty lub świadczyć inne usługi związane z podpisem elektronicznym. Zezwolenie może określać jedynie polityki certyfikacji, w ramach których łączące się podmioty świadczyły usługi certyfikacyjne jako akredytowane lub kwalifikowane podmioty świadczące usługi certyfikacyjne .
5. Jeśli zezwolenie, o którym mowa w ust. 1, nie zawiera nazwy polityki certyfikacji, w ramach której podmioty łączące się świadczyły usługi certyfikacyjne jako akredytowane lub kwalifikowane podmioty świadczące usługi certyfikacyjne, to w przypadku połączenia jest to równoznaczne z wydaniem decyzji o cofnięciu akredytacji lub wykreśleniu wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne w ramach tej polityki. Przepisy o wydawaniu decyzji o cofnięciu akredytacji lub wykreśleniu wpisu w rejestrze kwalifikowanych podmiotów świadczących usługi certyfikacyjne stosuje się odpowiednio.

Art. 64.

1. Treść zezwolenia ministra właściwego do spraw wewnętrznych na połączenie podmiotów, z których przynajmniej jeden jest akredytowanym lub kwalifikowanym podmiotem świadczącym usługi certyfikacyjne, łączące się podmioty ogłaszają niezwłocznie w dzienniku o zasięgu krajowym.
2. O ogłoszeniu, o którym mowa w ust. 1, łączące się podmioty zawiadamiają niezwłocznie ministra właściwego do spraw wewnętrznych.

Art. 65.

Zamiar połączenia podmiotów świadczących usługi certyfikacyjne, z których przynajmniej jeden jest akredytowanym lub kwalifikowanym podmiotem świadczącym usługi certyfikacyjne podlega zgłoszeniu Prezesowi Urzędu Ochrony Konkurencji i Konsumentów jeżeli łączna wartość usług świadczonych w następstwie zamierzonego połączenia przekroczyłaby 33% łącznej wartości usług netto wszystkich podmiotów świadczących usługi certyfikacyjne, w którymkolwiek z miesięcy przypadających w roku poprzedzającym rok zgłoszenia takiego zamiaru.

Art. 66.

W zakresie nieuregulowanym niniejszą ustawą do łączenia podmiotów świadczących usługi certyfikacyjne stosuje się przepisy ustawy z dnia 15 grudnia 2000 r. o ochronie konkurencji i konsumentów (Dz. U. Nr 122, poz. 1319).

## ROZDZIAŁ X
## PRZEPISY KARNE

Art. 67.

1. Kto świadczy usługi certyfikacyjne bez wymaganej akredytacji, podlega grzywnie do 5.000.000 złotych lub karze pozbawienia wolności do lat 5 albo obu tym karom łącznie.

2. Tej samej karze podlega, kto świadczy usługi certyfikacyjne w charakterze kwalifikowanego podmiotu świadczącego taki usługi bez wymaganego wpisu do właściwego rejestru.

Art. 68.

1. Kto świadczy usługi certyfikacyjne bez uprzedniego zawarcia wymaganej umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom tych usług, podlega grzywnie do 1.000.000 złotych.
2. Tej samej karze podlega, kto świadcząc usługi certyfikacyjne, wbrew warunkom określonym w ustawie nie udostępnia osobie uprawnionej warunków technicznych, jakim powinny odpowiadać bezpieczne urządzenia do składania oraz weryfikacji podpisów elektronicznych, lub nie ogłasza listy zawieszonych i unieważnionych certyfikatów osób składających podpis elektroniczny.
3. Grzywnie określonej w ust. 1 podlega również świadczący usługi certyfikacyjne oraz likwidator podmiotu świadczącego takie usługi, który nie przechowuje lub nie archiwizuje, w sposób określony w ustawie, bezpośrednio związanych z tym dokumentów i danych.

Art. 69.

Kto, świadcząc usługi certyfikacyjne, wbrew obowiązkowi określonemu w ustawie nie informuje osoby występującej o certyfikat o warunkach uzyskania i używania certyfikatu podlega grzywnie.

Art. 70.

1. Kto, będąc obowiązany do zachowania tajemnicy związanej ze świadczeniem usług certyfikacyjnych, ujawnia lub wykorzystuje wbrew warunkom określonym w ustawie, informacje objęte tą tajemnicą, podlega grzywnie do 1.000.000 złotych lub karze pozbawienia wolności do lat 3 albo obu tym karom łącznie.
2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 jako świadczący usługi certyfikacyjne albo w celu osiągnięcia korzyści majątkowej lub osobistej, podlega grzywnie do 5.000.000 złotych lub karze pozbawienia wolności do lat 5 albo obu tym karom łącznie.

Art. 71.

Karom określonym w art. 67-69 podlega także ten, kto dopuszcza się czynu, o którym mowa w tych przepisach, działając w imieniu lub w interesie innej osoby fizycznej, osoby prawnej lub jednostki organizacyjne nie mającej osobowości prawnej.

## ROZDZIAŁ XI
## PRZEPISY PRZEJŚCIOWE I KOŃCOWE

Art. 72.

W ustawie z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. Nr 16, poz. 93, z 1971 r. Nr 27, poz. 252, z 1976 r. Nr 19, poz. 122, z 1982 r. Nr 11, poz. 81, Nr 19, poz. 147 i Nr 30, poz. 210, z 1984 r. Nr 45, poz. 242, z 1985 r. Nr 22, poz. 99, z 1989 r. Nr 3, poz. 11, z 1990 r. Nr

34, poz. 198, Nr 55, poz. 321 i Nr 79, poz. 464, z 1991 r. Nr 107, poz. 464 i Nr 115, poz. 496, z 1993 r. Nr 17, poz. 78, z 1994 r. Nr 27, poz. 96, Nr 85, poz. 388 i Nr 105, poz. 509, z 1995 r. Nr 83, poz. 417, z 1996 r. Nr 114, poz. 542, Nr 139, poz. 646 i Nr 149, poz. 703, z 1997 r. Nr 43, poz. 272, Nr 115, poz. 741, Nr 117, poz. 751 i Nr 157, poz. 1040, z 1998 r. Nr 106, poz. 668 i Nr 117, poz. 758, z 1999 r. Nr 52, poz. 532 oraz z 2000 r. Nr 22, poz. 271, Nr 74, poz. 855 i 857 i Nr 114, poz. 1191) wprowadza się następujące zmiany:

1) art. 60 otrzymuje brzmienie:
„Art. 60. Z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonującej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny, w tym również przez ujawnienie tej woli na elektronicznym nośniku informatycznym (oświadczenie woli).”;

2) art. 78 otrzymuje brzmienie:
„Art. 78. § 1. Do zachowania pisemnej formy czynności prawnej wystarcza złożenie własnoręcznego podpisu na dokumencie obejmującym treść oświadczenia woli. Do zawarcia umowy wystarcza wymiana dokumentów obejmujących treść oświadczeń woli, z których każdy jest podpisany przez jedną ze stron lub dokumentów, z których każdy obejmuje treść oświadczenia woli jednej ze stron i jest przez nią podpisany.
§ 2. Forma pisemna zachowana jest również w razie, gdy oświadczenie woli złożone na elektronicznym nośniku informatycznym zostało dostatecznie utrwalone i zabezpieczone oraz gdy dołączono lub powiązano jego treść z podpisem elektronicznym w sposób umożliwiający ustalenie tożsamości składającego oświadczenie i stwierdzenie, że oświadczenie to po dołączeniu podpisu elektronicznego nie zostało zmienione.”.

Art. 73.

W ustawie z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 1999 r. Nr 82, poz. 928 oraz z 2000 r. Nr 12 , poz. 136, Nr 43, poz. 489, Nr 48 , poz. 550, Nr 62, poz. 718, Nr 70, poz. 816, Nr 73, poz. 852, Nr 109, poz. 1158 i Nr 122, poz. 1314) w art. 29 w ust. 1 po pkt 7 dodaje się pkt 7a w brzmieniu:

„7a) akredytacji podmiotów świadczących usługi certyfikacyjne w rozumieniu przepisów o podpisie elektronicznym.”.

Art. 74.

Do dnia 31 grudnia 2003 r. wnioski, o których mowa w art. 23 ust. 2 i art. 63 ust. 2, zamiast aktualnego wypisu z krajowego rejestru sądowego mogą zawierać wypis z ewidencji działalności gospodarczej.

Art. 75.

Banki, organy władzy publicznej i jednostki sektora publicznego, do dnia 1 lipca 2002 r., dostosują swoją działalność w zakresie świadczenia usług związanych z podpisem elektronicznym oraz wykorzystania systemów teleinformatycznych związanych ze świadczeniem tych usług do wymogów niniejszej ustawy.

Art. 76.

1. Ustawa wchodzi w życie z dniem 1 lipca 2001 r., z wyjątkiem art. 3 pkt 4-7 oraz art. 7 ust. 2, które wchodzą w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej.
2. Art. 3 pkt 1-3 tracą moc z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej.

# UZASADNIENIE

Ustawa o podpisie elektronicznym jest kolejnym aktem dostosowującym polskie ustawodawstwo do wymogów prawa Unii Europejskiej. Jednocześnie w związku z rozwojem techniki, powszechnym dostępem do Internetu i poczty elektronicznej i związanym z tym procesem handlu elektronicznego zaistniała konieczność stworzenia warunków prawnych pozwalających na skuteczne i bezpieczne wskazanie tożsamości podmiotów uczestniczących w elektronicznym obrocie prawnym tj. tworzenia i weryfikacji podpisów elektronicznych. Na podkreślenie zasługuje fakt, iż wiele państw posiada już właściwe regulacje w tym zakresie np. Niemcy, Austria, Czechy, Belgia, Francja, Finlandia, Słowenia, Słowacja.

Prezentowany projekt reguluje dziedzinę w prawie polskim zupełnie nową, technicznie zaawansowaną i regulowaną specyficznym wysoce technicznie wyspecjalizowanym językiem informatycznym.

Rodziło to wiele praktycznych trudności w sformułowaniu przepisów w sposób zgodny z wymogami języka techniki a jednocześnie w sposób zrozumiały dla przeciętnego odbiorcy prawa - zgodnie z zasadami techniki prawodawczej.

Podstawowe wytyczne do sformułowania przepisów ustawy określa dyrektywa Parlamentu Europejskiego i Rady nr 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych warunków ramowych dotyczących podpisu elektronicznego. Przygotowując projekt starano się nie naruszyć ducha dyrektywy i uszanować utrwalone zasady tworzenia prawa wewnętrznego.

Projekt jest wyrazem kompromisu pomiędzy oczekiwaniami profesjonalistów i potrzebami nieprofesjonalnych odbiorców pragnących używać podpisu elektronicznego w sprawach życia codziennego.

Ponadto w związku z postępem technologicznym ustawa nie wskazuje jednoznacznych środków za pomocą, których będą składane podpisy elektroniczne oraz środków bezpieczeństwa, które muszą zostać przedsięwzięte zarówno przez odbiorców usług certyfikacyjnych, jak i przez podmioty świadczące te usługi. Pod tym względem ustawa wskazuje jedynie jakie wymagania muszą spełniać odpowiednie urządzenia. Jest bowiem pewne, że rozwój techniki stworzy w przyszłości doskonalsze systemy zabezpieczeń.

Ustawa określiła warunki i skutki prawne stosowania podpisu elektronicznego, a także zasady świadczenia usług związanych z podpisem elektronicznym oraz nadzoru nad podmiotami świadczącymi te usługi.

W zakresie nie uregulowanym w ustawie, skutki prawne stosowania podpisu elektronicznego będą takie same jak określone, w szczególności w kodeksie cywilnym, skutki prawne podpisów własnoręcznych.

Wprowadzono następujące domniemania (art. 5):

1) podpis elektroniczny weryfikowany na podstawie ważnego kwalifikowanego certyfikatu pochodzi od osoby określonej w tym certyfikacie jako osoba składająca podpis elektroniczny,
2) podpis elektroniczny spełnia wymóg, o którym mowa w art. 4 pkt 1 lit. c), tzn. że został złożony za pomocą urządzeń i danych, które osoba fizyczna składająca podpis ma pod swoją wyłączną kontrolą,
3) podpis elektroniczny znakowany czasem przez akredytowany lub kwalifikowany podmiot został złożony nie później niż w czasie rzeczywistym wskazanym za pomocą tej usługi; domniemanie to przysługuje do dnia utraty ważności certyfikatu wykorzystywanego do

weryfikacji tego znakowania.

Domniemanie, o którym mowa w pkt 1) nie przysługuje po upływie terminu ważności certyfikatu lub od dnia jego unieważnienia oraz w okresie jego zawieszenia, chyba, że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu lub przed dniem jego unieważnienia albo zawieszenia.

Dokument opatrzony podpisem elektronicznym złożonym na podstawie ważnego kwalifikowanego certyfikatu jest równoważny pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi i spełnia wymogi w zakresie zachowania formy pisemnej, także gdy została zastrzeżona pod rygorem nieważności (art. 72 ustawy zmieniający art. 78 Kodeks Cywilny). Jednocześnie projekt nie uchyla innych norm ustaw szczególnych w zakresie spełnienia wymogu formy pisemnej.

