51. schôdza
1. čít.

NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY

II. volebné obdobie

Číslo: 928/2001

R-1081 – ÚPV
– Financie
23.4.2001 – Hospod. –9
– Verej. správa
– Obrana

T: 11. a 12. 6. 2001

984

Návrh

skupiny poslancov Národnej rady Slovenskej republiky

na vydanie

zákona o elektronickom podpise

Predkladajú:

František	Šebej	v. r.
Peter	Kresák	v. r.
Peter	Tatár	v. r.
Pál	Farkas	v. r.
Branislav	Orava	v. r.
Peter	Osuský	v. r.
Milan	Ištván	v. r.
Ján	Langoš	v. r.
Pavol	Prokopovič	v. r.
László	Gyurovszky	v. r.

Návrh uznesenia:

Národná rada Slovenskej republiky
schvaľuje
návrh skupiny poslancov Národnej rady Slovenskej republiky na vydanie zákona o elektronickom podpise

Bratislava apríl 2001

19. aprila 2001

NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY

II. volebné obdobie

Číslo: 928/2001

984

Návrh

skupiny poslancov Národnej rady Slovenskej republiky

na vydanie

zákona o elektronickom podpise

Predkladajú:

František	Šebej	v. r.
Peter	Kresák	v. r.
Peter	Tatár	v. r.
Pál	Farkas	v. r.
Branislav	Orava	v. r.
Peter	Osuský	v. r.
Milan	István	v. r.
Ján	Langoš	v. r.
Pavol	Prokopovič	v. r.
László	Gyurovszky	v. r.

Návrh uznesenia:

Národná rada Slovenskej republiky
schvaľuje
návrh skupiny poslancov Národnej rady Slovenskej republiky na vydanie zákona o elektronickom podpise

Bratislava apríl 2001

Z á k o n č. ...

z 2001

o elektronickom podpise

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

PRVÁ ČASŤ
ZÁKLADNÉ USTANOVENIA

§ 1
Predmet zákona

(1) Tento zákon upravuje
   (a) vzťahy vznikajúce v súvislosti s vytváraním a používaním elektronického podpisu v rámci elektronickej komunikácie,
   (b) práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu v rámci elektronickej komunikácie,
   (c) ochranu a hodnovernosť elektronických dokumentov podpísaných elektronickým podpisom.

(2) Tento zákon sa nevzťahuje na vyhotovenie a používanie elektronického podpisu pre utajované skutočnosti podľa osobitného zákona[1].

(3) Ustanovenia tohto zákona sa nevzťahujú na vyhotovenie a používanie elektronického podpisu v uzavretých systémoch.

§ 2
Účel zákona

Účelom zákona je:
   (a) umožniť využívanie elektronických podpisov a ich právne uznanie,
   (b) vytvoriť právny rámec pre tvorbu a využívanie elektronických podpisov s cieľom zabezpečiť funkčnosť vnútorného a medzinárodného trhu a urýchlenie administratívy,
   (c) ustanoviť podmienky pre vydávanie, používanie a správu certifikátov, vymedziť právne postavenie certifikačných autorít,
   (d) upraviť podmienky štátnej regulácie certifikačných činností,
   (e) upraviť postavenie a pôsobnosť orgánu štátnej správy, Úradu pre elektronický podpis (ďalej len Úrad) pri vykonávaní certifikačných činností,
   (f) ustanoviť podmienky výkonu kontroly certifikačných činností,
   (g) ustanoviť sankcie za porušenie zákona.

VYMEDZENIE NIEKTORÝCH POJMOV

§ 3

Na účely tohto zákona sa rozumie:

(1) pod *dokumentom* ľubovoľná konečná neprázdna postupnosť znakov. Pod *digitálnym dokumentom* sa rozumie digitálne (číselne) kódovaný dokument. Pod *elektronickým dokumentom* sa rozumie

---

[1] Zákon Národnej rady Slovenskej republiky č. 100/1996 Z. z. o ochrane štátneho tajomstva, služobného tajomstva, šifrovej ochrane informácií a o zmene a doplnení Trestného zákonníka v znení neskorších predpisov.

digitálny dokument uchovávaný na fyzickom nosiči; prenášaný alebo spracovávaný pomocou technických prostriedkov v elektrickej, magnetickej, optickej alebo inej forme.

(2) pod *súkromným kľúčom* tajná informácia, ktorá slúži na vytvorenie elektronického podpisu elektronického dokumentu. K danému súkromnému kľúču existuje verejný kľúč, pričom tento je súkromným kľúčom jednoznačne určený. Súkromný kľúč nie je možné efektívne odvodiť z verejného kľúča.

(3) pod *verejným kľúčom* informácia dostupná overovateľovi, ktorá slúži na overenie správnosti elektronického podpisu vytvoreného pomocou súkromného kľúča prislúchajúceho k danému verejnému kľúču.

(4) pod *prostriedkom na vytvorenie elektronického podpisu* technické zariadenie alebo programové vybavenie alebo algoritmy alebo ich kombinácia prostredníctvom ktorých môže podpisovateľ (na základe elektronického dokumentu a súkromného kľúča podpisovateľa) vytvoriť elektronický podpis elektronického dokumentu.

(5) pod *bezpečným zariadením na vytváranie elektronického podpisu* prostriedok na vytvorenie elektronického podpisu, ktorý spĺňa požiadavky zákona a všeobecne platného právneho predpisu, ktorý vydá Úrad a ktorý slúži na vytváranie zaručených elektronických podpisov.

(6) pod *podpísaným elektronickým dokumentom* elektronický dokument, pre ktorý bol vytvorený elektronický podpis, ak je tento elektronický dokument dostupný spolu s elektronickým podpisom daného dokumentu.

(7) pod *prostriedkom na overenie elektronického podpisu* technické zariadenie, programové vybavenie a algoritmy, prostredníctvom ktorých môže overovateľ (na základe podpísaného elektronického dokumentu a verejného kľúča prislúchajúceho k súkromnému kľúču, ktorý bol použitý na vytvorenie elektronického podpisu) overiť správnosť elektronického podpisu.

(8) pod *uzavretým systémom* systém slúžiaci výlučne pre vlastné potreby jeho účastníkov, ktorý vznikol na základe dohody účastníkov systému a ku ktorému majú prístup len účastníci systému. Uzavretý systém sa riadi vnútornými pravidlami, ktoré nie sú systémom vynútiteľné mimo hraníc systému.

(9) pod *certifikačnou službou* najmä vydávanie certifikátov, rušenie platnosti certifikátov, poskytovanie zoznamu zrušených certifikátov, potvrdzovanie existencie a platnosti certifikátov, vyhľadávanie a poskytovanie vydaných certifikátov, poskytovanie časových pečiatok. Medzi certifikačné služby patria aj expertné, konzultačné a iné služby, ktoré súvisia s elektronickými podpismi.

(10) pod *akreditovanou certifikačnou službou* najmä vydávanie kvalifikovaných certifikátov, rušenie platnosti kvalifikovaných certifikátov, poskytovanie zoznamu zrušených kvalifikovaných certifikátov, potvrdzovanie existencie a platnosti kvalifikovaných certifikátov, vyhľadávanie a poskytovanie vydaných kvalifikovaných certifikátov, vydávanie a overovanie časových pečiatok.

(11) pod *certifikačnou činnosťou* poskytovanie certifikačných služieb, prijímanie žiadosti o vydanie certifikátu, vedenie evidencie, prevádzka potrebných technických zariadení a iná činnosť potrebná na zabezpečenie poskytovania certifikačných služieb.

(12) pod *správou certifikátov* vydávanie, overovanie platnosti, rušenie, archivovanie certifikátov a certifikačné činnosti s tým spojené.

(13) pod *produktami pre elektronický podpis* technické zariadenia a programové vybavenie, alebo ich relevantné časti, ktoré sú určené pre poskytovateľov certifikačných služieb na vykonávanie certifikačných činností, alebo sú určené na vytváranie a overovanie elektronických podpisov.

(14) pod *Úradom pre elektronický podpis* ústredný orgán štátnej správy pre elektronický podpis.

(15) pod *poskytovateľom certifikačných služieb* fyzická alebo právnická osoba, ktorá vykonáva certifikačné činnosti podľa §3 ods. (9) a (11).

(16) pod *certifikačnou autoritou* poskytovateľ certifikačných služieb, ktorý spravuje certifikáty podľa § 3 ods. (12) zákona.

(17) pod *akreditovanou certifikačnou autoritou* certifikačná autorita, ktorá poskytuje akreditované certifikačné služby v súlade s týmto zákonom a všeobecne záväznými predpismi vydanými Úradom, a ktorá má na poskytovanie týchto služieb akreditáciu Úradu.

(18) pod *registračnou autoritou* poskytovateľ certifikačných služieb, ktorý v mene certifikačnej autority vykonáva vybrané certifikačné činnosti a sprostredkováva služby certifikačnej autority držiteľom certifikátov a žiadateľom o vydanie certifikátu.

(19) pod *podpisovateľom* fyzická osoba, ktorá je držiteľom súkromného kľúča a je schopná pomocou tohto kľúča vytvoriť elektronický podpis elektronického dokumentu. Podpisovateľ vytvára elektronický podpis buď vo svojom mene, alebo v mene inej fyzickej alebo právnickej osoby, ktorú zastupuje.

(20) pod *vydavateľom certifikátu* certifikačná autorita alebo Úrad.

(21) pod *držiteľom certifikátu*
   (a) fyzická osoba, ktorej bol certifikačnou autoritou na základe ustanovení tohto zákona vydaný certifikát,
   (b) certifikačná autorita,
   (c) Úrad.

(22) pod *overovateľom elektronického podpisu* fyzická osoba alebo právnická osoba, ktorá pomocou prostriedku na overenie elektronického podpisu, verejného kľúča, podpísaného elektronického dokumentu a elektronického podpisu tohto dokumentu môže overiť platnosť daného elektronického podpisu.

(23) pod *bezpečným zariadením na vytváranie časovej pečiatky* technické zariadenie a programové vybavenie, ktoré spĺňa požiadavky tohto zákona a všeobecne platného právneho predpisu, ktorý vydá Úrad, prostredníctvom ktorého možno (na základe časového údaju, elektronického dokumentu a súkromného kľúča na tento účel určeného) vytvoriť časovú pečiatku daného elektronického dokumentu.

DRUHÁ ČASŤ

§ 4
Elektronický podpis

Elektronický podpis je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá spĺňa nasledujúce požiadavky:
   (a) nie je možné ju (efektívne) vytvoriť bez znalosti súkromného kľúča,
   (b) na základe znalosti tejto informácie a verejného kľúča prislúchajúceho k súkromnému kľúču použitému pri jej vytvorení je možné overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, nebol po jej vytvorení zmenený.

§ 5
Zaručený elektronický podpis

(1) Zaručený elektronický podpis je elektronický podpis fyzickej osoby, elektronický podpis akreditovanej certifikačnej autority a elektronický podpis Úradu, ktorý spĺňa podmienky podľa § 4 tohto zákona a
   (a) je vytvorený pomocou súkromného kľúča, ktorý je na tento účel určený,
   (b) je ho možné vytvoriť len s použitím bezpečného zariadenia na vytváranie elektronického podpisu podľa §3, ods. (5),
   (c) zariadenie na vytvorenie elektronického podpisu fyzickej osoby podľa písm. (b) môže byť pod výlučnou kontrolou podpisovateľa,
   (d) spôsob vytvárania elektronického podpisu akreditovanej certifikačnej autority a elektronického podpisu Úradu umožňuje spoľahlivo určiť, ktorá fyzická osoba je za jeho vytvorenie zodpovedná,
   (e) na verejný kľúč prislúchajúci k súkromnému kľúču použitému na vytvorenie elektronického podpisu bol vydaný kvalifikovaný certifikát v zmysle tohto zákona.

(2) Verejný kľúč prislúchajúci k súkromnému kľúču určenému na vytváranie zaručeného elektronického podpisu Úradu je zverejnený spôsobom, ktorý ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

(3) Zaručený elektronický podpis je platný, ak sú splnené nasledujúce požiadavky:
   (a) existuje kvalifikovaný certifikát verejného kľúča prislúchajúceho k súkromnému kľúču použitému pri vytvorení tohto elektronického podpisu,
   (b) tento kvalifikovaný certifikát je platný alebo je preukázateľné, že bol platný v čase vytvorenia tohto elektronického podpisu,
   (c) elektronický dokument, ku ktorému je elektronický podpis pripojený alebo s ním inak logicky spojený, nebol po vytvorení elektronického podpisu zmenený, čo sa overilo použitím verejného kľúča uvedeného v certifikáte podľa písmena (a).

(4) Formát a spôsob vytvárania zaručeného elektronického podpisu ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

§ 6
Používanie elektronického podpisu

(1) Elektronický podpis sa môže používať bez obmedzenia, ak všeobecne záväzný právny predpis neustanovuje inak.
(2) Ak je v styku s verejnou správou možné používať elektronický podpis, tak tento elektronický podpis musí spĺňať podmienky podľa § 5 tohto zákona.

§ 7
Právne účinky elektronického podpisu

(1) Vytvorenie platného zaručeného elektronického podpisu elektronického dokumentu sa považuje za právny úkon v písomnej forme s právnymi účinkami vlastnoručného podpisu.[2]
(2) Vytvorenie elektronického podpisu, ktorý nie je platným zaručeným elektronickým podpisom podľa § 5 tohto zákona, sa považuje za právny úkon v písomnej forme s právnymi účinkami vlastnoručného podpisu len ak umožňuje zachytenie obsahu právneho úkonu a určenie osoby, ktorá právny úkon urobila.

§ 8
Certifikát

(1) Certifikát je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč je verejným kľúčom toho, komu je certifikát vydaný (držiteľa certifikátu).
(2) Certifikát sa skladá z tela certifikátu a elektronického podpisu tela certifikátu.
(3) Telo certifikátu je elektronický dokument, ktorý obsahuje najmä:
   (a) identifikačné údaje vydavateľa certifikátu,
   (b) identifikačné číslo certifikátu, ktoré je jedinečné medzi certifikátmi vydanými tým istým vydavateľom.
   (c) identifikačné údaje držiteľa certifikátu,
   (d) dátum a čas začiatku a konca platnosti certifikátu,
   (e) verejný kľúč držiteľa certifikátu,
   (f) identifikáciu algoritmov, pre ktoré je uvedený verejný kľúč určený,
   (g) identifikáciu algoritmov použitých pri vytvorení elektronického podpisu tela certifikátu.
(4) Elektronický podpis tela certifikátu je vytvorený vydavateľom certifikátu použitím súkromného kľúča, ktorý je na to určený.
(5) Ako identifikačné údaje držiteľa certifikátu podľa ods. (3), písm. (c) môže byť použitý aj pseudonym, za predpokladu, že na základe pseudonymu a údajov, ktoré certifikačná autorita pri podávaní žiadosti o vydanie certifikátu od žiadateľa získala, je možné jednoznačne určiť totožnosť držiteľa certifikátu. V tomto prípade certifikačná autorita v certifikáte výslovne uvedie, že sa v ňom ako identifikačný údaj držiteľa certifikátu uvádza pseudonym.
(6) Krížový certifikát je certifikát, ktorý vydáva jedna certifikačná autorita na verejný kľúč druhej certifikačnej autority. Vydaním krížového certifikátu umožňuje certifikačná autorita overovať elektronické podpisy založené na certifikátoch, ktoré druhá certifikačná autorita vydala a podpísala pomocou súkromného kľúča prislúchajúceho k verejnému kľúču, ktorý je uvedený v krížovom certifikáte.
(7) Zrušený certifikát je taký certifikát, ktorému certifikačná autorita, ktorá ho spravuje, predčasne ukončila platnosť.

---

[2] § 40 ods. 4 Zák. č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov

§ 9
Kvalifikovaný certifikát

(1) Kvalifikovaný certifikát je certifikát fyzickej osoby, certifikát akreditovanej certifikačnej autority, krížový certifikát akreditovanej certifikačnej autority a certifikát Úradu, ktorý spĺňa podmienky podľa § 8 a § 9, ods. (2), (3) a (4) tohto zákona.

(2) Kvalifikovaný certifikát fyzickej osoby je certifikát, ktorý spĺňa nasledujúce požiadavky:
   (a) je vydaný akreditovanou certifikačnou autoritou fyzickej osobe,
   (b) je v ňom uvedené, že je kvalifikovaný,
   (c) sú v ňom uvedené ohraničenia na použitie tohto certifikátu, ak tretia strana takého ohraničenia rozlišuje,
   (d) sú v ňom uvedené ohraničenia na výšku transakcií, v ktorých je možné certifikát použiť, ak tretia strana takéto ohraničenia rozlišuje,
   (e) elektronický podpis tela certifikátu je zaručeným elektronickým podpisom akreditovanej certifikačnej autority, ktorý bol vytvorený použitím súkromného kľúča, ktorý je na tento účel určený.

(3) Kvalifikovaný certifikát akreditovanej certifikačnej autority je certifikát, ktorý spĺňa nasledujúce požiadavky:
   (a) je vydaný Úradom akreditovanej certifikačnej autorite,
   (b) je v ňom uvedené, že je kvalifikovaný,
   (c) je v ňom uvedený účel, na ktorý je určený,
   (d) elektronický podpis tela certifikátu je zaručeným elektronickým podpisom Úradu.

(4) Kvalifikovaný krížový certifikát akreditovanej certifikačnej autority je krížový certifikát, ktorý spĺňa nasledujúce požiadavky:
   (a) je vydaný akreditovanou certifikačnou autoritou (akreditovanej) certifikačnej autorite,
   (b) je v ňom uvedené že je kvalifikovaný krížový certifikát,
   (c) elektronický podpis tela certifikátu je zaručeným elektronickým podpisom akreditovanej certifikačnej autority.

(5) Kvalifikovaný certifikát Úradu je certifikát, ktorý spĺňa požiadavky podľa ods. (3), písm. (b-d) a je vydaný Úradom na vlastný verejný kľúč Úradu.

(6) Formát a obsah kvalifikovaného certifikátu a požiadavky na správu kvalifikovaných certifikátov ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

(7) Kvalifikovaný certifikát je platný v danom čase, ak sú splnené nasledujúce požiadavky:
   (a) daný čas je medzi začiatkom a koncom platnosti certifikátu,
   (b) zaručený elektronický podpis tela certifikátu je platný,
   (c) certifikát nebol k danému času zrušený.

§ 10
Zoznam zrušených certifikátov

(1) Zoznam zrušených certifikátov je elektronický dokument, ktorým vydavateľ certifikátov, ktorý spravuje tieto certifikáty, oznamuje predčasné ukončenie ich platnosti.

(2) Zoznam zrušených certifikátov sa skladá z tela zoznamu zrušených certifikátov a elektronického podpisu tela zoznamu zrušených certifikátov.

(3) Telo zoznamu zrušených certifikátov je elektronický dokument, ktorý obsahuje najmä:
   (a) identifikačné údaje vydavateľa certifikátov, ktorý spravuje tieto certifikáty,
   (b) dátum a čas vydania zoznamu zrušených certifikátov,
   (c) dátum a čas najneskoršieho vydania ďalšieho zoznamu zrušených certifikátov,
   (d) zoznam identifikačných čísiel certifikátov, ktoré boli zrušené spolu s dátumom a časom ich zrušenia.

(4) Elektronický podpis tela zoznamu zrušených certifikátov je vytvorený vydavateľom certifikátov, ktorý spravuje tieto certifikáty použitím súkromného kľúča, ktorý je na to určený.

(5) Zoznam zrušených kvalifikovaných certifikátov je zoznam zrušených certifikátov, ktorým vydavateľ kvalifikovaných certifikátov, ktorý spravuje tieto certifikáty oznamuje predčasné skončenie ich platnosti. Zoznam zrušených kvalifikovaných certifikátov spĺňa požiadavky uvedené v odsekoch (1),(2),(3),(4) a navyše nasledujúce požiadavky:
   (a) je vydaný akreditovanou certifikačnou autoritou v zmysle tohto zákona alebo Úradom,

(b) elektronický podpis tela zoznamu zrušených certifikátov bol vytvorený použitím súkromného kľúča určeného na tento účel,
(c) na verejný kľúč prislúchajúci k súkromnému kľúču podľa písm. (b) vydala akreditovaná certifikačná autorita, resp. Úrad certifikát.

(6) Formát, frekvenciu vydávania a spôsob vydávania zoznamu zrušených kvalifikovaných certifikátov ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

§ 11
Časová pečiatka

(1) Časová pečiatka je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá spĺňa nasledujúce požiadavky:
(a) nie je (efektívne) možné ju vytvoriť bez znalosti súkromného kľúča určeného na tento účel,
(b) na základe znalosti verejného kľúča prislúchajúceho k súkromnému kľúču použitému pri jej vytvorení je možné overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, nebol po jej vytvorení zmenený,
(c) je vytvorená akreditovanou certifikačnou autoritou použitím súkromného kľúča určeného na tento účel,
(d) je možné ju vytvoriť len s použitím bezpečného zariadenia na vytváranie časovej pečiatky podľa §3, ods. (23),
(e) na verejný kľúč prislúchajúci k súkromnému kľúču použitému na jej vytvorenie bol akreditovanou certifikačnou autoritou vydaný kvalifikovaný certifikát,
(f) umožňuje jednoznačne identifikovať dátum a čas, kedy bola vytvorená.

(2) Formát časovej pečiatky a spôsob jej vytvárania, požiadavky na zdroj časových údajov pre časovú pečiatku a požiadavky na vedenie dokumentácie časových pečiatok ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

TRETIA ČASŤ

Prvý diel

§ 12
Úrad

(1) Zriaďuje sa Úrad pre elektronický podpis ako súčasť Národného bezpečnostného úradu podľa § 34, ods. (1) tohto zákona.

(2) Úrad vykonáva dozor nad dodržiavaním tohoto zákona. Za účelom výkonu tohoto dozoru je certifikačná autorita povinná povereným pracovníkom Úradu umožniť v nevyhnutnom rozsahu vstup do obchodných a prevádzkových priestorov, na požiadanie predložiť úplnú dokumentáciu, záznamy, doklady, písomnosti a iné podklady súvisiace s jej činnosťou, umožniť v nevyhnutnej miere prístup do svojho informačného systému a poskytnúť informácie a potrebnú súčinnosť. Pri zistení porušenia tohoto zákona je Úrad oprávnený udeľovať sankcie.

(3) Úrad posudzuje žiadosti certifikačných autorít pôsobiacich na území SR o akreditáciu, udeľuje a odníma certifikačným autoritám akreditáciu a vydáva osvedčenia o akreditácii.

(4) Úrad vydáva kvalifikované certifikáty verejných kľúčov podľa § 9 ods. (3) tohto zákona ním akreditovaným certifikačným autoritám.

(5) Úrad zverejňuje vlastný verejný kľúč podľa § 5 ods. (2) a vydáva kvalifikovaný certifikát svojho vlastného verejného kľúča podľa § 9, ods. (5) tohto zákona.

(6) Úrad vydáva kvalifikované certifikáty verejných kľúčov zahraničným certifikačným autoritám podľa § 25, ods. (1), písm. (c).

(7) *Úrad registruje certifikačné autority pôsobiace na území SR.*

(8) Úrad vedie zoznam akreditovaných certifikačných autorít pôsobiacich na území SR a zoznam certifikačných autorít, ktorým odňal akreditáciu. Tento zoznam je nepretržite verejne prístupný prostredníctvom verejne dostupného telekomunikačného kanála. Úrad je povinný poskytovať informácie podľa ods. (8) takým spôsobom, aby tieto informácie boli overiteľné.

(9) Úrad zruší kvalifikovaný certifikát, ktorý vydal akreditovanej certifikačnej autorite, ak akreditovanej certifikačnej autorite odníme akreditáciu, alebo ak táto ukončí svoju činnosť
(10) Požiadavky na správu kvalifikovaných certifikátov akreditovanou certifikačnou autoritou sa vzťahujú aj na Úrad.
(11) Úrad vedie register zahraničných certifikačných autorít, ktorých certifikáty boli Úradom uznané pre použitie v Slovenskej republike.
(12) Úrad certifikuje produkty pre elektronický podpis, najmä bezpečné zariadenia na vytváranie elektronického podpisu, a bezpečné zariadenia na vytváranie časových pečiatok, vydáva odporúčania, štandardy a smernice z oblasti elektronického podpisu.
(13) Úrad plní aj ďalšie funkcie, ktoré mu vyplývajú z tohto zákona. Úrad môže na plnenie svojich funkcií využiť aj iné štátne orgány, súkromné organizácie, alebo nezávislých odborníkov.

Druhý diel
Certifikačná autorita

§ 13

(1) Certifikačná autorita je poskytovateľ certifikačných služieb, ktorý spravuje certifikáty v zmysle § 3, ods. (12). Certifikačná autorita môže vykonávať aj iné certifikačné činnosti podľa § 3, ods. (11) tohto zákona.
(2) Poskytovanie certifikačných služieb podľa § 3, ods. (9) tohto zákona je podnikaním.
(3) Na vykonávanie certifikačných činností a poskytovanie certifikačných služieb v zmysle tohto zákona sa povolenie nevyžaduje.
(4) Akreditované certifikačné služby podľa § 3, ods. (10) sa poskytujú na základe akreditácie, ktorú udeľuje Úrad.
(5) Certifikačná autorita je povinná ešte pred začatím poskytovania služieb bezplatne zverejňovať:
   (a) certifikačný poriadok, ktorý obsahuje najmä informácie pre koho a za akých podmienok poskytuje služby, typy vydávaných certifikátov, práva a povinnosti používateľov svojich služieb, vzorovú žiadosť o poskytnutie služby, pravidlá používania a zrušovania certifikátov,
   (b) technické špecifikácie, formáty, normy a štandardy používané pri vykonávaní činností,
   (c) cenník svojich platených služieb a zoznam bezplatne poskytovaných služieb,
   (d) obmedzenia pri poskytovaní svojich služieb, ak také existujú,
   (e) spôsob overenia totožnosti žiadateľa o poskytnutie svojich služieb,
   (f) informácie o tom, či certifikačná autorita je na svoju činnosť akreditovaná Úradom.
(6) Certifikačná autorita je povinná:
   (a) zverejňovať svoje identifikačné údaje a informácie o svojich certifikátoch,
   (b) údaje uvedené v odseku (5) a odseku (6), písmeno (a) zverejniť aj elektronicky,
   (c) oznámiť Úradu začiatok svojej činnosti minimálne 30 dní pred začiatkom činnosti. V oznámení je certifikačná autorita povinná uviesť obchodné meno, sídlo a identifikačné údaje žiadateľa, doklad o oprávnení na vykonávanie podnikateľskej činnosti (v prípade právnických osôb výpis z obchodného registra nie starší ako 3 mesiace) a informácie určené na zverejnenie podľa ustanovení tohto zákona.

