

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 1999/93/WE

z dnia 13 grudnia 1999 r.

w sprawie wspólnotowych ram w zakresie podpisów elektronicznych

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 47 ust. 1 oraz art. 55 i 95,

uwzględniając wniosek Komisji¹,

uwzględniając opinię Komitetu Ekonomiczno - Społecznego²,

uwzględniając opinię Komitetu Regionów³,

stanowiąc zgodnie z procedurą określoną w art. 251 Traktatu⁴,

a także mając na uwadze, co następuje:

- 1) dnia 16 kwietnia 1997 r. Komisja przedłożyła Parlamentowi Europejskiemu, Radzie, Komitetowi Ekonomiczno - Społecznemu i Komitetowi Regionów komunikat w sprawie Inicjatywy Europejskiej dotyczącej handlu elektronicznego;
- 2) dnia 8 października 1997 r. Komisja przedłożyła Parlamentowi Europejskiemu, Radzie, Komitetowi Ekonomiczno - Społecznemu i Komitetowi Regionów komunikat w sprawie zapewnienie bezpieczeństwa i zaufania w komunikacji elektronicznej – ramy europejskie dla podpisów cyfrowych i szyfrowania;
- 3) dnia 1 grudnia 1997 r. Rada wezwała Komisję do przygotowania, możliwie najszybciej, projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie podpisów cyfrowych;
- 4) komunikacja elektroniczna i handel elektroniczny wymagają „podpisów elektronicznych” i odpowiednich usług umożliwiających uwierzytelnianie danych; rozbieżne reguły odnoszące się do prawnego uznawania podpisów elektronicznych i akredytacja podmiotów świadczących usługi certyfikacyjne w Państwach Członkowskich mogą stanowić poważną przeszkodę w komunikacji elektronicznej i handlu elektronicznym; jasne ramy wspólnotowe dotyczące podpisów elektronicznych wzmacniają zaufanie i ogólną akceptację nowych technologii; przepisy prawne Państw

¹ Dz.U. C 325 z 23.10.1998, str. 5.

² Dz.U. C 40 z 15.02.1999, str. 29.

³ Dz.U. C 93 z 06.04.1999, str. 33.

⁴ Opinia Parlamentu Europejskiego z dnia 13 stycznia 1999 r. (Dz.U. C 104 z 14.04.1999, str. 49). Wspólne stanowisko Rady z dnia 28 czerwca 1999 r. (Dz.U. C 243 z 27.08.1999, str. 33) i decyzja Parlamentu Europejskiego z dnia 27 października 1999 r. (dotychczas nieopublikowana w Dzienniku Urzędowym). Decyzja Rady z dnia 30 listopada 1999 r.

Członkowskich nie powinny ograniczać swobodnego przepływu towarów i usług na rynku wewnętrznym;

- 5) należy wspierać współdziałanie produktów podpisu elektronicznego; zgodnie z art. 14 Traktatu, rynek wewnętrzny obejmuje obszar bez granic wewnętrznych, na którym zagwarantowany jest swobodny przepływ towarów; należy spełnić zasadnicze wymogi, które obowiązują zwłaszcza produkty podpisu elektronicznego, aby w ten sposób zapewnić swobodny przepływ towarów na rynku wewnętrznym i wspierać zaufanie do podpisów elektronicznych, bez uszczerbku dla przepisów rozporządzenia Rady (WE) nr 3381/94 z dnia 19 grudnia 1994 r. ustanawiającego system wspólnotowy dotyczący kontroli wywozu dóbr podwójnego przeznaczenia⁵ oraz decyzji Rady 94/942/WPZiB z dnia 19 grudnia 1994 r. w sprawie przyjętego przez Radę wspólnego działania dotyczącego kontroli wywozu dóbr podwójnego przeznaczenia⁶;
- 6) niniejsza dyrektywa nie harmonizuje świadczenia usług odnoszących się do poufności informacji, jeśli obowiązują dla usług tego typu przepisy krajowe związane z porządkiem i bezpieczeństwem publicznym;
- 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 stałe 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 uwierzytelniania elektronicznego;
- 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 podpisów elektronicznych; 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, znakowania czasem, prowadzenia spisów, obliczania lub konsultacji, związane z podpisami elektronicznymi;
- 10) rynek wewnętrzny umożliwi ponadgraniczną działalność podmiotom świadczącym usługi certyfikacyjne, 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 świadczenia usług certyfikacyjnych we Wspólnocie przez otwarte sieci, podmioty powinny mieć możliwość świadczenia ich bez przeszkód i bez uprzedniego zezwolenia; uprzednie zezwolenie oznacza nie tylko zezwolenie, gdzie podmioty świadczące usługi certyfikacyjne musiałyby otrzymać decyzję od władz krajowych zanim będą mogły świadczyć usługi certyfikacyjne, ale również inne środki mające ten sam skutek;

⁵ Dz.U. L 367 z 31.12.1994, str. 1. Ostatnio zmienione rozporządzeniem (WE) nr 837/95 (Dz.U. L 90 z 21. 04. 1995, str. 1).

