

## SMĚRNICE 1999/ 93/EC EVROPSKÉHO PARLAMENTU A RADY

ze dne 13. prosince 1999

o zásadách Společenství pro elektronické podpisy

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na čl. 47 odst. 2, články 55 a 95 této smlouvy,

s ohledem na návrh Komise<sup>1</sup>,

s ohledem na stanovisko Hospodářského a sociálního výboru<sup>2</sup>,

s ohledem na stanovisko Výboru regionů<sup>3</sup>,

v souladu s postupem podle článku 251 Smlouvy<sup>4</sup>,

vzhledem k tomu, že

- (1) Komise předložila dne 16. dubna 1997 Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů sdělení o evropské iniciativě v oblasti elektronického obchodu;
- (2) Komise předložila dne 8. října 1997 Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů sdělení nazvané „O zajištění bezpečnosti a důvěryhodnosti elektronické komunikace - K evropským zásadám pro digitální podpisy a šifrování“;
- (3) dne 1. prosince 1997 Rada vyzvala Komisi, aby co nejdříve předložila návrh směrnice Evropského parlamentu a Rady o digitálních podpisech;
- (4) elektronická komunikace a obchod vyžadují „elektronické podpisy“ a s nimi související služby umožňující autentizaci dat; rozdíly v předpisech členských států týkajících se právního uznání elektronických podpisů a akreditace poskytovatelů certifikačních služeb by mohly vytvořit vážnou překážku používání elektronické komunikace a elektronického obchodu; vytvoření jasného rámce Společenství, který upraví podmínky vztahující se k elektronickým podpisům, posílí důvěru v nové technologie a jejich obecné uznání; legislativa členských států by neměla bránit volnému pohybu zboží a služeb na vnitřním trhu;
- (5) měla by být podporována interoperabilita produktů elektronického podpisu; v souladu s článkem 14 Smlouvy tvoří vnitřní trh oblast bez vnitřních hranic, v jejímž v rámci je zajištěn volný pohyb zboží; musí být splněny základní požadavky, jež jsou specifické v oblasti produktů elektronického podpisu, aby byl zajištěn volný pohyb v rámci vnitřního trhu a vybudována důvěra v elektronické podpisy, aniž by tím bylo dotčeno Nařízení Rady (ES) č. 3381/94 z 19. prosince 1994, kterým se stanoví zásady

<sup>1</sup> Úř. věst. č. C 325, 23.10.1998, s. 5.

<sup>2</sup> Úř. věst. č. C 40, 15.2.1999, s. 29.

<sup>3</sup> Úř. věst. č. C 93, 6.4.1999, s. 33.

<sup>4</sup> Stanovisko Evropského parlamentu ze dne 13. ledna 1999 (Úř. věst. č. C 104, 14.4.1999, s. 49), společné stanovisko Rady ze dne 28. června 1999 (Úř. věst. č. C 243, 27.8.1999, s. 33) a Rozhodnutí Evropského parlamentu ze dne 27. října 1999 (doposud nepublikováno v Úředním věstníku).

Společenství pro kontrolu vývozu zboží dvojího užití<sup>5</sup> a Rozhodnutí Rady 94/942/CFSP z 19. prosince 1994 o společném postupu přijatém Radou týkajícím se kontroly vývozu zboží dvojího užití<sup>6</sup>;