§ 14
Akreditácia

(1) Certifikačná autorita môže požiadať Úrad o akreditáciu.
(2) Akreditovanou certifikačnou autoritou môže byť právnická osoba alebo fyzická osoba, ktorá má vytvorené materiálne, priestorové, technické, personálne, organizačné a právne podmienky na poskytovanie akreditovaných certifikačných služieb. Podrobnosti ustanoví všeobecne záväzný predpis, ktorý vydá Úrad.
(3) Certifikačná autorita je povinná pri žiadosti o akreditáciu predložiť Úradu:
   (a) obchodné meno, sídlo a identifikačné údaje žiadateľa,
   (b) výpis z obchodného registra nie starší ako 3 mesiace,
   (c) výpis z registra trestov štatutárnych zástupcov právnickej osoby, nie starší ako 3 mesiace,
   (d) verejný kľúč, prislúchajúci k súkromnému kľúču, ktorý bude používať na podpisovanie ňou vydávaných certifikátov,
   (e) výsledok bezpečnostného auditu svojej činnosti spoločnosťou, ktorá má na vykonávanie auditu certifikačných autorít oprávnenie Úradu,

(f) zverejňované informácie podľa ustanovení tohto zákona.

(4) Ak žiadateľ o akreditáciu (certifikačná autorita) splnil podmienky na udelenie akreditácie v zmysle tohto zákona a všeobecne záväzného právneho predpisu, vydaného Úradom, Úrad do 90 dní od prijatia žiadosti vydá rozhodnutie o udelení akreditácie a vydá pre certifikačnú autoritu certifikát. Udelenie akreditácie oprávňuje cerifikačnú autoritu poskytovať akreditované certifikačné služby.

(5) V prípade nedostatkov v žiadosti o akreditáciu požiada Úrad certifikačnú autoritu o doplnenie žiadosti najneskôr do 7 dní a na toto obdobie preruší konanie o udelení akreditácie. Ak žiadateľ o akreditáciu do doby prerušenia konania nedoplní žiadosť, Úrad žiadosť zamietne.

(6) Ak Úrad zistí, že akreditovaná certifikačná autorita nespĺňa podmienky pre udelenie akreditácie, môže pozastaviť na určitý čas (najviac na 3 mesiace) platnosť akreditácie a uložiť jej nápravné opatrenia. Ak akreditovaná certifikačná autorita v stanovenom čase uložené opatrenia nesplní, Úrad jej odníme akreditáciu.

(7) Certifikačná autorita, ktorej nebola udelená alebo ktorej bola odňatá akreditácia, môže znova požiadať o udelenie akreditácie.

(8) Žiadosť o akreditáciu podlieha správnemu poplatku, ktorý je príjmom štátneho rozpočtu Slovenskej republiky.[3]

§ 15
Povinnosti certifikačnej autority pri poskytovaní certifikačných služieb

(1) Certifikačná autorita je povinná mať vypracované bezpečnostné pravidlá a pravidlá pre výkon certifikačných činností.

(2) Akreditovaná certifikačná autorita je povinná mať vypracované bezpečnostné pravidlá a pravidlá pre výkon certifikačných činností v súlade s pravidlami ustanovenými vo všeobecne záväznom právnom predpise, ktorý vydá Úrad.

(3) Certifikačná autorita je povinná dodržiavať svoje bezpečnostné pravidlá a pravidlá pre výkon certifikačných činností počas celej doby poskytovania svojich služieb.

(4) Certifikačná autorita je povinná používať svoj certifikát (certifikát certifikačnej autority) len na účely vykonávania certifikačných služieb.

(5) Certifikačná autorita je povinná vykonávať certifikačné činnosti tak, aby nebolo možné vytvárať kópie súkromných kľúčov alebo uchovávať údaje o súkromných kľúčoch používateľov jej služieb. Toto ustanovenie sa netýka tých súkromných kľúčov, ktoré certifikačná autorita používa na vykonávanie svojich vlastných certifikačných činností.

(6) Certifikačná autorita je povinná registrovať sa v zmysle osobitného zákona[4]

(7) Certifikačná autorita je povinná vydávať certifikáty klientom na základe zmluvy, ktorá je:
   (a) písomná s vlastnoručným podpisom, alebo
   (b) v podobe elektronického dokumentu, ktorý je podpísaný zaručeným elektronickým podpisom oboch zmluvných strán – v tom prípade je certifikačná autorita povinná zaručiť totožnosť údajov certifikátu podľa § 8, ods. (3), písm. (c), ktorý bol použitý ako podklad pre vydanie certifikátu a vydaného certifikátu.

(8) Certifikačná autorita je ešte pred uzavretím zmluvy povinná podrobne a zrozumiteľne informovať žiadateľa o certifikát (klienta) o svojej bezpečnostnej politike a pravidlách poskytovania certifikačných služieb a to buď písomnou formou alebo elektronicky.

(9) Ak klient žiada o vydanie kvalifikovaného certifikátu, akreditovaná certifikovaná autorita mu je okrem informácií uvedených v ods. (8) povinná poskytnúť aj informácie o podmienkach používania certifikátov, ohraničeniach na spôsob ich použitia a výšku transakcií, pri ktorých ich možno použiť, ako aj o metódach riešenia sporov.

(10) Informácie uvedené v ods. (8) a (9) je certifikačná autorita povinná poskytovať aj na požiadanie tretej strany, ktorá môže dokázať legálny záujem o uvedené informácie.

(11) Certifikačná autorita je povinná poskytnúť žiadateľovi o vydanie certifikátu informáciu o technických komponentoch a procedúrach, ktoré sú vhodné pre vytváranie a overovanie elektronického podpisu v používaných procedúrach elektronického podpisu.

(12) Akreditovaná certifikačná autorita je povinná poskytnúť žiadateľovi o vydanie kvalifikovaného certifikátu informáciu o technických komponentoch, procedúrach a zariadeniach, ktoré Úrad

---

[3] Zák. č. 145/1995 Z.z. v znení neskorších právnych predpisov o správnych poplatkoch.

[4] Zák. č. 52/1998 Z.z. o ochrane osobných údajov v informačných systémoch

certifikoval podľa § 12 ods. (12) ako produkty pre elektronický podpis vhodné pre vytváranie a overovanie zaručeného elektronického podpisu.

(13) Certifikačná autorita je povinná informovať držiteľa certifikátu o možných právnych dôsledkoch používanej procedúry na vytvorenie elektronického podpisu, o povinnostiach držiteľa certifikátu a zodpovednosti certifikačnej autority.

(14) Certifikačná autorita je povinná držiteľa certifikátu informovať, kedy je potrebné použiť nový elektronický podpis najmä ak sa znížila bezpečnostná úroveň starého elektronického podpisu

(15) Certifikačná autorita je povinná počas celej doby vykonávania certifikačných činností zabezpečovať:

(a) vydávanie certifikátov, ktoré budú obsahovať všetky náležitosti ustanovené týmto zákonom,

(b) že v prípade, ak ňou vydávané certifikáty majú ľubovoľné obmedzenia, budú tieto obmedzenia zrejmé (rozpoznateľné) pre tretie strany,

(c) službu zrušenia ňou vydaného certifikátu,

(d) zverejňovanie zoznamu zrušených certifikátov; zverejnenie zrušeného certifikátu sa uskutoční bezodkladne, s uvedením času jeho zrušenia. Certifikačná autorita je povinná tieto údaje zverejniť aj elektronicky.

(e) bezodkladné informovanie držiteľa certifikátu o zrušení jeho certifikátu; a to elektronickou alebo písomnou formou.

(16) O certifikačných činnostiach je certifikačná autorita povinná viesť prevádzkovú dokumentáciu v súlade s požiadavkami, ktoré ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

(17) Certifikačná autorita je povinná archivovať súvisiacu dokumentáciu s vydávanými certifikátmi podľa osobitného zákona[5]. Archív je možné viesť v elektronickej podobe.

(18) Certifikačná autorita je povinná oboznámiť Úrad o zmene skutočností, súvisiacich s certifikačnými službami, ktoré poskytuje.

§ 16
Zodpovednosť certifikačnej autority

(1) Akreditovaná certifikačná autorita, ktorá vydáva kvalifikované certifikáty alebo ich garantuje v súlade s § 25 ods. (1) písm. (b) tohto zákona je zodpovedná voči tretím osobám za to, že

(a) všetky informácie, ktoré kvalifikovaný certifikát obsahuje, boli v čase jeho vydania presné a správne,

(b) osoba uvedená v certifikáte v čase vydania certifikátu bola držiteľom súkromného kľúča, ktorý zodpovedá verejnému kľúču uvedenému v certifikáte,

(c) súkromný kľúč a k nemu prislúchajúci verejný kľúč si navzájom zodpovedali, keď sa použili produkty a procedúry elektronického podpisu pre vytvorenie a overenie elektronického podpisu, ktoré dodala alebo odporúčala certifikačná autorita,

(d) certifikát bude zrušený do stanoveného času po prijatí oprávnenej žiadosti o zrušenie,

(e) služba rušenia certifikátov je dostupná,

(f) akreditovaná certifikačná autorita spĺňa požiadavky § 14 ods. (2) tohto zákona.

(2) Ak je rozsah použitia kvalifikovaného certifikátu obmedzený, akreditovaná certifikačná autorita nezodpovedá za škody spôsobené tým, že sa certifikát použil v rozpore s obmedzeniami uvedenými v certifikáte.

(3) Ak je v kvalifikovanom certifikáte uvedené ohraničenie na výšku transakcií, na ktoré sa môže použiť, akreditovaná certifikačná autorita nezodpovedá za škody spôsobené prekročením tejto hodnoty.

(4) Zodpovednosť certifikačnej autority podľa ods. (1) nie je možné vopred vylúčiť.

§ 17
Prekážky v činnosti a ukončenie činnosti.

(1) Certifikačná autorita je povinná informovať Úrad, ak sa u nej vyskytli prekážky vo výkone certifikačných služieb v zmysle prevádzkového poriadku do 30 dní odo dňa, kedy prekážky zaregistrovala.

---

[5] Zákon č. 149/1975 Zb. o archívnictve v znení neskorších predpisov

(2) Akreditovaná certifikačná autorita je povinná informovať Úrad, ak sa u nej vyskytli prekážky vo výkone akreditovaných certifikačných služieb v zmysle prevádzkového poriadku do 6 hodín od okamihu, keď prekážky zaregistrovala.
(3) Certifikačná autorita je povinná v prípade plánovaného ukončenia výkonu certifikačných služieb tento zámer oznámiť:
   (a) Úradu najmenej 6 mesiacov vopred,
   (b) každému držiteľovi platného certifikátu, vydaného touto certifikačnou autoritou, najmenej 6 mesiacov vopred.
(4) Certifikačná autorita, ktorá nie je akreditovanou certifikačnou autoritou, sa môže v prípade ukončenia svojej činnosti dohodnúť s inou certifikačnou autoritou o prevzatí zoznamov vydaných a zrušených certifikátov a prevádzkovej dokumentácie. V prípade, že žiadna iná certifikačná autorita tieto neprevezme, zaniká platnosť všetkých certifikátov vydaných zanikajúcou certifikačnou autoritou ku dňu jej zániku.
(5) Akreditovaná certifikačná autorita sa môže v prípade ukončenia svojej činnosti dohodnúť s inou akreditovanou certifikačnou autoritou o prevzatí zoznamov vydaných a zrušených certifikátov a prevádzkovej dokumentácie. V prípade, že žiadna iná akreditovaná certifikačná autorita tieto neprevezme, prevezme ich Úrad.
(6) Pri ukončení činnosti certifikačnej autority je jej štatutárny zástupca povinný zabezpečiť vykonanie kontroly dodržania zákona o ochrane osobných údajov[6].

Tretí diel

§ 18
Registračná autorita

(1) Registračná autorita koná v mene certifikačnej autority a na základe uzatvorenej zmluvy.
(2) Vykonávanie certifikačných činností registračnou autoritou v mene certifikačnej autority podľa tohto zákona nie je viazané na žiadne povolenie.
(3) Registračná autorita je vo svojej činnosti viazaná certifikačným poriadkom certifikačnej autority v mene ktorej koná.

Štvrtý diel

§ 19
Povinnosti držiteľa certifikátu

(1) Držiteľ certifikátu je povinný
   (a) zaobchádzať so svojím súkromným kľúčom s náležitou starostlivosťou tak, aby nemohlo dôjsť k zneužitiu jeho súkromného kľúča,
   (b) uvádzať presné, pravdivé a úplné informácie vo vzťahu k certifikátu svojho verejného kľúča,
   (c) neodkladne požiadať certifikačnú autoritu, ktorá spravuje jeho certifikát, o zrušenie certifikátu, ak zistí, že:
      1. došlo k zneužitiu jeho elektronického podpisu,
      2. hrozí zneužitie jeho elektronického podpisu,
      3. nastali zmeny v údajoch, uvedených v certifikáte.
(2) Za škody spôsobené porušením svojich povinností zodpovedá držiteľ certifikátu podľa osobitných predpisov.

---

[6] Zák. č. 52/1998 Z.z. o ochrane osobných údajov v informačných systémoch

§ 20
Ochrana osobných údajov

Na informačný systém poskytovateľa certifikačných služieb sa primerane vzťahujú ustanovenia zákona o ochrane osobných údajov[7].

ŠTVRTÁ ČASŤ

§ 21
Vytvorenie elektronického podpisu

(1) Podpisovateľ vytvorí elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a daného elektronického dokumentu vytvorí nový údaj, ktorý spĺňa podmienky podľa § 4 tohto zákona.
(2) Podpisovateľ vytvorí zaručený elektronický podpis elektronického dokumentu tak, že na základe svojho súkromného kľúča a daného elektronického dokumentu vytvorí pomocou bezpečného zariadenia na vytvorenie elektronického podpisu nový údaj, ktorý spĺňa podmienky podľa § 5 ods. (1) tohto zákona.
(3) Vytvorením elektronického podpisu dohodnutým spôsobom a s použitím svojho súkromného kľúča potvrdzuje podpisovateľ autorstvo, resp. súhlas s obsahom podpisovaného dokumentu v elektronickej forme.
(4) Formu a spôsob vytvárania zaručeného elektronického podpisu ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

§ 22
Overovanie elektronického podpisu

(1) Overovanie elektronického podpisu je kontrola jeho platnosti. Podmienky platnosti sú pre zaručený elektronický podpis stanovené podľa §5, ods. (3) tohto zákona.
(2) Elektronický podpis (zaručený elektronický podpis) sa považuje za overený, ak bola preukázaná jeho platnosť. V opačnom prípade sa (zaručený) elektronický podpis zamieta.
(3) Overovateľ overuje elektronický podpis stanoveným spôsobom pomocou prostriedkov na overovanie elektronického podpisu, podpísaného elektronického dokumentu a verejného kľúča prislúchajúceho k udávanému podpisovateľovi.
(4) Pri overovaní elektronického podpisu overovateľ môže požadovať overenie autentickosti verejného kľúča; t.j toho, že verejný kľúč prislúcha podpisovateľovi. Na tento účel môže použiť certifikát verejného kľúča podpisovateľa, ktorý mu poskytne podpisovateľ.
(5) Pri overovaní zaručeného elektronického podpisu overovateľ na základe kvalifikovaného certifikátu verejného kľúča, ktorý mu poskytne podpisovateľ, overí, či verejný kľúč na overenie zaručeného elektronického podpisu prislúcha podpisovateľovi.
(6) Postup pri overovaní a podmienky overenia alebo odmietnutia zaručeného elektronického podpisu ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

§ 23
Rušenie certifikátov

(1) Certifikačná autorita je povinná zrušiť certifikát, ktorý spravuje, ak
  (a) zistí, že pri vydaní daného certifikátu neboli splnené požiadavky podľa zákona alebo všeobecne záväzných predpisov alebo vnútorných pravidiel certifikačnej autority, alebo
  (b) zistí, že daný certifikát bol vydaný na základe nepravdivých údajov, alebo sa údaje uvedené v danom certifikáte nezhodujú so skutočnosťou, alebo

---

[7] Tamže

(c) o zrušenie certifikátu certifikačnú autoritu požiada držiteľ daného certifikátu, alebo osoba, ktorej údaje sú uvedené v danom certifikáte, alebo
(d) certifikačnej autorite zrušenie certifikátu nariadi súd, alebo
(e) certifikačná autorita zistí, že držiteľ daného certifikátu zomrel (v prípade fyzickej osoby) alebo zanikol (v prípade právnickej osoby), alebo
(f) certifikačná autorita zistí, že súkromný kľúč prislúchajúci k verejnému kľúču uvedenému v danom certifikáte pozná iná osoba, než osoba uvedená v danom certifikáte.

(2) Pri rušení certifikátu podľa ods. (1), je certifikačná autorita povinná zrušiť certifikát najneskôr do 30 minút od prijatia žiadosti o zrušenie certifikátu podľa písm. (c); resp. do 30 minút od okamihu, kedy sa preukázateľne dozvedela o dôvode na zrušenie certifikátu podľa ods. (1), písm. (a), (b), (d), (e), (f).

(3) Certifikačná autorita je povinná zaradiť zrušený certifikát do prvého zoznamu zrušených certifikátov, ktorý vydá po zrušení daného certifikátu. Ak certifikačná autorita poskytuje službu okamžitého (on-line) overovania platnosti certifikátov, od okamihu zrušenia certifikátu je povinná poskytovať informáciu, že daný certifikát je zrušený.

(4) Rušenie certifikátov so spätnou platnosťou ani obnovovanie platnosti zrušeného certifikátu nie je prípustné.

(5) Certifikačná autorita držiteľom certifikátov a osobám uvedeným v certifikátoch, ktorých držiteľmi sú iné osoby, poskytne telefónne číslo a adresu svojej Internetovej stránky, kde sa môžu podávať žiadosti o zrušenie certifikátov. Akreditovaná certifikačná autorita je povinná umožniť podávanie žiadosti o zrušenie certifikátov v nepretržitej prevádzke.

(6) Certifikačná autorita je povinná viesť dokumentáciu o žiadostiach a podnetoch na rušenie certifikátov. V dokumentácii sú povinne zaznamenané najmä dátum a čas prijatia žiadosti o zrušenie certifikátu, alebo zistenia dôvodu na zrušenie certifikátu, dôvod na zrušenie certifikátu a údaje umožňujúce určiť totožnosť osoby, ktorá o zrušenie certifikátu požiadala, alebo určiť inštitúciu a osobu, ktorá podala podnet na jeho zrušenie.

§ 24
Administrácia certifikátov

(1) Certifikačná autorita vydaním certifikátu verejného kľúča potvrdzuje autenticitu predloženého verejného kľúča a skutočnosť, že držiteľ certifikátu disponuje súkromným kľúčom ku ktorému prináleží predložený verejný kľúč.

(2) Certifikačná autorita potvrdzuje autenticitu verejného kľúča držiteľa certifikátu tak, že po overení potrebných náležitostí vydá žiadateľovi certifikát v elektronickej forme, ktorý certifikačná autorita podpíše elektronickým podpisom s využitím svojho súkromného kľúča

(3) Overenie potrebných náležitostí žiadateľa o vydanie certifikátu (dokladov, vlastníctva súkromného kľúča prislúchajúceho k predloženému verejnému kľúču) realizuje certifikačná autorita priamo, alebo prostredníctvom registračnej autority konajúcej v mene certifikačnej autority.

(4) Certifikačná autorita je povinná vytvoriť podmienky, ktoré umožnia overovateľovi overiť platnosť certifikátu, ktorý certifikačná autorita vydala. Za týmto účelom je certifikačná autorita povinná zabezpečiť, aby jej verejný kľúč bol pre overovateľa dostupný z viacerých informačných zdrojov.

§ 25
Uznávanie zahraničných certifikátov

(1) Certifikát, alebo kvalifikovaný certifikát, ktorý vydala certifikačná autorita so sídlom mimo územia Slovenskej republiky (zahraničná certifikačná autorita), ktorého platnosť možno overiť v Slovenskej republike, možno uznať v Slovenskej republike ak
(a) zahraničná certifikačná autorita, ktorá ho vydala je akreditovaná v Slovenskej republike, alebo
(b) certifikačná autorita so sídlom v Slovenskej republike, ktorá spĺňa požiadavky zákona, garantuje platnosť certifikátu napr. vydaním krížového certifikátu verejného kľúča zahraničnej certifikačnej autority, alebo
(c) medzinárodná dohoda podpísaná Slovenskou republikou stanovuje, že (zahraničný) kvalifikovaný certifikát je uznávaný ako kvalifikovaný certifikát, alebo zahraničná certifikačná autorita je uznaná za akreditovanú certifikačnú autoritu v Slovenskej republike.

(2) Dňom vstupu Slovenskej republiky do Európskej únie sa certifikát vydaný certifikačnou autoritou majúcou sídlo v niektorej z krajín Európskej únie, ktorého platnosť možno overiť v Slovenskej republike stáva rovnoprávnym certifikátu vydanému v Slovenskej republike. Kvalifikovaný certifikát vydaný vyššie uvedenou certifikačnou autoritou bude mať rovnakú právnu účinnosť ako kvalifikovaný certifikát vydaný v Slovenskej republike.

§ 26

Vedenie archívu

(1) Certifikačná autorita je povinná uchovávať najmenej 10 rokov:
   (a) dokumentáciu organizačných a technických bezpečnostných prostriedkov, ktoré použila na zaistenie požiadaviek vyplývajúcich zo zákona a predpisov s ním súvisiacich,
   (b) originály žiadostí o vydanie certifikátov, spolu s príslušnými dokumentmi potvrdzujúcimi totožnosť žiadateľa
   (c) ku každému zrušenému certifikátu dokumenty podľa § 23, ods. (6) tohto zákona.

(2) Za predpokladu, že je zabezpečená ochrana a trvalosť zápisu, certifikačná autorita môže uchovávať vyššie uvedené dokumenty aj v elektronickej podobe.

PIATA ČASŤ

§ 27

Požiadavky na produkty pre elektronický podpis

(1) Na uchovávanie súkromných kľúčov a na vytváranie zaručených elektronických podpisov sa používajú bezpečné zariadenia na vytváranie elektronického podpisu, ktoré spoľahlivo chránia v nich uložený súkromný kľúč pred zneužitím nepovolanou osobou a umožňujú tak spoľahlivo rozoznať falšovanie zaručených elektronických podpisov a podpísaných elektronických dokumentov.

(2) Ustanovenie ods. (1) sa v primeranej miere vzťahujú na bezpečné zariadenia na vytváranie elektronického podpisu v prípade, keď sa tieto zariadenia používajú na vytváranie súkromných kľúčov.

(3) Bezpečné zariadenia na vytváranie elektronického podpisu a procedúry používané na vytváranie (zaručeného) elektronického podpisu musia
   (a) spoľahlivo zabezpečiť, že sa podpisovaný elektronický dokument pri vytváraní (zaručeného) elektronického podpisu nemení,
   (b) umožniť, aby sa elektronický dokument, ktorý sa bude elektronicky podpisovať, zobrazil podpisovateľovi ešte pred tým, ako sa spustí procedúra na vytvorenie (zaručeného) elektronického podpisu,
   (c) zaručiť, že pravdepodobnosť toho, že sa nejaký súkromný kľúč vytvorí viac než raz, bude zanedbateľná.

(4) Na vytváranie a uchovávanie kvalifikovaných certifikátov sa musia používať také zariadenia a procedúry, ktoré zabráňujú ich falšovaniu.

(5) Na overovanie zaručených elektronických podpisov sa budú používať technické zariadenia a procedúry, ktoré zaistia, že
   (a) podpísaný elektronický dokument nebol modifikovaný,
   (b) podpis sa spoľahlivo overí a výsledok overovania sa správne zobrazí,
   (c) overovateľ zaručeného elektronického podpisu môže spoľahlivo určiť elektronický dokument, pre ktorý bol vytvorený zaručený elektronický podpis, ktorý overovateľ overuje,
   (d) overovateľ môže určiť osobu, ktorej zaručený elektronický podpis prislúcha; pričom použitie pseudonymu je jasne vyznačené a
   (e) možno jasne rozoznať zmeny podpísaného elektronického dokumentu, ktoré boli vykonané po vytvorení zaručeného elektronického podpisu elektronického dokumentu.

(6) Ustanovenia § 27 ods. (1-5) sa v primeranej miere vzťahujú na bezpečné zariadenia na vytváranie časových pečiatok používaných na vytváranie časových pečiatok v zmysle § 11 tohto zákona.