⁶ Dz.U. L 367 z 31.12.1994, str. 8. Ostatnio zmieniona decyzją 99/193/WPZiB (Dz.U. L 73 z 19.03.1999, str.□).

- 11) systemy dobrowolnej akredytacji, które mają na celu zwiększenie poziomu świadczonych usług, mogą oferować podmiotom świadczącym usługi certyfikacyjne właściwe ramy 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 podmiotów świadczących usługi certyfikacyjne; podmioty świadczące usługi certyfikacyjne powinni mieć wolny wybór w odniesieniu do akredytacji i korzystania z systemów akredytacji;
- 12) usługi certyfikacyjne powinny świadczyć organy publiczne, osoby prawne lub fizyczne, jeżeli działają zgodnie z prawem krajowym; Państwa Członkowskie nie powinny zabraniać podmiotom świadczącym usługi certyfikacyjne działać bez dobrowolnej akredytacji; należy uważać na to, aby systemy akredytacji nie ograniczały konkurencyjności w dziedzinie usług certyfikacyjnych;
- 13) Państwa Członkowskie mogą decydować o tym, jak zapewnić nadzór nad przestrzeganiem przepisów niniejszej dyrektywy; niniejsza dyrektywa nie wyklucza możliwości tworzenia prywatnych sektorowych systemów nadzoru; niniejsza dyrektywa nie zobowiązuje podmiotów świadczących usługi certyfikacyjne do składania wniosku o nadzór w ramach obowiązującego systemu akredytacji;
- 14) ważne jest uzyskanie równowagi między potrzebami konsumentów i potrzebami przedsiębiorstw;
- 15) załącznik III zawiera wymogi dla bezpiecznych urządzeń służących do składania podpisów w celu zapewnienia funkcjonalności bezpiecznych podpisów elektronicznych; nie obejmuje on całego środowiska systemowego, w którym działa urządzenie; funkcjonowanie rynku wewnętrznego wymaga od Komisji oraz Państw Członkowskich szybkiego działania, aby móc wskazać organy odpowiedzialne za ocenę zgodności bezpiecznych urządzeń służących do składania podpisów z wymogami 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 podpisów elektronicznych we Wspólnocie; nie są konieczne żadne ustawowe ramy dla podpisów elektronicznych, które są używane wyłącznie w systemach opierających się na dobrowolnych cywilnoprawnych porozumieniach między określoną liczbą uczestników; swoboda stron w ustalaniu 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 dowodów w postępowaniu sądowym;
- 17) celem niniejszej dyrektywy nie jest harmonizowanie krajowych przepisów dotyczących prawa zobowiązań, w szczególności dotyczących zawierania i wykonywania umów lub innych pozaumownych przepisów formalnych w sprawie podpisu; dlatego przepisy w sprawie skuteczności prawnej podpisów elektronicznych powinny obowiązywać bez uszczerbku dla krajowych przepisów formalnych dotyczących zawierania umów czy ustalania miejsca zawierania umów;

