

31999L0093

L 13/12

ÚRADNÝ VESTNÍK EURÓPSKÝCH SPOLOČENSTIEV

19.1.2000

**SMERNICA EURÓPSKEHO PARLAMENTU A RADY 1999/93/ES
z 13. decembra 1999
o rámci spoločenstva pre elektronické podpisy**

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o založení Európskeho spoločenstva a najmä jej články 47 ods. 2, 55 a 95,

so zreteľom na návrh Komisie ⁽¹⁾,

so zreteľom na stanovisko Hospodárskeho a sociálneho výboru ⁽²⁾,

so zreteľom na stanovisko Výboru regiónov ⁽³⁾,

konajúc v súlade s postupom uvedeným v článku 251 zmluvy ⁽⁴⁾,

keďže:

- (1) 16. apríla 1997 Komisia predložila Európskemu parlamentu, Rade, Hospodárskemu a sociálnemu výboru a Výboru regiónov správu o európskej iniciatíve v elektronickom obchode;
- (2) 8. októbra 1997 Komisia predložila Európskemu parlamentu, Rade, Hospodárskemu a sociálnemu výboru a Výboru regiónov správu o zabezpečovaní ochrany a dôvery v elektronickú komunikáciu — smerujúcu k európskemu rámcu pre digitálne podpisy a šifrovanie;
- (3) 1. decembra 1997 Rada vyzvala Komisiu, aby čo najskôr predložila návrh smernice Európskeho parlamentu a Rady o digitálnych podpisoch;
- (4) elektronická komunikácia a obchod si nevyhnutne vyžadujú „elektronické podpisy“ a súvisiace služby, ktoré umožnia overovanie pravosti dát; rozdielne predpisy vzťahujúce sa na právne uznávanie elektronických podpisov a akreditáciu poskytovateľov certifikačných služieb v členských štátoch môžu tvoriť významnú prekážku využívania elektronickej komunikácie a elektronického obchodovania; naproti tomu jasný rámec spoločenstva týkajúci sa podmienok používania elektronických podpisov posilní dôveru v nové technológie a ich všeobecné prijatie; právne predpisy členských štátov by nemali brániť voľnému pohybu tovarov a služieb na vnútornom trhu;
- (5) vzájomná súčinnosť elektronických podpisových produktov by sa mala propagovať v súlade s článkom 14 zmluvy, vnútorný trh pozostáva z územia bez vnútorných hraníc, na ktorom je zabezpečený voľný pohyb tovarov; musia sa splniť základné požiadavky, ktoré sú špecifické pre elektronické podpisové produkty, aby sa zabezpečil voľný pohyb na vnútornom trhu a vybudovala dôvera v elektronické podpisy bez toho, že by sa to dotklo nariadenia Rady (ES) č. 3381/94 z 19. decembra 1994, ktoré stanovuje režim spoločenstva na kontrolu exportu tovaru dvojakého použitia ⁽⁵⁾, a rozhodnutia Rady 94/942/CFSP z 19. decembra 1994 o spoločnom postupe schválenom Radou na kontrolu vývozu tovarov dvojakého použitia ⁽⁶⁾;
- (6) táto smernica neuvádza do súladu poskytovanie služieb, pokiaľ ide utajovanie informácií, na ktoré sa vzťahujú vnútroštátne právne predpisy o zásadách občianskeho spoluzitia alebo verejnej bezpečnosti;
- (7) vnútorný trh zabezpečuje voľný pohyb osôb, následkom ktorého občania a obyvatelia Európskej únie stále častejšie prichádzajú do styku s úradmi v iných členských štátoch, než v ktorých majú bydlisko; dostupnosť elektronickej komunikácie môže byť v tomto ohľade významnou službou;
- (8) rýchly technický rozvoj a globálny charakter internetu si nevyhnutne vyžaduje otvorený prístup k rozličným technológiám a službám, ktoré sú schopné elektronicky overovať pravosť dát;
- (9) elektronické podpisy sa budú využívať v rozmanitých podmienkach a aplikáciách, ktorých dôsledkom bude široká paleta nových služieb a produktov súvisiacich alebo využívajúcich elektronické podpisy; definovanie takých produktov a služieb by sa nemalo obmedziť na vydávanie a správu certifikátov, ale by malo tiež obsahovať aj každú inú službu a produkt, ktorý využíva elektronické podpisy alebo súvisí s nimi, ako napr. registračné služby, služby časového označovania, služby adresárov, výpočtové služby alebo poradenské služby vzťahujúce sa na elektronické podpisovanie;
- (10) vnútorný trh umožňuje poskytovateľom certifikačných služieb rozvíjať svoje cezhraničné činnosti s cieľom zvyšovať svoju konkurencieschopnosť, a tak ponúkať spotrebiteľom i podnikateľom nové možnosti elektronickej výmeny informácií a obchodovania bezpečným spôsobom, bez ohľadu na hranice; na stimuláciu poskytovania certifikačných služieb na otvorených sieťach v rámci celého spoločenstva by poskytovatelia certifikačných služieb mali poskytovať svoje služby voľne, bez predchádzajúceho povolenia; predchádzajúcim povolením sa rozumie nielen akékoľvek povolenie, pri ktorom je príslušný poskytovateľ

⁽¹⁾ Ú. v. ES C 325, 23.10.1988, s. 5.