Należy również wskazać, że zgodnie z Dyrektywą UE wprowadzono do ustawy normę, na podstawie której nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu lub nie został złożony za pomocą bezpiecznego urządzenia do składania podpisu elektronicznego.

Podpis elektroniczny weryfikowany przy pomocy certyfikatu wywołuje skutki prawne określone ustawą, jeżeli został złożony w okresie ważności tego certyfikatu. Podpis elektroniczny złożony w okresie zawieszenia certyfikatu wykorzystywanego do jego weryfikacji wywołuje skutki prawne z chwilą uchylenia tego zawieszenia. Rozwiązanie takie zapewni pewność obrotu gospodarczego, w którym szczególnie ważne jest, aby strony umów zawieranych za pomocą podpisów składanych w formie elektronicznej miały pewność skuteczności podpisu swojego kontrahenta.

Mając na względzie zasadę swobody umów, ustawa przewiduje, że strony stosunku prawnego mogą, w drodze umowy, uznać za prawnie skuteczny, podpis elektroniczny weryfikowany na podstawie certyfikatu wydanego przez podmiot świadczący usługi certyfikacyjne nie mający siedziby na terytorium Rzeczypospolitej Polskiej i nie świadczący usług na jej terytorium. Przepisu tego nie będzie się stosować do podpisu elektronicznego weryfikowanego na podstawie certyfikatu wydanego przez podmiot świadczący usługi certyfikacyjne mający siedzibę na terytorium państw członkowskich Unii Europejskiej. Certyfikaty wydawane przez te podmioty zrównane będą bowiem pod względem prawnym z certyfikatami wydawanymi przez podmioty mające siedzibę na terytorium RP. Te szczególne uregulowania dotyczące podmiotów „unijnych" wejdą w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej.

Polska ustawa bazuje na postanowieniach dyrektywy, szczególnie w warstwie definicji. Dotyczy to zarówno definicji samego podpisu elektronicznego, jak i osoby składającej podpis elektroniczny i potwierdzają tożsamość tej osoby i jego formy kwalifikowanej oraz akredytacji, czyli zezwolenia udzielanego podmiotowi świadczącemu usługi certyfikacyjne umożliwiającego wydawanie kwalifikowanych certyfikatów lub znakowanie czasem.

Pojęciami podstawowymi dla zrozumienia materii ustawy są pojęcie certyfikatu rozumianego jako elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do określonej osoby składającej podpis elektroniczny i potwierdzają tożsamość tej osoby i jego formy kwalifikowanej, oraz akredytowanego i kwalifikowanego podmiotu świadczącego usługi certyfikacyjne na rzecz lub przez organy władzy publicznej i jednostki sektora publicznego, z wyłączeniem Narodowego Banku Polskiego.

Certyfikat, zgodnie z art. 13 ust. 1, jest wydawany na podstawie umowy o świadczenie usług certyfikacyjnych, która winna być, pod rygorem nieważności, sporządzona w formie pisemnej

(art. 15 ust. 1). Jednocześnie ustawa wskazuje, iż nieważność umowy o świadczenie usług certyfikacyjnych nie powoduje nieważności certyfikatu, jeżeli został on wydany na wniosek osoby zainteresowanej i spełnia pozostałe wymogi określone niniejszą ustawą (art. 15 ust. 2). Norma taka jest podyktowana koniecznością zapewnienia pewności obrotu gospodarczego, w szczególności służy ona ochronie odbiorców usług certyfikacyjnych działających w zaufaniu do wydanego i wykorzystywanego certyfikatu. Umowa o świadczenie usług certyfikacyjnych kształtuje jedynie stosunki prawne między stronami tej umowy tzn. między podmiotem świadczącym usługi certyfikacyjne a osobą składającą podpisy elektroniczne. Umowa ta nie musi być znana pozostałym odbiorcom usług certyfikacyjnych, w szczególności osoby te nie muszą mieć świadomości, czy umowa ta jest ważna czy też nie, co nie może wpływać negatywnie na ich prawa wynikłe z zawartych z osobą składającą podpis elektroniczny umów w formie elektronicznej.

W sposób szczególny wyróżniono także jedną z usług związanych z podpisem elektronicznym polegającą na dołączaniu do danych w postaci elektronicznej, logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia rzeczywistego czasu znakowania oraz poświadczenia elektronicznego tak powstałych danych przez świadczącego usługę. Usługa ta ma zasadnicze znaczenie dla pewności obrotu i ważności podpisów elektronicznych.

Certyfikaty wydawane są w ramach tzw. polityk certyfikacji. Są to szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób tworzenia oraz zakres i sposób stosowania certyfikatu w warunkach jednolitych wymagań bezpieczeństwa. Inne bowiem wymagania bezpieczeństwa musi spełniać podpis składany na potrzeby drobnego handlu a inne podpis składany w sprawach chronionych na podstawie przepisów o ochronie informacji niejawnych.

Zasadą jest swoboda wykonywania działalności gospodarczej w zakresie świadczenia usług certyfikacyjnych. Jednak świadczenie usług certyfikacyjnych na rzecz lub przez organy władzy publicznej i jednostki sektora publicznego, z wyłączeniem Narodowego Banku Polskiego, wymaga akredytacji i wpisania do rejestru akredytowanych podmiotów świadczących usługi certyfikacyjne.

Podmioty świadczące usługi certyfikacyjne zobowiązane będą do:

1) zapewnienia technicznych i organizacyjnych możliwości szybkiego i niezawodnego wydawania, zawieszania i unieważniania certyfikatów oraz określenia czasu dokonania tych czynności,
2) stwierdzenia tożsamości osoby ubiegającej się o uzyskanie certyfikatu, w sposób określony w polityce certyfikacji,
3) uzyskania dodatkowych danych, które mają być zawarte w certyfikacie,
4) zatrudnienia osób posiadających niezbędne doświadczenie i kwalifikacje,
5) zapewnienia środków przeciwdziałających fałszerstwom certyfikatów i innych poświadczanych elektronicznie przez nich danych,
6) zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych, w przypadku gdy usługi są świadczone przez akredytowane lub kwalifikowane podmioty świadczące usługi certyfikacyjne,
7) poinformowania osoby, która występuje o certyfikat, przed zawarciem z nią umowy o warunkach uzyskania i używania certyfikatu o wszelkich ograniczeniach jego użycia oraz - w przypadku gdy podmiot nie posiada akredytacji - również o istnieniu możliwości uzyskania certyfikatu od podmiotu akredytowanego,
8) używania systemów do znakowania czasem, tworzenia i przechowywania certyfikatów, w

sposób zapewniający możliwość wprowadzania i zmiany danych jedynie osobom upoważnionym oraz gwarantującym publiczny dostęp do certyfikatów, jeżeli osoby, którym wydano te certyfikaty wyraziły zgodę na taki dostęp,

9) udostępnienia, na wniosek odbiorcy usług certyfikacyjnych, wykazu bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych,
10) zapewnienia, w razie tworzenia przez nie danych służących do składania podpisu elektronicznego, poufności procesu ich tworzenia, a także nie przechowywania i nie kopiowania tych danych oraz nie udostępniania ich nikomu innemu poza osobą, która będzie składała za ich pomocą podpis elektroniczny,
11) zapewnienia za pomocą środków technicznych, aby dane służące do składania podpisów mogły, po zakończeniu procesu ich tworzenia, wystąpić tylko raz,
12) zapewnienia weryfikacji autentyczności i ważności certyfikatów oraz innych poświadczanych przez nich elektronicznie danych.

Podmiot świadczący usługi certyfikacyjne odpowiadać powinien wobec odbiorców usług certyfikacyjnych za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych usług, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okolicznościami, za które podmiot świadczący usługi certyfikacyjne nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności.
Ponieważ ustawa zgodnie z Dyrektywą Unii Europejskiej przewiduje instytucje udzielania gwarancji za certyfikat wydany przez podmiot świadczący usługi poza granicami Rzeczypospolitej Polskiej, podmiot świadczący usługi certyfikacyjne, który udzielił gwarancji za certyfikat, odpowiada wobec odbiorców usług certyfikacyjnych za wszelkie szkody spowodowane użyciem tego certyfikatu.

Podmiot świadczący usługi certyfikacyjne nie odpowiada wobec odbiorców usług certyfikacyjnych za szkody wynikające z użycia certyfikatu poza zakresem określonym w polityce certyfikacji, której identyfikator został wskazany w certyfikacie.

Podmiot świadczący usługi certyfikacyjne wydaje certyfikat na wniosek osoby zainteresowanej składaniem podpisów elektronicznych. Podstawą do wydania certyfikatu jest umowa określająca zakres stosowania certyfikatu, okres ważności certyfikatu, zakres świadczonych usług certyfikacyjnych oraz koszty świadczonych usług certyfikacyjnych.
Jednocześnie ze względu na fakt, iż umowa o świadczenie usług certyfikacyjnych wiąże tylko jej strony, natomiast umowy zawierane za pomocą podpisu elektronicznego będą wiązać osoby trzecie, które nie będą miały możliwości dowiedzenia się, czy certyfikat został wydany w sposób właściwy, projekt zakłada obowiązek jednoznacznego wskazania certyfikatu przez osobę składającą podpis elektroniczny.

Treść kwalifikowanego certyfikatu ustawa określiła analogicznie do treści określonej w dyrektywie. Certyfikat zawierał będzie numer certyfikatu, wskazanie, że certyfikat został wydany jako certyfikat kwalifikowany zgodnie z daną polityką certyfikacji, określenie podmiotu świadczącego usługi certyfikacyjne wydającego certyfikat i państwa, w którym ma on siedzibę oraz numer akredytacji lub pozycji w odpowiednim rejestrze akredytowanych podmiotów, imię i nazwisko lub pseudonim osoby składającej podpis elektroniczny, wskazanie w jakim charakterze lub w czyim imieniu działa osoba składająca podpis elektroniczny, oznaczenie początku i końca okresu ważności certyfikatu, poświadczenie elektroniczne podmiotu świadczącego usługi certyfikacyjne, wydającego dany certyfikat, ograniczenia zakresu ważności certyfikatu jeśli przewiduje to dana polityka certyfikacji, ograniczenia maksymalnej wartości transakcji, w której certyfikat może być wykorzystywany.
Certyfikat jest ważny w okresie w nim wskazanym, może być jednak wcześniej zawieszony a

nawet unieważniony.

Zasadniczą częścią ustawy są rozdziały dotyczące trybu udzielania akredytacji i dokonywania wpisu do rejestru akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne oraz sprawowania nad nimi nadzoru.

Określono tryb i zasady składania i rozpatrywania wniosków o udzielenie akredytacji lub dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne oraz tryby kontroli podmiotów świadczących usługi certyfikacyjne.

Minister właściwy do spraw wewnętrznych wskazany został jako organ właściwy do spraw związanych z podpisem elektronicznym realizującym swoje zadania poprzez:

1) akredytację podmiotów świadczących usługi certyfikacyjne,
2) prowadzenie rejestrów akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
3) wydawanie i unieważnianie zaświadczeń certyfikacyjnych, o których mowa w art. 22 ust. 2 i 3,
4) kontrolę legalności działalności podmiotów świadczących usługi certyfikacyjne,
5) nakładanie kar przewidzianych w ustawie,
6) podejmowanie innych działań przewidzianych przepisami niniejszej ustawy.

Ustawa tworzy Radę Akredytacyjną ministra właściwego do spraw wewnętrznych, jako organ doradczy i opiniodawczy w sprawach związanych z działalnością podmiotów świadczących usługi certyfikacyjne. Do zadań Rady należy opiniowanie projektów aktów normatywnych dotyczących działalności podmiotów świadczących usługi certyfikacyjne, opiniowanie sprawozdań ministra właściwego do spraw wewnętrznych z działalności akredytacyjnej, przedstawianie opinii w sprawach związanych z działalnością podmiotów świadczących usługi certyfikacyjne. Rada składa się z 12 osób powoływanych przez ministra właściwego do spraw wewnętrznych spośród osób posiadających wiedzę i doświadczenie w sprawach związanych z zadaniami określonymi w ustawie. Dwóch członków Rady powołuje się spośród osób reprezentujących podmioty świadczące usługi certyfikacyjne oraz siedmiu (po 1 osobie) spośród osób rekomendowanych przez ministra właściwego do spraw łączności, ministra właściwego do spraw instytucji finansowych, ministra właściwego do spraw gospodarki, Szefa Urzędu Ochrony Państwa, Szefa Wojskowych Służb Informacyjnych, Prezesa Narodowego Banku Polskiego, Komisję Papierów Wartościowych i Giełd.

Egzekucję przepisów ustawy zapewniają przepisy karne penalizujące istotne jej naruszenia.

Ze względu na nowatorski charakter regulowanej problematyki niezbędna staje się nowelizacja ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 1999 r. Nr 82, poz. 928 z późn. zm.) dodająca do zadań działu sprawy wewnętrzne sprawy z zakresu akredytacji podmiotów świadczących usługi certyfikacyjne w rozumieniu przepisów o podpisie elektronicznym.

Proponuje się, aby ustawa weszła w życie z dniem 1 lipca 2001 r. z wyjątkiem art. 3 pkt 4-7 oraz art. 7 ust. 2, które wejdą w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej. Jednocześnie przepisy art. 3 pkt 1-3 utracą moc z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej.