(7) Súlad technických zariadení a procedúr na vytváranie zaručených elektronických podpisov, časových pečiatok, ako aj iných produktov pre elektronický podpis s bezpečnostnými požiadavkami podľa § 12, ods. (12) overuje a potvrdzuje Úrad.
(8) Požiadavky na produkty pre elektronický podpis ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

ŠIESTA ČASŤ
AUDIT, KONTROLA A SANKCIE

§ 28
Audit

(1) Akreditovaná certifikačná autorita je povinná opakovane sa podrobovať externému auditu bezpečnosti poskytovania certifikačných činností tak, že audit je ukončený najneskôr do 12 mesiacov od dátumu obdržania akreditácie alebo od dátumu ukončenia predchádzajúceho auditu. Požiadavky na audit a kvalifikáciu audítorov a podrobnosti o rozsahu auditu stanoví Úrad.
(2) Akreditovaná certifikačná autorita je povinná predložiť záverečnú správu o výsledkoch auditu Úradu spolu s prípadnými opatreniami na nápravu a lehotami, do ktorých budú zistené nedostatky odstránené. Záverečnú správu o výsledkoch auditu je akreditovaná certifikačná autorita povinná Úradu predložiť do 14 dní od ukončenia auditu.
(3) Ak Úrad zo záverečnej správy o výsledkoch auditu zistí, že akreditovaná certifikačná autorita porušila povinnosti ustanovené v tomto zákone, uloží jej opatrenia na nápravu a lehotu, v ktorej je povinná nedostatky odstrániť.

§ 29
Kontrola

(1) Dohľad nad dodržiavaním ustanovení zákona vykonáva Úrad.
(2) Certifikačná autorita sa stáva subjektom dohľadu v okamihu podania žiadosti o registráciu. Súčasťou kontroly (akreditovanej) certifikačnej autority je aj kontrola registračných autorít konajúcich v jej mene.
(3) Úrad môže prijať voči certifikačnej autorite opatrenia na zaistenie dodržiavania zákona.
(4) Úrad môže dočasne, čiastočne alebo celkom zakázať certifikačnej autorite začať vykonávať, alebo pokračovať vo vykonávaní nejakej činnosti, ak zistí, že certifikačná autorita:
   (a) nie je dostatočne spoľahlivá na to, aby mohla pôsobiť ako certifikačná autorita,
   (b) nepreukázala, že má na to potrebné odborné predpoklady,
   (c) nemá dostatočné finančné krytie,
   (d) používa nevhodné technické zariadenia,
   (e) nespĺňa ďalšie požiadavky, ktoré na certifikačnú autoritu kladie zákon a všeobecne záväzné právne predpisy

   a nie je predpoklad, že by opatrenia podľa (3) mohli vyriešiť daný problém.
(5) Úrad môže nariadiť zrušenie kvalifikovaných certifikátov, ak zistil, že boli sfalšované, alebo neboli dostatočne chránené pred falšovaním, alebo keď zariadenia na tvorbu zaručených elektronických podpisov vykazovali bezpečnostné nedostatky, ktoré by mohli umožniť nepozorované falšovanie zaručených elektronických podpisov, alebo dokumentov podpisovaných takýmito podpismi.
(6) Zákazom činnosti alebo zastavením činnosti certifikačnej autority nie je dotknutá platnosť ňou dovtedy vydaných certifikátov.
(7) Zákazom činnosti alebo zastavením činnosti akreditovanej certifikačnej autority, ani zrušením jej akreditácie nie je dotknutá platnosť ňou dovtedy vydaných kvalifikovaných certifikátov.
(8) Zamestnanci Úradu poverení výkonom kontroly sú oprávnení vyžadovať od pracovníkov kontrolovanej akreditovanej certifikačnej autority, certifikačnej autority alebo registračnej autority súčinnosť pri kontrole, doklady a informácie, ktoré súvisia s vykonávaním certifikačných činností. Osoby vykonávajúce kontrolu sú povinné zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedeli pri výkone kontroly. Povinnosť mlčanlivosti trvá aj po ukončení ich vzťahu s Úradom.

Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné pre orgány činné v trestnom konaní; tým nie sú dotknuté ustanovenia osobitných zákonov[8].

SANKCIE

§ 30

(1) Za porušenie povinností vyplývajúcich z tohto zákona možno ukladať pokuty.
(2) Pokuty podľa odseku (1) ukladá Úrad.

§ 31

(1) Pokutu do 10 mil. Sk možno uložiť právnickej osobe alebo fyzickej osobe, ktorá poskytuje akreditované certifikačné služby bez akreditácie.
(2) Pokutu do 10 mil. Sk možno ďalej uložiť akreditovanej certifikačnej autorite,
   (a) ktorá neposkytuje certifikačné služby v súlade s týmto zákonom a s bezpečnostnými pravidlami, ktoré ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad,
   (b) ktorá neposkytuje službu rušenia certifikátov,
   (c) nezverejňuje ňou zrušené certifikáty,
   (d) nezverejňuje svoje identifikačné údaje alebo certifikáty, ktoré používa pri poskytovaní certifikačných služieb,
   (e) ktorá poruší ustanovenie § 17 ods. (6),
   (f) vykonáva činnosť, ktorá jej bola dočasne pozastavená.
(3) Pokutu do 5 mil. Sk a to aj opakovane možno uložiť akreditovanej certifikačnej autorite, ktorá neposkytne alebo zatají informácie pri kontrole vykonávanej Úradom (§ 29 ods. (8)), alebo pri takejto kontrole nespolupracuje s Úradom v zmysle § 12 ods. (2) tohto zákona.
(4) Pokutu do 500 tis. Sk a to aj opakovane možno uložiť akreditovanej certifikačnej autorite, ktorá nesplní povinnosti podrobiť sa auditu podľa § 28 ods. (1) alebo nepredloží záverečnú správu výsledku auditu v termíne podľa § 28 ods. (2) tohoto zákona.
(5) Pokutu do 1 mil. Sk možno uložiť certifikačnej autorite, ktorá
   (a) poruší povinnosť zrušiť certifikát,
   (b) poruší povinnosť viesť požadovanú dokumentáciu podľa § 15 ods. (16) tohto zákona.
(6) Pokutu do 500 tis. sk možno uložiť certifikačnej autorite, ktorá
   (a) nesplní oznamovaciu povinnosť podľa §13 ods. (6), pís. (c) tohto zákona,
   (b) neoznámi Úradu v lehote stanovenej týmto zákonom ukončenie svojej činnosti,
   (c) poruší ustanovenia § 20,
   (d) poruší ustanovenia § 26 ods. (1).
(7) Pokutu do 1 mil. Sk možno uložiť certifikačnej autorite, ktorej registračná autorita
   (a) neposkytuje registračné služby podľa postupov a v súlade s bezpečnostnými pravidlami,
   (b) nezabezpečí presnosť, pravdivosť a úplnosť údajov o registrovaných osobách,
   (c) nevedie dokumentáciu o spôsobe poskytovania a bezpečnosti registračných služieb,
   (d) nechráni osobné údaje registrovaných osôb v súlade so zákonom o ochrane osobných údajov[9],
(8) Pokutu do 100 tis. Sk možno uložiť fyzickej osobe ktorá zneužila súkromný kľúč podpisovateľa, alebo predložila nepravdivé údaje pri podávaní žiadosti o vydanie certifikátu.
(9) Pokutu do 1 mil. Sk možno uložiť právnickej osobe, ktorá zneužila súkromný kľúč podpisovateľa. Rovnakú pokutu a to aj opakovane možno uložiť certifikačnej autorite, ak porušila ustanovenia § 15 ods. (5) tohto zákona.
(10) Uloženou pokutou podľa ods. (8) a (9) nie je dotknuté právo na náhradu takto vzniknutej škody.
(11) Pri uložení pokuty sa prihliada na závažnosť, trvanie a následky protiprávneho konania,
(12) Pokutu podľa odseku (1) môže Úrad uložiť do jedného roka odo dňa, keď porušenie povinností zistí, najneskôr do troch rokov odo dňa, keď k porušeniu povinností došlo.

---

[8] Napríklad § 38 zákona č. 21/1992 Zb. o bankách v znení neskorších predpisov; § 40 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska.

[9] Tamže.

(13) Výnosy z pokút sú príjmom štátneho rozpočtu Slovenskej republiky.

SIEDMA ČASŤ
SPOLOČNÉ, PRECHODNÉ A ZÁVEREČNÉ USTANOVENIA

§ 32
Splnomocňovacie ustanovenie

(1) Podrobnosti o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku upraví všeobecne záväzný právny predpis, ktorý vydá Úrad.
(2) Podrobnosti o postavení certifikačnej autority upraví všeobecne záväzný právny predpis, ktorý vydá Úrad.

§ 33
Spoločné ustanovenie

Na konanie Úradu podľa tohto zákona sa vzťahuje všeobecný predpis o správnom konaní[10], ak tento zákon neustanovuje inak.

PRECHODNÉ USTANOVENIA

§ 34

(1) Zákon č. .../2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení zákona č. 52/1998 o ochrane osobných údajov v informačných systémoch v znení neskorších predpisov sa mení a dopĺňa takto:

V § ... ods. ... sa vkladajú písmená .... ktoré znejú:

„....) akredituje certifikačné autority a ruší ich akreditáciu podľa osobitného predpisu (5a),
.....) vydáva certifikáty akreditovaným certifikačným autoritám používané pri certifikačných službách podľa osobitného predpisu (5a),
.....) vykonáva kontrolu certifikačných autorít a registračných autorít podľa osobitného predpisu (5a). "

Poznámka pod čiarou k odkazu 5a znie:
„5a) Zákon č. .../2001 Z. z. o elektronickom podpise.".

(2) Zákon č. 40/1964 Zb., občiansky zákonník, v znení zákona č. 58/1969 Zb., zákona č.131/1982 Zb., zákona č. 131/1982 Zb., zákona č. 94/1988 Zb., zákona č. 188/1988 Zb., zákona č. 87/1990 Zb., 105/1990 Zb., zákona č. 116/1990 Zb., zákona č. 87/1991 Zb., zákona č. 509/1991 Zb., zákona č. 264/1992 Zb., zákona č. 278/1993 Z.z., zákona č. 249/1994 Z.z., zákona č. 153/1997 Z.z., zákona č. 211/1997 Z.z., zákona č. 252/1999 Z.z. a zákona č. 218/2000 Z.z. sa mení takto:
V § 40 ods. 3 sa dopĺňa veta:
"Právny úkon, ktorý bol urobený elektronickými prostriedkami je platný, ak je podpísaný elektronickým podpisom podľa osobitného zákona.[11]"

(3) Zákon č. 99/1963 Zb. Občiansky súdny poriadok, v znení zákona č. 36/1967 Zb., zákona č. 158/1969 Zb., zákona č. 49/1973 Zb., zákona č. 20/1975 Zb., zákona č. 133/1982 Zb., zákona č. 180/1990 Zb., zákona č. 328/1991 Zb., zákona č. 519/1991 Zb., zákona č. 263/1992 Zb., zákona č. 5/1993 Z.z., zákona č. 46/1994 Z.z., zákona č. 190/1995 Z.z., zákona č. 232/1995 Z.z., zákona č.

---

[10] Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok).

[11] Zákon č. .../2001 Zb. o elektronickom podpise.

233/1995 Z.z., zákona č. 22/1996 Z.z., zákona č. 58/1996 Z.z., zákona č. 281/1996 Z.z., zákona č. 211/1997 Z.z., zákona č. 359/1997 Z.z., zákona č. 124/1998 Z.z., zákona č. 144/1998 Z.z., zákona č. 87/1998 Z.z., zákona č. 169/1998 Z.z., zákona č. 225/1998 Z.z., zákona č. 233/998 Z.z., zákona č. 318/1998 Z.z., zákona č. 235/1998 Z.z., zákona č. 331/1998 Z.z., zákona č. 46/1999 Z.z., zákona č. 66/1999 Z.z., zákona č. 166/1999 Z.z., zákona č. 185/1999 Z.z. a zákona č. 223/1999 Z.z. sa mení takto:

Paragraf 42 ods. 1 prvá veta znie: "Podanie možno urobiť písomne, ústne do zápisnice, elektronickými prostriedkami podpísané zaručeným elektronickým podpisom podľa osobitného zákona, telegraficky alebo telefaxom".

(4) Zákon č. 511/1992 Zb. o správe daní a poplatkov a o zmenách v sústave územných finančných orgánov v znení zákona č. 102/1993 Z.z., zákona č. 165/1993 Z.z., zákona č. 253/1993 Z.z., zákona č. 254/1993 Z.z., zákona č. 253/1993 Z.z., zákona č. 172/1994 Z.z., zákona č. 187/1994 Z.z., zákona č. 249/1994 Z.z., zákona č. 367/1994 Z.z., zákona č. 374/1994 Z.z., zákona č. 58/1995 Z.z., zákona č. 146/1995 Z.z., zákona č. 304/1995 Z.z., zákona č. 386/1996 Z.z., zákona č. 12/1998 Z.z., zákona č. 219/1999 Z.z., zákona č. 367/1999 Z.z. a zákona č. 240/2000 Z.z. sa mení takto:

Paragraf 31 ods. 9 bude znieť: "Registrácia alebo oznámenie podľa tohto zákona sa predkladá správcovi dane na tlačive vydanom ministerstvom alebo ak tak vyhlási príslušný daňový úrad môže sa podať aj elektronickými prostriedkami, podpísané zaručeným elektronickým podpisom, podľa osobitného zákona, na ktorom musí daňový subjekt vyhlásiť, že ide o jeho prvú daňovú registráciu, alebo uviesť, či bol už niekedy daňovo registrovaný, a ak áno, kedy, u ktorého správcu dane, pridelené daňové identifikačné číslo, meno alebo názov, pod akým bol registrovaný a či bola registrácia odobratá alebo zrušená a dôvody, pre ktoré sa tak stalo. Ministerstvo a ústredné riaditeľstvo môže rozšíriť údaje požadované pri registrácii na registračnom tlačive alebo v elektronickej podobe, podpísanej zaručeným elektronickým podpisom ak pôjde o údaje nevyhnutné pre riadnu správu jednotlivých daní."

Paragraf 31 ods. 17 bude znieť: "Platiteľ dane z príjmov zo závislej činnosti a funkčných požitkov je povinný predkladať do 30 dní po uplynutí kalendárneho štvrťroka prehľad o zrazených a odvedených preddavkoch na túto daň a daň vyberanú osobitnou sadzbou dane za uplynulý štvrťrok správcovi dane na tlačive, ktorého vzor určí ministerstvo alebo alebo ak tak vyhlási príslušný daňový úrad môže sa podať aj elektronickými prostriedkami, podpísaný zaručeným elektronickým podpisom podľa osobitného zákona."

(5) Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) sa mení takto:
V § 19, ods. 1 znie: "Podanie možno urobiť písomne alebo ústne do zápisnice alebo ak je to technicky možné elektronickými prostriedkami podpísané elektronickým podpisom podľa osobitného zákona. Možno ho tiež urobiť telegraficky; také podanie obsahujúce návrh vo veci treba písomne alebo ústne do zápisnice doplniť najneskôr do 3 dní."

(6) Zákon č. 141/1961 Zb. o trestnom konaní súdnom (trestný poriadok) v znení zákona č. 57/1965 Zb., zákona č. 173/1968 Zb., zákona č. 58/1969 Zb., zákona č. 149/1969 Zb., 156/1969 Zb., zákona č. 48/1973 Zb., zákona č. 29/1978 Zb., zákona č. 43/1980 Zb., zákona č. 159/1989 Zb., zákona č. 178/1990 Zb., zákona č. 303/1990 Zb., zákona č. 558/1991 Zb., zákona č. 6/1993 Z.z., zákona č. 178/1993 Z.z., zákona č. 247/1994 Z.z., zákona č. 222/1998 Z.z., zákona č. 256/1998 Z.z., zákona č. 272/1999 Z.z., zákona č. 173/2000 Z.z. a zákona č. 366/2000 Z.z. sa mení takto:
V § 59 ods. 1 znie: "Podanie sa posudzuje vždy podľa svojho obsahu, aj keď je nesprávne označené. Možno ho urobiť písomne, ústne do zápisnice alebo ak je to technicky možné elektronickými prostriedkami podpísané zaručeným elektronickým podpisom podľa osobitného zákona, telegraficky, telefaxom alebo ďalekopisom. Podanie urobené telegraficky, telefaxom alebo ďalekopisom treba potvrdiť písomne alebo ústne do zápisnice. Ustanovenia § 158 zostávajú nedotknuté."

(7) Zákon č. 145/1995 Z.z.. o správnych poplatkoch v znení zákona č. 123/1996 Z.z., zákona č. 224/1996 Z.z., zákona č. 70/1997 Z.z., zákona č. 1/1998 Z.z., zákona č. 232/1999 Z.z., zákona č. 3/2000 Z.z., zákona č. 142/2000 Z.z. a zákona č. 211/2000 Z.z. sa mení takto:

V prílohe k zákonu (Prehľad sadzobníka správnych poplatkov) sa dopĺňa nová časť XX, ktorá znie:

"XX. ČASŤ

Konanie podľa zákona o elektronickom podpise

Položka 268

a) podanie žiadosti o akreditáciu poskytovateľa certifikačných služieb Sk 20 000,-

b) podanie žiadosti o uznanie zhody technických prostriedkov na vytvorenie a overenie elektronického podpisu Sk 10 000,-".

§ 35

Tento zákon nadobúda účinnosť 1. 1. 2002.

Poslanecký návrh zákona o elektronickom podpise
Dôvodová správa

Všeobecná časť

Používanie informačných a komunikačných technológií (IKT) v posledných desaťročiach vyvolalo hlboké zmeny v spoločnosti, ktorá prechádza z industriálnej do postindustriálnej, Informačnej éry. Tento proces prináša historickú šancu pre spoločenský, hospodársky a kultúrny rozvoj Slovenska. Elektronické obchodovanie umožňuje aj malým podnikom reálny prístup na globálny trh a ich zapojenie sa do deľby práce; znamená zníženie nákladov na obchodné transakcie, urýchlenie obratu; prináša nové služby a produkty s vysokým podielom pridanej hodnoty. Informatizácia spoločnosti vytvára predpoklady aj pre zefektívnenie administratívy a zvýšenie možností občanov podieľať sa na správe vecí verejných; prináša možnosti práce a vzdelávania na diaľku, zefektívnenia a skvalitnenia zdravotnej a sociálnej starostlivosti a prístupu občanov k informáciám.

Základným predpokladom Informačnej spoločnosti je zabezpečenie voľného pohybu informácií. Informácií v elektronickej podobe, ktoré však majú pre občana, hospodárske organizácie a verejnú správu tú istú právnu váhu, ako informácie v tradičnej papierovej podobe. Existujú dve základné prekážky, brániace zrovnoprávneniu informácií v elektronickej forme s informáciou v tradičnej, papierovej podobe: bezpečnostná a právna. Informáciu v elektronickej podobe je možné ľahko a nepozorovane modifikovať pomocou obyčajného textového editora; je problém určiť pôvodcu prijatej elektronickej správy, odosielateľ elektronickej správy môže popierať, že ju vytvoril a poslal, príjemca zasa že ju prijal. Riešenie týchto (bezpečnostných) problémov ponúka veda o šifrovaní - kryptológia - v podobe tzv. digitálnych podpisov. Druhý problém (právny) je v tom, že chýba právny rámec upravujúci používanie digitálnych podpisov.

Európska únia prijala Smernicu 1999/93/EC, ktorá je základom pre vytvorenie jednotného právneho rámca pre používanie elektronického podpisu v EÚ. (Elektronický podpis je technologicky neutrálnym zovšeobecnením digitálneho podpisu.) Smernica o.i. ukladá členským krajinám EÚ do 19. júla 2001 zladiť národnú legislatívu s jej požiadavkami/ustanoveniami, čo v prvom rade znamená prijať zákon o elektronickom podpise. Aj keď Slovensko nie je zatiaľ členskou krajinou EÚ, bude musieť realizovať ustanovenia smernice jednak kvôli zladeniu svojej legislatívy s legislatívou EÚ, ale predovšetkým preto, že absencia zákona o elektronickom podpise, resp. prijatie riešenia, ktoré nespĺňa požiadavky Smernice by boli vážnymi prekážkami rozvoja elektronického obchodovania a zapojenia Slovenska do medzinárodnej spolupráce. Osobitosti elektronického obchodu vedú a budú viesť k celému radu legislatívnych iniciatív tak v národnom ako aj v medzinárodnom meradle. Pre účastníkov elektronického obchodovania majú preto rozhodujúci význam právne predpisy, upravujúce oblasť elektronickej komunikácie.

V súčasnom období nemôžeme jednoznačne povedať, že náš právny poriadok túto oblasť pokrýva, hoci existujú právne predpisy, ktoré sa touto problematikou zaoberajú, resp. v ktorých je aspoň zmienka o elektronických dokumentoch.

Na druhej strane neexistuje nijaká právna úprava, ktorá by túto formu dokumentov zakazovala alebo vylučovala.

Podstata elektronického (digitálneho) podpisu spočíva v nasledovnom: Podpisovateľ má dva jedinečné údaje (čísla) - podpisovací (súkromný) kľúč a overovací (verejný) kľúč; súkromný kľúč uchováva v tajnosti a verejný kľúč je spravidla verejne dostupný, alebo ho podpisovateľ poskytuje tým, ktorým posiela digitálne podpísané dokumenty. Medzi súkromným a verejným kľúčom je vzájomne jednoznačný vzťah, ale jeden z druhého nie je možné efektívne odvodiť. Dokument, ktorý sa má podpísať (správa, textový súbor, obraz, zvuková nahrávka) sa digitalizuje; t.j. zapíše pomocou postupnosti čísiel a prevedie do formy umožňujúcej ďalšie, spravidla elektronické spracovanie. Podpisovateľ (pomocou zariadenia na vytváranie elektronického podpisu) vypočíta najprv na základe dokumentu novú hodnotu (číslo) zvanú odtlačok dokumentu a z tej potom pomocou svojho súkromného kľúča odvodí hodnotu (číslo), ktoré predstavuje elektronický podpis dokumentu. (Elektronický podpis dokumentu je teda súkromným kľúčom podpisovateľa zašifrovaný odtlačok dokumentu.) Ak niekto potrebuje overiť elektronický podpis dokumentu, najprv vypočíta odtlačok dokumentu a potom pomocou verejného kľúča podpisovateľa spätne transformuje (dešifruje) elektronický podpis dokumentu. Ak sa obe hodnoty (vypočítaná a dešifrovaná) zhodujú znamená to, že dokument nebol po vytvorení elektronického podpisu modifikovaný a že ho vytvoril niekto, kto poznal súkromný kľúč podpisovateľa. Aby bolo možné tvrdiť, že podpis dokumentu vytvoril oprávnený držiteľ súkromného (podpisovacieho) kľúča, je potrebné zaistiť dve veci: súkromný kľúč je starostlivo chránený, aby sa k nemu nedostal nikto iný, ako jeho oprávnený držiteľ; musí byť zaručené, že verejný kľúč naozaj prislúcha osobe, ktorá sa za jeho držiteľa vydáva. Na dôveryhodné spojenie identity podpisovateľa s verejným kľúčom slúži (elektronický) dokument zvaný certifikát verejného kľúča. Tento dokument vystavila dôveryhodná tretia strana, ktorá overila, že ten, komu certifikát vystavila (držiteľ certifikátu), disponuje súkromným kľúčom prislúchajúcim k verejnému kľúču uvedenému v certifikáte a overila totožnosť držiteľa certifikátu. Ale ak aj má príjemca elektronicky podpísaného dokumentu k dispozícii certifikát verejného kľúča, vydaný nezávislou dôveryhodnou treťou stranou, nestačí to ešte na overenie podpisu a určenie totožnosti podpisovateľa. Certifikát verejného kľúča má obmedzenú dobu platnosti a naviac ho za istých okolností možno zrušiť. Ak chce príjemca elektronicky podpísaného dokumentu overiť platnosť elektronického podpisu na základe certifikátu verejného kľúča, musí sa presvedčiť, či je certifikát platný. Potom použije v ňom uvedený verejný kľúč a overí platnosť elektronického podpisu dokumentu. Vydávanie, overovanie, rušenie certifikátov a ďalšie činnosti spojené s elektronickými podpismi sa nazývajú certifikačné činnosti a subjekty, ktoré ich vykonávajú - poskytovateľmi certifikačných služieb. Použitie elektronického podpisu by bolo značne obmedzené, keby sa elektronický podpis dal overiť len prostredníctvom lokálneho poskytovateľa certifikačných služieb, ktorý vydal certifikát na verejný kľúč prislúchajúci k súkromnému kľúču, pomocou ktorého bol podpis vytvorený. Preto sa vytvára technická a organizačná infraštruktúra, tzv. infraštruktúra verejného kľúča (public key infrastructure, PKI), spájajúca jednotlivých vydavateľov certifikátov, ktorá umožňuje automatizovanú správu certifikátov verejných kľúčov a prostredníctvom toho aj používanie elektronických podpisov.