⁽²⁾ Ú. v. ES C 40, 15.2.1999, s. 29.

⁽³⁾ Ú. v. ES C 93, 6.4.1999, s. 33.

⁽⁴⁾ Stanovisko Európskeho parlamentu z 13. januára 1999 (Ú. v. ES C 104, 14.4.1999, s. 49), spoločné stanovisko Rady z 28. júna 1999 (Ú. v. ES C 243, 27.8.1999, s. 33) a rozhodnutie Európskeho parlamentu z 27. októbra 1999 (ešte neuverejnené v úradnom vestníku). Rozhodnutie Rady z 30. novembra 1999.

⁽⁵⁾ Ú. v. ES L 367, 31.12.1994, s. 1. Nariadenie naposledy zmenené a doplnené nariadením (ES) č. 837/95 (Ú. v. ES L 90, 21.4.1995, s. 1).

⁽⁶⁾ Ú. v. ES L 367, 31.12.1994, s. 8. Rozhodnutie naposledy zmenené a doplnené rozhodnutím 99/193/CFSP (Ú. v. ES L 73, 19.3.1999, s. 1).

- certifikačnej služby povinný nadobudnúť rozhodnutie národných úradov skôr, než bude môcť poskytovať svoje certifikačné služby, ale aj každé iné opatrenie s rovnakým účinkom;
- (11) programy dobrovoľnej akreditácie zamerané na zvýšenie úrovne poskytovania služieb môžu vytvoriť poskytovateľom certifikačných služieb primeraný rámec na ďalšie rozvíjanie svojich služieb na takú úroveň dôvery, bezpečnosti a kvality, akú vyžaduje rozvíjajúci sa trh; tieto programy by mali podnietiť rozvoj najlepších pracovných metód medzi poskytovateľmi certifikačných služieb; malo by sa ponechať na vôľu poskytovateľov certifikačných služieb, či budú dodržiavať takéto akreditačné postupy a mať z nich prspech;
- (12) certifikačné služby môže ponúkať buď verejnoprávny subjekt, alebo právnická, či fyzická osoba, pokiaľ je založená v súlade s vnútroštátnymi právnymi predpismi; keďže členské štáty by nemali zakázať poskytovateľom certifikačných služieb činnosť mimo programov dobrovoľnej akreditácie, malo by byť zabezpečené, aby takéto akreditačné programy nezmenšovali konkurenciu v certifikačných službách;
- (13) členské štáty môžu rozhodnúť, ako zabezpečia dohľad nad súladom s ustanoveniami uvedenými v tejto smernici; táto smernica neobmedzuje zriaďovanie dozorných systémov na báze súkromného sektoru; táto smernica nezaväzuje poskytovateľov certifikačných služieb, aby požiadali o dozor podľa niektorého použiteľného akreditačného programu;
- (14) je dôležité dosiahnuť rovnováhu medzi potrebami spotrebiteľa a podnikateľa;
- (15) v prílohe III sú uvedené požiadavky na bezpečné zariadenia na vytvorenie podpisu na zabezpečenie funkčnosti zdokonalených elektronických podpisov; príloha sa nezaobrá celým systémovým prostredím, v ktorom také zariadenia pracujú; fungovanie vnútorného trhu si vyžaduje od Komisie a členských štátov rýchle konanie, aby umožnili určiť orgány poverené posúdením súladu bezpečných zariadení na vytvorenie podpisu s prílohou III; aby sa naplnili potreby trhu, posudzovanie súladu musí byť včasné a účinné;
- (16) táto smernica prispieva k využitiu a právnomu uznaniu elektronických podpisov v spoločnosti; regulačný rámec nie je potrebný na elektronické podpisy používané výlučne v systémoch, ktoré sú založené na dobrovoľných dohodách medzi určeným počtom účastníkov podľa súkromného práva; voľnosť zmluvných strán, pokiaľ ide o dojednanie podmienok, podľa ktorých si navzájom budú uznávať elektronicky podpísané dáta, by mala byť zachovaná v rozsahu, aký dovoľujú vnútroštátne právne predpisy; mala by sa uznávať právna účinnosť elektronických podpisov, použitých v takých systémoch, a ich prípustnosť ako dôkaz v konaní pred súdmi;
- (17) cieľom tejto smernice nie je harmonizácia vnútroštátnych právnych predpisov zmluvného práva, najmä o uzatváraní a plnení zmlúv alebo iných formalitách nezmluvnej povahy, vzťahujúcich sa na podpisovanie; z toho dôvodu ustanovenia, ktoré sa vzťahujú na právny účinok elektronických podpisov, by nemali mať vplyv na požiadavky ohľadne formy stanovenej vnútroštátnymi právnymi predpismi, pokiaľ ide o uzatváranie zmlúv alebo predpisy určujúce, kedy je zmluva uzavretá;
- (18) ukládanie a kopírovanie dát na vytvorenie podpisu môže spôsobiť ohrozenie právnej platnosti elektronických podpisov;
- (19) elektronické podpisy sa budú používať vo verejnom sektore v rámci orgánov štátnej správy krajín a správy spoločnosti a v styku takýchto orgánov s občanmi a hospodárskymi subjektami, napríklad v systémoch verejného obstarávania, daňovej správy, sociálneho zabezpečenia, zdravotníctva a justície;
- (20) harmonizované kritériá, vzťahujúce sa na právne účinky elektronických podpisov, zachovávajú logický právny rámec spoločnosti; vnútroštátne právne predpisy stanovujú rôzne požiadavky na platnosť vlastnoručných podpisov; keďže na osvedčenie totožnosti elektronicky podpisujúcej osoby možno použiť certifikáty; zdokonalené elektronické podpisy založené na kvalifikovaných certifikátoch majú za cieľ vyššiu úroveň bezpečnosti; zdokonalené elektronické podpisy, ktoré sú založené na kvalifikovanom certifikáte a ktoré sú vytvorené bezpečným zariadením na vytvorenie podpisu, možno považovať za právne rovnocenné s vlastnoručným podpisom, len ak sú splnené požiadavky na vlastnoručné podpisy;
- (21) na podporu všeobecného priaznivého prijatia metód elektronického overovania pravosti musí byť zabezpečené, aby elektronické podpisy bolo možné využiť ako dôkaz v konaní pred súdmi vo všetkých členských štátoch; právne uznanie elektronických podpisov by malo byť založené na objektívnych kritériách a nemalo by byť spojené s povolením činnosti dotknutého poskytovateľa certifikačných služieb; v právnych oblastiach, v ktorých možno využiť elektronické dokumenty a elektronické podpisy, sú rozhodujúce vnútroštátne právne predpisy; táto smernica nemá vplyv na právomoc národného súdu pri rozhodovaní o súlade s požiadavkami tejto smernice a nemá vplyv na vnútroštátne právne predpisy, pokiaľ ide o nezávislosť súdu pri hodnotení dôkazov;
- (22) zodpovednosť poskytovateľov certifikačných služieb, ktorí poskytujú certifikačné služby verejnosti, stanovujú vnútroštátne právne predpisy;
- (23) rozvoj medzinárodného elektronického obchodu si vyžaduje cezhraničné dohody za účasti tretích krajín; v záujme zabezpečenia vzájomnej súčinnosti na globálnej úrovni môžu byť prospešné ujednania multilaterálnych pravidiel s tretími krajinami o vzájomnom uznaní certifikačných služieb;