Wejście w życie ustawy stworzy warunki do bezpiecznego dla konsumentów stosowania podpisu elektronicznego. Ożywi obrót gospodarczy za pośrednictwem mediów elektronicznych oraz dostosuje kolejną dziedzinę życia do standardów europejskich.

Ze względu na fakt, że znaczna część podmiotów, które w myśl przepisów ustawy (art. 8) muszą uzyskać akredytacje ministra właściwego do spraw wewnętrznych, świadczy tego

typu usługi w dniu dzisiejszym, ustawa pozwala, aby banki, organy władzy publicznej i jednostki sektora publicznego, do dnia 1 lipca 2002 r., dostosowały swoją działalność w zakresie świadczenia usług związanych z podpisem elektronicznym oraz wykorzystywały systemów teleinformatycznych związanych ze świadczeniem tych usług do wymogów niniejszej ustawy.

Koszty związane z wejściem w życie ustawy związane będą z koniecznością utworzenia aparatu niezbędnego do wszczęcia postępowania akredytacyjnego. Środki na ten cel zostały przewidziane w budżecie Ministerstwa Spraw Wewnętrznych i Administracji na rok 2001.

**SEKRETARZ**
**KOMITETU INTEGRACJI EUROPEJSKIEJ**
***Jacek Saryusz-Wolski***

Warszawa,05.02.2001 r.

Sekr. Min. JSW/ 384 /2001/DLE/TK

**Pani**
**Jolanta Rusiniak**
**p.o. Sekretarza Rady Ministrów**

**Opinia o zgodności projektu ustawy o podpisie elektronicznym z prawem Unii Europejskiej, wyrażona na podstawie art. 2 ust. 1 pkt. 2 ustawy z dnia 8 sierpnia 1996 r. o Komitecie Integracji Europejskiej (Dz. U. Nr 106, poz. 494) przez Sekretarza Komitetu Integracji Europejskiej, Jacka Saryusz-Wolskiego, działającego z upoważnienia Przewodniczącego Komitetu Integracji Europejskiej**

W związku z przedłożonym projektem ustawy (pismo RM-10-15-01) pozwalam sobie wyrazić następującą opinię.

I. Celem projektowanej ustawy jest dostosowanie prawa polskiego w zakresie składania oświadczeń woli za pomocą podpisu elektronicznego oraz świadczenia usług związanych z podpisem elektronicznym.

II. Projekt ustawy określa warunki stosowania podpisu elektronicznego jako równorzędnego pod względem skutków prawnych podpisowi własnoręcznemu. Zasada równoważności

podpisu elektronicznego w stosunku do podpisu odręcznego jest jednym z najważniejszych postanowień prawa Unii Europejskiej dotyczących elektronicznych form stwierdzania tożsamości.

III. Wytyczne do sformułowania przepisów ustawy określa Dyrektywa Parlamentu Europejskiego i Rady nr 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych warunków ramowych dotyczących podpisu elektronicznego.

IV. Poza przepisami wynikającymi z ustawodawstwa Unii Europejskiej projekt ustawy zawiera postanowienia określające zasady nadzoru nad podmiotami świadczącymi usługi związane z podpisem elektronicznym, w tym usługi certyfikacyjne. Projekt ustanawia, dopuszczalną z punktu widzenia wspominając dyrektywy lecz nie zawsze stosowaną w Państwach Członkowskich, procedurę akredytacji. Zgodnie z projektem, akredytacja to decyzja potwierdzająca, iż podmiot świadczący usługi certyfikacyjne spełnia wymagania określone w ustawie o podpisie elektronicznym. Akredytacje w swoich ustawodawstwach wprowadziły także inne państwa kandydujące do Unii Europejskiej. Przykładem takiego państwa jest Słowenia. Przewidziano tam zarówno akredytację dobrowolną jest i obligatoryjną. Akredytację certyfikatów wykonuje tam specjalna Agencja.

V. Należy uznać, że projekt wdraża do ustawodawstwa polskiego najważniejsze postanowienia. Dyrektywy 99/93/WE, zarówno jeśli chodzi o definicje jak i podstawowe jej zasady. Dotyczy to zarówno definicji samego podpisu elektronicznego, jak i osoby składającej podpis elektroniczny oraz akredytacji. Projektowana definicja podpisu elektronicznego nie zawiera rozróżnienia na podpis zwykły i kwalifikowany tak jak ww. dyrektywa. Nie jest to jednak z nią sprzeczne. Podobnego rozróżnienia nie wprowadzają ustawy niemiecka i estońska.

VI. Projekt ustawy przewiduje, że strony stosunku prawnego mogą, w drodze umowy, uznać za prawnie skuteczny, podpis elektroniczny weryfikowany na podstawie certyfikatu wydanego przez podmiot świadczący usługi certyfikacyjne nie mający siedziby na terytorium Rzeczypospolitej Polskiej i nie świadczący usług na jej terytorium. Przepisu tego nie będzie się stosować do podpisu elektronicznego weryfikowanego na podstawie certyfikatu wydanego przez podmioty świadczące usługi certyfikacyjne mające siedzibę

na terytorium Państw Członkowskich Unii Europejskiej. Certyfikaty wydawane przez te podmioty zrównane będą bowiem pod względem prawnym z certyfikatami wydawanymi przez podmioty mające siedzibę na terytorium RP. Te szczególne uregulowania dotyczące podmiotów z Unii Europejskiej wejdą w życie z dniem uzyskania przez Polskę członkostwa w Unii Europejskiej.

VII. Dyrektywa 1999/93/WE ustanawia dodatkowo warunki uznania kwalifikowanych certyfikatów państw trzecich za równorzędne z kwalifikowanymi certyfikatami Unii (spełnienie warunków ustawy i dobrowolna akredytacja w Państwie Członkowskim, gwarancja udzielona przez wystawcę certyfikatu z Państwa Członkowskiego, umowa bilateralna lub multilatelarna zawarta przez Wspólnotę z państwem trzecim lub organizacją międzynarodową). Ustawa estońska wypełnia ww. postanowienia dyrektywy, jednakże tylko w stosunku do okresu przedczłonkowskiego. Konieczne jest jednak rozróżnienie pomiędzy okresem przed i po akcesji. Rozróżnienie takie wprowadza polski projekt ustawy w art. 3 stwierdzając, że certyfikaty wydane przez podmiot świadczący usługi certyfikacyjne nie mający siedziby na terytorium Rzeczypospolitej Polskiej i nie świadczący usług na jej terytorium zrównuje się pod względem prawnym z kwalifikowanymi certyfikatami wydanymi przez akredytowany lub kwalifikowany podmiot świadczący usługi certyfikacyjne mający siedzibę lub świadczący usługi na terytorium Rzeczypospolitej Polskiej, jeżeli:

1. podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, spełnia wymagania niniejszej ustawy i została mu udzielona akredytacja,
2. podmiot świadczący usługi certyfikacyjne mający siedzibę na terytorium Rzeczypospolitej Polskiej lub świadczący usługi na jej terytorium udzieli gwarancji za ten certyfikat,
3. przewiduje to umowa międzynarodowa o wzajemnym uznaniu certyfikatów,

(warunki obowiązujące przed członkostwem w znacznym stopniu zbliżone są do warunków wymienionych w dyrektywie)

oraz jeżeli:

1. podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, spełnia wymagania niniejszej ustawy i została mu udzielona akredytacja w państwie członkowskim Unii Europejskiej,
2. podmiot świadczący usługi certyfikacyjne mający siedzibę na terytorium Unii Europejskiej spełniający wymogi niniejszej ustawy udzieli gwarancji za ten certyfikat,
3. certyfikat ten został uznany za kwalifikowany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi,
4. podmiot świadczący usługi certyfikacyjne, który wydał ten certyfikat, został uznany w drodze umowy międzynarodowej zawartej pomiędzy Wspólnotą Europejską a państwami trzecimi lub organizacjami międzynarodowymi,

(warunki stosowane po uzyskaniu członkostwa, które są identyczne jak w dyrektywie i zostały przykładowo zastosowane w austriackiej ustawie o podpisie elektronicznym).

VIII. Projekt ustawy w art. 5 ust. 9 stwierdza, że nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu lub nie został złożony za pomocą bezpiecznego urządzenia do składania podpisu elektronicznego. W ustępie 9 brak punktu mówiącego o podpisie elektronicznym, którego dane nie posiadają kwalifikowanego certyfikatu wydanego przez podmiot będący w posiadaniu akredytacji (art. 5 ust.2 trzecie *tiret* dyrektywy). Jest to kwestia wymagająca bezwzględnej zmiany pomimo argumentacji projektodawcy, że warunek wymieniony przez dyrektywę jest spełniony poprzez sformułowanie mówiące o kwalifikowanym certyfikacie, jako że certyfikat taki jest zawsze wydany przez podmiot posiadający akredytację. Argumentacja ta nie jest przekonująca. Należy zauważyć, że akredytacja może zostać cofnięta oraz, że przepis ust. 9 ma w rzeczywistości charakter dowodowy i będzie rozpatrywany w oderwaniu od uregulowań ustawy natomiast w odniesieniu do sytuacji faktycznej. W tym zakresie sformułowania identyczne z Dyrektywą 1999/93/WE przewidują m.in. ustawy austriacka, słoweńska i estońska.

IX. NPPC nie zawiera odniesienia do Dyrektywy 1999/93/WE.

X. **W konkluzji stwierdzam, że projekt ustawy o podpisie elektronicznym jest zgodny z prawem Unii Europejskiej.**

SEKRETARZ
Komitetu Integracji Europejskiej
*Jacek Saryusz-Wolski*
Sekretarz Stanu

**Do wiadomości:**

Pan
Kazimierz Ferenc
Podsekretarz Stanu
Ministerstwo Spraw Wewnętrznych i Administracji

**URZĄD**
**KOMITETU INTEGRACJI EUROPEJSKIEJ**
*Cezary Banasiński*
Podsekretarz Stanu

Sekr. Min. CB./ /2001/

Warszawa, 21 luty 2001 r

**Pani**
**Jolanta Rusiniak**
**p.o. Sekretarza Rady Ministrów**
**Kancelaria Prezesa Rady Ministrów**

Szanowna Pani Minister

Z upoważnienia Sekretarza Komitetu Integracji Europejskiej, przekazuję uzasadnienie dostosowawczego charakteru projektu ustawy o podpisie elektronicznym.

Z poważaniem
PODSEKRETARZ STANU
Cezary Banasiński

URZĄD KOMITETU INTEGRACJI EUROPEJSKIEJ
Al. Ujazdowskie 9, 00-918 Warszawa tel. (022) 694-75-84, (022) 694-72-35, fax (022) 694-76-86

# UZASADNIENIE DOSTOSOWAWCZEGO CHARAKTERU PROJEKTU USTAWY O PODPISIE ELEKTRONICZNYM

Ustawa o podpisie elektronicznym zawiera regulacje w dziedzinie nowoczesnych technologii zgodne z wymogami prawa Unii Europejskiej, w szczególności implementuje ona Dyrektywę 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych warunków ramowych dotyczących podpisu elektronicznego.

Zasadniczym celem przyjęcia Dyrektywy było zniwelowanie różnic w uregulowaniach prawnych występujących w państwach członkowskich, mogących spowodować poważną barierę w zakresie elektronicznych sposobów komunikowania się i handlu elektronicznego. Jasne uregulowania na poziomie europejskim wzmocniły zaufanie i akceptację dla nowych technologii.

Pewne formy użytkowania podpisów elektronicznych zostały wyłączone z obszaru uregulowanego nową Dyrektywą. Chodzi tu o podpisy elektroniczne używane wyłącznie w systemach utworzonych na podstawie dobrowolnych porozumień pomiędzy zdefiniowaną grupą użytkowników. W ten sposób dochodzi do poszanowania wolności stron umowy w zakresie ustalania zasad uznawania podpisanych elektronicznie danych. Postanowienia te zostały odzwierciedlone w projekcie ustawy.

Zgodnie z Dyrektywą, państwa członkowskie nie mogą wymagać od przedsiębiorstw prowadzących działalność certyfikacyjną jakichkolwiek zezwoleń. Niezależnie od powyższego zakazu, państwa członkowskie mogą jednak wprowadzać lub utrzymywać w mocy dobrowolne systemy akredytacji mające na celu osiągnięcie podwyższonych standardów świadczenia usług certyfikacyjnych. Wszelkie zasady rządzące takimi systemami powinny być obiektywne, przejrzyste, proporcjonalne i nie dyskryminujące. Należy dodać, iż zakazane jest także ograniczanie przez państwa członkowskie ilości usługodawców w dobrowolnym systemie akredytacji. Projekt ustawy w pełni realizuje te założenia.

