

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 Komisji¹,

uwzględniając opinię Komitetu Społeczno-Ekonomicznego²,

uwzględniając opinię Komitetu Regionów³,

zgodnie z procedurą ustanowioną w art. 251 Traktatu⁴,

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

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.

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; 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 przeznaczenia⁵ oraz decyzji Rady 94/942/WPZB z 19 grudnia 1994 odnośnie przyjętej przez Radę wspólnej akcji kontroli eksportu dóbr podwójnego przeznaczenia⁶;
- (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 umożliwi 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

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).

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;

- (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 zważyć na to, aby systemy akredytacji nie ograniczały konkurencyjności w dziedzinie usług autoryzacyjnych;
- (13) państwa członkowskie mogą 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 potwierdzeniu 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 uprawnień 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 uchylać zgodnie z art. 2 decyzji Rady 1999/468/WE z 28 czerwca 1999 w sprawie ustalenia procedur wykonywania uprawnień implementacyjnych przeniesionych na Komisję⁷;
- (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:

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

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

2. „zaawansowany podpis elektroniczny” oznacza podpis elektroniczny spełniający następujące wymagania:
 - a) przyporządkowany jest wyłącznie podpisującemu; b) umożliwia identyfikację podpisującego;
 - b) stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą;
 - c) 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 wolnym 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 rozpoznawalna 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 konsumenckich⁸.

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 autoryzacom 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

⁸ Dz.U. WE nr L 95, z 21.04.1993, str. 29.

wielostronnych z krajami trzecimi i organizacjami międzynarodowymi. Rada stanowi kwalifikowaną większość.

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 większość. 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 danych⁹.
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.
2. 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.

⁹ Dz.U. WE nr L 281, z 23.11.1995, str. 31.

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
Przewodniczcicy
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.