- (24) aby sa zvýšila dôvera používateľov v elektronickú komunikáciu a elektronický obchod, poskytovatelia certifikačných služieb musia dodržiavať právne predpisy o ochrane údajov a súkromí jednotlivca;
- (25) predpisy o používaní pseudonymov v certifikátoch by nemali brániť členským štátom, aby vyžadovali identifikáciu osôb podľa právnych predpisov spoločenstva alebo vnútroštátnych právnych predpisov;
- (26) opatrenia potrebné na implementáciu tejto smernice budú prijaté podľa rozhodnutia Rady 1999/468/ES z 28. júna 1999, ktoré stanovuje postupy pri uplatňovaní výkonu právomocí udelených Komisii ⁽¹⁾;
- (27) dva roky po implementácii Komisia vykoná kontrolu tejto smernice tak, aby sa okrem iného ubezpečila, že pokrok technológie alebo zmeny v právnom prostredí nevytvorili prekážky dosiahnutia cieľov stanovených v tejto smernici; mala by preveriť jej dôsledky v pridružených technických odboroch a predložiť o tom správu Európskemu parlamentu a Rade;
- (28) v súlade so zásadami subsidiarity a proporcionality, stanovenými v článku 5 zmluvy, nemôžu členské štáty uspokojivo dosiahnuť cieľ, ktorým je vytvorenie harmonizovaného právneho rámca na zavedenie elektronického podpisovania a súvisiacich služieb, a preto ho lepšie dosiahne spoločenstvo; táto smernica nejde ďalej, než ako je potrebné na dosiahnutie tohto cieľa,
2. „zdokonalený elektronický podpis“ (*advanced electronic signature*) je elektronický podpis, ktorý spĺňa nasledujúce požiadavky:
- je jedinečne spojený so signatárom;
 - je schopný identifikovať signatára;
 - je vytvorený s využitím prostriedkov, ktoré môže signatár držať vo svojej výlučnej moci, a
 - je prepojený s dátami, na ktoré sa vzťahuje, takým spôsobom, že každú dodatočnú zmenu dát možno hneď zistiť;
3. „signatár“ (*signatory*) je osoba, ktorá je držiteľom zariadenia na vytvorenie podpisu a koná buď vo svojom vlastnom mene, alebo v mene fyzickej osoby alebo právnickej osoby alebo subjektu, ktorý zastupuje;
4. „dáta na vytvorenie podpisu“ (*signature-creation data*) sú jedinečné dáta, ako napr. kódy alebo súkromné šifrovacie kľúče, ktoré používa signatár na vytvorenie elektronického podpisu;
5. „zariadenie na vytvorenie podpisu“ (*signature-creation device*) je nakonfigurovaný softvér alebo hardvér, používaný na implementáciu dát na vytvorenie podpisu;
6. „bezpečné zariadenie na vytvorenie podpisu“ (*secure-signature-creation device*) je zariadenie na vytvorenie podpisu, ktoré spĺňa požiadavky uvedené v prílohe III;
7. „dáta na overenie podpisu“ (*signature-verification-data*) sú dáta, ako napr. kódy, alebo verejné šifrovacie kľúče, ktoré sa používajú na účely overenia elektronického podpisu;
8. „zariadenie na overenie podpisu“ (*signature-verification device*) je nakonfigurovaný softvér alebo hardvér, používaný na implementáciu dát na overenie podpisu;
9. „certifikát“ (*certificate*) je elektronické osvedčenie, ktoré spája dáta na overenie podpisu s osobou a potvrdzuje totožnosť tejto osoby;
10. „kvalifikovaný certifikát“ (*qualified certificate*) je certifikát podľa požiadaviek uvedených v prílohe I a vydaný poskytovateľom certifikačných služieb, ktorý splnil požiadavky stanovené v prílohe II;
11. „poskytovateľ certifikačných služieb“ (*certification-service-provider*) je subjekt alebo právnická alebo fyzická osoba, ktorá vydáva certifikáty alebo poskytuje iné služby súvisiace s elektronickými podpismi;
12. „elektronický podpisový produkt“ (*electronic-signature product*) je hardvér alebo softvér alebo ich relevantné komponenty, ktoré sú určené pre poskytovateľa certifikačných služieb na poskytovanie služieb elektronického podpisovania alebo ktoré sú určené na vytváranie elektronických podpisov alebo overovanie ich pravosti;
13. „dobrovoľná akreditácia“ (*voluntary accreditation*) je každé povolenie, ktoré upravuje osobitné práva a povinnosti pri poskytovaní certifikačných služieb, ktoré na žiadosť príslušného poskytovateľa certifikačných služieb udeľuje verejný alebo súkromný orgán, poverený vypracovaním takých práv a povinností a dohľadom nad ich dodržovaním, keď poskytovateľ certifikačných služieb nemá právo vykonávať práva vyplývajúce z povolenia, pokiaľ nedostal rozhodnutie orgánu.