Państwa członkowskie nie mogą też ustanawiać ograniczeń w stosunku do usług certyfikacyjnych świadczonych z terenu innych państw członkowskich. Projekt ustawy realizuje to zobowiązanie częściowo, a od chwili uzyskania członkostwa w UE - w sposób całkowity. Po spełnieniu określonych warunków, kwalifikowane certyfikaty wydane przez usługodawców z siedzibą w państwach nie będących członkami Unii Europejskiej powinny być, zgodnie z Dyrektywą i projektem ustawy, uznane za prawne odpowiedniki certyfikatów wydawanych przez usługodawców unijnych. Warunki te są następujące: spełnienie przez

usługodawcę wymagań Dyrektywy i uzyskanie przez niego akredytacji w ramach dobrowolnego systemu akredytacji obowiązującego w danym państwie członkowskim, uzyskanie gwarancji certyfikatu od usługodawcy posiadającego siedzibę w Unii oraz uznanie usługodawcy przez dwustronną lub wielostronną umowę międzynarodową.

Polski projekt ustawy bazuje na postanowieniach Dyrektywy, szczególnie w warstwie definicji:

- podpisu elektronicznego,
- certyfikatu,
- kwalifikowanego certyfikatu,
- podmiotu świadczącego usługi kwalifikacyjne, etc.

Projekt ustawy reguluje:

- **skutki prawne podpisu elektronicznego**; są one zgodne z Dyrektywą w zakresie ważności podpisu elektronicznego, jego równoważności z podpisem składanym własnoręcznie, dopuszczalności jako dowodu w sądzie. Nie można też odmówić skuteczności i legalności podpisowi elektronicznemu tylko na tej podstawie, że istnieje on w formie elektronicznej.

- **obowiązki podmiotów świadczących usługi certyfikacyjne**; zgodnie z Dyrektywą ustawodawca przewiduje szereg obowiązków, jakie musi spełnić podmiot świadczący usługi certyfikacyjne. Są to m.in. ( zgodnie z Aneksem II do Dyrektywy):

- obowiązek zapewnienia środków technicznych i organizacyjnych;
- obowiązek informowania osoby, która występuje o certyfikat o warunkach uzyskania i używania certyfikatu;
- zapewnienie poufności procesu tworzenia danych;
- posiadanie odpowiedniej wiedzy z dziedziny technologii podpisu elektronicznego:

- **świadczenie usług certyfikacyjnych**; projekt określa kto i w jakich warunkach wydaje certyfikaty, definiuje bezpieczne urządzenie do składania podpisów elektronicznych,

cechy kwalifikowanego certyfikatu (na podstawie Aneksu I oraz Aneksu III do Dyrektywy).

- **ważność certyfikatów**; w projekcie określono długość ważności certyfikatów, warunki ich uznania za nieważne, zawieszone lub odwołane.

- **udzielanie akredytacji i dokonywanie wpisu do rejestru**; projekt ustala warunki, jakie musi spełnić podmiot ubiegający się o akredytację lub wpis do rejestru podmiotów świadczących usługi certyfikacyjne. Akredytacja jest dozwolona przez Dyrektywę 1999/93/WE.

- **nadzór nad działalnością podmiotów świadczących usługi certyfikacyjne**; zgodnie z zaleceniami Dyrektywy ustawodawca przewiduje szeroki wachlarz środków kontroli podmiotów świadczących usługi certyfikacyjne w celu zapewnienia maksymalnej ochrony i bezpieczeństwa w wykorzystywaniu podpisu elektronicznego.

- **działalność Rady Akredytacyjnej**; ustawodawca powołuje organ doradczy i opiniodawczy w sprawach związanych z działalnością podmiotów świadczących usługi certyfikacyjne.

- **odpowiedzialność karną**; ustawodawca operuje sankcjami karnymi m.in. w przypadku naruszenia tajemnicy związanej ze świadczeniem usług certyfikacyjnych, nie informowaniem o warunkach uzyskania i używania certyfikatu lub świadczenia usług bez wymaganej akredytacji.

Ustawa o podpisie elektronicznym uwzględnia postanowienia zawarte w Dyrektywie Unii Europejskiej oraz w Aneksach dołączonych do niej. Obok konieczności przyjęcia projektu ustawy wynikającej ze zobowiązań Polski wobec Unii Europejskiej, ustawa stanowi odpowiedź (podobnie jak Dyrektywa) na gwałtowny rozwój technologiczny i globalny charakter wykorzystania Internetu, co wymaga otwartego dostępu do nowoczesnych technologii i usług umożliwiających elektroniczne przetwarzanie i autoryzację danych.

**Załącznik**

## TABELA ZBIEŻNOŚCI

| Lp | UE | JUE | JPL | Treść zmiany | Przepisy intertemporalne | Uwagi |
|---|---|---|---|---|---|---|
| 1. | Dyrektywa Parlamentu Europejskiego i Rady nr 1999/93/WE z 13 grudnia 1999 r. | Art. 1 | Art. 1 | | Ustawa wchodzi w życie z dniem 1 lipca 2001 r., za wyjątkiem art. 3 pkt 4-7 i art. 7 ust. 2. | |
| 2. | * | Art. 4 ust 1 | Art. 2 | | | |
| 3. | * | Art. 7 ust. 1 | Art. 3 | | | |
| 4. | * | Art. 2 | Art. 4 | | | Projekt nie przewiduje definicji zawartej w art. 2 pkt 1 Dyrektywy, wy, ponieważ autorzy przyjęli wyzsze wymagania dla podpisu elektronicznego, a zgodne z art. 2 pkt 2 Dyrektywy,<br>Projekt ponadto przewiduje następujące definicje: pkt10, 15-21.<br>Potrzeba wprowadzenia tych definicji wynika z konieczności |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | zbudowania rozwiązań systemowych. |
| 5. | * | Brak | Art. 5 ust. 3-8 | | | Są to rozwiązania systemowe służące zrównaniu podpisu elektronicznego z własnoręcznym. |
| 6. | * | Art. 5 | Art. 5 ust. 1, 2, 9 i art. 6 | | | |
| 7. | * | Brak | Art. 7 | | | Rozwiązanie systemowe, które jest tylko potwierdzeniem możliwości istniejącej ze względu na swobodę umów. |
| 8. | * | Art. 3 ust. 1 | Art. 8 ust. 1 | | | |
| 9. | * | Art. 3 ust. 2 | Art. 8 ust 2 | | | |
| 10. | * | Załącznik II | Art. 9 ust. 1 | | | Rozwiązanie systemowe zgodne z załącznikiem II dyrektywy |
| 11. | * | Art. 3 ust. 7 | Art. 9 ust. 3 | | | |
| 12. | * | Art. 6 | Art. 10 w związku z art. 1 pkt 19 | | | |
| 13. | * | Częściowo art. 8 | Art. 11 | | | Rozwiązanie systemowe mające na celu ochronę informacji zgromadzonych przy świadczeniu usług certyfikacyjnych. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 14. | * | Brak | Art. 12 | | | Rozwiązanie systemowe mające na celu ochronę informacji zgromadzonych przy świadczeniu usług certyfikacyjnych i zapewnienie skutecznej kontroli, o której mowa w art. 3 ust 3 Dyrektywy. |
| 15. | * | Brak | Art. 13 | | | Rozwiązanie systemowe. |
| 16. | * | Art. 2 pkt 2 | Art. 14 | | | Rozwiązanie konieczne do spełnienia definicji podpisu elektronicznego |
| 17. | * | Brak | Art. 15 | | | Rozwiązanie systemowe. |
| 18. | * | Brak | Art. 16 | | | Rozwiązanie systemowe, mające na celu upowszechnianie uznanych norm produktów dla podpisów elektronicznych oraz zapewnienie bezpieczeństwa obrotu w handlu elektronicznym. |
| 19. | * | Załącznik III i IV | Art. 17 ust. 1-5 | | | |
| 20. | * | Art. 3 ust.4 | Art. 17 ust 6 i 7 | | | |
| 21. | * | Brak | Art. 18 | | | Rozwiązanie systemowe. |
| 22. | * | Załącznik I | Art. 19 | | | |
| 23. | * | Brak | Art. 20 i 21 | | | Rozwiązanie systemowe mające na celu zapewnienie bezpieczeństwa obrotu w handlu elektronicznym oraz zrównania podpisu własnoręcznego z elektronicz- |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | nym, uwzględniając jednocześnie jego specyfikę. |
| 24. | * | Art. 2 pkt 13, art. 3 ust 2, art. 3 ust. 7. | Art. 22-28 | | | Regulacje te są niezbędna m.in. ze względu na zapewnienie możliwości wywiązywania się przez RP z obowiązku, o którym mowa w art. 11 Dyrektywy. |
| 25. | * | Art. 3 ust. 3 | Rozdział VII : art. 29-59 | | | Rozwiązanie systemowe mające na celu uregulowanie odpowiedniego systemu nadzoru nad podmiotami świadczącymi usługi certyfikacyjne. |
| 26. | * | Brak | Rozdział VIII : 60-62 | | | Rozwiązanie systemowe mające na celu udział różnych organów i środowisk podmiotów świadczących usługi certyfikacyjne w fazie decyzyjnej, co do udzielania akredytacji, jak również w ujednolicaniu form świadczenia usług certyfikacyjnych i wymagań wobec nich. |
| 27. | * | Brak | Rozdział IX : Art. 63-66 | | | Rozwiązanie systemowe, które jest uzupełnieniem regulacji w zakresie ochrony konkurencji i konsumentów. |
| 28. | * | Brak | Rozdział X : art. 67-71 | | | Przepisy karne, które maja na celu egzekwowanie wobec podmiotów świadczących usługi certyfikacyjne i osób je reprezentujących wywiązywania się z |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | obowiązków ustawowych mających szczególne znaczenie w zakresie ochrony interesów konsumentów i ochronę bezpieczeństwa obrotu prawnego. |
| 29. | * | Brak | Rozdział XI : art. 72-76 | | | Przepisy końcowe i przejściowe. |
| 30. | * | **Art. 8 ust. 2** | **Częściowo Art. 9 ust. 1 pkt 2, 9 i 10** | | | Ustawę o ochronie danych osobowych stosuje się w pełni. |
| 31. | * | **Art. 8 ust. 3** | **Art. 19 ust. 1 pkt 4** | | | |

Lp. - liczba porządkowa zmiany,

UE - sygnatura aktu europejskiego,

JUE - jednostka redakcyjna aktu europejskiego,

JPL - jednostka redakcyjna aktu polskiego,

Przepisy intertemporalne - uwagi co do wejścia w życie,

Uwagi - ewentualne inne uwagi

* - Dyrektywa Parlamentu Europejskiego i Rady nr 1999/93/WE z 13 grudnia 1999 r.

RP/RP

Projekt
z dnia 21.02.2001 r.

**ROZPORZĄDZENIE**
**MINISTRA FINANSÓW**

**z dnia ..... 2001 r.**

**w sprawie określenia szczegółowych zasad spełniania obowiązku zawarcia umowy ubezpieczenia odpowiedzialności cywilnej podmiotów świadczących usługi certyfikacyjne za szkody wyrządzone odbiorcom tych usług.**

Na podstawie art. 9 ust. 4 ustawy z dnia ..... 2001 r. o podpisie elektronicznym (Dz.U. Nr ...., poz. .....) zarządza się, co następuje:

**§ 1.**

Przepisy rozporządzenia stosuje się do akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne w rozumieniu przepisów ustawy o podpisie elektronicznym.

**§ 2.**

Umowę ubezpieczenia zawiera się najpóźniej w dniu dokonania wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne lub uzyskania akredytacji.

**§ 3.**

1. Umowę ubezpieczenia zawiera się na okres 12 miesięcy, chyba że ubezpieczający nie później niż 30 dni przed upływem okresu na jaki umowa została zawarta powiadomi zakład ubezpieczeń o jej wypowiedzeniu.
2. Umowa ubezpieczenia ulega przedłużeniu na okres kolejnych 12 miesięcy, chyba że ubezpieczający nie później niż 30 dni przed upływem okresu na jaki umowa została zawarta powiadomi zakład ubezpieczeń o jej wypowiedzeniu.

3. Pomimo braku powiadomienia, o którym mowa w ust. 2, przedłużenie umowy ubezpieczenia nie następuje jeżeli ubezpieczający do końca okresu ubezpieczenia nie zapłaci składki, a jeżeli składka ubezpieczeniowa była płacona w ratach - którejkolwiek raty składki.

**§ 4.**

Minimalna suma gwarancyjna ubezpieczenia wynosi 6.000.000 EURO.

**§ 5.**

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

**MINISTER FINANSÓW**

## UZASADNIENIE

Projekt ustawy o podpisie elektronicznym wprowadza obowiązek zawarcia umowy ubezpieczenia odpowiedzialności cywilnej akredytowanych lub kwalifikowanych podmiotów świadczących usługi certyfikacyjne za szkody wyrządzone odbiorcom tych usług (art. 9 ust. 1 pkt 5).

Niniejszy projekt rozporządzenia stanowi wypełnienie delegacji wynikającej z art. 9 ust. 4 ww. projektu ustawy.