Zákon o elektronickom podpise má viacero aspektov. V prvom rade je to aspekt právny: zákon zavádza elektronický podpis do právneho poriadku Slovenskej republiky, stanovuje podmienky, za ktorých má elektronický podpis právne účinky vlastnoručného podpisu a umožňuje tak zrovnoprávnenie elektronických dokumentov s papierovými dokumentmi. Elektronický podpis sa realizuje pomocou digitálneho podpisu. Výber vhodných kryptografických algoritmov pre digitálny (elektronický) podpis, stanovenie

ich parametrov a podmienok, ktoré musia spĺňať (napr. rozsah, doba platnosti, spôsob vytvárania), si vyžaduje zohľadnenie poznatkov z kryptológie aj v práve. Dôvera voči elektronickému podpisu sa zakladá na spoľahlivosti zariadení a metód, ktoré boli pri jeho vytváraní použité. Zákon preto musí určiť bezpečnostné požiadavky na zariadenia pre elektronický podpis a popísať procedúry, ktoré sa v súvislosti s elektronickým podpisom budú používať. Zmyslom zákona je umožniť aj používanie slovenských elektronických podpisov v zahraničí a, opačne, zahraničných elektronických podpisov na Slovensku. To si vyžaduje premietnuť do slovenského zákona o elektronickom podpise medzinárodné technické normy, upravujúce o.i. formáty dokumentov, procedúry ale aj bezpečnostné kritériá na technické zariadenia a procedúry používané v súvislosti s elektronickým podpisom. Aby bolo možné elektronický podpis používať, je potrebné vytvoriť vyššie spomínanú organizačnú a technickú infraštruktúru (PKI). Aj keď sa v súlade so Smernicou predpokladá, že na vytváraní slovenskej PKI sa bude podieľať najmä súkromný sektor, štát bude musieť vo vzťahu k tejto infraštruktúre plniť prinajmenšom koordinačnú, normotvornú, legislatívnu a kontrolnú úlohu. Na to bude musieť vytvoriť organizačné predpoklady (v podobe Úradu pre elektronický podpis) a definovať postavenie Úradu tak vo vzťahu k štátnym orgánom, ako aj inštitúciám a jednotlivcom, poskytujúcim služby súvisiace s elektronickým podpisom. Zákon o elektronickom podpise je v podstate projektom zložitého technického systému (PKI) a aby na základe neho bolo možné vybudovať plne funkčný systém, musí zákon v dostatočnej miere zohľadniť všetky vyššie uvedené aspekty.

Gestorom vládneho návrhu zákona bolo Ministerstvo hospodárstva SR, ktoré v spolupráci so Slovenskou asociáciou pre elektronický obchod pripravovalo zákon od jesene roku 1999. Keďže k príprave vládneho návrhu zákona nebola prizvaná odborná verejnosť, ani jej pripomienky k zákonu neboli zohľadnené a navyše zákon o elektronickom podpise neprešiel koncom roku 2000 Legislatívnou radou vlády; vytvorila sa pri Slovenskej informatickej spoločnosti koncom roku 2000 odborná skupina zložená z právnikov, informatikov, kryptológov, špecialistov na informačnú bezpečnosť a elektronický obchod, pracovníkov štátnej správy a finančných inštitúcií, ktorá pripravila vlastný návrh zákona o elektronickom podpise. Výsledky svojej práce zverejnila na Internete (www.informatika.sk/e-podpis/) a predložila na diskusiu odbornej verejnosti. Odbornou skupinou pripravený návrh zákona vychádza z požiadaviek Smernice 1999/93/EC, slovenského právneho poriadku, platných medzinárodných technických noriem a štandardov, ako aj zo skúseností a poznatkov členov odbornej skupiny z realizácie projektov certifikačných autorít, PKI alebo projektov podobného zamerania.

Ministerstvo hospodárstva SR predložilo začiatkom apríla dopracovaný návrh zákona o elektronickom podpise na rokovanie Legislatívnej rady vlády, ale termín jeho prerokovania bol opätovne posunutý. Návrh zákona zo začiatku apríla, ktorý prevzal aj niektoré riešenia zo zverejnenej pracovnej verzie návrhu odbornej skupiny, je z technického hľadiska neúplný, protirečivý a nedá sa použiť ako základ pre vybudovanie infraštruktúry potrebnej na používanie elektronického podpisu. Nedalo sa odhadnúť, v akej podobe ho Ministerstvo hospodárstva SR opätovne predloží v polovičke apríla do Legislatívnej rady vlády. Vzhľadom na pokročilý čas a neistý osud vládneho návrhu zákona sa odborná skupina rozhodla predložiť vypracovaný návrh zákona o elektronickom podpise formou poslaneckého návrhu zákona.

Smernica EÚ nie je vzorovým návrhom zákona o elektronickom podpise a mnohé závažné problémy necháva otvorené. To akým spôsobom sa budú zásadné problémy

riešiť, určuje filozofiu zákona. Poslanecký návrh zákona vychádza z nasledujúcich predpokladov.

1. Zákon o elektronickom podpise musí byť v súlade so Smernicou 1999/93/EC. Aj keď existuje viacero národných zákonov o elektronickom podpise, vzorový zákon o elektronickom podpise UNCITRAL a medzinárodné technické normy upravujúce elektronický podpis; východiskom pre poslanecký návrh zákona je v prvom rade Smernica 1999/93/EC.
2. Zákon o elektronickom podpise si vyžiada viaceré úpravy existujúcich právnych noriem. Poslanecký návrh zákona sa snaží minimalizovať potrebné zásahy do existujúceho právneho poriadku SR.
3. Terminológia. Zákon o elektronickom podpise je technický zákon a objavujú sa v ňom technické pojmy (z oblasti kryptológie, informatiky a informačnej bezpečnosti), ktoré v slovenskom právnom poriadku neboli dosiaľ použité. Pre viaceré z nich neexistuje zaužívaný slovenský termín, a preto poslanecký návrh zákona používa medzinárodnú odbornú terminológiu. Vychádzajúc z poznatkov z kryptológie a praktických skúseností s vytváraním PKI sa v poslaneckom návrhu zákona všeobecné pojmy Smernice a vzorového zákonu o elektronickom podpise UNCITRAL-u nahrádzajú konkrétnejšími a presne definovanými pojmami.
4. Úroveň zákona. Vzhľadom na predmet zákona, zákon by mohol byť všeobecný a ponechať všetky technické podrobnosti do vykonávacej vyhlášky, alebo podať podrobnú špecifikáciu navrhovaného systému a jeho prevádzkové pravidlá. Poslanecký návrh je medzi týmito dvoma krajnosťami; predstavuje dostatočne podrobnú špecifikáciu na to, aby pomocou neho bolo možné potrebnú štruktúru vybudovať, ale ponecháva do vykonávacích predpisov úpravy technických podrobností, ktoré si vyžadujú väčší priestor a podliehajú častejším zmenám.
5. Pôsobnosť zákona. Existuje viacero typov systémov, v ktorých sa bude používať elektronický podpis. Poslanecký návrh zákona upravuje používanie elektronického podpisu v otvorených systémoch. Poslanecký návrh zákona sa nevzťahuje na uzavreté systémy a na systémy, v ktorých sa pracuje s utajovanými skutočnosťami. V prvom prípade ide napr. o informačné systémy finančných organizácií, škôl, súkromných firiem, ktoré nie sú prístupné verejnosti. Ak by aj používanie elektronického podpisu v týchto systémoch muselo spĺňať podmienky stanovené zákonom, bolo by potrebné vybudovať plne funkčnú infraštruktúru, ktorá by musela umožňovať poskytovanie služieb, ktoré sa v danom systéme vôbec nepoužívajú. Ak sa všetky zainteresované strany pôsobiace v uzavretom systéme dohodnú, môže sa aj vytváranie a používanie elektronického podpisu v ich uzavretom systéme riadiť zákonom o elektronickom podpise. Miera súladu so zákonom o elektronickom podpise môže siahať od používania vybraných technických noriem a procedúr stanovených Úradom na základe zákona až po registráciu certifikačnej autority a akreditáciu certifikačnej autority uzavretého systému Úradom.
   Systémy s utajovanými skutočnosťami zasa musia spĺňať špeciálne požiadavky na ochranu citlivých údajov. Zahrnúť tieto systémy do zákona o elektronickom podpise by znamenalo zaoberať sa v tomto všeobecnom zákone špecifickými bezpečnostnými požiadavkami, ktoré by sa premietli aj do procedúr, dokumentácie, šifrovej ochrany informácií, procedurálnych opatrení, personálnej bezpečnosti a pod. Preto je jednoduchšie upraviť používanie elektronického podpisu v systémoch s utajovanými skutočnosťami špeciálnou právnou normou, ako rozširovať všeobecný zákon.

6. Realizácia elektronického podpisu digitálnym podpisom. Smernica 1999/93/EC definuje elektronický podpis technologicky neutrálne tak, že vymedzuje podmienky, ktoré by elektronický podpis mal spĺňať. Akékoľvek riešenie, ktoré spĺňa požiadavky dané Smernicou, možno použiť na realizáciu elektronického podpisu. Dôvodom takéhoto prístupu je ťažko predvídateľný vývoj technológií, ktorý môže priniesť nové zaujímavé a prakticky použiteľné riešenia (napr. biometrické metódy autentifikácie). Pri takto definovanom elektronickom podpise je reálny predpoklad, že všeobecnejšia definícia pokryje aj riešenia, ktoré sa objavia v budúcnosti. Digitálny podpis spĺňa podmienky kladené na elektronický podpis. Naviac, je to zatiaľ jediná známa a prakticky použiteľná metóda, umožňujúca spojiť identitu podpisovateľa dokumentu so samotným dokumentom. Keďže aj v ostatných krajinách sa elektronický podpis realizuje pomocou digitálneho podpisu, aj poslanecký návrh vychádza z realizácie elektronického podpisu pomocou digitálneho podpisu.
7. Úrovne elektronických podpisov. Poslanecký návrh zákona predpokladá dve úrovne elektronického podpisu, líšiace sa spôsobom vytvárania a overovania (o.i. bezpečnostnými požiadavkami, použitými technickými zariadeniami); "obyčajný" elektronický podpis a zaručený elektronický podpis. Zaručený elektronický podpis má právnu účinnosť vlastnoručného podpisu. "Obyčajnému" elektronickému podpisu nemožno síce podľa Smernice uprieť právnu účinnosť, ale ten, kto by ho chcel použiť na právne úkony, by musel dokazovať, že sú splnené náležitosti v zmysle § 40 ods. 3 a 4 Obč. Zákonníka.
8. Certifikačné služby a poskytovateľ certifikačných služieb. Pod certifikačnými službami sa v poslaneckom návrhu rozumie správa certifikátov (vydávanie, overovanie, rušenie a archivácia certifikátov), vydávanie časových pečiatok, konzultačné a expertné služby súvisiace s elektronickým podpisom. Špeciálnymi certifikačnými službami je aj poskytovanie zariadení na vytváranie/overovanie elektronického podpisu, resp. na realizáciu certifikačných činností, prípadne vykonávanie auditu a kontroly vydavateľov certifikátov. Poslanecký návrh zákona v súlade so Smernicou zavádza širší pojem poskytovateľa certifikačných činností, no potom sa sústreďuje na dva typy poskytovateľov certifikačných služieb: na vydavateľa, resp. správcu certifikátov a na subjekt manažujúci výlučne príjem žiadostí klientov o certifikáty a sprostredkovávajúci styk klientov s vydavateľom/správcom certifikátov. Prvý typ poskytovateľ certifikačných služieb sa v súlade s terminológiou používanou v PKI označuje ako certifikačná autorita, CA; druhý ako registračná autorita, RA.
9. Voľné poskytovanie certifikačných služieb. V súlade so Smernicou sa na poskytovanie certifikačných služieb nevyžaduje žiadne povolenie. Každý, kto spĺňa požiadavky zákona, môže poskytovať certifikačné služby, alebo vykonávať certifikačné činnosti. Štát prostredníctvom Úradu kontroluje dodržiavanie zákonom stanovených podmienok. Keďže zaručené elektronické podpisy majú právne účinky vlastnoručného podpisu, správa tzv. kvalifikovaných certifikátov (certifikátov verejných kľúčov, prislúchajúcich k súkromným kľúčom na vytváranie zaručených elektronických podpisov) si vyžaduje dodržiavanie prísnych bezpečnostných, technických a organizačných podmienok. Zákon by mohol presadzovať plnenie týchto pomienok nepriamo, pomocou prísnych sankcií (každý môže vydávať kvalifikované certifikáty bez predchádzajúceho povolenia, ale ak pri tom nespĺňa podmienky zákona, dostane vysokú pokutu). Takýto postup by však vytváral riziko vydávania "kvalifikovaných" certifikátov a používanie "zaručených" elektronických

podpisov na nich postavených, ktoré by nespĺňali príslušné bezpečnostné požiadavky a mohli by ohroziť dôveru voči slovenskému elektronickému podpisu tak v domácom, ako aj v medzinárodnom meradle. Preto je vydávanie (správa) kvalifikovaných certifikátov v poslaneckom návrhu zákona chápané ako certifikačná služba, ktorú môže poskytovať len CA, ktorá Úradu preukáže svoju spôsobilosť (t.j. zodpovedajúce finančné, technické, odborné, kvalifikačné, bezpečnostné, personálne a organizačné podmienky) vykonávať ju v súlade so zákonom. Úrad udelí CA na vyššie uvedené činnosti akreditáciu.

10. Elektronický podpis poskytovateľa certifikačných služieb. Ak je poskytovateľom certifikačných služieb fyzická osoba, je jej elektronický podpis aj elektronickým podpisom poskytovateľa certifikačných služieb. Ak je poskytovateľom certifikačných služieb právnická osoba, jej elektronický podpis (napríklad na certifikáte verejného kľúča, ktorý vydala) sa zakladá na elektronickom podpise fyzickej osoby (štatutára, alebo operátora povereného vydávaním certifikátov v mene danej certifikačnej autority) a digitálneho podpisu vytvoreného pomocou súkromného kľúča prislúchajúceho certifikačnej autorite. Tým sa spĺňa požiadavka Smernice, podľa ktorej má (kvalifikovaný) certifikát obsahovať elektronický podpis certifikačnej autority, ktorá ho vydala; obmedzenie vyplývajúce zo slovenského právneho poriadku, podľa ktorého podpis (ako prejav vôle) môže vytvárať len fyzická osoba a napokon aj technologické obmedzenia vyplývajúce z potreby automatického vytvárania a overovania elektronických podpisov.
11. Registračná autorita. Poslanecký návrh zákona oddeľuje, resp. vyčleňuje spomedzi certifikačných služieb registračné služby. Hoci by registračné služby mohla poskytovať priamo certifikačná autorita, z praktických dôvodov (dosažiteľnosť certifikčnej autority) poslanecký návrh zákona vytvára možnosť, aby registračné služby pre certifikačnú autoritu mohla poskytovať na zmluvnom základe aj iná právnická osoba alebo fyzická osoba, ktorá má na to vytvorené potrebné technické, kvalifikačné a bezpečnostné podmienky. Aby rozličné registračné autority tej istej certifikačnej autority nepoužívali pri vykonávaní svojej činnosti rozdielne postupy s rôznou úrovňou bezpečnosti, registračné autority sú riadené príslušnou certifikačnou autoritou a musia v priebehu poskytovania registračných služieb dodržiavať certifikačný poriadok a prevádzkové pravidlá certifikačnej autority.
12. Úrad pre elektronický podpis. Najvyšším orgánom štátnej správy pre elektronický podpis je Úrad pre elektronický podpis. Úrad plní dve základné funkcie: je najvyššou certifikačnou autoritou na území Slovenska, ktorá zastrešuje akreditované certifikačné autority na Slovensku a umožňuje tak vytvoriť súvislú PKI potrebnú pre používanie zaručených elektronických podpisov. Druhou hlavnou úlohou Úradu je dohľad nad dodržiavaním zákona o elektronickom podpise. Keďže Úrad musí aj kontrolovať certifikačné autority, posudzovať vhodnosť a bezpečnosť používaných technických prostriedkov, kryptografických metód a algoritmov koordinovať slovenskú s medzinárodnou PKI, podieľať sa na vypracovávaní medzinárodných noriem a štandardov v oblasti elektronického podpisu, musí mať na plnenie týchto funkcií vytvorené adekvátne postavenie a podmienky (technické, finančné, personálne, kvalifikačné). Keďže vytvorenie samostatného Úradu v krátkom čase by bolo veľmi náročné a na druhej strane bez Úradu by nebolo možné vytvoriť potrebnú infraštruktúru (PKI) a zabezpečiť jej fungovanie, poslanecký návrh zákona predpokladá vytvorenie Úradu v rámci Národného bezpečnostného úradu. Takéto riešenie umožňuje využiť existujúce chránené priestory, technickú infraštruktúru aj špecialistov danej inštitúcie. Úrad však nedokáže plniť všetky svoje povinnosti len

vlastnými silami. Preto poslanecký návrh zákona ráta s možnosťou zapojenia iných štátnych a súkromných inštitúcií a nezávislých expertov najmä do kontrolnej činnosti Úradu.

Vytvorenie Úradu pre elektronický podpis v rámci Národného bezpečnostného úradu si vyžiada náklady vo výške 119 mil. Sk (technické vybavenie 57.1 mil sk. programové vybavenie 1.5 mil Sk, technické zabezpečenie Úradu 20.8 mil Sk, materiálno-technické vybavenie a zabezpečenie 30.6, interné a externé služby 9 mil Sk). Ročné prevádzkové náklady (vrátane miezd a odvodov) Úradu pre elektronický podpis sa odhadujú na 67 mil. Sk. (Odhady nákladov sa uvádzajú v cenách platných k 1.4.2001). Zabezpečenie činnosti Úradu pre elektronický podpis si vyžiada 65 pracovníkov.

Poslanecký návrh zákona o elektronickom podpise je v súlade s Ústavou a s inými zákonmi Slovenskej republiky a nie je v rozpore s medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.

Osobitná časť

V prvej časti zákona je uvedný predmet a účel zákona a sú definované niektoré (väčšinou technické) pojmy, ktoré sa v zákone budú používať.

K § 1 a § 2

Predmet a účel zákona bol podrobne popísaný vo všeobecnej časti dôvodovej správy.

K § 3
Zákon o elektronickom podpise zavádza do právneho poriadku Slovenskej republiky technické pojmy, ktoré tento poriadok doteraz nepoznal, čím sa zároveň obohacuje právny jazyk. Pri vytváraní pojmového aparátu vychádza zákon zo Smernice 1999/93/EC a návrhu vzorového zákona o elektronickom podpise UNCITRAL-u. Keďže uvedené dokumenty sa snažia pokryť existujúce aj pripravované zákony používajúce rozličnú terminológiu, je ich terminológia veľmi všeobecná. Predkladaný zákon definuje konkrétne riešenia, a preto konkretizuje aj pojmy Smernice a UNCITRAL-u. Definície pojmov sú v zákone uvedené na dvoch miestach: v § 3 sú uvedené pomocné pojmy (objekty a subjekty zákona). Definíciám hlavných pojmov sú venované samostatné paragrafy.

Dokumentom označuje zákon ľubovoľnú konečnú neprázdnu postupnosť znakov. Podstatné sú na definícii dokumentu tri veci: v dokumente musí byť aspoň jeden znak, dokument musí byť uzavretý, t.j. nemôže obsahovať nekonečne veľa znakov a znaky dokumentu majú isté poradie. Pritom znak nemusí byť len písmeno ale môže to byť prvok ľubovoľnej konečnej neprázdnej množiny, nazývanej v informatike abecedou. Príkladom takej abecedy môže byť anglická abeceda, čínska abeceda, číslice 0,...,9, ale napríklad aj všetky možné obrazy z televíznej obrazovky. Definícia dokumentu pokrýva jednak bežné texty, počítačové programy, ale aj akékoľvek údaje vyznačujúce sa rozlíšením znakov a ich usporiadaním. Vo forme dokumentu možno zaznamenať obrazovú informáciu (nejaký objekt buď odfotografovať, alebo zosnímať kamerou) zvukovú informáciu (vytvoriť zvukový záznam, zapísať prednesený prejav, zaznamenať hodobnú skladbu), záznam z meracích prístrojov a pod. Na to, aby sa dal dokument podpísať elektronickým podpisom, musí sa z neho dať jednoznačne odvodiť istá číselná hodnota. Preto musí byť dokument zapísaný v podobe čísla; t.j. číselne (digitálne) zakódovaný. Tu sa využíva skutočnosť, že dokument tvorí konečná postupnosť znakov, pretože jednotlivé znaky abecedy možno očíslovať (je ich len konečne veľa) a potom v dokumente každý znak nahradiť jemu prislúchajúcim číslom. (Postupnosť čísel potom chápeme ako jedno veľké číslo.) Takýto dokument sa nazýva *digitálnym dokumentom.* Pre digitálny dokument je podstatný spôsob zápisu informácie, ktorú obsahuje (digitálne kódovanie) a nie jeho technická realizácia. Pojem *elektronický dokument* už zahŕňa aj fyzickú realizáciu digitálneho dokumentu: môže to byť textový súbor (interpretovateľný ako číselný súbor) na diskete, číselne kódovaná správa prechádajúca optickým káblom, ale aj digitálne kódovaná správa napísaná na papieri.

Elektronický podpis sa vytvára na základe elektronického dokumentu a tajnej informácie, ktorá sa nazýva *súkromný (podpisovací) kľúč.* Súkromný kľúč je číslo a je jednou časťou tzv. dvojice asymetrických kľúčov. Druhou zložkou tejto dvojice je verejný (overovací) kľúč, ktorý tiež predstavuje číslo. Medzi súkromným a verejným

kľúčom je vzájomne jednoznačný vzťah - jeden jednoznačne určuje druhý a opačne. Keďže súkromný kľúč sa používa na vytváranie elektronického podpisu elektronického dokumentu, aby niekto nepovolaný nemohol vytvoriť elektronický podpis v mene niekoho iného (napríklad, v cudzom mene prijať nejaký záväzok), súkromný (podpisovací) kľúč si musí jeho držiteľ uchovávať v tajnosti. Keďže verejný kľúč jednoznačne určuje súkromný kľúč, teoreticky je možné odvodiť na základe verejného kľúča súkromný kľúč. Zákon požaduje, aby to nebolo možné spraviť efektívne; t.j. aby na to nebol známy postup, ktorý by umožňoval odvodiť súkromný kľúč z verejného kľúča v krátkom čase, s dostupnou technikou a s vynaložením primeraných finančných prostriedkov. Z tejto požiadavky vyplynú obmedzenia na parametre súkromného kľúča (napríklad dĺžku, dobu platnosti).
Verejný kľúč slúži na overovanie elektronického podpisu vytvoreného pomocou k nemu prislúchajúcemu súkromnému kľúču. Keďže elektronický podpis nie je možné overiť pomocou iného verejného kľúča, ak sa dá určiť, kto je držiteľom verejného kľúča, overenie elektronického podpisu znamená aj určenie identity podpisovateľa.

Elektronický podpis sa vytvára spôsobom popísaným vo všeobecnej časti dôvodovej správy. Jednotlivé operácie, ktoré treba vykonať, aby sa vytvoril elektronický podpis elektronického dokumentu sú príliš komplikované na to, aby ich niekto robil ručne ceruzkou na papieri. Na vytváranie elektronického podpisu sa bude pravdepodobne používať technické zariadenie, ktorému podpisujúci bude zadávať údaje (elektronický dokument, ktorý sa má podpísať, súkromný kľúč, pomocou ktorého sa má elektronický podpis vytvoriť a i.). Toto zariadenie môže byť napríklad čipová karta, špecializované technické zariadenie (kryptografický modul), alebo počítač s programom, ktorý bude realizovať potrebné operácie. V závislosti od spôsobu použitia, požadovanej úrovne bezpečnosti a ďalších kritérií sa výrobca môže rozhodnúť niektoré operácie realizovať pomocou technického zariadenia a iné pomocou programu. Keďže podstatná na vytváraní elektronického podpisu je metóda (presný postup, algoritmus) a túto je možné realizovať aj iným spôsobom, ako bolo uvedené, medzi *prostriedky na vytváranie elektronickoho podpisu* treba zaradiť aj algoritmy na vytváranie elektronického podpisu.

Z vyššie uvedeného vyplýva, že ten istý elektronický podpis elektronického dokumentu možno vytvoriť pomocou rozličných zariadení. Ak tento podpis bude vytvorený pomocou programu bežiacemu na bežnom osobnom počítači, na ktorom okrem podpisovateľa pracujú aj iné osoby, bude pravdepodobnosť sfalšovania elektronického podpisu väčšia, ako v prípade, keď sa elektronický podpis bude vytvárať pomocou špeciálneho technického zariadenia, ktoré slúži len na tento účel, ku ktorému má prístup len jeho držiteľ a na obsluhu ktorého sú stanovené presné postupy. Pre istú triedu elektronických podpisov (zaručené elektronické podpisy), ktoré majú platnosť vlastnoručných podpisov budú Úradom pre elektronický podpis presne stanovené podmienky, ktoré musia spĺňať zariadenia na ich vytváranie. Smernica EÚ špecifikuje požiadavky na *bezpečné zariadenia na vytváranie elektronického podpisu* v Dodatku III a pred schválením je už aj podrobný technický štandard.

Na rozdiel od vlastnoručného podpisu papierového dokumentu, kde je na jednom fyzickom nosiči dokument a jeho podpis, elektronický podpis elektronického dokumentu (definovaný v § 4) môže mať podobu informácie ktorá je len logicky spojená s elektronickým dokumentom (môže byť uložená oddelene od daného elektronického dokumentu). Keďže navrhovaný spôsob vytvárania elektronického

podpisu nijakým spôsobom nemení pôvodný dokument, elektronický dokument, pre ktorý bol vytvorený elektronický podpis (ale tento elektronický podpis nie je dostupný) sa nedá odlíšiť od elektronického dokumentu, pre ktorý nebol vytvorený elektronický podpis. Preto sa za *podpísaný elektronický dokument* považuje len elektronický dokument, ku ktorému je dostupný aj príslušný elektronický podpis.

Podobne ako sa na vytváranie elektronického podpisu používalo technické zariadenie alebo počítačový program, aj na overenie elektronického podpisu je potrebné vykonať zložité matematické výpočty, ktoré bude vykonávať zariadenie, alebo program *(prostriedok na overenie elektronického podpisu).* Na rozdiel od vytvárania elektronického podpisu, keď sa pracovalo so súkromným kľúčom, ktorého prezradenie by malo za následok možnosť falšovania elektronického podpisu jeho držiteľa, verejný kľúč je verejne dostupná informácia. Keďže podpisovateľ môže mať viac dvojíc kľúčov, overovanie elektronického podpisu sa nerobí na základe verejného kľúča podpisovateľa, ale na základe toho verejného kľúča (podpisovateľa), ktorý tvorí dvojicu so súkromným kľúčom, použitým na vytvorenie daného elektronického podpisu.