PRIJALI TÚTO SMERNICU:

Článok 1

Rozsah

Účelom tejto smernice je uľahčiť využívanie elektronických podpisov a prispieť k ich právnomu uznaniu. Zakladá právny rámec pre elektronický podpis a určité certifikačné služby, aby sa zabezpečilo riadne fungovanie vnútorného trhu.

Nezaoberá sa aspektmi uzatvárania a platnosti zmlúv alebo inými zákonnými povinnosťami, kde platia požiadavky týkajúce sa formy predpísanej vnútroštátnymi právnymi predpismi alebo právnymi predpismi spoločenstva, a nemá vplyv ani na pravidlá a obmedzenia obsiahnuté vo vnútroštátnych právnych predpisoch alebo predpisoch spoločenstva, ktoré platia pre používanie dokumentov.

Článok 2

Definície

Na účely tejto smernice:

- „elektronický podpis“ (*electronic signature*) sú dáta v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k ostatným elektronickým dátam a ktoré slúžia ako metóda overovania pravosti;

⁽¹⁾ Ú. v. ES L 184, 17.7.1999, s. 23.

Článok 3

Prístup na trh

1. Členské štáty nepodmienia poskytovanie certifikačných služieb predchádzajúcim schválením.

2. Bez ohľadu na ustanovenie odseku 1 členské štáty môžu zaviesť alebo udržovať programy dobrovoľnej akreditácie, zamerané na zvyšovanie úrovne poskytovania certifikačných služieb. Všetky podmienky, ktoré sa na také programy vzťahujú, musia byť objektívne, transparentné, primerané a nediskriminačné. Členské štáty nesmú obmedziť počet akreditovaných poskytovateľov certifikačných služieb z dôvodov, na ktoré sa vzťahuje rámec tejto smernice.