- (6) tato směrnice neharmonizuje opatření týkající se služeb v oblasti důvěrných informací, které se řídí právními předpisy o veřejném pořádku nebo veřejné bezpečnosti jednotlivých členských států;
- (7) vnitřní trh zajišťuje volný pohyb osob a v důsledku toho občané členských států ES a jiné osoby zde sídlící stále častěji jednají s orgány jiných členských států; dostupnost elektronické komunikace by v tomto ohledu mohla být velice užitečná ;
- (8) rychlý technický rozvoj a globální charakter internetu vyžadují přístup otevřený různým technologiím a službám, které umožňují autentizaci dat elektronickou cestou;
- (9) elektronické podpisy budou používány v různých situacích a v různých aplikacích, což povede ke vzniku celé škály nových služeb a produktů souvisejících s elektronickými podpisy nebo je využívajících; definice těchto produktů a služeb by neměla být omezena na vydávání certifikátů a jejich správu, ale měla by také zahrnovat ostatní služby a produkty využívající elektronické podpisy nebo s nimi související, jako jsou registrační služby, služby časových značek, adresářové služby, výpočetní služby nebo poradenství v oblasti elektronických podpisů;
- (10) vnitřní trh umožňuje poskytovatelům certifikační služby rozvíjet přes hraniční činnost, a tak zvyšovat svoji konkurenceschopnost a nabízet spotřebitelům a podnikům nové příležitosti bezpečné výměny informací a obchodování elektronickou cestou bez ohledu na hranice; poskytovatelé by měli mít možnost poskytovat své služby, aniž by byli k této činnosti autorizováni, aby se tak v rámci Společenství podpořilo poskytování certifikačních služeb prostřednictvím otevřených sítí; autorizací se rozumí nejen jakákoliv autorizace, kterou poskytovatel certifikační služby musí získat od vnitrostátních orgánů před tím, než bude oprávněn poskytovat certifikační služby, ale i jakékoli jiné opatření se stejným účinkem;
- (11) dobrovolné akreditační systémy, jejichž cílem je zajištění vyšší úrovně poskytování služeb, mohou poskytovatelům certifikačních služeb nabídnout vhodný rámec pro další rozvoj jejich služeb a pro dosažení úrovně důvěryhodnosti, bezpečnosti a kvality požadované vývojem trhu; uvedené systémy by měly podpořit mezi poskytovateli certifikačních služeb rozvoj „best practice“; mělo by být ponecháno na poskytovatelích certifikačních služeb, zda budou vstupovat do těchto akreditačních systémů a využívat je;
- (12) certifikační služby mohou nabízet buď veřejnoprávní subjekty nebo právnické či fyzické osoby, které jsou založeny v souladu s vnitrostátními právními předpisy; členské státy by neměly bránit poskytovatelům certifikačních služeb, aby působili mimo rámec dobrovolných akreditačních systémů; mělo by být zajištěno, aby tyto akreditační systémy neomezovaly soutěž v oblasti certifikačních služeb;
- (13) členské státy si mohou zvolit způsob, jakým zajistí dohled nad dodržováním této směrnice; tato směrnice nevylučuje vytvoření systému dohledu na bázi soukromého sektoru; tato směrnice nezavazuje poskytovatele certifikačních služeb, aby se nacházeli pod dohledem jakéhokoli platného akreditačního systému;

---

<sup>5</sup> Úř. věst. č. L 367, 31.12.1994, s. 1. Nařízení pozměněné nařízením (ES) č. 837/95 (Úř. věst. č. L 90, 21.4.1995, s. 1).

<sup>6</sup> Úř. věst. č. L 367, 31.12.1994, s. 8. Nařízení pozměněné rozhodnutím 99/193/CFSP (Úř. věst. č. L 73, 19.3.1999, s. 1).