Zákon bude upravovať používanie elektronického podpisu v otvorených systémoch z dôvodov uvedených vo všeobecnej časti dôvodovej správy. Systémy, ktoré nie sú otvorené, sa považujú za uzavreté. V uzavretých systémoch sa môžu používať aj iné postupy, ako predpisuje tento zákon. Tieto však platia len v hraniciach daného systému ale nemusia platiť mimo neho. Na druhej strane zákon vychádza z medzinárodných noriem a štandardov a preto je vysoko pravdepodobné, že aj v uzavretých systémoch bude platiť väčšina pravidiel, ktoré stanovuje zákon.

Dôveryhodnosť elektronického podpisu ako potvrdenia identity podpisovateľa závisí od toho, nakoľko spoľahlivo sa podarí spojiť verejný (overovací) kľúč a identitu jeho držiteľa. Na to slúži elektronický dokument, certifikát, podrobne popísaný v § 8 a 9. Aby certifikát mohol spoľahlivo slúžiť na overovanie planosti elektronických podpisov, musí niekto garantovať, že údaje uvedené v certifikáte sú platné. Aktivity spojené so správou certifikátov majú charakter služieb; na jednej strane je poskytovateľ týchto služieb, na druhej strane je klient, ktorý o tieto služby žiada a platí za ne. V súlade so Smernicou sa medzi *certifikačné služby* zaraďujú popri službách súvisiacich so správou certifikátov aj ďalšie služby súvisiace s elektronickými podpismi.

Certifikačné služby majú dve úrovne. Vyššiu úroveň tvoria *akreditované certifikačné služby*, ktoré predpokladajú dodržiavanie vyšších, najmä bezpečnostných požiadaviek a štandardov. Tieto podmienky rámcovo stanovuje zákon a podrobne ich rozpracuje vykonávacia vyhláška. Akreditácia je predpokladom pre vydávanie certifikátov vyššej úrovne (kvalifikovaných certifikátov), pomocou ktorých sa overuje platnosť zaručených elektronických podpisov, ktoré zasa majú právne účinky vlastnoručných podpisov. Požiadavky na akreditáciu majú oporu aj v Smernici.

Zákon rozlišuje pojmy certifikačné služby a *certifikačné činnosti*. Certifikačné činnosti sú širším pojmom, popri certifikačných službách zahŕňajú aj podporné činnosti, nevyhnutné pre poskytovanie certifikačných služieb ako je napr. prevádzka technických zariadení a administratívna činnosť. Viaceré z požiadaviek, najmä bezpečnostných sa vzťahuje na certifikačné činnosti, ktoré nie sú certifikačnými službami.

Pod *správu certifikátov* spadajú všetky certifikačné činnosti súvisiace so životným cyklom certifikátu - od vydania, až po zánik platnosti a archiváciu. V § 3, ods. (15) sa zavádza pojem poskytovateľa certifikačných služieb. Kľúčovú úlohu pri vytváraní infraštruktúry verejného kľúča zahrávajú poskytovatelia certifikačných služieb, ktorí vykonávajú správu certifikátov.

Definícia *produktu pre elektronický podpis* je prevzatá zo Smernice a tento veľmi široký pojem označuje tak technické zariadenia, ako aj programové produkty, ktoré sa používajú v súvislosti s elektronickými podpismi. Zmysel tohto pojmu v zákone je dvojaký - jednak tvorcovia a dodávatelia produktov pre elektronický podpis môžu byť poskytovateľmi certifikačných služieb (a bude sa na nich vzťahovať požiadavka Smernice, aby poskytovanie certifikačných služieb nebolo viazané na žiadne povolenie). Na druhej strane tieto produkty musia spĺňať isté medzinárodne uznávané štandardy a zákon predpokladá, že Úrad bude posudzovať tieto produkty a vydávať im osvedčenia, aby tí, ktorí ich budú používať, mali záruku, že spĺňajú požiadavky stanovené zákonom.

Úrad pre elektronický podpis bol popísaný vo všeobecnej časti dôvodovej správy.

Poskytovateľ certifikačných služieb je fyzická osoba alebo právnická osoba, ktorá ponúka hociktoré z certifikačných služieb. Špecifická skupina certifikačných činností, definovaná ako správa certifikátov, je nevyhnutnou podmienkou pre používanie elektronického podpisu. Poskytovateľ certifikačných služieb, ktorý vykonáva všetky certifikačné činnosti patriace do správy certifikátov, sa nazýva *certifikačná autorita*. Ide o technický termín, ktorý je v odbornej verejnosti zaužívaný. Certifikačná autorita teda musí vykonávať správu certifikátov a okrem toho môže poskytovať aj iné certifikačné služby, resp. vykonávať certifikačné činnosti.

Akreditovaná certifikačná autorita musela Úradu preukázať svoju spôsobilosť vykonávať správu certifikátov na kvalitatívne vyššej úrovni (najmä pokiaľ ide o bezpečnosť, technologické, personálne a finančné zabezpečenie). Na základe toho jej Úrad udelí oprávnenie vydávať kvalifikované certifikáty (§ 8). Podrobne o akreditácii pojednáva § 14.

Na Slovensku pravdepodobne nebude veľa certifikačných autorít. Na zvýšenie dostupnosti certifikačných služieb certifikačná autorita môže vytvoriť vlastné organizačné zložky, ktoré budú zabezpečovať kontakt certifikačnej autority s klientami, alebo uzavrieť zmluvu s fyzickou osobou alebo právnickou osobou o tom, že bude poskytovať vybrané certifikačné služby v jej mene. Keďže ide v prvom rade o prijímanie žiadostí klientov o vydanie certifikátu spojených s ich registráciou a overením totožnosti, v odbornej terminológii sa poskytovateľ certifikačných služieb tohto typu nazýva *registračnou autoritou*. Podrobnejšie o registračnej autorite a jej vzťahu k certifikačnej autorite hovorí § 18.

Na vytvorenie elektronického podpisu (elektronického dokumentu) je potrebný súkromný kľúč (a príslušný elektronický dokument). *Podpisovateľom* (entitou, ktorá vytvára elektronický podpis elektronického dokumentu) môže byť len fyzická osoba, ktorá má na vytvorenie elektronického podpisu dokumentu predpoklady: je držiteľom súkromného kľúča a je schopná elektronický podpis vytvoriť (napr. má zariadenie na

vytvorenie elektronického podpisu a pozná heslo na odblokovanie v ňom uloženého súkromného kľúča). Podpisovateľ môže vytvárať elektronický podpis buď vo svojom vlastnom mene, alebo v mene fyzickej alebo právnickej osoby, ktorú zastupuje. Aby sa dalo rozlíšiť, koho vlastne reprezentuje podpisovateľ, certifikát verejného kľúča, ktorý sa použije na overenie elektronického podpisu, obsahuje informáciu o podpisovateľovi (napr. jeho postavení v zamestnaní) a ohraničenia na použitie certifikátu (napríklad na výšku transakcií). Podrobnosti o obsahu certifikátu a kvalifikovaného certifikátu upravuje zákon v § 8, resp. § 9.

Existuje viacero druhov certifikátov. Zákon sa zaoberá certifikátmi verejných kľúčov. Tieto certifikáty môžu vydávať certifikačné autority (pre svojich klientov) a Úrad (pre akreditované certifikačné autority.) Úrad si vydáva svoj vlastný certifikát verejného kľúča. Neakreditované certifikačné autority si taktiež vydávajú vlastné certifikáty na svoje verejné kľúče. Dve (akreditované aj neakreditované) certifikačné autority si môžu vzájomne vydať certifikáty svojich verejných kľúčov (čo sa nazýva krížová certifikácia). Úrad môže vykonať krížovú certifikáciu s orgánom v zahraničí, ktorý je na tej istej úrovni, (§ 25, ods. (1), písm. (c)). Vydávanie certifikátov rozličnými subjektami má mnoho podobných čŕt.. Aby nebolo potrebné rozoberať zvlášť vydávanie certifikátov certifikačnými autoritami, akreditovanými certifikačnými autoritami a Úradom, keď sa v zákone hovorí o vydávaní certifikátu a nie je potrebné rozlišovať, ktorý z uvedených subjektov a aký typ certifikát vydáva, používa sa v zákone na ich označenie pojem *vydavateľ certifikátov*.

Entita, ktorej bol vydaný certifikát verejného kľúča, sa nazýva *držiteľom certifikátu*. V súlade s vyššie uvedeným môže byť držiteľom certifikátu klient, certifikačná autorita a Úrad.

Na overenie elektronického podpisu je potrebné mať popri potrebnej informácii (podpísaný elektronický dokument a elektronický podpis, verejný kľúč prislúchajúci k súkromnému kľúču, pomocou ktorého bol príslušný elektronický podpis vytvorený), aj isté technické prostriedky (napr. počítač a pripojenie na Internet). Tie nemusí mať napr. osoba, ktorej je elektronicky podpísaný elektronický dokument určený. Preto overovanie elektronického podpisu je certifikačnou službou a jej poskytovateľ (*overovateľ elektronického podpisu*) nemusí byť totožný s príjemcom elektronického dokumentu. Overovateľom elektronického podpisu na druhej strane môže byť aj príjemca elektronicky podpísaného dokumentu, ak to je schopný sám spraviť v súlade s postupmi, stanovenými Úradom.

Na vytváranie časovej pečiatky je potrebné technické zariadenie, ktoré bude mať zabudovaný spoľahlivý zdroj časových údajov alebo bude pripojiteľné na takýto zdroj. *Bezpečné zariadenie na vytváranie časovej pečiatky,* ktoré sa v podstate zakladá na bezpečnom zariadení pre vytváranie elektronického podpisu, bude schopné pripojiť k predloženému elektronickému dokumentu časový údaj a takto doplnený dokument podpísať zaručeným elektronickým podpisom. Aby nebola časová pečiatka spochybniteľná, musí Úrad stanoviť požiadavky na zdroj spoľahlivých časových údajov, technické parametre bezpečného zariadenia na vytváranie časovej pečiatky, ako aj procedúry, ktoré by toto zariadenie malo podporovať.

* * *

Druhá časť zákona popisuje najdôležitejšie objekty súvisiace s elektronickým podpisom: elektronický podpis, zaručený elektronický podpis, certifikát, kvalifikovaný certifikát, zoznam zrušených certifikátov a časovú pečiatku.

K § 4

Definícia elektronického podpisu vychádza zo Smernice. Podľa nej "obyčajný" elektronický podpis (v Smernici "elektronický podpis") zaručuje autentickosť dokumentu - t.j. to, že dokument nebol dodatočne, po vytvorení elektronického podpisu nepozorovane zmenený. Táto požiadavka neznamená, že elektronicky podpísaný dokument je odolný voči akýmkoľvak pokusom o zmenu, ale to, že tieto zmeny nebudú také, že si ich príjemca elektronicky podpísaného dokumentu nevšimne. Pri vytvorení elektronického podpisu je povinné použitie súkromného kľúča. To znamená, že definíciu "obyčajného" elektronického podpisu spĺňa digitálny podpis, ale napríklad už nie zosnímaný, digitalizovaný a k dokumentu pripojený obrázok vlastnoručného podpisu, ktorý nevyhovuje ani podmienke (a) ani podmienke (b), pretože nie je viazaný na "podpísaný" dokument takým spôsobom, ktorý by vylúčil modifikáciu dokumentu (možno ho napr. z pôvodného dokumentu vybrať a preniesť na iný dokument). Na druhej strane, tzv. kontrolná suma, alebo odtlačok dokumentu síce umožňuje zistiť narušenie pôvodného dokumentu, ale nevylučuje nahradenie pôvodného dokumentu sfalšovaným, ku ktorému sa pripojí jeho korektne vypočítaná kontrolná suma. Napokon, aj keď elektronický podpis zaručuje autentickosť dokumentu, nemusí umožniť určiť identitu podpisovateľa, pretože umožňuje síce overiť korešpondenciu medzi verejným a súkromným kľúčom, ale nemá prostriedky na spojenie verejného kľúča s identitou jeho držiteľa. (Keď príjemca dostane elektronicky podpísaný dokument, v ktorom mu oznamujú, že v nejakej súťaži vyhral hlavnú cenu a dokument je elektronicky podpísaný elektronickým podpisom v mene riaditeľa súťaže, príjemca síce môže overiť autentickosť dokumentu, ak má k dispozícii verejný (overovací) kľúč, ale nemôže sa spoľahnúť na pravdivosť obsahu dokumentu, pretože nevie, kto elektronický podpis dokumentu vytvoril.) Aj keď existujú kryptografické riešenia spĺňajúce presne kritériá kladené na "obyčajný" elektronický podpis, dá sa očakávať použitie silnejších riešení, postavených na certifikátoch, ktoré dopĺňajú chýbajúci článok medzi verejným kľúčom a identitou podpisovateľa. Medzi elektronické podpisy budú patriť aj riešenia, ktoré neúspešne ašpirovali na zaručený elektronický podpis. Rôznorodosť riešení spĺňajúcich definíciu elektronického podpisu neumožňuje preto vo všeobecnosti definovať podmienku platnosti elektronického podpisu. Predpokladá sa, že bude stanovená dohodou strán používajúcich elektronický podpis, zohľadňujúca použitú technológiu a postupy pri vytváraní a overovaní elektronického postupu.

K § 5

Vyššou a z hľadiska zákona aj najvyššou kategóriou elektronického podpisu je zaručený elektronický podpis. Zaručený elektronický podpis spĺňa dodatočné požiadavky: bol vytvorený pomocou bezpečného zariadenia na vytváranie elektronického podpisu, toto zariadenie môže byť pod výlučnou kontrolou podpisovateľa a na verejný kľúč prislúchajúci k súkromnému kľúču použitému na jeho vytvorenie, existuje kvalifikovaný certifikát. Tým sú splnené požiadavky Smernice na zaručený elektronický podpis, pretože na základe kvalifikovaného certifikátu sa dá jednoznačne určiť identita

podpisovateľa. Podpisovacie zariadenie môže mať podpisovateľ pod výlučnou kontrolou; zákon mu kladie za povinnosť, aby chránil svoj súkromný kľúč. To znamená, že len zanedbaním povinností zo strany podpisovateľa môže dôjsť k prezradeniu jeho verejného kľúča a možnosti vytvárať falošné zaručené podpisy. Zaručený elektronický podpis musí mať podľa Smernice (Dodatok I, písm (h)) aj poskytovateľ certifikačných služieb vydávajúci kvalifikované certifikáty, t.j. podľa zákona akreditovaná certifikačná autorita a Úrad. Za tieto entity budú vytvárať zaručené elektronické podpisy poverené fyzické osoby spôsobom, ktorý umožní jednoznačne určiť fyzickú osobu, ktorá daný elektronický podpis vytvorila a na druhej strane klientovi umožní overovanie platnosti zaručeného elektronického podpisu (Úradu a akreditovanej certifikačnej autority) štandardným spôsobom. Zaručené elektronické podpisy Úradu a akreditovanej certifikačnej autority sa budú vyskytovať v kvalifikovaných certifikátoch, ktoré tieto entity vydávajú. Úrad aj akreditovaná certifikačná autorita budú potrebovať používať zaručené elektronické podpisy aj na iné účely, ako je vydávanie kvalifikovaných certifikátov (napríklad vydávanie zoznamu zrušených certifikátov, službu časových pečiatok, vedenie archívu a pod.) Keďže od zaručeného elektronického podpisu akreditovanej certifikačnej autority (Úradu) sa bude odvodzovať platnosť množstva zaručených elektronických podpisov, bude spôsob vytvárania zaručeného elektronického podpisu akreditovanej certifikačnej autority a Úradu potrebné upraviť detailne vyhláškou Úradu, aby sa zaručila vysoká úroveň bezpečnosti a jednoduché overovanie platnosti daného zaručeného podpisu.

Aby bol zaručený elektronický podpis platný, musí existovať kvalifikovaný certifikát na verejný kľúč, pomocou ktorého sa dá podpis overiť. Tento kvalifikovaný certifikát musí byť v čase vytvorenia zaručeného elektronického podpisu platný. (Keďže certifikát má obmedzenú dobu platnosti, bez vyššie uvedeného ustanovenia by po uplynutí doby platnosti kvalifikovaného certifikátu stratili platnosť všetky zaručené elektronické podpisy, ktoré sa opierali o daný kvalifikovaný certifikát.) Napokon, musí sa dať overiť, či dokument nebol po podpísaní modifikovaný. Keďže zaručený elektronický podpis je zvláštnym prípadom "obyčajného" elektronického podpisu, garantuje aj autentickosť elektronicky podpísaného elektronického dokumentu. Ak sú pre zaručený elektronický podpis uvedené tri podmienky splnené, je platný. Ak elektronický podpis nespĺňa požiadavky ods. (5), písm. (a) alebo (b), zostáva "obyčajným" elektronickým podpisom, nakoľko spĺňa požiadavku na spôsob vytvárania a garanciu autentickosti podpísaného dokumentu.

Pri overovaní zaručeného elektronického podpisu je potrebné overiť aj platnosť zaručeného elektronického podpisu Úradu na kvalifikovanom certifikáte obsahujúcom verejný kľúč akreditovanej certifikačnej autority. Na overenie elektronického podpisu Úradu je potrebné poznať verejný kľúč Úradu. Ten síce môže byť uvedený v kvalifikovanom certifikáte, ale kto taký certifikát vydá, a hlavne, čím ho podpíše? Postupnosť (kvalifikovaných) certifikátov verejných kľúčov nemôže byť nekonečná, ani cyklická a musí sa niekde nejako začať. Tým začiatkom je zaručený certifikát verejného kľúča Úradu, ktorý si Úrad sám vydal a podpísal súkromným kľúčom, prislúchajúcim ku kľúču, ktorý je uvedený v certifikáte! Aby bolo možné certifikát použiť, treba ho overiť a to sa dá spraviť tak, že verejný kľúč Úradu bude dostupný ešte z iného spoľahlivého a dôveryhodného zdroja. Tým sa vytvorí pevný bod, na ktorom je možné postaviť dôveru v certifikáty a elektronické podpisy akreditovaných certifikačných autorít, podliehajúcich Úradu.

K § 6

Elektronický podpis možno používať všade tam, kde to výslovne nezakazuje zákon. Podmienky si dohodnú zainteresované strany.

Jedným z cieľov zavádzania elektronických podpisov je aj zjednodušenie administratívy tým, že sa niektoré procedúry (napríklad podávania a spracúvania žiadostí a dokumentov štandardného formátu) zautomatizujú. Ak bude potrebné zaistiť autentickosť dokumentov elektronickým podpisom, bude na to potrebné použiť zaručený elektronický podpis. Použitie "obyčajného" elektronického podpisu by mohlo spôsobovať problémy s jeho overovaním, a preto zákon s jeho používaním v otvorených systémoch verejnej správy neuvažuje. Na druhej strane, môžu napr. štátne orgány, orgány miestnej samosprávy a podobné inštitúcie vytvárať pre vlastné potreby uzavreté systémy s redukovanou PKI a používať v nich aj obyčajné elektronické podpisy.

K § 7

Platný zaručený elektronický podpis má rovnakú právnu váhu ako vlastnoručný podpis, nakoľko podmienky na jeho vytvorenie spĺňajú požiadavky stanovené § 40 ods. 4 Zák.č.40/1964 Zb. (Občiansky zákonník).

Podľa Smernice však nie je možné zamietnuť možnosť použiť elektronický podpis len preto, že je v elektronickej forme alebo preto, že nespĺňa náležitosti zaručeného elektronického podpisu. Zákon preto v súlade so Smernicou neodmieta možnosť použiť na právne úkony aj "obyčajný" elektronický podpis. Aby však bol "obyčajný" elektronický podpis použiteľný pre právne úkony, musí ten kto ho na tento účel hodlá použiť, dokázať, že daný elektronický podpis bol vytvorený spôsobom, ktorý zaručuje splnenie vyššie uvedených požiadaviek Občianskeho zákonníka.

K § 8

Certifikát je elektronický dokument, ktorý vydáva dôveryhodná tretia strana (vydavateľ certifikátu) na verejný kľúč držiteľa certifikátu. Týmto dokumentom spája identitu držiteľa certifikátu s verejným kľúčom, ktorý je v certifikáte uvedený a umožňuje tak, ako bolo povedané vyššie, priradiť k elektronickému podpisu identitu podpisovateľa.

Existujú medzinárodné štandardy, ktoré upravujú formát certifikátu. Štandardný formát certifikátu je dôležitý preto, lebo certifikát sa bude spracúvať pomocou programu. Ak by sa certifikát hoci v nepatrnej miere odchyľoval od predpísaného formátu, program by ho mohol spracovať nesprávne, alebo by ho vôbec nedokázal spracovať. Formát certifikátu uvedený v zákone vychádza zo štandardu X 509 v3. Skladá sa z dvoch častí - informačnej a kontrolnej. V informačnej časti certifikátu, nazývanej v zákone telo certifikátu, sa uvádzajú údaje, ktoré umožnia určiť vydavateľa certifikátu a samotný certifikát. Tieto údaje sú dôležité kvôli tomu, že keď sa bude overovať elektronický podpis, bude potrebné overiť aj platnosť certifikátu verejného kľúča, pomocou ktorého sa elektronický podpis overuje. To znamená, že bude potrebné u vydavateľa daného certifikátu zistiť, či je ešte daný certifikát platný.

Držiteľ certifikátu môže v certifikáte uviesť svoje meno, alebo pseudonym. Ak však uvedie pseudonym, musí sa v prípade potreby dať jednoznačne určiť, kto je za daným pseudonymom (napríklad na základe čísla certifikátu, pseudonymu a osobných údajov držiteľa certifikátu, ktoré si pri prijímaní žiadosti o vydanie certifikátu vyžiadal a potom uchoval vydavateľ certifikátu). Certifikát nemá neobmedzenú platnosť, vydáva sa na určitý čas, ktorý musí byť v certifikáte presne určený - údajom o začiatku a konci platnosti certifikátu. Rozhodujúcou informáciou uvedenou v certifikáte je verejný kľúč držiteľa certifikátu. Aby sa uľahčilo použitie certifikátu, obsahuje certifikát aj údaje o algoritmoch, v ktorých sa v ňom uvedený verejný kľúč dá použiť. Bez tejto informácie by sa mohlo stať, že by sa overovateľ elektronického podpisu pri overovaní elektronického podpisu snažil na to použiť nesprávny algoritmus (a mohol tak zamietnuť platný elektronický podpis). Kontrolnú časť certifikátu tvorí elektronický podpis vydavateľa certifikátu, ktorým vydavateľ certifikátu potvrdzuje platnosť údajov uvedených v informačnej časti certifikátu. Aby bolo možné overiť elektronický podpis vydavateľa certifikátu, je potrebné vedieť, aký algoritmus sa použil na vytvorenie tohto elektronického podpisu. Táto informácia je tiež uvedená v informačnej časti certifikátu. Certifikát môže okrem výslovne uvedených údajov obsahovať aj iné údaje. Najčastejšie sa zvyknú uvádzať atribúty držiteľa certifikátu (napríklad jeho titul, adresa, zamestnanie a pod.)

Vydavateľ certifikátu nemôže vytvoriť podpis certifikátu pomocou ľubovoľného súkromného kľúča, ale len pomocou súkromného kľúča, ktorý je na to určený. Dôvodom tejto požiadavky je, že overovateľ elektronického podpisu bude potrebovať aj verejný kľúč na overenie platnosti elektronického podpisu vydavateľa certifikátu, ktorým je certifikát podpísaný. Tento verejný kľúč bude používať veľký počet potenciálnych overovateľov elektronických podpisov, a preto by mal byť dostupný zo spoľahlivého a hodnoverného zdroja. Používanie rozličných kľúčov na vytváranie elektronických podpisov vydavateľa certifikátu by komplikovalo overovanie týchto podpisov a spôsobovalo aj bezpečnostné riziká.

Aby "domáci" overovateľ mohol overiť elektronický podpis, vytvorený pomocou súkromného kľúča, na verejný kľúč ktorého vydal certifikát "cudzí" vydavateľ certifikátov, vydajú si domáci a cudzí vydavateľ certifikátov navzájom certifikáty na svoje verejné kľúče. Takéto certifikáty sa nazývajú krížovými certifikátmi (pretože sa najčastejšie vydávajú reciprocne) a používajú sa nasledovne: overovateľ má elektronický dokument podpísaný elektronickým podpisom, ku ktorému má certifikát verejného kľúča, vydaný cudzím vydavateľom certifikátov a krížový certifikát verejného kľúča cudzieho vydavateľa certifikátov, vydaný domácim vydavateľom certifikátov. Keďže pozná verejný kľúč domáceho vydavateľa certifikátov, overí pomocou neho elektronický podpis na krížovom certifikáte; ak je tento podpis v poriadku, overovateľ vie, že verejný kľúč uvedený v krížovom certifikáte je verejným kľúčom cudzieho vydavateľa certifikátov. Pomocou verejného kľúča cudzieho vydavateľa certifikátov potom overí podpis na certifikáte verejného kľúča a napokon použije verejný kľúč uvedený v tomto certifikáte na overenie elektronického podpisu elektronického dokumentu.