3. Každý členský štát zabezpečí vytvorenie vhodného systému, ktorý umožní dohľad nad poskytovateľmi certifikačných služieb, zriadenými na jeho území, ktorí vydávajú kvalifikované certifikáty pre verejnosť.

4. Súlad bezpečných zariadení na vytvorenie podpisu s požiadavkami uvedenými v prílohe III bude určovať príslušný verejný alebo súkromný orgán, ktorý určí členský štát. V zmysle postupu uvedeného v článku 9 Komisia stanoví pre členské štáty kritériá, podľa ktorých určia, či by sa mal orgán zriadiť.

Určenie súladu s požiadavkami uvedenými v prílohe III, vydané orgánmi podľa prvého odseku, budú uznávať všetky členské štáty.

5. V súlade s postupom uvedeným v článku 9 môže Komisia stanoviť a v *Úradnom vestníku Európskych spoločenstiev* uverejniť referenčné čísla všeobecne uznávaných noriem pre elektronické podpisové produkty. Keď elektronický podpisový produkt vyhoví týmto normám, členské štáty budú predpokladať súlad medzi požiadavkami uvedenými v prílohe II, písm. f) a prílohou III.

6. Členské štáty a Komisia budú spolupracovať pri podpore vývoja a používania zariadení na overovanie podpisov so zreteľom na odporúčania na bezpečné overovanie podpisov, uvedené v prílohe IV a v záujme spotrebiteľov.

7. Členské štáty môžu používanie elektronického podpisu vo verejnom sektore podmieniť splnením ďalších možných požiadaviek. Tieto požiadavky budú objektívne, transparentné, primerané a nediskriminačné a budú sa vzťahovať výlučne na špecifické znaky príslušného použitia. Také požiadavky nesmú byť prekážkou cezhraničných služieb pre občanov.

Článok 4

Zásady vnútorného trhu

1. Každý členský štát bude uplatňovať voči poskytovateľom certifikačných služieb, zriadeným na svojom území a nimi poskytovaným službám vnútroštátne právne predpisy, ktoré prijme podľa tejto smernice. Členské štáty nesmú v oblastiach definovaných v tejto smernici obmedziť poskytovanie certifikačných služieb, ktoré majú pôvod v inom členskom štáte.

2. Členské štáty zabezpečia na vnútornom trhu voľný obeh elektronických podpisových produktov, ktoré sú v súlade s touto smernicou.

Článok 5

Právne účinky elektronických podpisov

1. Členské štáty zabezpečia, aby zdokonalené elektronické podpisy, ktoré sú založené na kvalifikovanom certifikáte a ktoré sú vytvorené bezpečným zariadením na vytvorenie podpisu:

- a) splňali zákonné požiadavky na podpis vo vzťahu k dátam v elektronickej forme rovnakým spôsobom, ako vlastnoručný podpis splňa takéto požiadavky vo vzťahu k dátam na papieri, a
- b) boli prípustné ako dôkaz v konaní pred súdmi.

2. Členské štáty zabezpečia, aby elektronickému podpisu nebola odopretá právna účinnosť a prípustnosť ako dôkazu v konaní pred súdmi len z dôvodov, že:

- má elektronickú formu alebo
- nie je založený na kvalifikovanom certifikáte alebo
- nie je založený na kvalifikovanom certifikáte vydanom akreditovaným poskytovateľom certifikačných služieb alebo
- nie je vytvorený bezpečným zariadením na vytvorenie podpisu.

Článok 6

Zodpovednosť

1. Ako minimum členské štáty zabezpečia, aby s vydaním certifikátu ako kvalifikovaného certifikátu pre verejnosť alebo s poskytnutím záruky za taký certifikát pre verejnosť poskytovateľ certifikačných služieb zodpovedal za škodu spôsobenú každému subjektu alebo právnickej, či fyzickej osobe, ktorá sa odôvodnene spoľahne na tento certifikát:

- a) pokiaľ ide o presnosť všetkých informácií obsiahnutých v kvalifikovanom certifikáte v čase vydania a aj ohľadne skutočnosti, že certifikát obsahuje všetky náležitosti, ktoré sú pre kvalifikovaný certifikát predpísané;
- b) v ubezpečení, že v čase vydania certifikátu bol signatár, identifikovaný v kvalifikovanom certifikáte, držiteľom dát na vytvorenie podpisu zodpovedajúcich dátam na overenie podpisu, uvedeným alebo identifikovaným v certifikáte;
- c) v ubezpečení, že dáta na vytvorenie podpisu a dáta na overenie podpisu možno použiť komplementárne v prípadoch, keď autorom oboch je poskytovateľ certifikačných služieb;

pokiaľ poskytovateľ certifikačných služieb preukáže, že nekonal nedbalosť.