Przepis § 1 rozporządzenia wskazuje zakres podmiotowy zastosowania przepisów. Jest on zgodny z zakresem podmiotowym przewidzianym w art. 9 ust. 1 pkt 5 projektu ustawy o podpisie elektronicznym, który wskazuje, iż obowiązek zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych mają:

1) akredytowane podmioty świadczące usługi certyfikacyjne tj. podmioty, które w trybie przepisów ustawy uzyskały decyzję administracyjną potwierdzającą spełnienie wymogów określonych daną ustawą wymaganych przy pełnieniu usług certyfikacyjnych.
2) kwalifikowane podmioty świadczące usługi certyfikacyjne tj. podmioty świadczące usługi certyfikacyjne po wpisaniu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Zgodnie z wytycznymi delegacji ustawowej rozporządzenie określa termin powstania obowiązku ubezpieczenia odpowiedzialności cywilnej najpóźniej jako dzień dokonania wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne lub uzyskania decyzją ministra właściwego do spraw wewnętrznych akredytacji.

Ustalono okres na jaki zawiera się umowę ubezpieczenia oraz czas trwania odpowiedzialności zakładu ubezpieczeń.

Proponuje się aby umowa ubezpieczenia była zawierana na okres 12 miesięcy z możliwością jej automatycznego przedłużenia, na następny okres 12 miesięcy, jeżeli

ubezpieczający nie wypowie tej umowy w oznaczonym terminie. Rozwiązanie takie gwarantuje ciągłość ochrony ubezpieczeniowej.

Projekt ustala wysokość minimalnej sumy gwarancyjnej ubezpieczenia na 6.000.000 EURO. Powyższa kwota określona została w odniesieniu do wymogów stawianych w innych państwach europejskich, ze szczególnym uwzględnieniem prawodawstwa hiszpańskiego (Królewskie Rozporządzenie z dnia 17 września 1999 r. dotyczące podpisu elektronicznego).

Powyższa regulacja nie powoduje żadnych skutków finansowych dla budżetu państwa.

**Projekt z dnia 22 lutego 2001 r.**

**Rozporządzenie**
**Rady Ministrów**

**z dnia ..... 2001 r.**

w sprawie określenia polityk certyfikacji wykorzystywanych do ochrony informacji niejawnych i innych informacji prawnie chronionych

Na podstawie art. 16 ust. 3 ustawy z dnia .... o podpisie elektronicznym (Dz. U. Nr ...., poz. ...), zarządza się, co następuje:

§ 1

1. Rozporządzenie określa trzy polityki certyfikacji wykorzystywanych do ochrony informacji niejawnych i innych informacji prawnie chronionych na trzech różnych poziomach bezpieczeństwa - podstawowym, średnim i wysokim. Certyfikaty wydawane w ramach tych polityk będą wykorzystywane do weryfikacji podpisów elektronicznych i do zapewnienia poufności informacji.
2. Polityki certyfikacji posiadają następujące nazwy i identyfikatory obiektów:
   1) podstawowa:
      a) nazwa: PL_Basic:1.0,
      b) identyfikator obiektu: { joint-iso-ccitt(2) country(16) PL(616) certificate-policy(1) 1 },
   2) średnia:
      a) nazwa: PL_Medium:1.0,
      b) identyfikator obiektu: { joint-iso-ccitt(2) country(16) PL(616) certificate-policy(1) 2 },
   3) wysoka:
      a) nazwa: PL_High:1.0,
      b) identyfikator obiektu: { joint-iso-ccitt(2) country(16) PL(616) certificate-policy(1) 3 }.

§ 2

1. Zakres stosowania poszczególnych polityk certyfikacji jest następujący:
   1) podstawowa: ochrona informacji prawnie chronionych nie będących informacjami niejawnymi w rozumieniu ustawy o ochronie informacji niejawnych oraz do informacji niejawnych będących tajemnicą służbową o klauzuli "zastrzeżone";
   2) średnia: ochrona informacji określonych w pkt a) oraz informacji niejawnych będących tajemnicą służbową o klauzuli "poufne";
   3) wysoka: ochrona informacji określonych w pkt b) i informacji niejawnych będących tajemnicą państwową o klauzuli "tajne" oraz do świadczenia usługi znakowania czasem.
2. Podmioty świadczące usługi związane z podpisem elektronicznym wydające certyfikaty z identyfikatorami polityk, o których mowa w §1 mogą określić w certyfikacie maksymalną kwotę transakcji, która może być opatrzona podpisem elektronicznym weryfikowanym na jego podstawie, przy czym kwota ta nie może być wyższa niż, dla polityki:
   1) podstawowej - 5.000 EURO,
   2) średniej - 50.000 EURO.

§ 3

Tworzenie danych służących do szyfrowania klucza wykorzystywanego przez algorytm zapewniający poufność przekazu oraz do składania podpisów i poświadczeń elektronicznych weryfikowanych na podstawie certyfikatów i zaświadczeń certyfikacyjnych z identyfiatorem polityk, o których mowa w §1 musi spełniać następujące warunki:

1) danymi służącymi do składania podpisów i poświadczeń elektronicznych są klucze prywatne asymetrycznego algorytmu szyfrowego RSA, przy czym długość klucza dla poszczególnych polityk wynosi:
   a) podstawowej: 768 bity;
   b) średniej: 1024 bity;
   c) wysokiej: 2048 bitów,

2) procedury stosowane przy tworzeniu kluczy określonych w pkt 1) muszą używać jako argumentu ciągu losowego pochodzącego ze źródła generującego ciąg losowy w oparciu o zjawisko fizyczne; argument ten musi być tej samej długości co tworzony klucz; zabronione jest tworzenie ciągów losowych przy pomocy algorytmów pseudolosowych,
3) badanie jakości generatorów losowych, o których mowa w pkt 2) musi być wykonywane, dla danej polityki certyfikacji, nie rzadziej niż:
   a) podstawowa - 1 miesiąc;
   b) średnia - 1 tydzień;
   c) wysoka - 1 dzień,
4) wynik badania, o którym mowa w pkt 3) musi być przechowywany przez podmiot świadczący usługi związane z podpisem elektronicznym nie krócej niż 10 lat,
5) algorytmem skrótu wiadomości dla wszystkich trzech polityk jest Secure Hash Algorithm - SHA-1,
6) system teleinformatyczny służący do tworzenia danych służących do składania podpisów i poświadczeń elektronicznych nie może być podłączony do sieci publicznej i muszą być zastosowane odpowiednie mechanizmy zabezpieczające przed nieautoryzowanym dostępem.

§ 4

1. Klucze prywatne, o których mowa w § 3, wykorzystywane przez podmiot świadczący usługi związane z podpisem elektronicznym do tworzenia poświadczeń elektronicznych mogą pojawić się w pełnej formie jedynie podczas ich tworzenia w urządzeniu do tworzenia kluczy lub w urządzeniu do składania poświadczeń elektronicznych. Poza tymi przypadkami muszą być one przechowywane w modułach kluczowych z wykorzystaniem tzw. schematu progowego "m of n" gdzie m wynosi 2, natomiast n wynosi ponad 3.
2. Klucze prywatne, o których mowa w § 3, wykorzystywane przez podmiot świadczący usługi związane z podpisem elektronicznym lub przez osobę składającą podpisy elektroniczne do zapewnienia poufności podpisanych lub poświadczanych danych oraz do składania podpisów elektronicznych są przechowywane w indywidualnych modułach kluczowych. Użycie klucza musi być poprzedzone autoryzacją w postaci PIN-u lub przy pomocy cech biometrycznych. Kilkakrotne pod rząd wykonanie autoryzacji ze skutkiem negatywnym musi prowadzić do blokady modułu kluczowego.

§ 5

1. Zaświadczenie certyfikacyjne i certyfikaty wydawane przez podmioty świadczące usługi związane z podpisem elektronicznym w ramach jednej z polityk certyfikacji, o których mowa w § 1 mogą być wydawane nie później niż do 31 grudnia 2005 roku.
2. Maksymalny okres ważności certyfikatu, o którym mowa w ust. 1, nie może być dłuższy niż 2 lata.
3. Maksymalny okres ważności zaświadczenia certyfikacyjnego, o którym mowa w ust. 1, dla danej polityki certyfikacji nie może być dłuższy niż:
   1) dla polityki podstawowej - 2 lata,
   2) dla polityki średniej - 5 lat,
   3) dla polityki wysokiej - 8 lat.

§ 6

1. Podpisy elektroniczne, certyfikaty oraz listy unieważnionych i zawieszonych certyfikatów muszą spełniać Polskie Normy, a w przypadku ich braku muszą być zgodne z międzynarodowymi standardami lub zaleceniami, tj.:
   1) dla podpisów elektronicznych - PKCS#7 Cryptographic Message Syntax Standard,
   2) dla certyfikatów - X.509 v3,
   3) dla list unieważnionych i zawieszonych certyfikatów - X.509 v2 CRL.
2. Szczegóły elektronicznego zapisu struktury danych określonych w ust. 1 muszą być zapisane z użyciem formalnej notacji zawartej w rekomendacji CCITT lub ITU-T X.208: Specification of Abstract Syntax Notation One - ASN.I - 1988 lub jej odpowiednika.
3. Szczegóły elektronicznego zapisu struktur danych, o których mowa w ust. 1 i 2, oraz zapisu podpisywanych danych, wykorzystywanego przez podmiot świadczący usługi związane z podpisem elektronicznym są publicznie dostępne i są w szczególności udostępniane nieodpłatnie odbiorcy usług certyfikacyjnych na jego wniosek.

§ 7

1. Podmioty świadczące usługi związane z podpisem elektronicznym wydające certyfikaty z identyfikatorami polityk określonymi w § 1 muszą zapewnić możliwość zgłoszenia unieważnienia lub zawieszenia certyfikatu przez 24 godziny na dobę.
2. Szczegóły procedury zgłoszenia, o którym mowa w ust. 1, muszą być uzgodnione z zainteresowanymi osobami najpóźniej w momencie wydania certyfikatu.
3. Listy unieważnionych i zawieszonych certyfikatów wydane w ramach polityk określonych w § 1 muszą zapewnić określenie momentu unieważnienia lub zawieszenia certyfikatu z dokładnością do jednej sekundy.
4. Podmioty określone w ust. 1 świadczące usługi związane z podpisem elektronicznym muszą zapewnić, że różnica czasów między odebraniem zgłoszenia o unieważnieniu lub zawieszeniu certyfikatu i czasem określonym na liście, o której mowa w ust. 3, będzie nie większa niż jedna godzina.
5. Podmioty określone w ust. 1 świadczące usługi związane z podpisem elektronicznym muszą zapewnić, że listy, o których mowa w ust. 3, będą, dla danej polityki certyfikacji, aktualizowane i wydawane nie rzadziej niż:
   1) dla polityki podstawowej - co 12 godzin,
   2) dla polityki średniej - co 4 godziny,
   3) dla polityki wysokiej - co 1 godzinę.
6. Niezależnie od wymagania określonego w ust. 5, podmiot, o którym mowa w ust. 1 świadczący usługi związane z podpisem elektronicznym, po uzyskaniu zgłoszenia o zawieszeniu lub unieważnieniu certyfikatu z powodu kompromitacji klucza prywatnego osoby podpisującej, jest obowiązany do niezwłocznej aktualizacji listy. Nowa lista musi być wydana nie później niż w ciągu jednej godziny od otrzymania zgłoszenia.

§ 8

1. Bezpieczne urządzenia do tworzenia i przechowywania kluczy prywatnych służących do składania podpisów lub poświadczeń elektronicznych oraz do składania podpisów lub poświadczeń elektronicznych muszą spełniać Polskie Normy, a w przypadku ich braku muszą spełniać wymagania określone w Information Technology Security Evaluation Criteria (ITSEC) dla poziomu E3 z "wysoką" siłą mechanizmów ochronnych.
2. Bezpieczne urządzenia do weryfikacji podpisów lub poświadczeń elektronicznych muszą spełniać Polskie Normy, a w przypadku ich braku muszą spełniać wymagania określone w Information Technology Security Evaluation Criteria (ITSEC) dla poziomu E2 z "wysoką" siłą mechanizmów ochronnych.

§ 9

1. Podmioty świadczące usługi związane z podpisem elektronicznym w ramach polityk certyfikacji określonych w § 1 muszą zapewnić stosowanie środków ochrony fizycznej wszędzie tam, gdzie tworzone i używane są przez nich klucze prywatne, o których mowa w § 3 oraz przechowywane są informacje związane z potrzebą weryfikacji niezaprzeczalności podpisu elektronicznego weryfikowanego na podstawie wydanych przez te podmioty certyfikatów.
2. Środki ochrony fizycznej, o których mowa w ust. 1 obejmują przynajmniej instalacje systemu ochrony p.poż. oraz systemu alarmowego włamania i napadu klasy min. SA3. W przypadku podmiotu świadczącego usługi związane z podpisem elektronicznym w ramach "wysokiej" polityki certyfikacji musi być zastosowany również system telewizji przemysłowej.

§ 10

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

## UZASADNIENIE

Rozporządzenie stanowi wykonanie delegacji ustawowej z art. 16 ust. 3 ustawy o podpisie elektronicznym.

Rozporządzenie przewiduje trzy polityki certyfikacji: podstawową, średnią i wysoką. Ich zastosowanie jest zależne od rodzaju informacji, które będą podpisywane. Im wyższe wymagania w zakresie ochrony informacji niejawnych lub innych informacji prawnie chronionych, tym wyższa polityka certyfikacji będzie musiała znaleźć zastosowanie. Posiadanie certyfikatu wydanego w ramach wysokiej polityki certyfikacji pozwala na podpisywanie wszelkich danych, bez względu na klauzulę tajności.