- 18) przechowywanie i kopiowanie danych do składania podpisu mogłoby stanowić zagrożenie dla prawnej skuteczności podpisów elektronicznych;
- 19) podpisy elektroniczne stosowane będą w sektorze publicznym w dziedzinie administracji państwowej i wspólnotowej oraz w komunikacji między tymi administracjami, jak też między nimi i obywatelami oraz podmiotami gospodarczymi, np. przy zamówieniach publicznych, podatkach, ubezpieczeniach społecznych, opiece zdrowotnej i wymiarze sprawiedliwości;
- 20) zharmonizowane kryteria odnoszące się do prawnej skuteczności podpisów elektronicznych zachowają spójne ramy prawne w całej Wspólnocie; w prawie krajowym ustalone są różne wymogi dotyczące obowiązującej mocy podpisu własnoręcznego; certyfikaty mogą służyć potwierdzeniu tożsamości osoby podpisującej się elektronicznie; bezpieczne podpisy elektroniczne wykorzystujące kwalifikowane certyfikaty mają na celu wysoki poziom bezpieczeństwa; bezpieczne podpisy elektroniczne wykorzystujące kwalifikowane certyfikaty i stworzone przy użyciu bezpiecznego urządzenia służącego do składania podpisów, mogą zostać uznane za prawnie równoważne podpisom własnoręcznym tylko wtedy, gdy spełnione są wymogi dla podpisów własnoręcznych;
- 21) w celu wspierania ogólnej akceptacji elektronicznych metod uwierzytelniania należy zapewnić, 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 podmiotu świadczącego usługi certyfikacyjne; określenie obszarów prawa, w których można używać dokumentów elektronicznych i podpisów elektronicznych podlega prawu krajowemu; niniejsza dyrektywa nie narusza uprawnień sądów krajowych do stanowienia o zgodności z wymaganiami niniejszej dyrektywy; nie narusza ona również krajowych przepisów o swobodnej sądowej ocenie materiałów dowodowych;
- 22) podmioty świadczące usługi świadczący powszechnie swoje usługi certyfikacyjne podlegają krajowym przepisom dotyczącym odpowiedzialności;
- 23) rozwój międzynarodowego handlu elektronicznego wymaga ponadgranicznych porozumień z udziałem państw trzecich; w celu zapewnienia międzynarodowego współdziałania, korzystne mogą być porozumienia z państwami trzecimi o regułach wielostronnych w odniesieniu do wzajemnego uznawania usług autoryzacyjnych;
- 24) dla wzmocnienia zaufania użytkowników do komunikacji elektronicznej i do handlu elektronicznego podmioty świadczące usługi certyfikacyjne muszą przestrzegać przepisów dotyczących ochrony danych i prywatności;
- 25) przepisy dotyczące stosowania pseudonimów w certyfikatach nie stanowią przeszkody dla Państw Członkowskich przed wymaganiami potwierdzenia tożsamości osób zgodnie z prawem wspólnotowym lub krajowym;

- 26) środki niezbędne do wykonania niniejszej dyrektywy przyjmuje się zgodnie z decyzją Rady 1999/468/WE z dnia 28 czerwca 1999 r., ustanawiającą warunki wykonywania uprawnień wykonawczych przyznanych Komisji⁷;
- 27) Komisja przeprowadzi, dwa lata po wykonaniu niniejszej dyrektywy, kontrolę, aby między innymi stwierdzić, czy postęp technologiczny lub zmiany w środowisku prawnym nie stworzyły przeszkód w realizacji celów niniejszej dyrektywy; powinna zbadać związki ze zbliżonymi dziedzinami technicznymi, a następnie przedłożyć sprawozdanie Parlamentowi Europejskiemu i Radzie;
- 28) zgodnie z określonymi w art. 5 Traktatu zasadami pomocniczości i proporcjonalności, cel stworzenia zharmonizowanych ram prawnych dla dostarczenia podpisów elektronicznych i odpowiednich usług, nie może 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,

PRZYJMUJE NINIEJSZĄ DYREKTYWĘ:

Artykuł 1

Zakres

Celem niniejszej dyrektywy jest ułatwienie użytkowania podpisów elektronicznych oraz przyczynienie się do ich uznania prawnego. Ustanawia ona ramy prawne dla podpisów elektronicznych i niektórych usług certyfikacyjnych, w celu zapewnienia właściwego funkcjonowania rynku wewnętrznego.

Nie obejmuje aspektów związanych z zawieraniem i ważnością umów lub innych zobowiązań prawnych, dla których wymagana jest określona forma przewidziana przez prawo krajowe lub wspólnotowe, nie narusza również zasad i ograniczeń, prawa krajowego lub wspólnotowego, regulujących korzystanie z dokumentów.

Artykuł 2

Definicje

Do celów niniejszej dyrektywy:

1. „podpis elektroniczny” oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia;
2. „bezpieczny podpis elektroniczny” oznacza podpis elektroniczny spełniający następujące wymogi:
 - a) przyporządkowany jest wyłącznie podpisującemu;
 - b) umożliwia ustalenie tożsamości podpisującego;

⁷ Dz.U. L 184 z 17.07.1999, str. 23.