2. Ako minimum členské štáty zabezpečia, aby poskytovateľ certifikačných služieb, ktorý vydal certifikát ako kvalifikovaný certifikát pre verejnosť, zodpovedal za škodu spôsobenú subjektu alebo právnickej osobe alebo fyzickej osobe, ktorá sa odôvodnene spolieha na certifikát, opomenutím zaregistrovania zrušenia certifikátu, pokiaľ poskytovateľ certifikačných služieb nepreukáže, že nekonal z nedbanlivosti.

3. Členské štáty zabezpečia, aby poskytovateľ certifikačných služieb mohol do kvalifikovaného certifikátu uviesť obmedzenia využitia tohto certifikátu pod podmienkou, že tieto obmedzenia sú zistiteľné tretími osobami. Poskytovateľ certifikačných služieb nebude zodpovedať za škodu vzniknutú využitím kvalifikovaného certifikátu, ktoré presiahne obmedzenia v ňom uvedené.

4. Členské štáty zabezpečia, aby poskytovateľ certifikačných služieb mohol uviesť v kvalifikovanom certifikáte obmedzenie hodnoty transakcií, na ktoré certifikát možno využiť, pod podmienkou, že toto obmedzenie je zistiteľné tretími osobami.

Poskytovateľ certifikačných služieb nebude zodpovedať za škodu vzniknutú tým, že bola prekročená maximálna medza.

5. Ustanovenia odsekov 1 až 4 nemajú vplyv na smernicu Rady 93/13/EHS z 5. apríla 1993 o neprimeraných podmienkach v spotrebiteľských zmluvách ⁽¹⁾.

Článok 7

Medzinárodné aspekty

1. Členské štáty zabezpečia, aby certifikáty, ktoré ako kvalifikované certifikáty pre verejnosť vydal poskytovateľ certifikačných služieb v tretej krajine, boli uznávané ako právne rovnocenné s certifikátmi, ktoré vydal poskytovateľ certifikačných služieb zriadený v spoločenstve, ak:

- poskytovateľ certifikačných služieb spĺňa podmienky uvedené v tejto smernici a je akreditovaný v rámci programu dobrovoľnej akreditácie, zavedeného v členskom štáte, alebo
- poskytovateľ certifikačných služieb založený v spoločenstve, ktorý spĺňa podmienky uvedené v tejto smernici, za certifikát ručí alebo
- certifikát alebo poskytovateľ certifikačných služieb je uznaný podľa bilaterálnej alebo multilaterálnej dohody medzi spoločenstvom a tretími krajinami alebo medzinárodnými organizáciami.

2. Na uľahčenie cezhraničných certifikačných služieb s tretími krajinami a právneho uznávania zdokonalených elektronických podpisov pochádzajúcich z tretích krajín Komisia, tam, kde je to vhodné, vypracuje návrhy, aby sa dosiahla účinná implementácia noriem a medzinárodných dohôd aplikovateľných na certifikačné služby. Najmä a podľa potreby predloží Rade návrhy vhodných mandátov na rokovanie o bilaterálnych a multilaterálnych dohodách s tretími krajinami a s medzinárodnými organizáciami. Rada rozhodne kvalifikovanou väčšinou.

3. Vždy, keď Komisia dostane informácie o akýchkoľvek ťažkostiach, s ktorými sa stretli podniky spoločenstva, pokiaľ ide o prístup na trh v tretích krajinách, môže v prípade potreby predložiť Rade návrh vhodného mandátu na rokovanie o porovnateľných právach pre podniky spoločenstva v týchto tretích krajinách. Rada rozhodne kvalifikovanou väčšinou.

Opatrenia prijaté podľa tohto odseku nemajú vplyv na povinnosti spoločenstva a členských štátov podľa príslušných medzinárodných dohôd.

Článok 8

Ochrana dát

1. Členské štáty zabezpečia, aby poskytovatelia certifikačných služieb a národné orgány zodpovedné za akreditáciu alebo dohľad spĺňali požiadavky uvedené v smernici Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane osobnosti s ohľadom na spracovanie osobných dát a o voľnom pohybe takých dát ⁽²⁾.

2. Členské štáty zabezpečia, aby poskytovateľ certifikačných služieb, ktorý vydáva certifikáty pre verejnosť, smel zhromažďovať osobné dáta len priamo od subjektu dát alebo s výslovným súhlasom subjektu dát a len v rozsahu, aký je potrebný na účely vydania a udržiavania certifikátu v platnosti. Dáta sa nesmú zhromažďovať alebo spracúvať na iný účel bez výslovného súhlasu subjektu dát.

3. Bez vplyvu na právny účinok, ktorý majú pseudonymy podľa vnútroštátnych právnych predpisov, členské štáty nebudú brániť poskytovateľom certifikačných služieb, aby v certifikáte uvádzali namiesto mena signatára jeho pseudonym.