Należy pamiętać, że rozporządzenie nie określa wszystkich polityk certyfikacji, które będą miały zastosowanie w ramach świadczenia usług certyfikacyjnych, a jedynie te , które będą wykorzystywane do ochrony informacji niejawnych i innych informacji prawnie chronionych. W szczególności oprócz uregulowanych w rozporządzeniu polityk będzie miała jeszcze zastosowanie polityka w obszarze drobnego handlu elektronicznego przede wszystkim w internecie.

Projektowane rozporządzenie zakłada, iż danymi służącymi do składania podpisu elektronicznego będzie klucz prywatny opartry na asymetrycznym algorytmie szyfrowym RSA, jednakże ta technologia może mieć charakter tymczasowy i zostać zastąpiona inną. Należy przypomnieć, że ustawa nie wskazuje rozwiązań technologicznych wykorzystywanych do składania podpisów elektronicznych.

Z braku polskich odpowiedników norm technologicznych rozporządzenie odwołuje się do standardów światowych.

Długość okresów ważności certyfikatów i zaświadczeń certyfikacyjnych, o których mowa w § 5 ust. 2 i 3, jest podyktowana koniecznością nadążania za postępem technologicznym.

Rozporządzenie nie spowoduje dodatkowych skutków finansowych dla budżetu państwa.

# DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

## z dnia 13 grudnia 1999 r.

## w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego

## (99/93/WE)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ-

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności zaś jego art. 47 ust. 2, art. 55 i 95,

na wniosek Komisji[1],

uwzględniając opinię Komitetu Społeczno-Ekonomicznego[2],

uwzględniając opinię Komitetu Regionów[3],

zgodnie z procedurą ustanowioną w art. 251 Traktatu[4],

a także mając na uwadze, co następuje:

(1) 16 kwietnia 1997 Komisja przedłożyła Parlamentowi Europejskiemu, Radzie, Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów Zawiadomienie w sprawie Inicjatywy Europejskiej dotyczącej handlu elektronicznego;

(2) 8 października 1997 Komisja przekazała Parlamentowi Europejskiemu, Radzie, Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów Zawiadomienie odnośnie bezpieczeństwa i zaufania do komunikacji elektronicznej – ramy europejskie dla podpisu cyfrowego i szyfrowania;

(3) 1 grudnia 1997 Rada wezwała Komisję do przygotowania tak szybko jak to możliwe propozycji dyrektywy Parlamentu Europejskiego i Rady odnośnie podpisu cyfrowego;

(4) komunikacja elektroniczna i handel elektroniczny wymagają „podpisu elektronicznego" i odpowiednich usług umożliwiających autoryzację danych; rozbieżne reguły odnośnie prawnego uznawania podpisu elektronicznego i akredytacja dostawców usług autoryzacyjnych w państwach członkowskich mogą stanowić poważną przeszkodę w komunikacji elektronicznej i handlu elektronicznym; jasne ramy wspólnotowe odnośnie podpisu elektronicznego wzmacniają zaufanie i ogólną akceptację nowych technologii;

[1] Dz.U. WE nr C 325, z 23.10.1998, str. 5.
[2] Dz.U. WE nr C 40, z 15.02.1999, str. 29.
[3] Dz.U. WE nr C 93, z 06.04.1999, str. 33.
[4] Opinia Parlamentu Europejskiego z 13 stycznia 1999 (Dz.U. WE nr C 104, z 14.04.1999, str. 49). Wspólne stanowisko Rady z 28 czerwca 1999 (Dz.U. WE nr C 243, z 27.08.1999, str. 33) i decyzja Parlamentu Europejskiego z 27 października 1999 (jeszcze nie publikowana w Dzienniku Urzędowym). Decyzja Rady z 30 listopada 1999.

przepisy prawne państw członkowskich nie powinny ograniczać swobodnego przepływu towarów i usług na rynku wewnętrznym;

(5) należy wspierać interoperacyjność produktów związanych z podpisem elektronicznym; zgodnie z art. 14 Traktatu rynek wewnętrzny obejmuje obszar, na którym nie ma żadnych granic, i na którym zagwarantowany jest swobodny przepływ towarów; należy spełnić wymagania podstawowe, które obowiązują zwłaszcza produkty związane z podpisem elektronicznym, aby w ten sposób zapewnić swobodny przepływ towarów na rynku wewnętrznym i wspierać zaufanie do podpisu elektronicznego, nie naruszając postanowień rozporządzenia Rady (WE) nr 3381/94 z 19 grudnia 1994 odnośnie uregulowań wspólnotowych w sprawie kontroli eksportu dóbr podwójnego przeznaczenia[5] oraz decyzji Rady 94/942/WPZB z 19 grudnia 1994 odnośnie przyjętej przez Radę wspólnej akcji kontroli eksportu dóbr podwójnego przeznaczenia[6];

(6) niniejsza dyrektywa nie harmonizuje dostaw usług w dziedzinie poufności informacji, jeśli obowiązują dla usług tego typu przepisy krajowe publicznego porządku i bezpieczeństwa;

(7) rynek wewnętrzny zapewnia swobodny przepływ osób, w wyniku czego obywatele i rezydenci Unii Europejskiej muszą coraz częściej wchodzić w kontakt z władzami państwa członkowskiego, innego niż to, w którym mają swoje miejsce zamieszkania; możliwość komunikacji elektronicznej mogłaby w takich przypadkach być bardzo użyteczna;

(8) szybki rozwój technologiczny i globalny charakter Internetu wymagają koncepcji otwartej na różne technologie i usługi w dziedzinie autoryzacji elektronicznej;

(9) podpisy elektroniczne wykorzystywane będą w wielu różnych zastosowaniach, z którymi wiąże się szeroki wachlarz nowych usług i produktów, w związku z lub przy zastosowaniu podpisu elektronicznego; definicja takich produktów i usług nie powinna ograniczać się do wystawiania i zarządzania certyfikatami, lecz powinna zawierać wszystkie pozostałe usługi i produkty, które korzystają z podpisów elektronicznych lub są z nimi związane, takie jak usługi dotyczące rejestrowania, oznaczania czasu, prowadzenia spisów, obliczania lub konsultacji, związane z elektronicznym podpisem;

(10) rynek wewnętrzny umożliwia ponadgraniczną działalność dostawcom usług autoryzacyjnych, w celu zwiększenia ich konkurencyjności i tym samym otwarcia dla konsumentów i przedsiębiorstw nowych możliwości bezpiecznej wymiany informacji i handlu elektronicznego bez względu na granice; w celu wspierania oferowania usług autoryzacyjnych we Wspólnocie poprzez otwarte sieci, powinna istnieć możliwość udostępniania ich bez przeszkód i bez wcześniejszej autoryzacji; wcześniejsza autoryzacja oznacza nie tylko zezwolenie, przy czym dostawcy usług autoryzacyjnych musieliby otrzymać decyzję od władz krajowych zanim dostaną zezwolenie na dostarczanie tych usług autoryzacyjnych, ale również inne środki mające ten sam efekt;

[5] Dz.U. WE nr L 367, z 31.12.1994, str. 1. Rozporządzenie zmienione rozporządzeniem (WE) nr 837/95 (Dz.U. WE nr L 90, z 21. 04. 1995, str. 1).
[6] Dz.U. WE nr L 367, z 31.12.1994, str. 8. Decyzja zmieniona decyzją 99/193/WPZB (Dz.U. WE nr L 73, 19.03.1999, str. 1).

(11) systemy dobrowolnej akredytacji, które mają na celu zwiększenie poziomu świadczonych usług, mogą oferować dostawcom usług autoryzacyjnych właściwe warunki ramowe dla dalszego rozwoju ich usług w celu osiągnięcia, na dopiero rozwijającym się rynku, wymaganego poziomu zaufania, bezpieczeństwa i jakości; systemy te powinny wspierać rozwój najlepszych praktyk dostawców usług autoryzacyjnych;
dostawcy usług autoryzacyjnych powinni mieć wolny wybór odnośnie akredytacji i korzystania z systemów akredytacji;

(12) usługi autoryzacyjne powinny oferować organy publiczne, osoby prawne lub fizyczne, o ile działają zgodnie z prawem krajowym; państwa członkowskie nie powinny zabraniać dostawcom usług autoryzacyjnych działać bez dobrowolnej akredytacji; należy zważać na to, aby systemy akredytacji nie ograniczały konkurencyjności w dziedzinie usług autoryzacyjnych;

(13) państwa członkowskie mogę decydować o tym, jak zapewnią nadzór nad zachowaniem postanowień niniejszej dyrektywy; niniejsza dyrektywa nie wyklucza możliwości tworzenia prywatnych systemów nadzoru; niniejsza dyrektywa nie zobowiązuje dostawców usług autoryzacyjnych do składania wniosku o nadzór w ramach obowiązującego systemu akredytacji;

(14) ważne jest stworzenie wyważonego stosunku między potrzebami konsumentów a przedsiębiorstwami;

(15) załącznik III zawiera wymagania dla bezpiecznych urządzeń generujących podpisy w celu zapewnienia funkcjonalności zaawansowanych podpisów elektronicznych; nie obejmuje on całego środowiska systemowego, w którym działa urządzenie; funkcjonowanie rynku wewnętrznego wymaga szybkiego działania od Komisji oraz państw członkowskich, aby móc wskazać organy odpowiedzialne za ocenę zgodności bezpiecznych urządzeń generujących podpisy z wymaganiami załącznika III; aby sprostać wymaganiom rynku ocena ta musi być przeprowadzana wydajnie i w odpowiednim czasie;

(16) niniejsza dyrektywa przyczynia się do używania i uznania prawnego podpisu elektronicznego we Wspólnocie; nie potrzeba żadnych ustawowych warunków ramowych dla podpisu elektronicznego, który używany jest wyłącznie w systemach opierających się na dobrowolnych cywilnoprawnych porozumieniach między określoną liczbą uczestników; wolność stron do ustalania warunków, zgodnie z którymi akceptują one elektronicznie podpisane dane, powinna być respektowana, o ile jest to możliwe w ramach prawa krajowego; podpisom elektronicznym używanym w tych systemach nie należy odmawiać skuteczności prawnej i dopuszczalności jako dowód w postępowaniu sądowym;

(17) nie jest celem niniejszej dyrektywy harmonizowanie krajowych uregulowań dotyczących prawa zobowiązań, w szczególności odnośnie zawierania i wypełniania umów, innych pozaumownych przepisów formalnych w sprawie podpisu; dlatego powinny obowiązywać uregulowania w sprawie skuteczności prawnej podpisu elektronicznego nie naruszając krajowych przepisów formalnych dotyczących zawierania umów czy ustalania miejsca zawierania umów;

(18) gromadzenie i kopiowanie danych do generowania podpisu mogłoby narazić moc obowiązującą podpisu elektronicznego;

(19) podpisy elektroniczne stosowane będą w sektorze publicznym w dziedzinie administracji państwowej i wspólnotowej oraz w komunikacji między tymi administracjami, jak też między nimi a obywatelami i podmiotami gospodarczymi, np. przy zamówieniach publicznych, podatkach, ubezpieczeniach społecznych, opiece zdrowotnej i wymiarze sprawiedliwości;

(20) poprzez zharmonizowane kryteria w połączeniu z mocą obowiązującą podpisu elektronicznego możliwe jest utrzymanie koherentnych ram prawnych w całej Wspólnocie; w ustawodawstwie krajowym ustalone są różne wymagania co do obowiązującej mocy podpisu odręcznego; autoryzacje mogą służyć potwierdzaniu tożsamości osoby podpisującej się elektronicznie; zaawansowane podpisy elektroniczne oparte na autoryzacjach kwalifikowanych mają na celu wysoki poziom bezpieczeństwa; zaawansowane podpisy elektroniczne, które opierają się na kwalifikowanej autoryzacji i zostały stworzone przez bezpieczne urządzenie generujące podpisy, mogą zostać uznane za prawnie równoważne podpisom ręcznym tylko wtedy, gdy spełnione są wymagania dla podpisu ręcznego;

(21) w celu wspierania ogólnej akceptacji elektronicznych metod autoryzacji należy umożliwić to, żeby podpisy elektroniczne mogły stanowić dowód w postępowaniu sądowym we wszystkich państwach członkowskich; uznanie prawne podpisów elektronicznych powinno opierać się na obiektywnych kryteriach i nie powinno być powiązane z zezwoleniem dla danego dostawcy usług autoryzacyjnych; określenie obszarów prawa, w których można używać dokumentów elektronicznych i podpisu elektronicznego podlega prawu krajowemu; niniejsza dyrektywa nie narusza uprawnienia sądów krajowych do stanowienia o zgodności z wymaganiami niniejszej dyrektywy; nie narusza ona również krajowych przepisów o wolnej sądowej ocenie materiałów dowodowych;

(22) dostawcy usług oferujący swoje usługi autoryzacyjne publicznie podlegają krajowym regulacjom dotyczącym odpowiedzialności;

(23) rozwój międzynarodowego handlu elektronicznego wymaga ponadgranicznych porozumień z udziałem państw trzecich; w celu zapewnienia międzynarodowej interoperacyjności, korzystne mogą być porozumienia z państwami trzecimi o regułach wielostronnych odnośnie wzajemnego uznawania usług autoryzacyjnych;