Certifikát môže byť z rozličných dôvodov zrušený ešte pred uplynutím riadnej doby jeho platnosti. Certifikát ruší certifikačná autorita, ktorá ho spravuje a tým ukončuje jeho platnosť. Zrušenie certifikátu neznamená, že sa zrušený certifikát vymaže z pamäti,

skartuje alebo zabudne. Zrušenie certifikátu znamená, že certifikát nemožno používať na overovanie elektronických podpisov, vytvorených pomocou súkromného kľúča prislúchajúceho k verejnému kľúču uvedenému v certifikáte, po okamihu, keď bol daný certifikát zrušený. Na druhej strane, zrušený certifikát sa bude stále používať na overenie platnosti elektronických podpisov, vytvorených pomocou súkromného kľúča prislúchajúceho k verejnému kľúču uvedenému v certifikáte, ktoré boli vytvorené počas doby platnosti certifikátu (t.j. od začiatku jeho platnosti, po okamih jeho zrušenia). Rušenie certifikátov je mimoriadne dôležitá činnosť a bude ešte podrobne popísané v ďalších častiach.

K § 9

Na overenie zaručeného elektronického podpisu sa používa kvalifikovaný certifikát. Kvalifikovaný certifikát je certifikát verejného kľúča - fyzickej osoby, akreditovanej certifikačnej autority, krížový certifikát akreditovanej certifikačnej autority a Úradu. Po formálnej stránke sa od obyčajného certifikátu odlišuje tým, že je v ňom výslovne uvedené: že je akreditovaným certifikátom, na aký účel sa môže používať (prípadne ohraničenia na jeho použitie). Kvalifikovaný certifikát môže vydať akreditovaná certifikačná autorita fyzickej osobe a inej akreditovanej certifikačnej autorite, Úrad akreditovanej certifikačnej autorite a Úrad sám sebe na svoj verejný kľúč. Kvalifikovaný certifikát musí obsahovať zaručený elektronický podpis vydavateľa certifikátu. Kvalifikovaný certifikát je platný, ak mu neuplynula doba platnosti, nebol zrušený a je podpísaný platným zaručeným elektronickým podpisom vydavateľa zaručených certifikátov.

K § 10

Zrušenie certifikátu musí byť nejakým spôsobom dokumentované pre všetkých potenciálnych overovateľov elektronických podpisov, ktorí by na overenie elektronického podpisu chceli použiť daný (zrušený) certifikát. Aby nedošlo k sporu o platnosť elektronického podpisu vytvoreného v istom časovom okamihu a vymáhaniu škody spôsobenej použitím dokumentu podpísaného elektronickým podpisom, pre ktorý bol certifikát verejného kľúča zrušený, overovateľ elektronického podpisu musí mať možnosť spoľahlivým spôsobom overiť, či certifikát, pomocou ktorého overuje platnosť elektronického podpisu je v danom okamihu platný, alebo už bol zrušený. Zoznam zrušených certifikátov je jedným zo základných riešení tohto problému. Zoznam zrušených certifikátov vytvára a udržuje certifikačná autorita pre tie certifikáty, ktoré spravuje a zverejňuje na ňom certifikáty, ktorým predčasne ukončila platnosť. Zmysel zoznamu zrušených certifikátov je nasledovný: podpisovateľ podpíše nejaký záväzok napríklad pomocou zaručeného elektronického podpisu a potom požiada príslušnú certifikačnú autoritu o zrušenie svojho certifikátu. Príjemca elektronicky podpísaného záväzku si potrebuje overiť elektronický podpis, aby sa presvedčil o platnosti zmluvy. Má k dispozícii (kvalifikovaný) certifikát verejného kľúča. Ak by sa nepresvedčil o platnosti certifikátu, mohol by podpisovateľ odmietnuť uznať svoj elektronický podpis a tvrdiť, že tento podpis vytvoril niekto namiesto neho. Ak však certifikačná autorita vedie zoznam zrušených certifikátov, overovateľ počká na vydanie aktuálneho zoznamu zrušených certifikátov a ak v ňom nenájde ten, ktorý chce použiť, môže pomocou neho overiť elektronický podpis. Zoznam zrušených certifikátov má opäť medzinárodnými štandardami stanovený presný formát. Aby nebolo možné sfalšovať ho, vydaný zoznam

zrušených certifikátov sa podpisuje elektronickým podpisom. Na vytvorenie elektronického podpisu zoznamu zrušených certifikátov sa z bezpečnostných dôvodov používa zvláštny súkromný kľúč.
Podobne sa sa vytvára aj zoznam zrušených kvalifikovaných certifikátov. Oproti zoznamu zrušených "obyčajných" certifikátov sa pri vytváraní zoznamu zrušených kvalifikovaných certifikátov musia používať bezpečné zariadenia a procedúry, aby sa neznížila dôveryhodnosť zaručených elektronických podpisov. Porovnateľná úroveň bezpečnosti je podmienkou pre uznávanie slovenských (kvalifikovaných) certifikátov v zahraničí a procedúry rušenia (kvalifikovaných) certifikátov, vytvárania a sprístupňovania zoznamu zrušených (kvalifikovaných) certifikátov patria medzi tie, od ktorých v rozhodujúcej miere závisí dôveryhodnosť a tým aj použiteľnosť (kvalifikovaných) certifikátov. Preto podrobnosti o rušení kvalifikovaných certifikátov, formáty potrebných dokumentov, spôsob a frekvenciu vydávania, resp. spôsob sprístupňovania zoznamu zrušených kvalifikovaných certifikátov stanoví Úrad jednotne na základe medzinárodných štandardov. Pre rušenie kvalifikovaných certifikátov sú ustanovenia Úradu záväzné; pre rušenie "obyčajných" certifikátov majú - ak to výslovne nebude uvedené inak - charakter odporúčaní.

K § 11

Pri používaní elektronických dokumentov v obchodnom a úradnom styku bude potrebné (o.i.) mať možnosť dôveryhodným spôsobom určiť, kedy sa s daným elektronickým dokumentom niečo robilo (napríklad, určiť presný termín podania daňového priznania). To sa dá spraviť tým spôsobom, že nezávislá dôveryhodná tretia strana na predložený elektronický dokument vydá časovú pečiatku. Časová pečiatka sa vytvára tak, že sa k elektronickému dokumentu pripojí časový údaj (a prípadne iné identifikačné údaje) a celé sa to (dokument + časový údaj) podpíše zaručeným elektronickým podpisom vydavateľa časových pečiatok (akreditovanej certifikačnej autority). Časová pečiatka potom dokazuje, že daný elektronický dokument existoval v čase (údaj o ktorom k dokumentu pred vytvorením zaručeného elektronického podpisu pridal vydavateľ časovej pečiatky) uvedenom v dokumente. Ak vznikne potreba zistiť, či daný elektronický dokument, ku ktorému bola vydaná časová pečiatka, v nejakom termíne už existoval, overí sa zaručený elektronický podpis vydavateľa časovej pečiatky. Ak je tento zaručený elektronický podpis platný, je zaručená neporušenosť (autentickosť) elektronického dokumentu, a teda aj platnosť časového údaja, ktorý obsahuje. Časové pečiatky sa budú používať aj na označovanie zoznamov zrušených kvalifikovaných certifikátov, záznamov o prevádzke systémov akreditovanej certifikačnej autority a ďalších dokumentov, ktoré vznikajú v súvislosti s certifikačnými činnosťami a pri ktorých je potrebné dôveryhodným spôsobom preukázať čas, kedy boli vytvorené. V porovnaní s vytváraním zaručeného elektronického podpisu vzniká pri vytváraní časovej pečiatky ešte jeden závažný problém - odkiaľ zobrať hodnoverný časový údaj. Sú v podstate možné dve riešenia - buď bude zdroj spoľahlivého časového údaju súčasťou bezpečného zariadenia na vytváranie časovej pečiatky, alebo ho bude toto zariadenie získavať z externého dôveryhodného zdroja spoľahlivým spôsobom. Technické podrobnosti prijateľného riešenia bude špecifikovať Úrad.

* * *

V tretej časti zákona sú popísané subjekty, ktoré tvoria infraštruktúru verejného kľúča (PKI); funkcie, ktoré plnia, ich povinnosti a vzájomné vzťahy.

K § 12

Najvyšším orgánom štátnej správy pre elektronický podpis je Úrad pre elektronický podpis. Tento, ako bolo už uvedené vo všeobecnej časti dôvodovej správy, plní v podstate dve hlavné funkcie: vykonáva dohľad nad dodržiavaním zákona o elektronickom podpise a je najvyššou certifikačnou autoritou v Slovenskej republike. Plnenie týchto funkcí si vyžaduje špecializované technické vybavenie, chránené priestory, kompetencie a vysokokvalifikovaných odborníkov. Vybudovanie samostatného funčného Úradu pre elektronický podpis by bola drahá a časovo náročná záležitosť. Viaceré činnosti, ktoré má Úrad pre elektronický podpis podľa zákona o elektronickom podpise vykonávať, súvisia s činnosťami Národného bezpečnostného úradu a obe tieto inštitúcie by mali úzko spolupracovať. Preto je prirodzené a účelné vytvoriť Úrad pre elektronický podpis ako súčasť NBÚ.

Aby Úrad mohol vykonávať dozor nad dodržiavaním zákona, musí mať možnosť kontrolovať subjekty, na ktoré sa zákon vzťahuje - na certifikačné a registračné autority, akreditované certifikačné autority. Kontrolované subjekty musia pracovníkom Úradu vykonávajúcim kontrolu umožniť prístup k svojim systémom a poskytnúť im požadované informácie týkajúce sa certifikačných činností; na druhej strane sú pracovníci Úradu povinní zachovávať mlčanlivosť o skutočnostiach, ktoré sa pri výkone kontroly dozvedeli. Podrobnejšie popisuje kontrolu a audit § 28 a § 29. Úrad môže ukladať kontrolovanej certifikačnej autorite (registračnej autorite) nápravné opatrenia a pri vážnom porušení zákona a všeobecne záväzných predpisov ním vydaných, udeľovať certifikačnej autorite sankcie.

Úrad registruje "obyčajné" certifikačné autority pôsobiace v SR. Tie, ktoré dosahujú vyššiu úroveň poskytovaných certifikačných služieb, môžu požiadať o Úrad o akreditáciu. Úrad má vypracovanú (verejne dostupnú) akreditačnú schému a pri posudzovaní žiadosti o akreditáciu overí, či certifikačná autorita spĺňa kritériá stanovené v tejto schéme. Ak áno, vydá jej osvedčenie o akreditácii a zaradí ju do zoznamu akreditovaných certifikačných autorít pôsobiacich na území SR. Ak nie, odmietne jej udeliť akreditáciu. Akreditovaná certifikačná autorita musí počas svojej činnosti spĺňať kritériá akreditačnej schémy. Ak si nedokáže udržať potrebnú úroveň, Úrad jej odníme akreditáciu.

Úrad vedie zoznam akreditovaných certifikačných autorít pôsobiacich na území SR a zoznam certifikačných autorít, ktorým odňal akreditáciu. V tomto zozname sú aj zahraničné akreditované certifikačné autority, ktoré akreditoval Úrad, alebo ktorým Úrad priznal postavenie akreditovanej certifikačnej autority na základe medzinárodnej zmluvy. Zoznam akreditovaných certifikačných autorít musí byť verejne prístupný, aby bolo možné vybrať si poskytovateľa akreditovaných certifikačných služieb v SR. Tento zoznam Úrad bude spolu s akreditačnou schémou (v súlade so Smernicou EÚ) poskytovať Európskej komisii.

Úrad vydáva akreditovaným certifikačným autoritám, ktorým udelil akreditáciu, alebo zahraničným certifikačným autoritám, ktorým uznal akreditáciu, kvalifikované

certifikáty verejných kľúčov. Tým im umožní vydávať kvalifikované certifikáty pre klientov (alebo aj pre vlastnú potrebu, napríklad pre operátorov zabezpečujúcich vedenie archívu, vydávanie zoznamu zrušených certifikátov, vydávanie certifikátov a pod., ak to umožnia predpisy upravujúce činnosť akreditovaných certifikačných autorít, vydané Úradom). Úrad predstavuje aj najvyššie postavenú certifikačnú autoritu, akreditovanú zo zákona, a preto si musí sám vystaviť kvalifikovaný certifikát svojho vlastného verejného kľúča. (Zdôvodnenie tohoto postupu je uvedené v časti dôvodovej správy k § 5.) Ak akreditovaná certifikačná autorita ukončí svoju činnosť, alebo jej Úrad odníme akreditáciu, Úrad zruší kvalifikovaný certifikát verejného kľúča, ktorý jej vydal (a zverejní ho v svojom zozname zrušených kvalifikovaných certifikátov). V súvislosti so správou kvalifikovaných certifikátov Úradom (to sú tie kvalifikované certifikáty, ktoré Úrad sám vydal, alebo prevzal do správy po zániku akreditovanej certifikačnej autority) sa Úrad riadi pravidlami pre správu kvalifikovaných certifikátov akreditovanými certifikačnými autoritami, ktoré sám v podobe všeobecne záväzného právneho predpisu vydal.

Na vytvorenie a prevádzku PKI bude potrebných veľa technických zariadení, programov, resp. na nich postavených systémov. Certifikačné autority nemajú kvalifikovaných odborníkov ani technické prostriedky na to, aby analyzovali, či tieto prostriedky pre elektronický podpis spĺňajú kritériá dostatočné na to, aby pomocou nich bolo možné vytvoriť systém vyhovujúci akreditačnej schéme, resp. taký, ktorý vyhovuje medzinárodným kritériám. Úrad preto bude musieť vytvoriť certifikačné pracovisko, ktoré bude testovať rozličné produkty pre elektronický podpis a vydávať im osvedčenia, posudzovať súlad medzinárodne certifikovaných produktov s domácimi kritériami. Okrem toho bude musieť sledovať vývoj v oblasti informačnej bezpečnosti a kryptológie, aby dokázal v dostatočnom predstihu zareagovať na zastarávanie používaných riešení, meniace sa medzinárodné normy (ako napríklad nedávne nahradenie medzinárodného šifrovacieho štandardu DES novým štandardom - AES). Poznatky, ktoré Úrad takto získa sa premietnu do technických noriem a právnych predpisov, upravujúcich používanie elektronického podpisu a prevádzku PKI.

Úrad musí byť pripravený plniť aj iné úlohy, ktoré sa po nadobudnutí účinnosti zákona objavia. Vzhľadom na to predpokladaný rozsah a charakter úloh ktoré bude musieť Úrad riešiť, bude pravdepodobne presahovať jeho personálne možnosti, zákon predpokladá, že Úrad bude spolupracovať so štátnymi aj súkromnými organizáciami a odborníkmi, napríklad z akademickej a súkromnej sféry.

K § 13

Prvoradou úlohou certifikačnej autority je správa certifikátov; t.j. vydávanie, overovanie, rušenie a archivovanie certifikátov. Okrem toho môže certifkačná autorita vykonávať aj iné cerifikačné činnosti, alebo poskytovať iné certifikačné služby (napríklad konzultačné služby, môže poskytovať produkty pre elektronický podpis, môže školiť, može pomáhať budovať PKI pre štátne a súkromné organizácie a pod.). Tieto činnosti sa považujú za podnikanie a v súlade so Smernicou sa nevyžaduje pre ne nejaké zvláštne povolenie. Každý, kto spĺňa požiadavky stanovené týmto zákonom, môže poskytovať certifikačné služby. Ak však hodlá certifikačná autorita poskytovať certifikačné služby vyššej úrovne, akreditované certifikačné služby, musí spĺňať kritériá stanovené akreditačnou schémou vydanou Úradom a požiadať Úrad o akreditáciu.

Keďže zaručený elektronický podpis možno používať napr. na uzatváranie obchodných kontraktov, poskytovanie akreditovaných certifikačných služieb, medzi ktoré patrí aj vydávanie kvalifikovaných certifikátov, potrebných na overovanie zaručených elektronických podpisov bez predchádzajúcej akreditácie, prináša veľké riziká. Tieto riziká vyplývajú z toho, že nie je zaručené používanie bezpečných technických zariadení, dodržiavanie prevádzkových pravidiel, vhodných pracovných postupov a pod.

Certifikačná autorita musí pred začatím svojej činnosti zverejniť rozličné informácie. Zverejnené informácie by klientovi mali stačiť napr. na to, aby si vedel vybrať medzi rozličnými certrifikačnými autoritami, tú u ktorej si nechá vystaviť certifikát, čo má spraviť pre vydanie certifikátu, aké doklady na to potrebuje, ako vyzerá žiadosť o vydanie certifikátu, koľko bude vydanie certifikátu stáť, na čo sa certifikát dá použiť, aké produkty pre elektronický podpis použitie certifikátu podporujú, kde a akým spôsobom overí platnosť certifikátu, odkiaľ bude získavať zoznam zrušených certifikátov, ako často sa tento zoznam bude vydávať, ako požiadať o zrušenie vlastného certifikátu, za čo certifikačná autorita zodpovedá a za akých podmienok a pod. Podobné informácie by certifikačná autorita mala zverejňovať aj o ostatných certifikačných službách, ktoré hodlá poskytovať.

Certifikačná autorita je povinná registrovať sa ešte pred začatím činnosti na Úrade pre elektronický podpis. Zákon predpisuje potrebné doklady, ktoré musí certifikačná autorita zverejňovať a ktoré musí pri registrácii poskytnúť Úradu.

K § 14

Zmyslom akreditácie je získať oprávnenie na poskytovanie akreditovaných certifikačných služieb, ktoré predstavujú certifikačné služby vyššej úrovne. Hociktorá certifikačná autorita môže požiadať Úrad o akreditáciu. Podmienkou udelenia akreditácie je, aby certifikačná autorita spĺňala požiadavky akreditačnej schémy, stanovené Úradom vo všeobecne záväznom právnom predpise. Pôjde predovšetkým o to, aby mala technické prostriedky a priestorové podmienky potrebné na zaistenie požadovanej bezpečnostnej úrovne, dostatočné finančné prostriedky na financovanie svojej činnosti, ale aj na krytie prípadných škôd, ktoré bude musieť nahradiť, kvalifikovaný personál, schopný zaistiť prevádzku certifikačnej autority v súlade s predpísanými požiadavkami, vypracovanú základnú dokumentáciu (certifikačný poriadok, bezpečnostnú politiku a i.). Certifikačná autorita sa pred podaním žiadosti o akreditáciu podrobí bezpečnostnému auditu, ktorého cieľom je zistiť, či certifikačná autorita spĺňa požiadavky stanovené akreditačnou schémou. Tento audit nebude robiť Úrad, ale auditorská spoločnosť. Aby mal audit požadovanú odbornú úroveň a váhu, Úrad stanoví podmienky, ktoré musí spĺňať inštitúcia (auditorská spoločnosť), aby mohla vykonávať audit certifikačných autorít a udelí osvedčenie tým inštitúciám, ktoré splnenie podmienok stanovených Úradom na auditorskú spoločnosť pre certifikačné autority preukázali. Výsledok bezpečnostného auditu, spolu s údajmi o certifikačnej autorite, verejným kľúčom certifikačnej autority a údajmi, ktoré podľa zákona certifikačná autorita má zverejňovať, sú súčasťou žiadosti o akreditáciu. Úrad môže rozhodnúť na základe predložených údajov (do 90 dní od podania žiadosti o akreditáciu), alebo vykonať vlastnú kontrolu certifikačnej autority, alebo požiadať certifikačnú autoritu o doplnenie údajov. Po troch mesiacoch, predĺžených o čas

potrebný na doplňanie žiadosti, Úrad certifikačnej autorite buď akreditáciu udelí, alebo je zamietne.

Ak úrad zistí, že v minulosti ním akreditovaná certifikačná autorita nespĺňa kritériá podľa akreditačnej schémy, môže jej uložiť pokutu a navrhnúť opatrenia na nápravu. Keď akreditovaná certifikačná autorita do troch mesiacov od návrhu opatrení nedokáže stanovené opatrenia prijať a dosiahnuť nápravu zisteného stavu, Úrad jej odníme akreditáciu. Zamietnutie alebo strata akreditácie neznamená celkovú diskvalifikáciu certifikačnej autority. Tá sa môže opätovne pokúsiť získať akreditáciu. Keďže vyhodnotenie žiadosti o akreditáciu je časovo a odborne náročný proces, za žiadosť o akreditáciu sa platí správny poplatok.

K § 15

Zákon stanovuje, aké dokumenty musí mať certifikačná autorita vypracované a čím sa má pri vykonávaní certifikačných činností riadiť. V prvom rade ide o bezpečnostnú politiku. Bezpečnostná politika certifikačnej autority je postavená na identifikácii hrozieb, odhadnutí ich závažnosti a návrhu opatrení na elimináciu rizík, ktoré z hrozieb pre činnosť certifikačnej autority vyplývajú. Bezpečnostná politika zahŕňa opatrenia z oblasti fyzickej bezpečnosti, technickej, hardvérovej a softvérovej bezpečnosti, ale aj prevádzky systému a personálnej bezpečnosti. Certifikačná autorita musí mať pripravené riešenia pre prípad rozličných bezpečnostných incidentov - od krádeže technického zariadenia, cez sabotáž, nedbalosť zamestnanca, prienik hackera do systému až po poškodenie celého systému a jeho vyradenie z prevádzky na dlhší čas. Bezpečnostné aspekty sa premietajú aj do ďalšieho dôležitého materiálu - pravidiel pre výkon certifikačných činností, ktorý popisuje, akým spôsobom certifikačná autorita bude postupovať napr. pri: prijímaní žiadostí o vydanie certifikátu, generovaní kryptografických kľúčov klientom alebo pre klienta, vyhodnocovaní žiadosti o vydanie certifikátu, vydávaní certifikátu, odovzdávaní certifikátu klientovi, používaní certifikátu, overovaní certifikátu, rušení certifikátu, vypršaní platnosti certifikátu; za čo a za akých podmienok certifikačná autorita zodpovedá a pod.

Certifikačná autorita je povinná mať tieto dokumenty vypracované ešte pred začiatkom činnosti a v priebehu svojej činnosti ich dodržiavať. Úrad stanoví požiadavky, ktoré by mali byť zohľadnené v bezpečnostnej politike a pravidlách pre výkon akreditovaných certifikačných činností akreditovanej certifikačnej autority. Tak v prípade obyčajnej ako aj akreditovanej certifikačnej autority sa pri audite zisťuje, či (akreditovaná) certifikačná autorita dodržiava bezpečnostnú politiku a pravidlá certifikačných činností.

Certifikačná autorita bude mať viacero súkromných kľúčov a certifikátov. Z bezpečnostného hľadiska je dôležité, aby každý súkromný kľúč používala len na účely, na ktoré je určený. Zvlášť to platí pre súkromný kľúč, ktorý slúži na podpisovanie certifikátov verejných kľúčov. Prezradenie tohto kľúča umožní vydávanie falošných certifikátov a prakticky znamená stratu dôvery v postihnutú certifikačnú autoritu. Aby sa minimalizovalo riziko prezradenia súkromného kľúča certifikačnej autority, nesmie certifikačná autorita používať svoj súkromný kľúč (a príslušný certifikát) na iné účely, než je určené.

Základom elektronického podpisu je súkromný kľúč. Zákon neurčuje, kto bude vytvárať dvojicu asymetrických kľúčov na vytváranie a overovanie elektronických podpisov: súkromný a verejný kľúč. Ak by túto službu poskytovala certifikačná autorita, je po odovzdaní súkromného kľúča a certifikátu klientovi povinná zaistiť spoľahlivé odstránenie súkromného kľúča klienta a informácií, ktoré o ňom v systéme mala (napríklad inicializačné údaje pre generátor náhodných čísel použitý pre vytváranie kľúčov) zo systému. Ak by pri niektorých certifikačných činnostiach mala certifikačná autorita možnosť získať prístup k súkromnému kľúču klienta, nesmie sa v žiadnom prípade pokúšať kopírovať tento kľúč alebo získať nejakú informáciu o ňom (napríklad súkromný kľúč v šifrovanej podobe). Keďže v systéme certifikačnej autority sa používa viacero súkromných kľúčov na zaistenie certifikačných činností, toto obmedzenie sa na tieto kľúče nevzťahuje. Predpokladá sa však, že bezpečnostná politika a pravidlá pre výkon certifikačných činností detailne popíšu postupy, ktoré sa pri manažmente kryptografických kľúčov (vrátane súkromných kľúčov) používaných v certifikačnej autorite musia dodržiavať.

Keďže certifikačná autorita zbiera, uchováva a používa osobné údaje svojich klientov (napr. na overenie identity žiadateľa o vydanie certifikátu, o zrušenie certifikátu; na overenie ďalších údajov, ktoré sa majú uviesť v certifikáte a pod.), vzťahuje sa na ňu zákon č. 52/1998 Z.z. o ochrane osobných údajov v informačných systémoch. Preto je povinná registrovať sa v zmysle uvedeného zákona.

Vydaním certifikátu vzniká medzi certifikačnou autoritou a klientom-držiteľom certifikátu vzťah, ktorý je potrebné zmluvne upraviť. Zákon požaduje, aby zmluva mala písomný charakter a bola vlastnoručne podpísaná. Pripúšťa aj možnosť použitia zaručeného elektronického podpisu oboch zmluvných strán; v tom prípade sa však musí zhodovať identifikačný údaj v "starom" certifikáte klienta s identifikačným údajom v novom "certifikáte".

Aj keď je certifikačná autorita povinná zverejňovať svoj certifikačný poriadok, musí klienta ešte pred uzavretím zmluvy písomne informovať o tom, aké služby a za akých podmienok poskytuje, aké sú klientove práva a povinnosti. Akreditovaná certifikačná autorita je okrem toho klienta povinná písomne informovať o tom, na čo sa dajú ňou vydané kvalifikované certifikáty používať, aké sú obmedzenia na ich použitie a akým spôsobom sa riešia prípadné spory. Ak (akreditovaná) certifikačná autorita podá klientovi požadované informácie elektronicky, musí na to použiť médium s trvalým záznamom informácie, aby nedošlo k ich zničeniu, alebo úmyselnej zmene.
Certifikačná autorita je povinná poskytnúť tie isté informácie ako poskytuje žiadateľovi o certifikát aj tretej strane, napr. overovateľovi elektronického podpisu založenému na certifikáte, ktorý vydala, orgánom činným v trestnom konaní, súdu a pod.