- c) stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą; i
 - d) jest tak powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych może zostać wykryta;
3. „podpisujący” oznacza osobę posiadającą urządzenie służące do składania podpisów, która działa w imieniu własnym lub w imieniu osób prawnych lub fizycznych, lub podmiotu, którego jest przedstawicielem;
 4. „dane służące do składania podpisu” oznacza niepowtarzalne dane, takie jak kod lub prywatny klucz kryptograficzny, które są używane przez podpisującego do składania podpisu elektronicznego;
 5. „urządzenie służące do składania podpisów” oznacza skonfigurowane oprogramowanie lub sprzęt używane do wykorzystania danych służących do składania podpisu;
 6. „bezpieczne urządzenie służące do składania podpisów” oznacza urządzenie służące do składania podpisów, które spełnia wymogi załącznika III;
 7. „dane służące do weryfikacji podpisu” oznacza dane, takie jak kod lub publiczne klucze kryptograficzne, używane do weryfikacji podpisu elektronicznego;
 8. „urządzenie służące do weryfikacji podpisów” oznacza skonfigurowane oprogramowanie lub sprzęt używane do wykorzystywania danych służących do weryfikacji podpisu;
 9. „certyfikat” oznacza zaświadczenie elektroniczne, za pomocą którego dane służące do weryfikacji podpisu są przyporządkowane osobie i potwierdzają tożsamość tej osoby;
 10. „certyfikat kwalifikowany” oznacza certyfikat spełniający wymogi ustanowione w załączniku I i wystawiany przez podmiot świadczący usługi certyfikacyjne, który spełnia wymogi ustanowione w załączniku II;
 11. „podmiot świadczący usługi certyfikacyjne” oznacza podmiot lub osobę prawną bądź fizyczną, która wystawia certyfikaty lub udostępnia inne usługi związane z podpisami elektronicznymi;
 12. „produkt podpisu elektronicznego” oznacza oprogramowanie lub sprzęt, względnie ich specyficzne składniki, które mają być użyte przez podmiot świadczący usługi certyfikacyjne do udostępnienia usług podpisu elektronicznego lub do składania lub weryfikacji podpisów elektronicznych;
 13. „dobrowolna akredytacja” oznacza zezwolenie, które ustala prawa i obowiązki związane ze świadczeniem usług certyfikacyjnych, przyznane na wniosek danego podmiotu świadczącego usługi certyfikacyjne przez organ państwowy bądź prywatny, który jest właściwy do ustalania tych praw i obowiązków oraz do nadzorowania ich przestrzegania, jednak podmiot świadczący usługi certyfikacyjne 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 świadczenia usług certyfikacyjnych od uprzedniego zezwolenia.
 2. Bez uszczerbku dla przepisu ust. 1, Państwa Członkowskie mogą wprowadzić lub utrzymywać, systemy dobrowolnej akredytacji, które mają na celu wzrost poziomu świadczonych usług certyfikacyjnych. Wszelkie wymogi związane z tym systemem muszą być obiektywne, przejrzyste, proporcjonalne i niedyskryminujące. Państwa Członkowskie nie mogą ograniczać liczby akredytowanych podmiotów świadczących usługi certyfikacyjne z powodów objętych zakresem niniejszej dyrektywy.
 3. Państwa Członkowskie zapewniają stworzenie właściwego systemu do nadzoru podmiotów świadczących usługi certyfikacyjne, które mają swoją siedzibę na ich terytorium i wydają kwalifikowane certyfikaty.
 4. Zgodność bezpiecznych urządzeń służących do składania podpisu z wymogi ustanowionymi w załączniku III, stwierdza właściwy organ publiczny lub prywatny, wskazany przez Państwo Członkowskie. Komisja, zgodnie z procedurą ustanowioną w art. 9, formułuje kryteria obowiązujące Państwa Członkowskie w celu ustalenia, czy taki organ powinien być powołany.
- Stwierdzenia zgodności z wymogami ustanowionymi w załączniku III wydawane przez organy określone w akapicie pierwszym, uznawane są przez Państwa Członkowskie.
5. Komisja może, zgodnie z procedurą przewidzianą w art. 9, ustanowić numery referencyjne dla powszechnie uznanych norm dotyczących produktów podpisu elektronicznego i opublikować je w *Dzienniku Urzędowym Wspólnot Europejskich*. Państwa Członkowskie zakładają, że wymogi spełnione są zgodnie z załącznikiem II lit. f) i załącznikiem. III, gdy produkt podpisu elektronicznego odpowiada tym normom.
 6. Państwa Członkowskie i Komisja współpracują w celu wspierania rozwoju i stosowania urządzeń służących do weryfikacji podpisu, uwzględniając zalecenie w sprawie bezpiecznej weryfikacji podpisu zawarte w załączniku IV i w interesie konsumenta.
 7. Państwa Członkowskie mogą poddać stosowanie podpisów elektronicznych w sektorze publicznym ewentualnym wymogom dodatkowym. Wymogi te muszą być obiektywne, przejrzyste, proporcjonalne i niedyskryminujące, i mogą odnosić się jedynie do szczególnych cech danych zastosowań. Wymagania te nie mogą stanowić przeszkód w ponadgranicznych usługach dla obywatela.