- (14) je důležité, aby bylo dosaženo rovnováhy mezi potřebami spotřebitelů a výrobců;
- (15) příloha III obsahuje požadavky na prostředky pro bezpečné vytváření podpisů tak, aby byla zajištěna funkčnost zaručených elektronických podpisů; nepokrývá celý systém prostředí, ve kterém se tyto prostředky používají; fungování vnitřního trhu vyžaduje, aby Komise a členské státy jednaly rychle a umožnily tak ustanovení subjektů, které budou pověřeny vyhodnocování shody prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III; pro splnění požadavků trhu je nezbytné, aby vyhodnocování shody bylo prováděno včas a efektivně;
- (16) tato směrnice přispívá k používání a k právnímu uznání elektronických podpisů v rámci Společenství; pro elektronické podpisy používané výlučně v systémech, které jsou provozovány na základě dobrovolných dohod uzavřených podle soukromého práva určitým počtem účastníků, není nezbytný regulační rámec; v mezích stanovených vnitrostátními předpisy je nezbytné respektovat svobodu smluvních stran sjednávat si mezi sebou podmínky uznávání elektronických podpisů; měla by být uznána právní účinnost elektronických podpisů používaných v takových systémech a jejich přípustnost jako důkazů v soudním řízení;
- (17) cílem této směrnice není harmonizace vnitrostátních právních předpisů týkajících se smluvních vztahů, zejména uzavírání a realizace smluv, ani jiných náležitostí nesmluvní podstaty týkajících se podpisů; z tohoto důvodu je nezbytné, aby se ustanovení o právních účincích elektronických podpisů nedotkla požadavků na formu, které upravují vnitrostátní právní předpisy pro uzavírání smluv, ani pravidel upravujících místo uzavření smlouvy;
- (18) uchovávání a kopírování dat pro vytváření podpisů by mohlo ohrozit právní platnost elektronických podpisů;
- (19) elektronické podpisy budou používány ve veřejném sektoru uvnitř vnitrostátních orgánů a orgánů Společenství a při komunikaci mezi těmito orgány navzájem a mezi těmito orgány a občany a hospodářskými subjekty, například v oblasti veřejných zakázek, daní, sociálního zabezpečení, zdravotnictví a soudnictví;
- (20) harmonizovaná kritéria týkající se právních účinků elektronických podpisů budou zárukou jednotného právního rámce Společenství; vnitrostátní právní předpisy upravují různé požadavky týkající se právní platnosti vlastnoručních podpisů; pro potvrzení totožnosti osoby, která se elektronicky podepisuje, lze použít certifikáty; zaručené elektronické podpisy založené na kvalifikovaných certifikátech vedou k zajištění vyšší úrovně bezpečnosti; zaručené elektronické podpisy založené na kvalifikovaných certifikátech a vytvořené prostředky pro bezpečné vytváření podpisů lze z právního hlediska považovat za rovnocenné vlastnoručním podpisům pouze za předpokladu, že jsou naplněny požadavky na vlastnoruční podpisy;
- (21) aby došlo k obecnému přijetí elektronických autentizačních metod, je třeba zajistit, aby elektronické podpisy mohly být ve všech členských státech používány jako důkazy v soudním řízení; právní uznání elektronických podpisů by mělo být založeno na objektivních kritériích a nemělo by záviset na autorizaci poskytovatelů certifikačních služeb; vnitrostátní právní předpisy vymezi právní oblasti, ve kterých lze používat elektronické dokumenty a elektronické podpisy; touto směrnicí nejsou dotčeny pravomoci vnitrostátního soudu rozhodovat o souladu s požadavky této směrnice ani vnitrostátní předpisy o volném právním hodnocení důkazů;
- (22) poskytovatelé certifikačních služeb, kteří poskytují certifikační služby veřejnosti, podléhají vnitrostátním právním předpisům o odpovědnosti;

- (23) rozvoj mezinárodního elektronického obchodu vyžaduje uzavírání přes hraničních dohod týkajících se třetích států; pro zajištění interoperability na globální úrovni bude výhodné uzavírat se třetími státy dohody o mnohostranných pravidlech v oblasti vzájemného uznávání certifikačních služeb;
- (24) pro zvýšení důvěry uživatelů v elektronickou komunikaci a elektronický obchod je nezbytné, aby poskytovatelé certifikačních služeb dodržovali právní předpisy o ochraně dat a soukromí jednotlivců;
- (25) ustanovení o používání pseudonymů v certifikátech by neměla bránit členským státům, aby vyžadovaly ověřování totožnosti osob podle vnitrostátních právních předpisů či právních předpisů Společenství;
- (26) opatření nezbytná pro zavedené této směrnice jsou přijímána v souladu s Rozhodnutím Rady 1999/468/ES z 28. června 1999 o postupech pro výkon prováděcích pravomocí svěřených Komisi<sup>7</sup>;
- (27) dva roky po zavedení této směrnice ji Komise přezkoumá, aby se mimo jiné přesvědčila, že vývoj technologií nebo změny v právním prostředí nevytvořily překážky pro dosažení cílů v této směrnici stanovených; Komise by měla přezkoumat vliv na související technické oblasti a předložit zprávu Evropskému parlamentu a Radě;
- (28) V souladu se zásadami subsidiarity a proporcionality uvedenými v článku 5 Smlouvy není možné, aby členské státy samostatně v dostatečné míře dosáhly vytvoření harmonizovaného právního rámce pro používání elektronických podpisů a souvisejících služeb, a je tedy vhodné, aby toho bylo dosaženo v rámci celého Společenství; tato směrnice nestanoví více, než co je nezbytné pro dosažení tohoto cíle,

PŘIJALY TUTO SMĚRNICI:

#### Článek 1

##### Působnost

Účelem této směrnice je umožnit použití elektronických podpisů a přispět k jejich právnímu uznávání. Aby bylo možné zajistit řádné fungování vnitřního trhu, stanovuje tato směrnice právní rámec pro elektronické podpisy a některé certifikační služby.