(24) dla wzmocnienia zaufania użytkowników do komunikacji elektronicznej i do handlu elektronicznego dostawcy usług autoryzacyjnych muszą przestrzegać przepisów odnośnie ochrony danych i prywatności;

(25) postanowienia odnośnie stosowania pseudonimów w autoryzacjach nie powstrzymują państw członkowskich przed wymaganiem identyfikacji osób zgodnie z prawem wspólnotowym czy krajowym;

(26) środki konieczne do wdrożenia niniejszej dyrektywy należy uchwalać zgodnie z art. 2 decyzji Rady 1999/468/WE z 28 czerwca 1999 w sprawie ustalenia procedur wykonywania uprawnień implementacyjnych przeniesionych na Komisję[7];

(27) Komisja przeprowadzi, dwa lata po wdrożeniu niniejszej dyrektywy, kontrolę, aby między innymi stwierdzić, czy postęp technologiczny lub zmiany w środowisku prawnym nie przyniosły ze sobą przeszkód w realizacji celów niniejszej dyrektywy; powinna sprawdzić implikacje spokrewnionych dziedzin technicznych a następnie przedłożyć raport Parlamentowi Europejskiemu i Radzie;

(28) zgodnie z zawartymi w art. 5 Traktatu zasadami subsydiarności i proporcjonalności, cel stworzenia zharmonizowanych prawnych warunków ramowych dla dostarczenia podpisu elektronicznego i odpowiednich usług, może nie zostać osiągnięty w wystarczającym stopniu przez państwa członkowskie i tym samym możliwe jest osiągnięcie go w większym stopniu przez Wspólnotę; niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tego celu-

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

*Artykuł 1*

Zakres stosowania

Celem niniejszej dyrektywy jest ułatwienie stosowania podpisu elektronicznego oraz przyczynienie się do jego uznania prawnego. Ustanawia ona prawne warunki ramowe dla podpisu elektronicznego i określonych usług autoryzacyjnych, w celu zapewnienia właściwego funkcjonowania rynku wewnętrznego.
Nie obejmuje aspektów związanych z zawieraniem i obowiązywaniem umów czy innych zobowiązań prawnych, dla których należy wypełnić przepisy formalne prawa krajowego czy wspólnotowego, nie narusza również reguł i ograniczeń prawa krajowego czy wspólnotowego odnośnie zastosowania dokumentów.

*Artykuł 2*

Definicje

W sensie niniejszej dyrektywy termin:

1. „podpis elektroniczny” oznacza dane w formie elektronicznej, które dodane są do innych danych elektronicznych lub są z nimi logicznie powiązane i służą do autoryzacji;

2. „zaawansowany podpis elektroniczny” oznacza podpis elektroniczny spełniający następujące wymagania:

   a) przyporządkowany jest wyłącznie podpisującemu;
   b) umożliwia identyfikację podpisującego;
   c) stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą;

[7] Dz.U. WE nr L 184, z 17.07.1999, str. 23.

d) jest tak powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych może zostać wykryta;

3. „podpisujący” oznacza osobę posiadającą urządzenie do generowania podpisów, która działa w imieniu własnym lub w imieniu osób prawnych lub fizycznych, lub stron, których jest przedstawicielem;

4. „dane do generowania podpisu” oznacza jednorazowe dane jak kod lub prywatny klucz kryptograficzny, które są używane przez podpisującego do stworzenia podpisu elektronicznego;

5. „urządzenie generujące podpisy” oznacza skonfigurowane oprogramowanie lub sprzęt używane do zaimplementowania danych do generowania podpisu;

6. „bezpieczne urządzenie generujące podpisy” oznacza urządzenie generujące podpisy, które spełnia wymagania załącznika III;

7. „dane do sprawdzania podpisu” oznacza dane jak kod lub publiczne klucze kryptograficzne, używane do sprawdzenia podpisu elektronicznego;

8. „urządzenie sprawdzające podpisy” oznacza skonfigurowane oprogramowanie lub sprzęt używane do zaimplementowania danych do sprawdzania podpisu;

9. „autoryzacja” oznacza zaświadczenie elektroniczne, za pomocą którego dane do sprawdzania podpisu są przyporządkowane osobie i potwierdzają tożsamość tej osoby;

10. „autoryzacja kwalifikowana” oznacza autoryzację spełniającą wymogi załącznika I i wystawiana jest przez dostawcę usług autoryzacyjnych, która spełnia wymogi załącznika II;

11. „dostawca usług autoryzacyjnych” oznacza jednostkę lub osobę prawną bądź fizyczną, która wystawia autoryzacje lub udostępnia inne usługi związane z podpisem elektronicznym;

12. „produkt dla podpisu elektronicznego” oznacza oprogramowanie lub sprzęt wzgl. ich specyficzne komponenty, które mają być użyte przez dostawcę usług autoryzacyjnych do udostępnienia usług dla podpisu elektronicznego lub do tworzenia i kontroli podpisu elektronicznego;

13. „dobrowolna akredytacja” oznacza zezwolenie, które ustala prawa i obowiązki związane ze świadczeniem usług autoryzacyjnych, przyznane na wniosek danego dostawcy usług autoryzacyjnych przez organ państwowy bądź prywatny, który jest właściwy do ustalania tych praw i obowiązków jak też do kontroli ich przestrzegania, jednak dostawca usług autoryzacyjnych nie jest uprawniony do korzystania z praw wynikających z zezwolenia, zanim nie otrzyma zawiadomienia o decyzji;

*Artykuł 3*

Dostęp do rynku

1. Państwa członkowskie nie uzależniają udostępniania usług autoryzacyjnych od wcześniejszego zezwolenia.
2. Nie naruszając ust. 1 państwa członkowskie mogą wprowadzić wzgl. utrzymywać systemy dobrowolnej akredytacji, które mają na celu wzrost poziomu świadczonych usług autoryzacyjnych. Wszelkie wymagania związane z tym systemem muszą być obiektywne, transparentne, proporcjonalne i nie dyskryminujące. Państwa członkowskie nie mogą ograniczać liczby akredytowanych dostawców usług autoryzacyjnych z powodów podpadających pod zakres obowiązywania niniejszej dyrektywy.
3. Państwa członkowskie zapewniają stworzenie właściwego systemu do nadzoru dostawców usług autoryzacyjnych, którzy mają swoją siedzibę na ich terytorium i wydają kwalifikowane autoryzacje.
4. Zgodność bezpiecznych urządzeń do generowania podpisu z wymaganiami zgodnie z załącznikiem III stwierdza właściwy organ publiczny lub prywatny, wskazany przez państwo członkowskie.
   Stwierdzenia zgodności z wymaganiami załącznika III wydawane przez organy wymienione w części pierwszej, uznawane są przez państwa członkowskie.
5. Komisja może zgodnie z procedurą z art. 9 ustanowić numer referencyjny dla ogólnie uznanych norm odnośnie produktów dla podpisu elektronicznego i publikować je w Dzienniku Urzędowym Wspólnot Europejskich. Państwa członkowskie wychodzą z założenia, że wymagania spełnione są zgodnie z załącznikiem II lit. f) i załącznikiem III, kiedy produkt do podpisu elektronicznego odpowiada tym normom.
6. Państwa członkowskie i Komisja współpracują w celu wspierania rozwoju i stosowania urządzeń sprawdzających podpis, uwzględniając zalecenie odnośnie bezpiecznego sprawdzania podpisu zawarte w załączniku IV i w interesie konsumenta.
7. Państwa członkowskie mogą poddać zastosowanie podpisu elektronicznego w sektorze publicznym ewentualnym wymaganiom dodatkowym. Wymagania te muszą być obiektywne, transparentne, proporcjonalne i nie dyskryminujące i mogą odnosić się jedynie do specyficznych cech danych zastosowań. Wymagania te nie mogą stanowić przeszkód w ponadgranicznych usługach dla obywatela.

*Artykuł 4*

Zasady rynku wewnętrznego

1. Każde państwo członkowskie stosuje postanowienia krajowe, wydane na podstawie niniejszej dyrektywy, do osiadłych na ich terenie dostawców usług autoryzacyjnych i ich usług. Państwa członkowskie nie mogą ograniczać udostępniania usług autoryzacyjnych pochodzących z innych państw członkowskich w dziedzinach objętych tą dyrektywą.
2. Państwa członkowskie zapewnią, że produkty dla podpisu elektronicznego, spełniające wymagania niniejszej dyrektywy, znajdują się w wolnych obrocie na rynku wewnętrznym.

*Artykuł 5*

Skutek prawny podpisu elektronicznego

1. Państwa członkowskie zapewnią, że zaawansowany podpis elektroniczny, opierający się na kwalifikowanej autoryzacji i stworzony przez bezpieczne urządzenie generujące podpisy:

a) spełnia wymogi prawne co do podpisu w odniesieniu do danych w formie elektronicznej w ten sam sposób co podpis odręczny w odniesieniu do danych znajdujących się na papierze, oraz
b) dopuszczony jest jako dowód w postępowaniu sądowym.

2. Państwa członkowskie zapewnią, żeby nie odmawiano podpisowi elektronicznemu skuteczności prawnej i dopuszczalności jako dowód w postępowaniu sądowym jedynie dlatego, że:
   - jest w formie elektronicznej, lub
   - nie opiera się na kwalifikowanej autoryzacji, lub
   - nie opiera się na kwalifikowanej autoryzacji pochodzącej od akredytowanego dostawcy usług autoryzacyjnych, lub
   - nie jest wystawiony przez bezpieczne urządzenie generujące podpisy.

*Artykuł 6*

Odpowiedzialność

1. Państwa członkowskie zapewnią jako minimum, że dostawca usług autoryzacyjnych, wystawiający autoryzacje będące autoryzacjami kwalifikowanymi lub gwarantujący taką autoryzację publicznie, w odniesieniu do szkód względem organu, osoby prawnej lub fizycznej, które w rozsądny sposób mają zaufanie do autoryzacji, odpowiada za to, że:
   a) wszelkie informacje zawarte w kwalifikowanej autoryzacji w momencie jej wydania są prawidłowe, a autoryzacja zawiera wszelkie dane wymagane przez autoryzację kwalifikowaną,
   b) podpisujący podany w autoryzacji kwalifikowanej w momencie jej wydania posiadał dane do generowania podpisu, które odpowiadają podanym w autoryzacji wzgl. zidentyfikowanym danym do sprawdzania podpisu,
   c) w przypadkach gdy dostawca usług autoryzacyjnych tworzy zarówno dane do generowania podpisu jak też dane do sprawdzania podpisu, mogą być użyte te dwa komponenty w sposób komplementarny, chyba że dostawca usług autoryzacyjnych udowodni, że nie działał niedbale.

2. Państwa członkowskie zapewnią jako minimum, że dostawca usług autoryzacyjnych, który dokonał publicznej autoryzacji będącej autoryzacją kwalifikowaną, w odniesieniu do szkód względem organu, osoby prawnej lub fizycznej, która w sposób uzasadniony ma zaufanie do tej autoryzacji, odpowiada za przypadek, że cofnięcie autoryzacji nie zostało zarejestrowane, chyba że dostawca usług autoryzacyjnych udowodni, że nie działał niedbale.
3. Państwa członkowskie troszczą się o to, żeby dostawcy usług autoryzacyjnych mogli podawać w autoryzacji kwalifikowanej ograniczenia co do użycia autoryzacji; ograniczenia te muszą być rozpoznawalne dla stron trzecich. Dostawca usług autoryzacyjnych nie odpowiada za szkody, które wynikają z użycia wykraczającego za te ograniczenia.
4. Państwa członkowskie troszczą się o to, żeby dostawcy usług autoryzacyjnych mogli podawać w autoryzacji kwalifikowanej granicę dla wartości transakcji, do której może być użyta autoryzacja; granica ta musi być rozpoznawalne dla stron trzecich.
   Dostawca usług autoryzacyjnych nie odpowiada ze szkody wynikające z przekroczenia górnej granicy.

5. Ustępy 1 do 4 obowiązują nie naruszając postanowień dyrektywy Rady 93/13/EWG z 5 kwietnia 1993 w sprawie nieuczciwych warunków w umowach konsumenckich[8].

*Artykuł 7*

Aspekt międzynarodowy

1. Państwa członkowskie troszczą się o to, aby autoryzacje wystawiane publicznie przez dostawcę usług autoryzacyjnych państwa trzeciego jako autoryzacje kwalifikowane były równoważne prawnie autoryzacjom wystawianym przez dostawcę usług autoryzacyjnych osiadłym na terenie Wspólnoty, jeśli:
   a) dostawca usług autoryzacyjnych spełnia wymagania niniejszej dyrektywy i jest akredytowany w dobrowolnym systemie akredytacji jednego państwa członkowskiego, lub
   b) dostawca usług autoryzacyjnych osiadły we Wspólnocie spełnia wymagania niniejszej dyrektywy, gwarantuje autoryzację, lub
   c) autoryzacja lub dostawca usług autoryzacyjnych uznawane są w ramach umowy dwustronnej lub wielostronnej między Wspólnotą i krajami trzecimi lub organizacją międzynarodową.