Artykuł 4

Reguły rynku wewnętrznego

1. Każde Państwo Członkowskie stosuje przepisy krajowe, wydane na mocy niniejszej dyrektywy, do mających siedzibę na ich terytorium podmiotów świadczących usługi certyfikacyjne i ich usług. Państwa Członkowskie nie mogą ograniczać świadczenia usług certyfikacyjnych pochodzących z innych Państw Członkowskich w dziedzinach objętych tą dyrektywą.

2. Państwa Członkowskie zapewnią, że produkty podpisu elektronicznego, spełniające wymogi niniejszej dyrektywy, znajdują się w wolnym obrocie na rynku wewnętrznym.

Artykuł 5

Skutki prawne podpisów elektronicznych

1. Państwa Członkowskie zapewnią, że bezpieczne podpisy elektroniczne wykorzystujące kwalifikowany certyfikat i złożone za pomocą bezpiecznego urządzenia służącego do składania podpisów:

- a) spełniają wymogi prawne co do podpisu w odniesieniu do danych w formie elektronicznej w ten sam sposób, co podpis własnoręczny w odniesieniu do danych znajdujących się na papierze, oraz
- b) dopuszczalne są jako dowody w postępowaniu sądowym.

2. Państwa Członkowskie zapewnią, żeby nie odmawiano podpisowi elektronicznemu skuteczności prawnej i dopuszczalności jako dowodu w postępowaniu sądowym jedynie dlatego, że:

- jest w formie elektronicznej, lub
- nie wykorzystuje kwalifikowanego certyfikatu, lub
- nie wykorzystuje kwalifikowanego certyfikatu pochodzącego od akredytowanego podmiotu świadczącego usługi certyfikacyjne, lub
- nie jest złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu.

Artykuł 6

Odpowiedzialność

1. Państwa Członkowskie zapewniają jako minimum, że podmiot świadczący usługi certyfikacyjne, wystawiający certyfikaty będące certyfikatami kwalifikowanymi lub gwarantujący publicznie takie certyfikaty, odpowiada za szkody wyrządzone podmiotowi, osobie prawnej lub fizycznej, które w rozsądny sposób polegają na certyfikacie:

- a) w zakresie odpowiedzialności wszelkich informacji zawartych w kwalifikowanym certyfikacie w momencie jego wydania oraz w zakresie kompletności danych przewidzianych dla certyfikatu kwalifikowanego,

- b) w celu zapewnienia, że podpisujący określony w certyfikacie kwalifikowanym w momencie jego wydania posiada dane służące do składania podpisu, które odpowiadają podanym lub określonym w certyfikacie danym służącym do weryfikacji podpisu,
- c) w celu zapewnienia, że w przypadkach, gdy podmiot świadczący usługi certyfikacyjne tworzy zarówno dane służące do składania podpisu, jak i dane służące do weryfikacji podpisu, mogą być one użyte w sposób komplementarny;

chyba że podmiot świadczący usługi certyfikacyjne udowodni, że nie działał niedbale.

2. Państwa Członkowskie zapewniają jako minimum, że podmiot świadczący usługi certyfikacyjne, który wystawił certyfikat będący certyfikatem kwalifikowanym, odpowiada za szkodę wyrządzoną podmiotowi, osobie prawnej lub fizycznej, które w sposób uzasadniony polegają na tym certyfikacie, w przypadku niespełnienia obowiązku rejestracji odwołania certyfikatu, chyba że podmiot świadczący usługi certyfikacyjne udowodni, że nie działał niedbale.

3. Państwa Członkowskie zapewniają, że podmioty świadczące usługi certyfikacyjne mogą podawać w certyfikacie kwalifikowanym ograniczenia zakresu użycia certyfikatu; ograniczenia te muszą być rozpoznawalne dla stron trzecich. Podmiot świadczący usługi certyfikacyjne nie odpowiada za szkody, które wynikają z użycia wykraczającego za te ograniczenia.

4. Państwa Członkowskie zapewniają, że podmioty świadczące usługi certyfikacyjne mogą podawać w certyfikacie kwalifikowanym granicę wartości transakcji, do której może być użyty certyfikat; granica ta musi być rozpoznawalne dla stron trzecich.

Podmiot świadczący usługi certyfikacyjne nie odpowiada ze szkody wynikające z przekroczenia górnej granicy.