Tato směrnice se nevztahuje na hlediska spojená s uzavíráním a platností smluv či jiných právních závazků, pokud vnitrostátní právní předpisy nebo právní předpisy Společenství upravují požadavky na jejich formu, touto směrnicí nejsou rovněž dotčena pravidla a omezení, která upravují používání dokumentů a která jsou obsažena ve vnitrostátních právních předpisech či právních předpisech Společenství.

---

<sup>7</sup> OJ L 184, 17. 7. 1999, p. 23.

## Článek 2

### Definice

Pro účely této směrnice:

- (1) „elektronickým podpisem“ se rozumí data v elektronické podobě, která jsou připojena k jiným elektronickým datům nebo jsou s nimi logicky spojena a která slouží jako metoda autentizace;
- (2) „zaručeným elektronickým podpisem“<sup>+</sup> se rozumí elektronický podpis, který splňuje tyto požadavky:
  - (a) je jednoznačně spojen s podepisující osobou;
  - (b) umožňuje identifikovat podepisující osobu;
  - (c) je vytvořen s využitím prostředků, které podepisující osoba může mít plně pod svou kontrolou;
  - (d) je spojen s daty, ke kterým se vztahuje tak, aby bylo možno zjistit jakoukoliv následnou změnu těchto dat;
- (3) „podepisující osobou“ se rozumí jakákoliv osoba, která má prostředek pro vytváření podpisu a která jedná svým jménem nebo jménem jiné fyzické nebo právnické osoby nebo subjektu, který zastupuje;
- (4) „data pro vytváření podpisu“ se rozumí jedinečná data, jako jsou kódy nebo soukromé kryptografické klíče, která podepisující osoba používá k vytváření elektronického podpisu;
- (5) „prostředkem pro vytváření podpisu“ se rozumí konfigurovaný software nebo hardware používaný k implementaci dat pro vytváření podpisu;
- (6) „prostředkem pro bezpečné vytváření podpisu“ se rozumí prostředek pro vytváření podpisu, který splňuje požadavky uvedené v příloze III;
- (7) „data pro ověřování podpisu“ se rozumí data, jako jsou kódy nebo veřejné kryptografické klíče, která se používají pro ověřování elektronického podpisu;
- (8) „prostředkem pro ověřování podpisu“ se rozumí konfigurovaný software nebo hardware používaný k implementaci dat pro ověřování podpisu;
- (9) „certifikátem“ se rozumí elektronické osvědčení, které spojuje data pro ověřování podpisu s určitou osobou a potvrzuje identitu této osoby;
- (10) „kvalifikovaným certifikátem“ se rozumí certifikát, který splňuje požadavky uvedené v příloze I a je vydán poskytovatelem certifikačních služeb, který splňuje požadavky uvedené v příloze II;
- (11) „poskytovatelem certifikačních služeb“ se rozumí subjekt nebo právnická či fyzická osoba, která vydává certifikáty nebo poskytuje jiné služby spojené s elektronickými podpisy;
- (12) „produktům elektronického podpisu“ se rozumí hardware nebo software, nebo jejich součásti, který je určen k tomu, aby jej poskytovatel certifikačních služeb používal pro zajištění služeb vztahujících se k elektronickým podpisům nebo který je určen pro vytváření nebo ověřování elektronických podpisů;

---

<sup>+</sup> V originálu „advanced electronic signature“, pojem „zaručený elektronický podpis“ je použit v zákonu o elektronickém podpisu.

- (13) „dobrovolnou akreditací“ se rozumí jakákoliv autorizace, která stanoví zvláštní práva a povinnosti pro poskytování certifikačních služeb a kterou uděluje na žádost dotčeného poskytovatele certifikačních služeb veřejnoprávní či soukromý subjekt pověřený stanovením těchto práv a povinností a dohledem nad jejich dodržováním, přičemž poskytovatel certifikačních služeb není oprávněn vykonávat práva vyplývající z autorizace, dokud neobdrží rozhodnutí od tohoto subjektu.