Článok 9

Výbor

1. Komisii bude pomáhať „Výbor pre elektronický podpis“ (*Electronic-Signature Committee*), ďalej len „výbor“.

2. Pri odkazoch na tento odsek, platia vždy články 4 a 7 rozhodnutia 1999/468/ES, s prihliadnutím na ustanovenia článku 8 citovaného rozhodnutia.

Lehota uvedená v článku 4 ods. 3 rozhodnutia 1999/468/EC bude tri mesiace.

3. Výbor schváli svoje vlastné pravidlá postupu.

Článok 10

Úlohy výboru

Výbor vyjasní požiadavky uvedené v prílohách tejto smernice, kritériá, na ktoré sa odvoláva článok 3 ods. 4, a všeobecne uznávané normy pre elektronické podpisové produkty, stanovené a uverejnené podľa článku 3 ods. 5, v súlade s postupom uvedeným v článku 9 ods. 2

⁽¹⁾ Ú. v. ES L 95, 21.4.1993, s. 29.

⁽²⁾ Ú. v. ES L 281, 23.11.1995, s. 31.

Článok 11

Oznamovanie

1. Členské štáty oznámia Komisii a ostatným členským štátom nasledujúce:

- a) informácie o národných dobrovoľných akreditačných programoch, vrátane všetkých dodatočných požiadaviek podľa článku 3 ods. 7;
- b) mená a adresy národných orgánov zodpovedných za akreditáciu a dohľad, ako aj orgánov podľa článku 3 ods. 4;
- c) mená a adresy všetkých akreditovaných národných poskytovateľov certifikačných služieb.

2. Všetky informácie, dodané podľa odseku 1, a zmeny týchto informácií členské štáty oznamujú bezodkladne.

Článok 12

Kontrola

1. Komisia bude kontrolovať vykonanie tejto smernice a podá o ňom správu Európskemu parlamentu a Rade najneskôr do 19. júla 2003.

2. Kontrola okrem iného posúdi, či by sa rozsah tejto smernice nemal upraviť so zreteľom na vývoj technológie, trhu a práva. Na základe získaných skúseností bude správa obsahovať najmä posúdenie aspektov harmonizácie. Podľa potreby bude správa doplnená legislatívnymi návrhmi.

Článok 13

Implementácia

1. Členské štáty prijímajú zákony, iné právne predpisy a správne opatrenia, ktoré budú v súlade s touto smernicou do 19. júla 2001. Bez odkladu o tom budú informovať Komisiu.

Keď členské štáty schvália tieto opatrenia, budú obsahovať odkaz na túto smernicu alebo budú sprevádzané takýmto odkazom pri príležitosti ich oficiálneho zverejnenia. Členské štáty stanovia metódy takéhoto odkazu.

2. Členské štáty oznámia Komisii text hlavných ustanovení domáceho práva, ktoré schvália v oblasti upravenej touto smernicou.

Článok 14

Platnosť

Táto smernica nadobudne platnosť v deň uverejnenia v *Úradnom vestníku Európskych spoločenstiev*.

Článok 15

Adresáti

Táto smernica je adresovaná členským štátom.

V Bruseli 13. decembra 1999

Za Európsky parlament

prezident

N. FONTAINE

Za Radu

prezident

S. HASSI

PRÍLOHA I

Požiadavky na kvalifikované certifikáty

Kvalifikované certifikáty musia obsahovať:

- a) označenie, že certifikát sa vydáva ako kvalifikovaný certifikát;
- b) identifikačné údaje poskytovateľa certifikačnej služby a štát, v ktorom je zriadený;
- c) meno alebo pseudonym signatára, ktorý bude identifikovaný ako taký;
- d) ustanovenie o osobitnom atribúte signatára, ktoré sa zahrnie, ak je relevantné, v závislosti od účelu, na ktorý je certifikát určený;
- e) dáta na overenie podpisu, zodpovedajúce dátam na vytvorenie podpisu, ktorých držiteľom je signatár;
- f) označenie začiatku a konca platnosti certifikátu;
- g) identifikačný kód certifikátu;
- h) zdokonalený elektronický podpis poskytovateľa certifikačných služieb, ktorý ho vydal;
- i) obmedzenia rozsahu použitia certifikátu, pokiaľ je to potrebné, a
- j) obmedzenia hodnoty transakcií, na ktoré certifikát možno použiť, pokiaľ je to potrebné.