5. Przepisy ust. 1-4 obowiązują bez uszczerbku dla przepisów dyrektywy Rady 93/13/EWG z dnia 5 kwietnia 1993 r., w sprawie niedozwolonych klauzul w umowach konsumenckich⁸.

Artykuł 7

Aspekty międzynarodowe

1. Państwa Członkowskie zapewniają, że certyfikaty wystawiane powszechnie przez podmiot świadczący usługi certyfikacyjne z siedzibą w państwie trzecim jako certyfikaty kwalifikowane, były równoważne prawnie certyfikatom wystawianym przez podmiot świadczący usługi certyfikacyjne mający siedzibę na terenie Wspólnoty, jeśli:

- a) podmiot świadczący usługi certyfikacyjne spełnia wymogi niniejszej dyrektywy i jest akredytowany w dobrowolnym systemie akredytacji jednego z Państw Członkowskich, lub

⁸ Dz.U. L 95 z 21.04.1993, str. 29.

- b) podmiot świadczący usługi certyfikacyjne mający siedzibę we Wspólnocie spełniający wymogi niniejszej dyrektywy, gwarantuje certyfikat, lub
- c) certyfikat lub podmiot świadczący usługi certyfikacyjne uznawane są w ramach umowy dwustronnej lub wielostronnej między Wspólnotą i państwami trzecimi lub organizacją międzynarodową.

2. W celu ułatwienia ponadgranicznych usług certyfikacyjnych z państwami trzecimi i prawnego uznania bezpiecznych podpisów elektronicznych pochodzących z państw trzecich, Komisja, gdy sytuacja tego wymaga, przedkłada wnioski mające na celu osiągnięcie efektywnego stosowania norm i umów międzynarodowych mających zastosowanie do usług autoryzacyjnych. W szczególności, przedkłada w razie potrzeby Radzie wnioski o udzielenie stosownych pełnomocnictw do negocjacji umów dwu - i wielostronnych z państwami trzecimi i organizacjami międzynarodowymi. Rada stanowi większością kwalifikowaną.

3. W każdym przypadku, gdy Komisja zostanie powiadomiona o trudnościach, które napotykają przedsiębiorstwa Wspólnoty w odniesieniu do dostępu do rynku w państwach trzecich, może w razie konieczności przedstawić Radzie wnioski o stosowne pełnomocnictwa do negocjowania porównywalnych praw dla przedsiębiorstw wspólnotowych w tych państwach trzecich. Rada stanowi kwalifikowaną większością.

Środki podjęte na mocy tego ustępu nie naruszają zobowiązań Wspólnoty i Państw Członkowskich wynikających ze stosownych umów międzynarodowych.

Artykuł 8

Ochrona danych

1. Państwa Członkowskie zapewnią, że podmioty świadczące usługi certyfikacyjne i krajowe organy właściwe do akredytacji i nadzoru spełniają wymogi dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r., w sprawie ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych i swobodnego przepływu tych danych⁹.

2. Państwa Członkowskie zapewnią, że podmioty świadczące usługi certyfikacyjne, wydające powszechnie certyfikaty, mogą gromadzić dane osobowe tylko bezpośrednio od danej osoby, lub po wyraźnej zgodzie danej osoby i tylko, o ile jest to konieczne do wydania i utrzymania certyfikatu. Dane nie mogą być zbierane ani przetwarzane w żadnym innym celu bez wyraźnej zgody danej osoby.

3. Bez uszczerbku dla skuteczności prawnej pseudonimów na mocy prawa krajowego, Państwa Członkowskie nie zabraniają podmiotom świadczącym usługi certyfikacyjne wydawania certyfikatów z pseudonimem zamiast nazwiska.

Artykuł 9

Komitet

⁹ Dz.U. L 281 z 23.11.1995, str. 31.

1. Komisja wspomagana jest przez „Komitet ds. Podpisów Elektronicznych,” zwany dalej „Komitetem”.

2. Tam gdzie dokonano odwołania do tego ustępu, mają zastosowanie art. 4 i 7 decyzji 1999/468/WE, z uwzględnieniem przepisów jej art. 8.

Okres określony w art. 4 ust. 3 decyzji 1999/468/WE ustala się na trzy miesiące.

3. Komitet przyjmuje swój regulamin.

Artykuł 10

Zadania Komitetu

Komitet precyzuje wymogi ustanowione w załącznikach do niniejszej dyrektywy, kryteria określone w art. 3 ust. 4 i ogólnie uznane normy dla produktów podpisu elektronicznego, które zostaną ustalone i opublikowane zgodnie z art. 3 ust. 5 według procedury przewidzianej w art. 9 ust. 2.