### Článek 3

#### Přístup na trh

1. Členské státy nebudou poskytování certifikačních služeb podmiňovat autorizací.
  2. Aniž by tím bylo dotčeno ustanovení odstavce 1, mohou členské státy zavést nebo ponechat v platnosti dobrovolné akreditační systémy, jejichž cílem je zvýšit úroveň zajišťování certifikačních služeb. Veškeré podmínky spojené s těmito systémy musí být objektivní, transparentní, úměrné a nediskriminační. Členské státy nesmí omezovat počet akreditovaných poskytovatelů certifikačních služeb z důvodů, které spadají do působnosti této směrnice.
  3. Každý členský stát zajistí zavedení odpovídajícího systému, který umožní dohled nad poskytovateli certifikačních služeb, kteří vydávají kvalifikované certifikáty pro veřejnost a mají sídlo na jeho území.
  4. Příslušné veřejnoprávní či soukromé subjekty pověřené členskými státy stanoví shodu prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III. V souladu s postupem uvedeným v článku 9 stanoví Komise kritéria, podle nichž členské státy stanoví, zda může být daný subjekt pověřen.
- Rozhodnutí subjektů, které jsou uvedeny v prvním pododstavci, o shodě s požadavky uvedenými v příloze III uznají všechny členské státy.
5. Komise může v souladu s postupem uvedeným v článku 9 stanovit a zveřejnit v Úředním věstníku Evropských společenství referenční čísla obecně uznávaných standardů pro produkty elektronického podpisu. Pokud produkt elektronického podpisu splňuje tyto standardy, předpokládají členské státy, že rovněž existuje shoda s požadavky uvedenými v příloze II, bodě f) a v příloze III.
  6. Členské státy a Komise spolupracují při podpoře rozvoje a používání prostředků pro ověřování podpisu s ohledem na doporučení pro bezpečné ověřování uvedené v příloze IV a v zájmu spotřebitele.
  7. Členské státy mohou používání elektronických podpisů ve veřejnoprávním sektoru podmínit případnými doplňujícími požadavky. Tyto požadavky musí být objektivní, transparentní, úměrné a nediskriminační a musí se vztahovat výlučně na specifické vlastnosti daného použití. Tyto podmínky nesmějí vytvářet překážky pro přes hraniční služby.

## Článek 4

### Zásady vnitřního trhu

1. Každý členský stát bude pro poskytovatele certifikačních služeb se sídlem na svém území a pro služby, které poskytují, uplatňovat vnitrostátní předpisy, které přijme v souladu s touto směrnicí. Členské státy nesmí v oblastech, na které se vztahuje tato směrnice, omezovat poskytování certifikačních služeb pocházejících z jiného členského státu.
2. Členské státy umožní volný oběh produktů elektronického podpisu, které jsou v souladu s touto směrnicí, na vnitřním trhu.

## Článek 5

### Právní účinky elektronických podpisů

1. Členské státy zajistí, aby zaručené elektronické podpisy založené na kvalifikovaných certifikátech a vytvořené pomocí prostředků pro bezpečné vytváření podpisu:
  - (a) splňovaly právní požadavky na podpis ve vztahu k datům v elektronické podobě stejně, jako vlastnoruční podpisy splňují tyto požadavky ve vztahu k datům na papíře;  
a
  - (b) byly přijímány jako důkazy v soudním řízení.
2. Členské státy zajistí, aby elektronickým podpisům nebyla odpírána právní účinnost a aby nebyly odmítány jako důkazy v soudním řízení pouze z toho důvodu, že:
  - jsou v elektronické podobě, nebo
  - nejsou založeny na kvalifikovaném certifikátu, nebo
  - nejsou založeny na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb, nebo
  - nejsou vytvořeny pomocí prostředku pro bezpečné vytváření podpisu.

## Článek 6

### Odpovědnost

1. Členské státy zajistí, aby poskytovatel certifikačních služeb, který vydá pro veřejnost certifikát jako kvalifikovaný certifikát nebo který se veřejnosti za takový certifikát zaručí, byl odpovědný za škodu způsobenou jakémukoliv subjektu nebo právnické či fyzické osobě, která se na tento certifikát důvodně spoléhá, a to přinejmenším:
  - (a) pokud jde o přesnost veškerých informací obsažených v kvalifikovaném certifikátu v době jeho vydání a o uvedení veškerých předepsaných údajů pro kvalifikovaný certifikát;
  - (b) pokud jde o ujištění, že v době vydání certifikátu měla podepisující osoba uvedená v kvalifikovaném certifikátu data pro vytváření podpisu odpovídající datům pro ověřování podpisu, která jsou uvedena v certifikátu nebo z něj identifikovatelná;

- (c) pokud jde o ujištění, že data pro vytváření podpisu a data pro ověřování podpisu mohou být použita doplňujícím způsobem v těch případech, kdy poskytovatel certifikačních služeb generuje oboje tato data;

ledaže poskytovatel certifikačních služeb prokáže, že nejednal nedbale.