2. W celu ułatwienia ponadgranicznych usług autoryzacyjnych z krajami trzecimi i prawnego uznania zaawansowanego podpisu elektronicznego pochodzącego z kraju trzeciego, Komisja przedkłada wnioski mające na celu osiągnięcie efektywnej implementacji standardów i porozumień międzynarodowych odnośnie usług autoryzacyjnych. W szczególności przedkłada w razie potrzeby Radzie wnioski o udzielenie stosownych mandatów do negocjacji umów dwu- i wielostronnych z krajami trzecimi i organizacjami międzynarodowymi. Rada stanowi kwalifikowaną większością.
3. Jeśli Komisja otrzyma informację o trudnościach, na które napotykają przedsiębiorstwa Wspólnoty odnośnie dostępu do rynku w krajach trzecich, może w razie konieczności przedstawić Radzie wnioski o stosowne mandaty do negocjowania porównywalnych praw dla przedsiębiorstw Wspólnoty w tych krajach trzecich. Rada stanowi kwalifikowaną większością. Środki podjęte zgodnie z tym ustępem nie naruszają zobowiązań Wspólnoty i państw członkowskich relewantnych porozumień międzynarodowych.

*Artykuł 8*

Ochrona danych

1. Państwa członkowskie troszczą się o to, żeby dostawcy usług autoryzacyjnych i krajowe organy właściwe do akredytacji i nadzoru spełniali wymagania dyrektywy Parlamentu Europejskiego i Rady 95/46/WE z 24 października 1995 w sprawie ochrony osób fizycznych przy przetwarzaniu osobistych danych i wolnego przepływu danych[9].
2. Państwa członkowskie troszczą się o to, żeby dostawcy usług autoryzacyjnych, wystawiający publicznie autoryzacje, mogli gromadzić dane osobowe tylko bezpośrednio od danej osoby, lub po wyraźnej zgodzie danej osoby i tylko, o ile jest to konieczne do wystawienia i utrzymania autoryzacji. Dane nie mogą być zbierane czy przetwarzane w żadnym innym celu bez wyraźnej zgody danej osoby.

[8] Dz.U. WE nr L 95, z 21.04.1993, str. 29.
[9] Dz.U. WE nr L 281, z 23.11.1995, str. 31.

3. Nie naruszając skuteczności prawnej pseudonimów w prawie krajowym, państwa członkowskie nie zabraniają dostawcom usług autoryzacyjnych w wydawaniu autoryzacji z pseudonimem zamiast nazwiska.

*Artykuł 9*

Komitet

1. Komisję wspiera „Komitet ds. podpisu elektronicznego" (dalej nazywany „Komitetem").
2. Przy odniesieniach do tego ustępu stosuje się art. 4 i 7 decyzji 1999/468/WE, przy czym należy uwzględnić art. 8 tej samej decyzji.
   Okres ustalony zgodnie z art. 4 ust. 3 decyzji 1999/468/WE wynosi trzy miesiące.
3. Komitet ustala swój regulamin.

*Artykuł 10*

Zadania Komitetu

Komitet precyzuje wymagania zawarte w załącznikach, kryteria zgodnie z art. 3 ust. 4 i ogólnie uznane standardy dla produktów związanych z podpisem elektronicznym, które zostaną ustalone i opublikowane zgodnie z art. 3 ust. 5 według procedury zawartej w art. 9 ust. 2.

*Artykuł 11*

Zawiadomienie

1. Państwa członkowskie przekazują Komisji i pozostałym państwom członkowskim następujące informacje:
   a) dane do krajowych dobrowolnych systemów akredytacji włącznie z dodatkowymi wymaganiami zgodnie z art. 3 ust. 7,
   b) nazwy i adresy krajowych organów właściwych do akredytacji i nadzoru oraz organów wymienionych w art. 3 ust. 4, jak też
   c) nazwy i adresy wszystkich akredytowanych krajowych dostawców usług autoryzacyjnych.

2. Informacje zgodnie z ust. 1 i odnośne zmiany państwa członkowskie muszą przekazywać tak szybko jak to możliwe.

*Artykuł 12*

Kontrola

1. Komisja sprawdza wdrażanie niniejszej dyrektywy i sporządza raport dla Parlamentu Europejskiego i Rady najpóźniej do 19 czerwca 2003.
2. Przy kontroli należy stwierdzić między innymi, czy zakres stosowania niniejszej dyrektywy powinien zostać zmieniony w obliczu technologicznego i prawnego rozwoju oraz rozwoju rynku. Raport obejmuje w szczególności ocenę aspektów harmonizacji na podstawie zebranych doświadczeń. Do raportu należy dołączyć propozycje przepisów prawnych.

*Artykuł 13*

Implementacja

1. Państwa członkowskie uchwalą konieczne ustawy, rozporządzenia i przepisy administracyjne w celu wdrożenia niniejszej dyrektywy przed 19 lipca 2001 i niezwłocznie powiadomią o tym Komisję. W przypadku wprowadzania w życie przez państwa członkowskie wspomnianych środków, powinny one zawierać odniesienie do niniejszej dyrektywy lub odniesienie to powinno towarzyszyć ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.
2. Państwa członkowskie przekażą Komisji tekst ważniejszych krajowych przepisów prawnych, które uchwalą na obszarze objętym tą dyrektywą.

*Artykuł 14*

Wejście w życie

Niniejsza dyrektywa wchodzi w życie w dniu jej opublikowania w *Dzienniku Urzędowym Wspólnot Europejskich*.

*Artykuł 15*

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Brukseli, dnia 13 grudnia 1999 roku.

*W imieniu Rady*
*Przewodniczący*
S. HASSI

*ZAŁĄCZNIK I*

Wymagania względem autoryzacji kwalifikowanej

Autoryzacje kwalifikowane muszą zawierać następujące dane:

a) informację, że dana autoryzacja została wystawiona jako autoryzacja kwalifikowana;
b) dane dostawcy usług autoryzacyjnych i państwa, w którym ma swoją siedzibę;
c) nazwę podpisującego lub pseudonim, który jako taki można zidentyfikować;
d) miejsce dla specyficznego atrybutu podpisującego, który jest przyznawany w zależności od przeznaczenia autoryzacji;
e) dane do sprawdzania podpisu, które odpowiadają danym do generowania podpisu kontrolowanym przez podpisującego;
f) dane odnośnie początku i końca obowiązywania autoryzacji;
g) kod identyfikacyjny autoryzacji;
h) zaawansowany podpis elektroniczny wystawiającego dostawcy usług autoryzacyjnych;
i) jeżeli konieczne, ograniczenia zakresu obowiązywania autoryzacji, oraz
j) jeżeli konieczne, granice wartości transakcji, do której można stosować autoryzacje.

*ZAŁĄCZNIK II*

Wymagania odnośnie dostawców usług autoryzacyjnych wystawiających autoryzacje kwalifikowane

Dostawcy usług autoryzacyjnych:

a) muszą udowodnić konieczną niezawodność co do świadczenia usług autoryzacyjnych;
b) muszą zapewnić prowadzenie usług szybkiego i bezpiecznego zarządzania oraz pewnego i natychmiastowego odwołania;
c) muszą zapewnić dokładne określenie daty i godziny wystawienia czy cofnięcia autoryzacji;
d) muszą sprawdzić za pomocą stosownych środków zgodnych z prawem krajowym tożsamość i jeżeli konieczne specyficzne atrybuty osoby, dla której wystawiają autoryzację;
e) muszą zatrudnić personel z koniecznymi do swoich usług wiedzą, doświadczeniem i kwalifikacjami; do tego należą w szczególności kompetencje managera, znajomość technologii podpisu elektronicznego i znajomość stosownych procedur bezpieczeństwa; dalej muszą stosować właściwe procedury administracyjne i zarządzania, które odpowiadają uznanym normom;
f) muszą stosować godne zaufania systemy i produkty, które są chronione przed zmianami i które zapewniają techniczne i kryptograficzne bezpieczeństwo procedur, które wspierają;
g) muszą przedsięwziąć środki przeciwko fałszowaniu autoryzacji, w przypadkach, gdy tworzą dane do generowania podpisu, zapewnią poufność podczas tworzenia tych danych;
h) muszą dysponować wystarczającymi środkami finansowymi, aby działać zgodnie z wymogami niniejszej dyrektywy. Muszą, w szczególności, być w stanie ponieść odpowiedzialność za szkody, np. przy wykupieniu odpowiedniego ubezpieczenia;
i) muszą w odpowiednim okresie nagrywać wszystkie istotne informacje o autoryzacji kwalifikowanej, aby w szczególności przy postępowaniu sądowym móc udowodnić autoryzację;
j) nie mogą gromadzić czy kopiować danych do generowania podpisu osób, którym oferuje się wykonywanie kluczowych usług zarządzania;
k) zanim połączy je stosunek wynikający z umowy z osobą, która życzy sobie otrzymać autoryzację dla poparcia swojego podpisu elektronicznego, muszą ją poinformować za pomocą trwałego środka komunikacyjnego o dokładnych warunkach stosowania autoryzacji, do których należą między innymi ograniczenia stosowania autoryzacji, istnienie systemu dobrowolnej akredytacji i postępowanie w przypadku skarg i postępowania pojednawczego. Informacje te muszą mieć formę elektroniczną i być sformułowane w sposób jasny, można je przekazać elektronicznie. Ważne części tych informacji udostępnia się na wniosek stronom trzecim polegającym na autoryzacji.
l) muszą stosować godne zaufania systemy do gromadzenia autoryzacji w formie umożliwiającej sprawdzenie, tak że:
   - tylko osoby uprawnione mogą wprowadzać i zmieniać dane;
   - można sprawdzić prawdziwość informacji;
   - autoryzacje można publicznie cofnąć tylko w wypadkach, dla których wyraził zgodę właściciel autoryzacji;
   - zmiany techniczne, które wpływają negatywnie na zachowanie tych wymogów bezpieczeństwa, są dla operatora widoczne.

*ZAŁĄCZNIK III*

Wymagania dla urządzeń tworzących podpisy

1. Bezpieczne urządzenia tworzące podpisy muszą poprzez odpowiednie techniki i procedury przynajmniej zapewnić, że:
   a) dane do tworzenia podpisu użyte do stworzenia podpisu praktycznie pojawiają się tylko raz oraz zapewniona jest ich poufność;
   b) dane do tworzenia podpisu użyte do stworzenia podpisu nie mogą, przy zachowaniu rozsądnego zabezpieczenia, być uzyskane oraz podpisy są chronione przed fałszowaniem przy użyciu dostępnej technologii;
   c) dane do tworzenia podpisu użyte do stworzenia podpisu chronione są przez prawnie podpisującego przed użyciem przez innych w sposób godny zaufania.

2. Bezpieczne urządzenia tworzące podpisy nie zmieniają danych do podpisania i nie stoją na przeszkodzie, żeby dane te zostały przedstawione podpisującemu przed procesem podpisywania.

*ZAŁĄCZNIK IV*

Zalecenia odnośnie bezpiecznego sprawdzania podpisu

Podczas procesu sprawdzania podpisu należy zapewnić w ramach racjonalnego bezpieczeństwa, żeby:

a) dane użyte do kontroli podpisu odpowiadały danym, które pokazuje kontrolujący,
b) podpis był sprawdzany w sposób godny zaufania a wynik tej kontroli był właściwie pokazywany,
c) kontrolujący mógł w razie potrzeby, w sposób godny zaufania stwierdzić treść podpisanych danych,
d) prawdziwość i ważność autoryzacji wymaganej w czasie sprawdzania były sprawdzane w sposób godny zaufania,
e) wynik sprawdzania i tożsamość podpisującego były pokazywane we właściwy sposób,
f) użycie pseudonimu podane było jednoznacznie, i
g) ważne zmiany związane z bezpieczeństwem mogły zostać rozpoznane.

LISTA PRZEKAZANYCH DOKUMENTÓW
DO
**PROJEKTU USTAWY O**
**PODPISIE ELEKTRONICZNYM**

przyjętego przez Radę Ministrów
w dniu 06 lutego 2001r.

Obszar Negocjacyjny: „Swoboda świadczenia usług"

| | |
|---|---|
| 1. | Deklaracja dotycząca dostosowawczego charakteru projektu ustawy wraz z uzasadnieniem dostosowawczego charakteru |
| 2. | Projekt ustawy wraz z uzasadnieniem i projektami aktów wykonawczych |
| 3. | Zestawienie przepisów dostosowujących projektowanej nowelizacji z odpowiednimi przepisami dyrektywy Unii Europejskiej (tabela) |
| 4. | Opinia Urzędu Komitetu Integracji Europejskiej o zgodności projektu z prawem Unii Europejskiej wydana dnia 05 lutego 2001r. |
| 5. | Tłumaczenie zweryfikowane dyrektywy prawa Unii Europejskiej, w wersji papierowej i elektronicznej:<br>DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY z dnia 13 grudnia 1999r. w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego (99/93/WE) |

**Tłoczono z polecenia Marszałka Sejmu Rzeczypospolitej Polskiej**
Skierowano do druku 23 lutego 2001 r.
Cena - 3,36zł + 22% VAT