Aby klient mohol používať elektronický podpis, certifikačná autorita ho ešte pred vydaním certifikátu musí informovať o tom, aké technické zariadenia a procedúry na vytváranie a overovanie elektronických podpisov môže použiť. Výber týchto zariadení a procedúr je ohraničený napr. parametrami kryptografických kľúčov (súkromného a verejného), použitými algoritmami (na vytváranie elektronického podpisu certifikačnej autority v certifikáte), algoritmami na vytváranie elektronického podpisu, pre ktorý je súkromný kľúč klienta určený a pod.

Akreditovaná certifikačná autorita musí klientovi - žiadateľovi o kvalifikovaný certifikát naviac poskytnúť aj zoznam bezpečných zariadení na vytvorenie elektronického podpisu a zoznam zariadení na overenie elektronického podpisu, ktorým vydal Úrad certifikát (v tomto prípade osvedčenie o zhode s bezpečnostnými a technickými požiadavkami), ktoré klient môže použiť na vytváranie a overovanie zaručených elektronických podpisov. Na základe tejto informácie si klient môže vybrať zariadenia, pomocou ktorých bude môcť vytvárať a overovať zaručené elektronické podpisy v súlade s bezpečnostnými požiadavkami Úradu.

Vývoj poznania v kryptológii a zvyšovanie výkonu počítačov môže spôsobiť, že používaný súkromný kľúč nebude po nejakom čase dosť bezpečný; napríklad, že ho bude možné efektívne vypočítať z dostupnej informácie (napr. na základe príslušného verejného kľúča). Certifikačná autorita je povinná sledovať vývoj v kryptológii a keď sa objavia pochybnosti o bezpečnosti používaných súkromných kľúčov, upozorniť svojich klientov, aby prešli na nové súkromné kľúče (napríklad na kľúče, ktoré majú väčšiu dĺžku). Odbornú pomoc bude v tomto smere certifikačným autoritám poskytovať Úrad.

Certifikačná autorita musí v priebehu vykonávania certifikačných činností plniť aj ďalšie povinnosti stanovené zákonom, ako je dodržiavanie stanoveného formátu vydávaných certifikátov, vedenie prevádzkovej dokumentácie, rušenie certifikátov. Rušenie certifikátov je popísané v § 23. Zákon ukladá certifikačnej autorite, aby v stanovenom čase (do 30 minút od okamihu, ako dostala podnet na zrušenie certifikátu) certifikát zrušila. Pre certifikačnú autoritu, ktorá má nepretržitú službu rušenia certifikátov, to znamená, že certifikát bude skutočne zrušený do 30 minút od prijatia žiadosti o zrušenie, v prípade certifikačnej autority, ktorá nemá nepretržitú prevádzku a žiadosťo zrušenie nedošla v priebehu prevádzkových hodín, k zrušeniu certifikátu dôjde v prvý pracovný deň po doručení žiadosti. Certifikačná autorita je povinná zverejniť zrušenie certifikátu prostredníctvom zoznamu zrušených certifikátov. Zákon ukladá certifikačnej autorite zaradiť zrušený certifikát do prvého zoznamu zrušených certifikátov, ktorý vydá po jeho zrušení; t.j. certifikačná autorita nesmie zverejnenie faktu, že došlo k zrušeniu certifikátu odkladať. Keďže podnet na zrušenie certifikátu nemusel dať len klient (ale napríklad súd, Úrad a pod.) certifikačná autorita je o tejto skutočnosti povinná klienta informovať hneď po zrušení jeho certifikátu (napr. písomne, elektronickou poštou a pod.). Keďže rušenie certifikátov je rozhodujúce z hľadiska udržania dôveryhodnosti elektronického podpisu a prevádzkové možnosti jednotlivých certifikačných autorít ovplyvnia spôsob rušenia certifikátov, certifikačná autorita je povinná informovať žiadateľa o vydanie certifikátu, akým spôsobom prebieha rušenie certifikátov, ako dlho môže trvať spracovanie žiadosti o zrušenie certifikátu a v akých intervaloch vydáva zoznam zneplatnených certifikátov.

Certifikačná autorita je okrem prevádzkovej dokumentácie viesť archív certifikátov a údajov, ktoré s nimi súvisia (napr. zoznamy zrušených certifikátov). Podrobnosti stanovuje § 26.

Úrad má vďaka informáciám, ktoré dostal pri registrácii certifikačnej autority prehľad o tom, aké služby a činnosti, pre koho a za akých podmienok bude vykonávať. Aj bezpečnostný audit certifikačnej autority sa viazal na dokumenty, ktoré boli v istom čase platné. Úrad posúdil predložené materiály a v prípade potreby vykonal vlastnú kontrolu na overenie a doplnenie predloženej informácie a ak nenašiel závažné

nedostatky, do činnosti certifikačnej autority nezasahoval. Ak však v certifikačnej autorite došlo k zmenám (bezpečnostný incident, rozšírenie ponuky certifikačných služieb, zmena vlastníka a pod.) ktoré môžu ovplyvňovať certifikačné služby, ktoré certifikačná autorita poskytuje, je certifikačná autorita povinná o zmenách informovať Úrad. Podľa § 17, ods (1) "obyčajná" certifikačná autorita má na to lehotu 30 dní, akreditovaná § 17 ods. (2) 6 hodín. Úrad určí o akých skutočnostiach, akou formou a dokedy po tom, ako k zmene došlo, ho certifikačná autorita, resp. akreditovaná certifikačná autorita o zmene je povinná informovať.

K § 16

Vzťahy medzi klientom a "obyčajnou" certifikačnou autoritou upravuje zmluva, ktorú spolu uzatvorili. Táto zmluva by mala upravovať aj povinnosti klienta, certifikačnej autority a zodpovednosť certifikačnej autority.
Činnosť akreditovanej certifikačnej autority je podrobne upravená týmto zákonom a predpismi, ktoré vydá Úrad a tak možno stanoviť aj zodpovednosť akreditovanej certifikačnej autority voči tretím osobám. Akreditovaná certifikačná autorita zodpovedá za dodržiavanie podmienok pre výkon akreditovaných činností, najmä rušenie kvalifikovaných certifikátov a vydávanie zoznamu zrušených kvalifikovaných certifikátov v súlade s ustanoveniami zákona. Na tom je totiž postavená vyššia úroveň dôvery v kvalifikovaný certifikát, ktorý vydala. Akreditovaná certifikačná autorita ďalej zodpovedá za to, že overila predpísaným spôsobom totožnosť žiadateľa o certifikát ako aj to, že disponoval súkromným kľúčom prislúchajúcim k verejnému kľúču uvedenému v certifikáte, a napokon, za presnosť a správnosť údajov certifikátu v čase jeho vydania.
Akreditovaná certifikačná autorita zodpovedá za to, že súkromný a príslušný verejný kľúč sa dajú bez problémov používať v bezpečných zariadeniach na vytváranie a overovanie elektronických podpisov, ktoré odporúčala; t.j. že pomocou zariadenia na overenie elektronického podpisu a verejného kľúča (a podpísaného elektronického dokumentu) možno overiť zaručený elektronický podpis vytvorený pre elektronický dokument pomocou daného súkromného kľúča a bezpečného zariadenia na vytváranie elektronického podpisu.
Akreditovaná certifikačná autorita nemôže ovplyvniť používanie ňou vydaných kvalifikovaných certifikátov a preto nezodpovedá za škody spôsobené tým, že sa ňou vydaný kvalifikovaný certifikát použil v rozpore s jeho určením (napr. obmedzeniami na výšku transakcií, spôsob použitia).
Ak nastane spor v súvislosti so zárukami uvedenými v ods. (1), akreditovaná certifikačná autorita sa vopred nemôže zbaviť zodpovednosti, ale musí dokázať, že svoje povinnosti neporušila.

K § 17

Prekážky vo výkone certifikačných činností patria k tým zmenám, o ktorých musí certifikačná autorita informovať Úrad. Vzhľadom na to, že Úrad "obyčajné" certifikačné autority len registruje (a môže kontrolovať), lehota na oznámenie je 30 dní od vzniku problému. Akreditovaná certifikačná autorita musí Úrad informovať o problémoch narúšajúcich jej normálne fungovanie do 6 hodín od ich objavenia, nakoľko Úrad udelením akreditácie garantuje to, že certifikačná autorita dosahuje vysokú úroveň poskytovaných certifikačných služieb. Ak to viac nie je pravda, Úrad musí zasiahnuť a uložiť akreditovanej certifikačnej autorite nápravné opatrenia (napr. zákaz poskytovania

niektorých služieb) a v krajnom prípade jej odňať akreditáciu. Aj "obyčajná" aj akreditovaná certifikačná autorita musí viesť prevádzkovú dokumentáciu, ktorú umožní spoľahlivo zistiť, kedy k mimoriadnej udalosti došlo.

Pri plánovanom ukončení činnosti certifikačnej autority musí mať Úrad dosť času na prípadnú kontrolu a jej klient na to, aby si nechal vystaviť certifikát u inej certifikačnej autority.

Ak "obyčajná" certifikačná autorita nájde certifikačnú autoritu, ktorá preberie správu ňou vydaných certifikátov, môže pokračujúca certifikačná autorita overovať a rušiť prevzaté certifikáty, po vypršaní ich platnosti ich archivovať. Bude musieť - buď ona, alebo Úrad - zverejniť informáciu o zrušení certifikátu zanikajúcej certifikačnej autority. Prevzané platné certifikáty však zostávajú naďalej platné - pri ich overovaní sa síce zistí, že certifikát certifikačnej autority, ktorá ich pôvodne vydala, je zrušený, ale podpisy na certifikátoch boli vytvorené v čase, keď certifikát platil, a teda sú platné. Časom vyprší aj ich platnosť a pokračujúca certifikačná autorita ich presunie do archívu. Prebratie agendy zanikajúcej certifikačnej autority prináša so sebou viaceré bezpečnostné riziká (zodpovednosť za neporiadne vedenú dokumentáciu, riziko kontroly a následných sankcií, chyby v obsahu vydaných certifikátov a pod.) a tak sa môže stať, že sa zanikajúcej certifikačnej autorite nepodarí nájsť pokračovateľa, ktorý by prebral jej agendu. V takom prípade nemá kto vykonávať správu jej certifikátov a teda v deň zániku certifikačnej autority zaniká aj platnosť všetkých jej certifikátov.

V prípade akreditovanej certifikačnej autority, ktorá vydávala kvalifikované certifikáty by dôsledky zrušenia všetkých kvalifikovaných certifikátov, ktoré zanikajúca akreditovaná certifikačná autorita vydala, a najmä nemožnosť overovať zaručené podpisy, ktoré boli v minulosti vytvorené a v prípade vedenia archívu kvalifikovaných certifikátov by boli overiteľné, mohli byť príliš veľké. Ak sa preto nenájde akreditovaná certifikačná autorita, ktorá by prebrala agendu zanikajúcej akreditovanej certifikačnej autority, musí túto agendu prebrať Úrad.

Pri zániku certifikačnej autority (obyčajnej alebo akreditovanej) sa rušia informačné systémy, ktoré obsahovali osobné údaje, na ochranu ktorých sa vzťahoval zákon o ochrane osobných údajov č. 52/1998. Tento zákon upravuje aj ničenie osobných údajov. Štatutárny zástupca zanikajúcej akreditovanej certifikačnej autority je povinný zaistiť, skontrolovanie toho, či pri rušení informačných systémov sa osobné údaje ktoré obsahovali, zničili v súlade so zákonom 52/1998.

K § 18

Úloha registračnej autority bola popísaná vo všeobecnej časti dôvodovej správy. Registračná autorita je sprostredkovateľom medzi klientom a certifikačnou autoritou. Registračná autorita prijíma žiadosti o vydanie certifikátov, overuje identitu žiadateľa o vydanie certifikátu, kontroluje údaje potrebné pre vydanie certifikátu na základe dokumentov predložených žiadateľom, uchováva potrebné údaje o žiadateľovi, spracúva podklady pre vydanie certifikátu certifikačnú autoritu a spoľahlivým spôsobom ich posiela certifikačnej autorite, poskytuje klientom informácie o činnosti certifikačnej autority. Ak klientovi generovala kľúče certifikačná autorita, registračná autorita odovzdáva klientovi prostriedok pre elektronický podpis s klientovým

súkromným kľúčom (napr. bezpečné zariadenie na vytváranie elektronického podpisu, alebo pamäťové médium). Registračná autorita prijíma aj žiadosti o zrušenie certifikátu, prípadne môže poskytovať aj iné certifikačné služby, na ktoré má vytvorené podmienky a na ktorých sa dohodne s certifikačnou autoritou, v mene ktorej koná.

Registračné služby sú zvláštnym druhom certifikačných služieb. Keďže na poskytovanie certifikačných služieb sa nevyžaduje žiadne povolenie, aj registračné služby môže poskytovať každý, kto na to má vytvorené primerané predpoklady (technické, priestorové, bezpečnostné, kvalifikačné, finančné a personálne). Keďže registračná autorita koná v mene certifikačnej autority, pravidlá pre výkon registračných činností určujú pravidlá pre výkon certifikačných činností príslušnej certifikačnej autority. Certifikačná autorita je oprávnená kontrolovať dodržiavanie týchto pravidiel, pretože voči Úradu zodpovedá aj za "svoje" registračné autority. Vzťah medzi registračnou a certifikačnou autoritou je upravený zmluvou.

K § 19

Strata bezpečného zariadenia na vytváranie elektronického podpisu alebo prezradenie súkromného kľúča držiteľa certifikátu môžu mať za následok vytváranie falošných (zaručených) elektronických podpisov. Uvedenie nepresných alebo nepravdivých údajov pri podávaní žiadosti o vydanie certifikátu zasa môže spôsobiť vydanie (kvalifikovaného) certifikátu s nepravdivými údajmi. Takéto udalosti môžu viesť k podvodom a následne spôsobiť stratu dôvery v elektronické podpisy. Preto je žiadateľ o vydanie certifikátu povinný uvádzať pravdivé a úplné údaje potrebné na vydanie certifikátu a keď sa údaje ktoré uviedol v žiadosti o vydanie certifikátu zmenia, je o tejto skutočnosti povinný informovať príslušnú certifikačnú autoritu. Okrem toho je povinný chrániť svoj súkromný kľúč a v prípade jeho prezradenia, podozrenia že došlo k prezradeniu alebo zmeny údajov uvedených v certifikáte (napr. postavenie v zamestnaní, oprávnenia) je držiteľ certifikátu povinný požiadať certifikačnú autoritu, ktorá jeho certifikát spravuje o jeho zrušenie. Ak držiteľ certifikátu zanedbá uvedené povinnosti a v dôsledku toho vznikne nejaká škoda, je za túto škodu zodpovedný v zmysle platných právnych predpisov.

K § 20

Informačné systémy registračnej autority, certifikačnej autority, akreditovanej certifikačnej autority a Úradu obsahujú osobné údaje a preto sa na ne vzťahuje zákon o ochrane osobných údajov v informačných systémoch. Tieto informačné systémy sú ich zriaďovatelia povinní registrovať v zmysle zákona o ochrane osobných údajov a podliehajú dozoru zo strany splnomocnenca na ochranu osobných údajov v informačných systémoch.

K § 21

Vytváranie elektronického podpisu bolo podrobne popísané vo všeobecnej časti dôvodovej správy.
Úrad stanoví vyhláškou podrobnosti vytvárania zaručeného elektronického podpisu: aké produkty pre elektronický podpis spĺňajú podmienky kladené na bezpečné zariadenia na vytváranie elektronického podpisu, aké algoritmy sa môžu používať, aké sú parametre

súkromných kľúčov použiteľných na vytváranie zaručených elektronických podpisov (napr. dĺžka kľúča, doba životnosti kľúča), aký formát má zaručený elektronický podpis mať a pod.

K § 22

Overovanie elektronického podpisu bolo popísané vo všeobecnej časti dôvodovej správy. Overenie elektronického podpisu znamená overenie toho, či elektronický podpis spĺňa formálne požiadavky (formát) a či je platný. Keďže zákon (v súlade so Smernicou) nepredpisuje povinný formát elektronického podpisu a ponecháva to na dohodu zúčastnených strán, aj podrobnosti overovania "obyčajných" elektronických podpisov si dohodnú zainteresované strany.
Zaručený elektronický podpis je definovaný presnejšie, a preto je aj princíp jeho overovania v zákone presne popísaný. Technické podrobnosti overovania zaručených elektronických podpisov sa však budú meniť v závislosti na vývoji medzinárodných noriem, používaných algoritmov a bezpečnostných požiadaviek, a preto zákon ponecháva na Úrad vydávanie podrobných predpisov.

K § 23

Certifikát je základom pre overovanie platnosti elektronického podpisu. Preto výskyt certifikátu, ktorý obsahuje nesprávnu alebo nepresnú informáciu, môže uviesť do omylu overovateľa elektronického podpisu, ktorý ho používa. Na druhej strane, certifikát môže spĺňať všetky formálne náležitosti, ale došlo k prezradeniu súkromného kľúča na vytváranie podpisov, ktoré sa pomocou daného certifikátu overujú. Nepovolaná osoba, ktorá získala cudzí súkromný kľúč, môže vytvárať elektronické podpisy na dokumenty v cudzom mene a nič netušiaci overovateľ ich pomocou priloženého certifikátu overí. Z hľadiska dôvery voči elektronickému podpisu je preto mimoriadne dôležité, aby sa zabránilo používaniu takýchto certifikátov. To sa dosahuje tým, že sa hneď, ako sa zistí že certifikát nespĺňa podmienky stanovené zákonom, alebo došlo k prezradeniu príslušného súkromného kľúča, je certifikačná autorita, ktorá certifikát spravuje (t.j. tá, ktorá ho vydala, alebo tá, ktorá ho prebrala od zaniknuvšej certifikačnej autority) povinná ho zrušiť; t.j. zrušiť mu platnosť. Zákon stanovuje, kto a z akých dôvodov môže iniciovať zrušenie certifikátu.

Pri rušení certifikátu je dôležitý čas. Ak by sa rušenie certifikátov odkladalo, zvyšovalo by sa riziko výskytu a použitia falošných elektronických podpisov, resp. elektronicky podpísaných dokumentov obsahujúcich nepravdivé údaje (napr. o postavení a právomociach podpisovateľa dokumentu, uvedených v pripojenom certifikáte jeho verejného kľúča). Preto je certifikačná autorita povinná do pol hodiny od prijatia podnetu certifikát zrušiť. V prípade certifikačnej autority poskytujúcej službu rušenia certifikátov nepretržite to znamená zrušenie certifikátu do 30 minút od podania podnetu, v prípade "obyčajnej" certifikačnej autority to môže znamenať až polhodinu od začiatku najbližšieho pracovného dňa po podaní podnetu na zrušenie certifikátu. Keďže zrušený certifikát je až do okamihu, keď sa o jeho zrušení dozvie, pre overovateľa elektronického podpisu platný, zákon ukladá certifikačnej autorite zaradiť zrušený certifikát na najbližší zoznam zrušených certifikátov, ktoré certifikačná autorita vydá. Ten síce môže byť zverejnený až s istým časovým odstupom od zrušenia daného certifikátu, ale overovateľ elektronického podpisu vie, kedy sa nový zoznam zrušených

certifikátov zverejní a počká s overovaním elektronického podpisu až do tej doby. Certifikačná autorita vedie svoj vlastný zoznam certifikátov, v ktorom má uvedený stav každého certifikátu. Ak poskytuje možnosť okamžitého overenia platnosti certifikátov, musí poskytovať aktuálnu informáciu o zrušení certifikátu od okamihu jeho zrušenia a nie až od okamihu zverejnenia zoznamu zrušených certifikátov.

Aj keď sa môže stať, že dôvod na zrušenie certifikátu nastal omnoho skôr, ako sa na to prišlo, nie je možné zrušiť certifikát so spätnou platnosťou, ale len od okamihu prijatia žiadosti na zrušenie certifikátu. Rovnako sa môže stať, že sa dôvod na zrušenie certifikátu (podozrenie o prezradení súkromného kľúča držiteľa certifikátu) nepotvrdí. To však nemôže byť dôvodom na obnovenie platnosti zrušeného certifikátu. Obnovovanie platnosti zrušených certifikátov by vnieslo chaos do zoznamov zrušených certifikátov a preto ho zákon nepovoľuje. (Držiteľ omylom zrušeného certifikátu má možnosť požiadať o vydanie nového certifikátu svojho verejného kľúča a nakoľko tento certifikát bude mať prinajmenšom iné identifikačné číslo ako zrušený certifikát, a preto k problémom pri rozlišovaní zrušeného a platného certifikátu nedôjde.)

Aby držiteľ certifikátu, resp. osoby, ktoré sú uvedené v certifikáte mohli bez problémov požiadať o zrušenie certifikátu, je im certifikačná autorita povinná poskytnúť viacero možností ako podať žiadosť. Akreditovaná certifikačná autorita musí naviac prevádzkovať službu rušenia certifikátov nepretržite.

Zrušené certifikáty môžu byť predmetom sporov. Certifikačná autorita musí preto viesť podrobnú dokumentáciu, ktorá umožní v prípade potreby spoľahlivo zistiť kto, kedy, z akých dôvodov a ktorý certifikát požadoval zrušiť.

K § 24

Zákon stanovuje postup pri prijímaní žiadosti o vydanie certifikátu, vydaní certifikátu a používaní certifikátu. Postup pri riešení udalostí, ktoré majú za následok spochybnenie platnosti certifikátu, upravoval predchádzajúci paragraf.

K § 25

Elektronické podpisy by mali umožniť aj komunikáciu prekračujúcu hranice. Na to je potrebné zabezpečiť, aby slovenské elektronické podpisy mali medzinárodnú platnosť a opačne, stanoviť podmienky, za ktorých bude možné na Slovensku používať zahraničné elektronické podpisy. Podmienky pre platnosť cudzích elektronických podpisov na svojom teritóriu si stanovuje každý štát sám. Smernica EÚ dáva v tomto ohľade odporúčania, ktoré predkladaný návrh zákona zohľadňuje. Pre overenie elektronického podpisu vydaného zahraničnou certifikačnou autoritou je rozhodujúca možnosť overiť platnosť certifikátu príslušného verejného kľúča. To naráža na dva problémy: ako overiť platnosť podpisu zahraničnej certifikačnej autority, ktorá certifikát vydala a ako zistiť, či certifikát nebol medzičasom zrušený. Zahraničná certifikačná autorita má tri možnosti ako hodnoverne poskytnúť svoj verejný kľúč potenciálnym overovateľom elektronických podpisov pomocou certifikátov, ktoré vydala: môže získať akreditáciu Úradu a stať sa akreditovanou certifikačnou autoritou aj pre Slovensko. V tom prípade jej Úrad vydá kvalifikovaný certifikát jej verejného kľúča. V druhom prípade si s nejakou slovenskou (akreditovanou) certifikačnou autoritou vydajú vzájomne krížové

certifikáty svojich verejných kľúčov. To je možné v prípade, keď obe certifikačné autority dosahujú rovnakú bezpečnostnú úroveň poskytovaných certifikačných služieb (napríklad, obe získali akreditáciu podľa porovnateľných akreditačných schém). Tretia možnosť je založená na medzinárodnej dohode. Ak Slovensko uzavrie s nejakým štátom dohodu o vzájomnom uznávaní certifikátov, Úrad vydá dohodou určeným zahraničným certifikačným autoritám certifikáty ich verejných kľúčov. V druhom a treťom prípade je nutné zabezpečiť overovateľom elektronických podpisov založených na certifikátoch vydaných zahraničnými certifikačnými autoritami, prístup k zoznamom zrušených certifikátov zahraničných certifikačných autorít; vo vyššie uvedenom prvom prípade (zahraničná certifikačná autorita akreditovaná podľa slovenskej akreditačnej schémy Úradom) je požiadavka dosažiteľnosti zoznamov zneplatnených certifikátov nutnou podmienkou úspešnej akreditácie, a teda je splnená.

Zákon predpokladá, že po vstupe Slovenska do EÚ budú mať certifikáty vydávané v EÚ rovnakú právnu účinnosť ako slovenské certifikáty.

K § 26

Keďže (zaručené) elektronické podpisy sa budú používať aj na právne úkony, musia byť overiteľné aj po uplynutí platnosti certifikátov, ktoré sa používali na ich overovanie. Certifikačná autorita je preto povinná uchovávať všetky relevantné dokumenty (certifikáty, zoznamy zrušených certifikátov, žiadosti o vydanie certifikátov, žiadosti o zrušenie certifikátov, bezpečnostné politiky, pravidlá certifikačných činností), ktoré sú potrebné na overenie toho, či daný certifikát v nejakom časovom okamihu existoval a aký bol jeho stav (platný alebo zrušený), aké boli podmienky správy certifikátov a vykonávania certifikačných činností. Ak sa budú pre nejaké iné účely uchovávať elektronické dokumenty dlhšie a bude potrebné zabezpečiť overovanie platnosti ich elektronických podpisov, môže iný zákon stanoviť pre certifikačnú autoritu povinnosť archivovať údaje aj dlhšie.

Vzhľadom na rozsah údajov, ktoré bude potrebné archivovať, je archív možné viesť aj v elektronickej podobe. V tom prípade však treba zohľadniť aj životnosť pamäťových médií, dostupnosť zariadení na prácu s nimi a nutnosť ochrany ich autentickosti a integrity.