2. Členské státy přinejmenším zajistí, aby poskytovatel certifikačních služeb, který vydá certifikát jako kvalifikovaný certifikát, byl odpovědný za škody způsobené kterémukoliv subjektu nebo právnické či fyzické osobě, které se na tento certifikát důvodně spoléhají, pokud opomene zaregistrovat revokaci certifikátu, ledaže poskytovatel certifikačních služeb prokáže, že nejednal nedbale.

3. Členské státy zajistí, aby poskytovatel certifikačních služeb mohl v kvalifikovaném certifikátu uvést omezení pro jeho použití za předpokladu, že omezení je rozpoznatelné třetími stranami. Poskytovatel certifikačních služeb není odpovědný za škody vyplývající z použití kvalifikovaného certifikátu, které přesahuje omezení v něm uvedená.

4. Členské státy zajistí, aby poskytovatel certifikačních služeb mohl v kvalifikovaném certifikátu uvést omezení hodnoty transakce, pro kterou lze certifikát použít za předpokladu, že omezení je rozpoznatelné třetími stranami.

Poskytovatel certifikačních služeb není odpovědný za škody vyplývající z překročení tohoto maximálního omezení.

5. Ustanovením odstavců 1 až 4 není dotčena Směrnice Rady 93/13/EHS z 5. dubna 1993 o nerovných podmínkách ve spotřebitelských smlouvách (o zneužití postavení ve spotřebitelských smlouvách)<sup>8</sup>.

## Článek 7

### Mezinárodní hlediska

1. Členské státy zajistí, aby certifikáty, které poskytovatel certifikačních služeb se sídlem ve třetím státu vydá jako kvalifikované certifikáty, byly uznávány jako právně rovnocenné certifikátům vydaným poskytovatelem certifikačních služeb se sídlem ve Společenství, pokud:

- (a) poskytovatel certifikačních služeb splňuje podmínky uvedené v této směrnici a byl akreditován v rámci dobrovolného akreditačního systému ustanoveného v členském státě; nebo
- (b) poskytovatel certifikačních služeb se sídlem ve Společenství, který splňuje podmínky uvedené v této směrnici, se za tento certifikát zaručí; nebo
- (c) certifikát nebo poskytovatel certifikačních služeb je uznáván na základě dvoustranné nebo mnohostranné dohody mezi Společenstvím a třetími státy nebo mezinárodními organizacemi.

2. S cílem usnadnit přes hraniční certifikační služby s třetími státy a právní uznání zaručených elektronických podpisů pocházejících ze třetích států učiní Komise v oblastech, kde je to vhodné, návrhy vedoucí k efektivní implementaci standardů a mezinárodních dohod vztahujících se k certifikačním službám. V případě potřeby předloží Radě návrhy na

---

<sup>8</sup> Úř. věst. č. L 95, 21.4.1993, s. 29.



odpovídající zmocnění pro jednání o dvoustranných a mnohostranných dohodách se třetími státy a mezinárodními organizacemi. Rada rozhoduje kvalifikovanou většinou.

3. Kdykoliv bude Komise informována o obtížích s přístupem na trh třetích států, může předložit Radě návrhy na udělení odpovídajícího zmocnění pro vyjednávání srovnatelných práv pro působení Společenství v těchto třetích státech. Rada se usnáší kvalifikovanou většinou.

Opatřeními přijatými v souladu s tímto odstavcem nebudou dotčeny závazky Společenství a členských států vyplývající z příslušných mezinárodních dohod.

## Článek 8

### Ochrana dat

1. Členské státy zajistí, aby poskytovatelé certifikačních služeb a vnitrostátní subjekty odpovědné za akreditaci nebo dohled plnily požadavky stanovené ve směrnici Evropského parlamentu a Rady 95/46/ES z 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů<sup>9</sup>.

2. Členské státy zajistí, aby poskytovatel certifikačních služeb, který vydává certifikáty pro veřejnost, mohl shromažďovat osobní údaje získané pouze přímo od dotčené osoby nebo s jejím výslovným souhlasem a pouze v rozsahu nezbytném pro vydání a správu certifikátu. Pro jiné účely nelze údaje shromažďovat ani zpracovávat bez výslovného souhlasu dotčené osoby.

3. Aniž jsou dotčeny právní účinky přiznané vnitrostátními předpisy pseudonymům, nesmějí členské státy bránit poskytovatelům certifikačních služeb, aby v certifikátu namísto jména podepisující osoby uvedli pseudonym.