Artykuł 11

Powiadomienie

1. Państwa Członkowskie przekazują Komisji i pozostałym Państwom Członkowskim następujące informacje:

- a) dane o krajowych dobrowolnych systemach akredytacji włącznie z dodatkowymi wymogami na podstawie art. 3 ust. 7,
- b) nazwy i adresy krajowych organów właściwych do akredytacji i nadzoru oraz organów określonych w art. 3 ust. 4,
- c) nazwy i adresy wszystkich akredytowanych krajowych podmiotów świadczących usługi certyfikacyjne.

2. Informacje przedkładane zgodnie z ust. 1 i dotyczące zmian w zakresie tych informacji, Państwa Członkowskie muszą przekazywać możliwie najszybciej.

Artykuł 12

Przegląd

1. Komisja sprawdza wykonanie niniejszej dyrektywy i sporządza sprawozdanie dla Parlamentu Europejskiego i Rady najpóźniej do dnia 19 czerwca 2003 r.

2. Przy przeglądzie należy stwierdzić, między innymi, czy zakres stosowania niniejszej dyrektywy powinien zostać zmieniony w obliczu technologicznego i prawnego rozwoju oraz rozwoju rynku. Sprawozdanie obejmuje w szczególności ocenę aspektów harmonizacji na podstawie zebranych doświadczeń. Do sprawozdania należy dołączyć, w miarę potrzeb, projekty legislacyjne.

Artykuł 13

Wykonanie

1. Państwa Członkowskie wprowadzą w życie przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy w terminie do dnia 19 lipca 2001 r. i niezwłocznie powiadomią o tym Komisję.

Podejmowane przez Państwa Członkowskie wspomniane środki zawierają odniesienie do niniejszej dyrektywy lub odniesienie to towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określone są przez Państwa Członkowskie.

2. Państwa Członkowskie przekażą Komisji teksty głównych przepisów prawa krajowego, które przyjmą w dziedzinie objętej niniejszą dyrektywą.

Artykuł 14

Wejście w życie

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

Artykuł 15

Adresaci

Niniejsza dyrektywa skierowana jest do Państw Członkowskich.

Sporządzono w Brukseli, dnia 13 grudnia 1999 r.

W imieniu Parlamentu Europejskiego

N. FONTAINE

Przewodniczący

W imieniu Rady

S. HASSI

Przewodniczący

ZAŁĄCZNIK I

Wymogi dotyczące certyfikatów kwalifikowanych

Certyfikaty kwalifikowane muszą zawierać następujące dane:

- a) wskazanie, że dany certyfikat została wystawiony jako certyfikat kwalifikowany;
- b) dane określające podmiot świadczący usługi certyfikacyjne i państwo, w którym ma swoją siedzibę;
- c) nazwę podpisującego lub pseudonim, który można jako taki rozpoznać;
- d) zastrzeżenie szczególnej cechy podpisującego, włączane gdy jest to stosowne, w zależności od przeznaczenia certyfikatu;
- e) dane służące do weryfikacji podpisu, które odpowiadają danym służącym do składania podpisu kontrolowanym przez podpisującego;
- f) dane dotyczące początku i końca okresu ważności certyfikatu;
- g) kod identyfikacyjny certyfikatu;
- h) bezpieczny podpis elektroniczny wystawiającego podmiotu świadczącego usługi certyfikacyjne;
- i) w odpowiednim przypadku, ograniczenia zakresu użycia certyfikatu, oraz
- j) w odpowiednim przypadku, granice wartości transakcji, do których można stosować certyfikat.

ZAŁĄCZNIK II

Wymogi wobec podmiotów świadczących usługi certyfikacyjne, wystawiających certyfikaty kwalifikowane

Podmioty świadczące usługi certyfikacyjne mają obowiązek:

- a) udowodnić wiarygodność niezbędną do świadczenia usług certyfikacyjnych;
- b) zapewnić świadczenie usług szybkiego i bezpiecznego zarządzania oraz pewnego i natychmiastowego odwołania;
- c) zapewnić dokładne określenie daty i godziny wystawienia lub cofnięcia certyfikatu;
- d) sprawdzić za pomocą stosownych środków zgodnych z prawem krajowym tożsamość i, w odpowiednim przypadku, cechy szczególne osoby, dla której wydają kwalifikowany certyfikat;
- e) zatrudnić personel posiadający wiedzę fachową, doświadczenie i kwalifikacje niezbędne dla świadczonych usług, w szczególności kompetencje na poziomie zarządzania, znajomość technologii podpisu elektronicznego i znajomość stosownych procedur bezpieczeństwa; muszą również stosować właściwe procedury administracyjne i zarządzania, które odpowiadają uznanym normom;
- f) stosować godne zaufania systemy i produkty, które są chronione przed zmianami i które zapewniają techniczne i kryptograficzne bezpieczeństwo procedur, które wspierają;
- g) podejmować środki przeciwko fałszowaniu certyfikatów oraz w przypadkach, gdy tworzą dane służące do składania podpisu, zapewnią poufność podczas tworzenia tych danych;
- h) dysponować wystarczającymi środkami finansowymi, aby działać zgodnie z wymogami niniejszej dyrektywy, w szczególności aby ponosić ryzyko odpowiedzialności za szkody, na przykład, przez wykupienie odpowiedniego ubezpieczenia;
- i) w odpowiednim okresie przechowywać wszystkie istotne informacje dotyczące certyfikatu kwalifikowanego, w szczególności w celu udowodnienia certyfikacji w postępowaniu sądowym. Informacje mogą być przechowywane w formie elektronicznej;
- j) nie gromadzić ani nie kopiować danych służących do składania podpisu osób, którym podmiot świadczący usługi certyfikacyjne świadczy usługi zarządzania kluczami;
- k) przed powstaniem stosunku zobowiązaniowego z osobą ubiegającą się o certyfikat dla wspierania swojego podpisu elektronicznego, poinformować tę osobę za pomocą trwałego środka komunikacyjnego o dokładnych warunkach stosowania certyfikatu, do których należą, między innymi, ograniczenia użycia certyfikatu, istnienie systemu dobrowolnej akredytacji i postępowanie w przypadku skarg i rozstrzygania sporów. Informacje takie, które mogą być przekazywane elektronicznie, muszą być w formie

pisemnej w łatwo zrozumiałym języku. Odpowiednie części tych informacji udostępnia się na wniosek stronom trzecim polegającym na certyfikacie.

- l) stosować godne zaufania systemy do przechowywania certyfikatów w formie umożliwiającej weryfikację, tak że:
- tylko osoby uprawnione mogą wprowadzać i zmieniać dane;
 - można sprawdzić prawdziwość informacji;
 - certyfikaty można publicznie cofnąć tylko w wypadkach, dla których wyraził zgodę właściciel certyfikatu;
 - zmiany techniczne, które naruszają wymogi bezpieczeństwa, są dla operatora oczywiste.

ZAŁĄCZNIK III

Wymogi dotyczące urządzeń służących do składania podpisu

1. Bezpieczne urządzenia służące do składania podpisów muszą przez właściwe środki techniczne i proceduralne zapewnić co najmniej, że:
 - a) dane służące do składania podpisu użyte do złożenia podpisu praktycznie pojawiają się tylko raz oraz zapewniona jest ich poufność;
 - b) dane służące do składania podpisu użyte do złożenia podpisu nie mogą, przy zachowaniu rozsądnego zabezpieczenia, być pozyskane oraz podpisy są chronione przed fałszowaniem przy użyciu dostępnej technologii;
 - c) dane służące do składania podpisu użyte do złożenia podpisu chronione są przez uprawnionego podpisującego się w sposób godny zaufania przed użyciem przez innych.
2. Bezpieczne urządzenia służące do składania podpisu nie zmieniają danych służących do składania podpisu i nie uniemożliwiają, by dane te zostały przedstawione podpisującemu przed złożeniem podpisu.

ZAŁĄCZNIK IV

Zalecenia dotyczące bezpiecznej weryfikacji podpisu

Podczas procesu weryfikacji podpisu należy zapewnić z uzasadnioną pewnością, żeby:

- a) dane użyte do weryfikacji podpisu odpowiadały danym, które widzi weryfikujący,
- b) podpis był weryfikowany w sposób godny zaufania, a wynik tej weryfikacji był właściwie przedstawiany,
- c) weryfikujący mógł w razie potrzeby, w sposób godny zaufania stwierdzić treść podpisanych danych,
- d) prawdziwość i ważność certyfikatu wymaganego w czasie weryfikacji były weryfikowalne w sposób godny zaufania,
- e) wynik weryfikacji i tożsamość podpisującego były pokazywane we właściwy sposób,
- f) użycie pseudonimu było jednoznacznie wskazane, oraz
- g) ważne zmiany związane z bezpieczeństwem mogły zostać rozpoznane.