PRÍLOHA II

Požiadavky na poskytovateľov certifikačných služieb, vydávajúcich kvalifikované certifikáty

Poskytovatelia certifikačných služieb musia:

- a) preukázať spoľahlivosť potrebnú na poskytovanie certifikačných služieb;
- b) zabezpečiť prevádzku rýchleho a bezpečného adresára a bezpečnú a okamžitú zrušovaciu službu;
- c) zabezpečiť, aby bolo možné presne určiť dátum a čas vydania alebo zrušenia certifikátu;
- d) v súlade s vnútroštátnymi právnymi predpismi vhodnými prostriedkami overovať totožnosť a prípadne všetky špecifické atribúty osoby, ktorej sa kvalifikovaný certifikát vydáva;
- e) zamestnávať personál, ktorý má pre poskytované služby potrebné odborné vedomosti, prax a kvalifikáciu, najmä spôsobilosť na manažérskej úrovni, odborné znalosti o technológii elektronického podpisovania a je oboznámený s vhodnými bezpečnostnými postupmi; musí tiež používať administratívne a riadiace postupy, ktoré sú primerané a zodpovedajú uznávaným normám;
- f) využívať dôveryhodné systémy a produkty, ktoré sú chránené proti úpravám a zabezpečujú technickú a kryptografickú bezpečnosť nimi podporovaného procesu;
- g) prijať opatrenia proti falšovaniu certifikátov a v prípadoch, keď poskytovateľ certifikačných služieb dáta na vytvorenie podpisu generuje, ručiť za utajenie počas procesu generovania takýchto dát;
- h) udržiavať dostatočné finančné zdroje na prevádzku v súlade s požiadavkami uvedenými v tejto smernici, najmä znášať riziko zodpovednosti za škody, napr. primeraným poistením sa;
- i) zaznamenávať všetky relevantné informácie, týkajúce sa kvalifikovaného certifikátu počas primeranej doby, najmä na zabezpečenie dôkazov o certifikácii na účely súdneho konania. Takú evidenciu možno viesť elektronicky;
- j) neukladať ani nekopírovať dáta na vytvorenie podpisu osoby, ktorej poskytovateľ certifikačných služieb poskytol kľúčové manažérske služby;
- k) pred uzavretím zmluvného vzťahu s osobou, ktorá žiada o certifikát na podporu svojho elektronického podpisu, informovať túto osobu trvanlivými komunikačnými prostriedkami o presných podmienkach využívania certifikátu, vrátane všetkých obmedzení jeho použitia, existencie dobrovoľného akreditačného programu a postupov pri sťažnostiach a urovnávaní sporov. Takéto informácie, ktoré možno poslať elektronicky, musia byť písomné a ľahko pochopiteľné. Dôležité časti týchto informácií musia byť na vyžiadanie dostupné tiež tretím osobám, spoliehajúcim sa na certifikát;
- l) využívať spoľahlivé systémy na ukladanie certifikátov v overiteľnej forme tak, aby:
 - zápisy a zmeny mohli robiť len oprávnené osoby,
 - pravosť informácií bolo možné skontrolovať,
 - certifikáty boli na prezeranie verejne dostupné len v prípadoch, keď dal na to súhlas držiteľ certifikátu, a
 - operátorovi boli zrejme akékoľvek technické zmeny, ktoré ohrozujú tieto bezpečnostné požiadavky.

PRÍLOHA III

Požiadavky na bezpečné zariadenia na vytvorenie podpisu

1. Bezpečné zariadenia na vytvorenie podpisu musia vhodnými technickými a procedurálnymi prostriedkami zabezpečovať aspoň, aby:
 - a) dáta na vytvorenie podpisu, použité na vygenerovanie podpisu, sa mohli vyskytnúť prakticky iba jedenkrát a aby bolo primerane zabezpečené ich utajenie;
 - b) dáta na vytvorenie podpisu, použité na vygenerovanie podpisu, sa s rozumnou mierou istoty nedali odvodiť a podpis bol chránený proti falšovaniu s využitím v súčasnosti dostupnej technológii;
 - c) dáta na vytvorenie podpisu, použité na vygenerovanie podpisu, oprávnený signatár spoľahlivo chránil proti využitiu inými.
 2. Bezpečné zariadenia na vytvorenie podpisu nesmú pozmeniť dáta, ktoré majú byť podpísané, alebo zabrániť ich zobrazeniu signatárovi skôr, ako sa začne proces podpisovania.
-

PRÍLOHA IV

Odporúčania pre bezpečné overovanie podpisu

Počas procesu overovania podpisu by malo byť s primeranou istotou zabezpečené, aby:

- a) dáta použité na overenie podpisu korešpondovali s dátami zobrazenými pre overovateľa;
 - b) podpis bol spoľahlivo overený a výsledok takéhoto overenia sa správne zobrazil;
 - c) overovateľ mohol podľa potreby spoľahlivo potvrdiť obsah podpísaných dát;
 - d) pravosť a platnosť požadovaného certifikátu v čase overenia podpisu bola spoľahlivo overená;
 - e) výsledok overovania a totožnosť signatára boli správne zobrazené;
 - f) zreteľne bolo uvedené použitie pseudonymu a
 - g) všetky zmeny významné z hľadiska bezpečnosti bolo možné zistiť.
-