## Článek 9

### Výbor

1. Komisi je nápomocen Výbor pro elektronický podpis, dále nazývaný „Výbor“.

2. Odkazuje-li se na toto ustanovení, použijí se články 4 a 7 Rozhodnutí 1999/468/ES s ohledem na článek 8 uvedeného rozhodnutí.

Doba uvedená v čl. 4 odst. 3 Rozhodnutí 1999/468/ES je tři měsíce.

3. Výbor přijme svůj jednací řád.

## Článek 10

### Cíle výboru

Výbor objasní požadavky uvedené v přílohách této směrnice, kritéria uvedená v čl. 3 odst. 4 a všeobecně uznávané standardy pro produkty elektronického podpisu stanovené a zveřejněné v souladu s čl. 3 odst. 5, a to v souladu s postupem uvedeným v čl. 9 odst. 2.

---

<sup>9</sup> Úř. věst. č. L 281, 23.11.1995, s. 31.

## Článek 11

### Oznámení

1. Členské státy oznámí Komisi a ostatním členským státům:
  - (a) informace o dobrovolných akreditačních systémech na vnitrostátní úrovni, včetně veškerých doplňujících požadavků podle čl. 3 odst. 7;
  - (b) názvy a sídla vnitrostátních orgánů odpovědných za akreditaci a dohled, jakož i subjektů uvedených v čl. 3 odst. 4;
  - (c) názvy a sídla všech vnitrostátních akreditovaných poskytovatelů certifikačních služeb.
2. Členské státy oznámí veškeré informace uvedené v odstavci 1 co nejdříve, což platí i pro případné změny.

## Článek 12

### Přezkoumání

1. Komise přezkoumá působení této směrnice a podá o něm zprávu Evropskému parlamentu a Radě nejpozději do 19. července 2003.
2. V rámci přezkoumání lze mimo jiné stanovit, zda je vhodné změnit působnost této směrnice s přihlédnutím k rozvoji techniky, trhu a právního rámce. Zpráva bude obsahovat na základě získaných zkušeností zejména zhodnocení hledisek týkajících se harmonizace. V případě potřeby budou ke zprávě připojeny legislativní návrhy.

## Článek 13

### Realizace

1. Členské státy uvedou v účinnost právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději do 19. července 2001. Neprodleně o nich uvědomí Komisi.  
Tato opatření přijatá členskými státy musí obsahovat odkaz na tuto směrnici anebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.
2. Členské státy sdělí Komisi znění nejdůležitějších ustanovení vnitrostátních právních předpisů, které přijmou v oblasti působnosti této směrnice.

## Článek 14

### Nabytí účinnosti

Tato směrnice nabývá účinnosti dnem vyhlášení v *Úředním věstníku Evropských společenství*.

## Článek 15

### Určení

Tato směrnice je určena členskými státy.

V Bruselu dne 13. prosince 1999

Za Evropský parlament  
předseda

N. Fontaine

Za Radu  
předseda

S. Hassi

## PŘÍLOHA I

### Požadavky na kvalifikované certifikáty

Kvalifikované certifikáty musí obsahovat:

- (a) označení, že certifikát je vydán jako kvalifikovaný certifikát;
- (b) označení poskytovatele certifikačních služeb a státu, ve kterém má poskytovatel sídlo;
- (c) jméno podepisující osoby nebo pseudonym, který je jako takový označen;
- (d) zvláštní znaky podepisující osoby, pokud jsou důležité pro účel, pro nějž je certifikát určen;
- (e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, která jsou pod kontrolou podepisující osoby;
- (f) označení počátku a konce doby platnosti certifikátu;
- (g) identifikační kód certifikátu;
- (h) zaručený elektronický podpis poskytovatele certifikačních služeb, který certifikát vydává;
- (i) případně omezení použitelnosti certifikátu; a
- (j) případně omezení hodnot transakcí, pro něž lze certifikát použít.

## PŘÍLOHA II

### Požadavky na poskytovatele certifikačních služeb, kteří vydávají kvalifikované certifikáty

Poskytovatelé certifikačních služeb musí:

- (a) prokázat spolehlivost nezbytnou pro poskytování certifikačních služeb;
- (b) zajistit provozování rychlého a bezpečného seznamu a bezpečné a okamžité revokační služby;
- (c) zajistit, aby datum a čas, kdy je certifikát vydán nebo revokován, mohly být přesně určeny;
- (d) ověřit odpovídajícími prostředky v souladu s vnitrostátními právními předpisy totožnost a případně zvláštní znaky osoby, které je kvalifikovaný certifikát vydáván;
- (e) zaměstnávat personál, který má odborné znalosti, zkušenosti a kvalifikaci nezbytné pro poskytování služeb, zejména schopnosti řízení, odborné znalosti v oblasti technologie elektronických podpisů a důkladnou znalost příslušných bezpečnostních postupů; rovněž musí používat adekvátní administrativní a řídicí postupy, které odpovídají uznávaným standardům a jsou s nimi ve shodě;
- (f) používat důvěryhodné systémy a produkty, které jsou chráněny proti modifikacím, a zajistit technickou a kryptografickou bezpečnost postupů, které tyto systémy a produkty podporují;
- (g) přijmout opatření proti padělání certifikátů a pokud poskytovatel certifikačních služeb generuje data pro vytváření podpisu, zajistit jejich utajení v průběhu generování těchto dat;
- (h) mít k dispozici dostatečné finanční zdroje na provoz v souladu s požadavky uvedenými v této směrnici, a zejména k tomu, aby mohl nést odpovědnost za vzniklé škody, např. uzavřením vhodného pojištění;
- (i) zaznamenávat veškeré informace vztahující se ke kvalifikovaným certifikátům a uchovávat je po přiměřenou dobu, především pro potřeby poskytnutí důkazu o certifikaci pro účely soudního řízení. Záznamy mohou být v elektronické podobě;
- (j) neuchovávat ani nekopírovat data pro vytváření podpisu osoby, které poskytovatel certifikačních služeb poskytl službu klíčového hospodářství;
- (k) před uzavřením smluvního vztahu s osobou, která požaduje certifikát na podporu svého elektronického podpisu, informovat tuto osobu pomocí komunikačních prostředků umožňujících trvalý dálkový přístup o přesných lhůtách a podmínkách použití certifikátu, včetně veškerých omezení stanovených pro jeho použití, o existenci dobrovolného akreditačního systému a o postupech při řešení reklamací a sporů. Tyto informace, které lze předat elektronickou cestou, musí mít písemnou podobu a musí být ve snadno srozumitelném jazyce. Příslušné části těchto informací musí být na vyžádání k dispozici třetím stranám, které se spoléhají na tento certifikát;
- (l) používat důvěryhodný systém pro uchovávání certifikátů v ověřitelné podobě takovým způsobem, aby:
  - vstupy a změny mohly provádět pouze pověřené osoby,
  - bylo možno kontrolovat autentičnost informací,

- certifikáty byly veřejně přístupné pro vyhledávání pouze tehdy, pokud k tomu držitel certifikátu poskytl souhlas,

a

- operátorovi byly zjevné jakékoliv technické změny porušující tyto bezpečnostní požadavky .

### **PŘÍLOHA III**

#### **Požadavky na prostředek pro bezpečné vytváření podpisu**

1. Prostředky pro bezpečné vytváření podpisu musí vhodnými technickými prostředky a postupy přinejmenším zajistit, aby:

- (a) se data pro vytváření podpisu používaná pro generování podpisu mohla vyskytnout pouze jedenkrát a aby bylo dostatečně zajištěno jejich utajení;
- (b) bylo dostatečně zajištěno, že data pro vytváření podpisu používaná pro generování podpisu nelze odvodit a že podpis je chráněn současnou dostupnou technologií proti padělání ;
- (c) podepisující osoba měla možnost svá data pro vytváření podpisu používaná pro generování podpisu spolehlivě chránit proti jejich zneužití třetí osobou.

2. Prostředky pro bezpečné vytváření podpisu nesmějí měnit data, která mají být podepsána, ani bránit tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.

### **PŘÍLOHA IV**

#### **Doporučení pro bezpečné ověřování podpisu**

V průběhu procesu ověřování podpisu by s dostatečnou jistotou mělo být zajištěno, aby:

- (a) data používaná pro ověřování podpisu odpovídala datům zobrazeným ověřovateli;
- (b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl správně zobrazen;
- (c) ověřovatel mohl, podle potřeby, spolehlivě zjistit obsah podepsaných dat;
- (d) bylo možno spolehlivě ověřit pravost a platnost certifikátu nezbytného v době ověřování podpisu;
- (e) výsledek ověření a identita podepisující osoby byly správně zobrazeny;
- (f) použití pseudonymu bylo jasně označeno; a
- (g) všechny změny ovlivňující bezpečnost mohly být odhaleny.