K § 27

Nutným predpokladom používania elektronických podpisov je spoľahlivá ochrana súkromných kľúčov. Ak by sa totiž nepovolaná osoba dostala k cudziemu súkromnému kľúču, mohla by vytvárať elektronické podpisy v cudzom mene, podpisovať falošné záväzky a pod. Súkromný kľúč síce môže byť uložený aj na pamäťovom médiu a chránený tým, že je zašifrovaný, ale na vytvorenie elektronického podpisu sa musí dešifrovať a použiť v otvorenej podobe. Vtedy hrozí kopírovanie súkromného kľúča, alebo jeho použitie na vytvorenie elektronického podpisu iného dokumentu, ako chcel podpisovateľ a ďalšie riziká. Aby sa tieto riziká minimalizovali, súkromný kľúč sa musí primerane chrániť a používať len v spoľahlivom prostredí. Pre zaručené elektronické podpisy zákon stanovuje požiadavky, ktoré takéto spoľahlivé prostredie (bezpečné zariadenie na vytváranie elektronického podpisu) musí spĺňať.

Kryptografické kľúč (súkromný a verejný kľúč) na vytváranie a overovanie elektronického podpisu sa musia niekde vytvárať. Buď ich vytvára certifikačná autorita a ukladá pri zachovaní potrebných bezpečnostných opatrení do bezpečných zariadení na vytváranie elektronických podpisov klientov, alebo si ich klienti generujú sami pomocou svojich bezpečných zariadení na vytváranie elektronických podpisov. V prípade, že sa bezpečné zariadenie na vytváranie elektronického podpisu použije aj na vytváranie kryptografických kľúčov, musí byť zaistená bezpečnosť celého procesu, aby nedošlo k prezradeniu súkromného kľúča. To znamená, že súkromný kľúč, ktorý bol vytvorený v bezpečnom zariadení na vytvárenie elektronického podpisu, nesmie opustiť toto zariadenie v otvorenej (nešifrovanej) podobe.

Zákon výslovne uvádza tri zásadné požiadavky na bezpečné zariadenie na vytváranie elektronického podpisu: podpisovaný dokument sa vytváraním elektronického podpisu nemôže zmeniť. To znamená, že overovateľ elektronického podpisu musí mať možnosť získať z elektronicky podpísaného dokumentu pôvodný nepodpísaný dokument.
Keďže elektronický dokument (napríklad wordovský súbor) obsahuje okrem viditeľnej informácie aj doplnkové informácie (napr. o formáte dokumentu, použitých fontoch, ale aj o systéme, na ktorom bol dokument vytvorený), ktoré sa bežne nezobrazujú, podpisovateľ by mohol v skutočnosti podpísať iný dokument, ako hodlal podpisovať. To by mohol prípadný protivník využiť a upraviť podpisovací systém tak, že by zobrazoval iný dokument a iný podpisoval. Bezpečné zariadenie na vytváranie elektronického podpisu musí preukázateľne zobrazovať ten dokument, ktorý podpisovateľ podpisuje.
Ak sa v bezpečnom zariadení na vytváranie elektronického podpisu vytvárajú kryptografické kľúče, potom je potrebné minimalizovať možnosť toho, že sa nejaký kľúč vytvorí dvakrát. Táto požiadavka je dôležitá predovšetkým pre bezpečné zariadenia na vytváranie elektronického podpisu (kryptografické moduly) certifikačnej autority, ktoré sa používajú aj na vytváranie kryptografických kľúčov pre klientov. Z tejto požiadavky vyplýva nevyhnutnosť použitia kvalitného generátora náhodných čísel a dodržania korektných postupov pri vytváraní kľúčov. (Požiadavky na kryptografické moduly podrobne popisuje medzinárodne uznávaný americký štandard FIPS 140-1, resp. FIPS 140-2).

Prezradenie súkromného kľúča certifikačnej autority by umožnilo vydávať falošné certifikáty (napr. certifikáty znejúce na cudzie meno). To by následne umožnilo vytváranie falošných (v cudzom mene) elektronických podpisov. Preto zákon stanovuje základnú požiadavku, ktorú musia spĺňať zariadenia používané na správu kvalifikovaných certifikátov - musia byť schopné zabrániť falšovaniu certifikátov.

Zákon tiež špecifikuje základné požiadavky, ktoré musia spĺňať procedúry a zariadenia na overovanie zaručených elektronických podpisov, aby overovateľ spoľahlivo overil platný zaručený elektronický podpis a rozpoznal neplatný (zaručený) elektronický podpis.

Bezpečné zariadenie na vytváranie časovej pečiatky vytvára aj zaručený elektronický podpis dokumentu (doplneného o časový údaj), a preto sa naň vzťahujú všetky požiadavky súvisiace s ochranou súkromného kľúča, vytváraním zaručeného elektronického podpisu a prípadne vytváraním kryptografických kľúčov.

Úrad vydá požiadavky, ktoré musia produkty pre elektronický podpis spĺňať, bude takéto zariadenia posudzovať a v prípade, keď stanovené podmienky spĺňajú, vydávať im osvedčenia. Zoznam takýchto Úradom certifikovaných produktov budú mať klienti k dispozícii prostredníctvom akreditovaných certifikačných autorít, aby si mohli vybrať zariadenie (produkt), ktorý ich potrebám a požiadavkám najlepšie vyhovuje a spĺňa bezpečnostné kritériá stanovené Úradom. Keďže kapacita Úradu nie je dostatočná na to, aby posúdil všetky možné produkty pre elektronický podpis, Úrad sa bude podieľať na činnosti medzinárodných organizácií, ktoré vypracujú štandardy a budú vydávať medzinárodné zoznamy produktov pre elektronický podpis, ktoré týmto štandardom vyhovujú. Proces štandardizácie, posudzovania a certifikácie produktov pre elektronický podpis už prebieha niekoľko rokov.

K § 28

Úrad môže prostredníctvom akreditačnej schémy predpísať certifikačným autoritám uchádzajúcim sa o akreditáciu a akreditovaným certifikačným autoritám postupy, ktoré musia uplatňovať pri vykonávaní akreditovaných činností a úroveň bezpečnostných požiadaviek, ktoré musia spĺňať. Akreditované certifikačné autority povinne zakomponovali požiadavky Úradu do svojich dokumentov (certifikačný poriadok, bezpečnostná politika, pravidlá pre výkon certifikačných činností,...). Najmenej raz do roka je akreditovaná certifikačná autorita povinná podrobiť sa externému auditu. Cieľom tohto uaditu je posúdenie toho, do akej miery sa zhoduje spôsob vykonávania certifikačných činností s postupmi popísanými v dokumentácii, a to najmä z hľadiska bezpečnosti. Audit nebude vykonávať Úrad, ale audítori alebo audítorské firmy. Aby bola zaručená odborná úroveň auditu, Úrad stanoví tak požiadavky na kvalifikáciu audítorov, ako aj na podrobnosť auditu.

Výsledok auditu akreditovaná certifikačná autorita v stanovenom čase musí predložiť úradu a ten podľa predloženej správy rozhodne o ďalšom postupe (všetko je v poriadku, akreditovaná certifikačná autorita môže pokračovať v činnosti; v činnosti akreditovanej certifikačnej autority sa vyskytli problémy, ktoré majú jasné príčiny a sú zrejmé postupy na ich odstránenie; akreditovaná certifikačná autorita má vážne problémy a nespĺňa požiadavky stanovené akreditačnou schémou; akreditovanú certifikačnú autoritu musí skontrolovať samotný Úrad).

K § 29

Úrad kontroluje všetky certifikačné autority (a pre ne pracujúce registračné autority) pôsobiace v otvorených systémoch na území Slovenska, od okamihu, ako podali žiadosť o registráciu, či konajú v súlade s týmto zákonom. Ak Úrad zistí, že certifikačná autorita nespĺňa požiadavky na výkon certifikačných činností, môže jej uložiť nápravné opatrenia, alebo jej čiastočne, dočasne alebo celkom zastaviť činnosť.
Keďže Úrad udelením akreditácie certifikačnej autorite garantuje vyššiu úroveň ňou poskytovaných certifikačných služieb, musí kontrolovať, či od akreditácie nedošlo k zníženiu úrovne výkonu akreditovaných certifikačných činností. Ak Úrad zistí, že došlo k nedostatkom, ktoré majú bezpečnostné dôsledky (o takýchto udalostiach ho je sama akreditovaná certifikačná autorita povinná do 6 hodín informovať), môže akreditovanej certifikačnej autorite nariadiť zrušenie platnosti "podozrivých" certifikátov. Úrad môže

akreditovanej certifikačnej autorite pozastaviť akreditáciu, odňať akreditáciu, zakázať jej vykonávať niektoré činnosti alebo jej pozastaviť činnosť celkom.

Zastavením činnosti certifikačnej autority (akreditovanej certifikačnej autority) nestrácajú automaticky platnosť certifikáty, ktoré daná certifikačná autorita vydala. (Ak by Úrad mal o ich platnosti pochybnosti, musí certifikačnej autorite najprv nariadiť ich zrušenie.)

Aby mohli zamestnanci Úradu vykonať kontrolu certifikačnej, akreditovanej certifikačnej autority a registračných autorít, ktoré v ich mene poskytujú registračné služby, zákon ukladá zamestnancom kontrolovaných inštitúcií povinnosť spolupracovať pri kontrole. Aby boli chránené záujmy kontrolovaných inštitúcií, zákon zaväzuje kontrolujúcich zachovávavním mlčanlivosti o skutočnostiach zistených pri kontrole a to aj po ukončení pracovného vzťahu s Úradom; výnimkou sú prípady stanovené osobitnými zákonmi.

K § 30 a § 31

Popri nápravných opatreniach môže Úrad za porušenie zákona udeľovať pokuty akreditovaným certifikačným autoritám, certifikačným autoritám, právnickým a fyzickým osobám. Za porušenie zákona registračnou autoriou zodpovedá certifikačná autorita, v mene ktorej koná; ak sa nejedná o organizačnú zložku certifikačnej autority, sankcie, ktoré za nedostatky v registračnej činnosti registračnej autority dostala certifikačná autorita, sú ošetrené v zmluve medzi registračnou a certifikačnou autoritou.

Výška pokút je odstupňovaná podľa závažnosti porušenia zákona a zodpovedá výške pokút, ktoré za podobné porušenia zákona o elektronickom podpise stanovujú zákony o elektronickom podpise v zahraničí.

K § 32

Zavedenie elektronického podpisu a zaručeného elektronického podpisu do praxe si bude vyžadovať mnohé úpravy existujúcich postupov. Zákon ukladá Úradu povinnosť pripraviť zodpovedajúce právne predpisy.

K § 34

Zákon identifikuje zákony a právne normy, ktorých sa bezprostredne dotkne prijatie zákona o elektronickom podpise a navrhuje ich úpravy. Stanovuje výšku správnych poplatkov za podanie žiadosti o akreditáciu a certifikáciu zariadení na vytváranie a overenie elektronického podpisu. Keďže náklady na zriadenie a prevádzku certifikačných a registračných autorít sa budú pohybovať v miliónových čiastkach, zákon nezaťažuje poskytovateľov certifikačných služieb vysokými správnymi poplatkami.

K § 35

Zákon o elektronickom podpise by mal vstúpiť do platnosti od 1.1.2002. Tento termín je navrhnutý z dvoch dôvodov: na vytvorenie Úradu sú potrebné prostriedky, ktoré je

možné vyčleniť až v štátnom rozpočte na rok 2002. Tak príprava Úradu, ako aj vypracovanie rozsiahlych predpisov, technických noriem a iných dokumentov upravujúcich vytváranie a používanie elektronického podpisu a výkon certifikačných činností, si vyžiada značné množstvo práce. Základné dokumenty by sa však pri využití existujúcich odborných kapacít mohli dať do stanoveného času vytvoriť.

DOLOŽKA ZLUČITEĽNOSTI

návrhu zákona s právom Európskej únie

1. **Navrhovateľ zákona:**

   skupina poslancov NR SR.

2. **Názov návrhu zákona:**

   Zákon o elektronickom podpise.

3. ***V práve Európskej únie je problematika návrhu zákona upravená:***

- v smernici Európskeho parlamentu a Rady 1999/93 z 13.12.1999 o rámci Spoločenstva pre elektronické podpisy, (OJ L 013, 19/01/2000)

- v rozhodnutí Komisie 2000/709 zo 6.11.2000 o minimálnych kritériách, ktoré majú členské štáty brať do úvahy pri tvorbe orgánov v súlade s článkom 3 ods.4 smernice 1999/93 (OJ L 289, 16/11/2000)

- v smernici 2000/31 z 8.6.2000 o určitých právnych aspektoch služieb informačnej spoločnosti, najmä elektronického obchodu vo vnútornom trhu, (smernica o elektronickom obchode, OJ L 178, 17/07/2000)

- v rozhodnutí Rady z 25.1.1999 prijímajúcom špecifický program pre výskum, technologický rozvoj a realizáciu užívateľsky zrozumiteľnej (user-friendly) informačnej spoločnosti, (OJ L 064, 12/03/1999)

- v rezolúcii Rady o spotrebiteľskej dimenzii informačnej spoločnosti z 19.1.1999, (OJ C 023, 28/01/1999), ktorá však nie je právne záväzným aktom.

4. **Návrh zákona svojou problematikou (úprava elektronického podpisu, certifikačných a registračných služieb) nepatrí** medzi prioritné oblasti upravené v článku 70 Európskej dohody o pridružení. Nepriamo sa však dotýka oblasti ochrana spotrebiteľa. Svojou problematikou nepatrí ani medzi priority odporúčané v Bielej knihe - Príprave krajín strednej a východnej Európy na integráciu do vnútorného trhu únie.

5. **Charakteristika právnych noriem Európskej únie, ktorými je upravená problematika návrhu zákona:**

Smernica 1999/93 z 13.12.1999 o rámci Spoločenstva pre elektronické podpisy, o.i. definuje ťažiskové pojmy ako sú: elektronický podpis, podpisovateľ, certifikát verejného kľúča, poskytovateľ certifikačných služieb, atď. Ďalej upravuje právny účinok elektronického podpisu, povinnosti a zodpovednosť poskytovateľa certifikačných služieb, ako aj medzinárodné aspekty úpravy (uznávanie zahraničných certifikátov a uznávanie elektronických podpisov zahraničných subjektov).

Rozhodnutie Komisie 2000/709 zo 6.11.2000 obsahuje kritériá, ktoré majú spĺňať vnútroštátne orgány zodpovedné za hodnotenie bezpečnosti technických prostriedkov používaných na tvorbu podpisu. Ide najmä o nezávislosť a transparentnosť pri činnosti takých orgánov ako aj ich technické a personálne zabezpečenie.

Smernica 2000/31 z 8.6.2000 o elektronickom obchode stanovuje pravidlá upravujúce služby informačnej spoločnosti v prostredí vnútorného trhu; relevantná je úprava uzatvárania zmlúv elektronickými prostriedkami.

Rozhodnutie Rady z 25.1.1999 prijímajúce špecifický program pre výskum, technologický rozvoj a realizáciu užívateľsky zrozumiteľnej (user-friendly) informačnej spoločnosti, je platné pre obdobie od 25.1.1999 do 31.12.2002 a obsahuje množstvo pravidiel pre zabezpečenie realizácie tohto programu.

Rezolúcia Rady o spotrebiteľskej dimenzii informačnej spoločnosti z 19.1.1999 vyzýva k zabezpečeniu záujmov spotrebiteľa v informačnej spoločnosti, o.i. aj doplnením existujúcej legislatívy v tejto oblasti vzhľadom na elektronický obchod, jeho riziká a možnosti.

6. **Vyjadrenie stupňa kompatibility s právnou normou EÚ:**
kompatibilita návrhu zákona je úplná.

Ministerstvo financií SR
Odbor štátneho rozpočtu

Bratislava, 19.4.2001

Národná rada
Slovenskej republiky

Vec: stanovisko odboru štátneho rozpočtu k rozpočtovým dôsledkom návrhu poslanca NR SR Františka Šebeju na vydanie zákona NR SR č. ...../2001 o elektronickom podpise

V dôvodovej správe k predloženému návrhu zákona sa v súvislosti s jeho realizáciou kvantifikujú rozpočtové dopady na vytvorenie Úradu pre elektronický podpis v rámci Národného bezpečnostného úradu v objeme 186 mil. Sk, z toho 119,0 mil. Sk na vytvorenie Úradu a 67 mil. Sk ročné prevádzkové náklady.

Návrh obsahuje pomerne podrobnú špecifikáciu nákladov na zriadenie i prevádzkovanie Úradu. Podrobné stanovisko k tejto špecifikácii vypracujú príslušné rozpočtové kapitoly v rámci riadneho medzirezortného pripomienkového konania.

Pri kvantifikácii rozpočtových dôsledkov sa však abstrahuje od nákladov, ktoré by schválením tohto návrhu zákona vznikli v tých organizáciách štátnej správy, ktoré by mali umožniť záujemcom takýto kontakt (daňové úrady, inštitúcie zabezpečujúce styk s obyvateľstvom...).

Pretože MF SR nedisponuje informáciami, do akej miery sú tieto inštitúcie vybavené príslušnými zariadeniami, nemožno ani kvantifikovať ďalšie rozpočtové požiadavky, ktoré by tieto inštitúcie na štátny rozpočet vzniesli.

Ďalšie náklady môžu vzniknúť v nadväznosti na potrebu kryptovania v prípade, ak sa nakladá s tajnými informáciami. Aj

tieto náklady bude možné upresniť až v nadväznosti na stanoviská príslušných rezortov.

Upozorňujeme, že v predchádzajúcich návrhoch na prijatie zákona o elektronickom podpise sa uplatňovala i požiadavka na vznik akreditačného úradu na Ministerstve vnútra SR. V predloženom návrhu sa výdavky na jeho zdriadenie nekvantifikujú.

Navrhujeme v dôvodovej správe jednoznačnejšie formulovať i náklady, ktoré vzniknú užívateľovi elektronického podpisu (najmä prípadné poplatky za akreditáciu a pod.).

V súhrne odbor štátneho rozpočtu konštatuje, že prijatím navrhovaného zákona vzniknú okrem tých rozpočtových dôsledkov, ktoré kvantifikuje predkladateľ i ďalšie, ich upresnenie v súčasnosti nie je možné jednoznačne spracovať.

Odbor štátneho rozpočtu sa v súčasnej etape pripomienkovania nevyjadruje k legislatívnej a obsahovej stránke predloženého návrhu zákona.

Ing. Miloš Nosál, CSc.
riaditeľ odboru
štátneho rozpočtu

Nosál

Odhad nákladov na zriadenie Úradu pre elektronické podpisy

Celkové realizačné náklady:

Technické vybavenie	57 100 000
Programové vybavenie	1 390 000
Technické zabezpečenie úradu	20 800 000
Materiálno . technické vybavenie a zabezpečenie	30 600 000
Výkon interných a externých služieb	9 000 000
REALIZAČNÉ NÁKLADY SPOLU	**118 890 000**

Celkové ročné prevádzkové náklady:

ROČNÉ PREVÁDZKOVÉ NÁKLADY	**67 039 000**

Konkretizácia položiek:

TECHNICKÉ VYBAVENIE

Bezpečný server ústrednej certifikačnej autority + horúca záloha	17 500 000
Time Stamp Server (server časovej pečiatky) + záloha	5 000 000
Firewall (3x)	1 800 000
Archivačný server	500 000
Web server	500 000
Bezpečný pracovný server	700 000
Pracovná stanica (40 x)	5 000 000
Bezpečná pracovná stanica (10 x)	3 000 000
Prístrojové vybavenie pre servis	10 000 000
Prezentačná (školiaca) a reprodukčná technika	3 000 000
Vybavenie oddelenia certifikácie tech. prostriedkov bezp. EP	5 000 000
Prevádzkové a zálohové médiá	300 000
Klimatizácia archívu	800 000
Záložný zdroj energie	1 500 000
Rezerva	3 000 000
SPOLU	**57 100 000**

PROGRAMOVÉ VYBAVENIE

Programové vybavenie ústrednej CA (1 licencia)	500 000
Programové vybavenie pre TSS	300 000
Programové vybavenie pre archivačný server	300 000
Sieťový software pre vnútornú sieť NUEP	50 000
Antivirový software (50 licencií - multilicencia)	20 000
Vytvorenie WEB stránky	20 000
Rezerva	200 000

SPOLU	**1 390 000**

TECHNICKÉ ZABEZPEČENIE ÚRADU

Uzavretý TV systém	1 500 000
Elektronická poplachová signalizácia	3 000 000
Elektrická požiarna signalizácia	3 000 000
Systém kontroly prístupu	2 500 000
Bezpečný turniketový prechod	1 500 000
Trezorové hospodárstvo	3 000 000
Mechanické zábrany	800 000
Stavebné úpravy	3 500 000
Rezerva	2 000 000
SPOLU	**20 800 000**

MATERIÁLNO - TECHNICKÉ VYBAVENIE A ZABEZPEČENIE

Stavebné úpravy objektu	10 000 000
Realizácia vnútornej štrukturovanej dátovej siete	1 500 000
Vybavenie nábytkom	8 000 000
Kancelárske potreby, pracovné pomôcky a spotrebný materiál	600 000
Klimatizácia určených priestorov	1 000 000
Prevádzkové motorové vozidlá (4)	5 000 000
Iné	4 500 000
SPOLU	**30 600 000**

VÝKON INTERNÝCH A EXTERNÝCH SLUŽIEB

Školenie odborných pracovníkov UCA u zahr. dodávateľa SW	5 000 000
Odborný audit systémov	3 500 000
Rezerva	500 000
SPOLU	**9 000 000**

PREVÁDZKOVÉ NÁKLADY / 1 ROK

Technické vybavenie - 20 % ročne z nadobúdacej ceny	11 420 000
Programové vybavenie - 10 % ročne z nadobúdacej ceny	139 000
Technické zabezpečenie úradu - 10 % ročne z nadobúdacej ceny	2 080 000
Mzdové prostriedky interných pracovníkov	28 000 000
MTZ - údržba objektu, klimatizácie, vybavenie objektu, atď.	3 500 000
Prevádzka a údržba služobných vozidiel	3 000 000
Služby telekomunikácií	5 000 000
Prenájom rýchlych dátových okruhov	600 000
Kontrolná činnosť NUEP	1 000 000
Metodická a štandardizačná činnosť NUEP	1 000 000
Spracovanie a vydávanie dokumentov a doporučení	800 000
Odborná literatúra	300 000
Styk so zahraničnými partnermi - uznávanie zahr. certifikátov	1 500 000
Služby externých organizácií a expertov	4 000 000
Zabezpečenie fyzickej ostrahy objektu	1 200 000
Energie (elektrická energ., voda, a pod.)	1 500 000
Rezerva	2 000 000
SPOLU	**67 039 000**

Návrh štruktúry a obsahu všeobecne záväzných predpisov k poslaneckému návrhu zákona o elektronickom podpise

Navrhované všeobecne záväzné predpisy vydá Národný bezpečnostný úrad - úrad pre elektronický podpis ako záväzné pre vykonávanie zákona NR SR č. ...../2001 Z.z. o elektronickom podpise.

1. Vyhláška Úradu pre elektronický podpis č. ..../200. z ....., ktorou sa vykonáva zákon Národnej rady Slovenskej republiky č...../2001 Z.z. o elektronickom podpise

Predmet vyhlášky:

a. Táto vyhláška upravuje používanie elektronického podpisu podľa zákona NR SR č. ...../2001 Z.z. o elektronickom podpise na území Slovenskej republiky v obchodnom a administratívnom styku

b. určuje spôsoby, metódy, postupy pri poskytovaní služieb v súvislosti s elektronickým podpisom, a povinnosti ich akreditovaných poskytovateľov a ich postavenie

c. stanovuje obsah prevádzkovej dokumentácie, ktorú musí akreditovaný poskytovateľ certifikačných služieb povinne viesť

d. upravuje postup pri žiadosti poskytovateľov certifikačných služieb o akreditáciu, postup Úradu pre elektronický podpis (ďalej iba úradu) pri jej udeľovaní a odnímaní

e. stanovuje požiadavky na audit akreditovaných poskytovateľov certifikačných služieb. požiadavky na kvalifikáciu audítorov, podrobnosti a rozsah auditu ako aj podmienky pre spoluprácu auditorov a úradu

f. konkretizuje činnosť úradu v oblasti elektronického podpisu v SR

2. Vyhláška Úradu pre elektronický podpis č. ..../200. z ....., ktorou sa stanovujú podmienky pre bezpečné zariadenia na vytváranie elektronického podpisu, bezpečné zariadenia na vytváranie časovej pečiatky a spôsob ich hodnotenia

Predmet vyhlášky:

a. Predmetom vyhlášky je stanovenie povinných technických parametrov, spôsob konštrukcie, implementácie a používania hardverových prostriedkov pre bezpečné vytváranie elektronického podpisu

b. Spôsob hodnotenia (certifikácie) prostriedkov, uvedených v bode a. úradom.

c. Stanovenie vlastností programového vybavenia pre bezpečné vytváranie elektronického podpisu a spôsob jeho tvorby. Vyhláška stanovuje formy a spôsob predloženia programovej dokumentácie pre jej hodnotenie úradom.

d. Predmetom vyhlášky je stanovenie povinných technických parametrov, spôsob konštrukcie, zabezpečenia, implementácie a používania hardverových prostriedkov pre bezpečné vytváranie časovej pečiatky a spôsoby bezpečného začlenenia takto vytvorených dát do kvalifikovaného certifikátu.

e. Spôsob hodnotenia (certifikácie) prostriedkov, uvedených v bode d. úradom.

f. Stanovenie vlastností programového vybavenia pre bezpečné vytváranie časovej pečiatky a spôsob jeho tvorby. Vyhláška stanovuje formy a spôsob predloženia programovej dokumentácie pre jej hodnotenie úradom.

3. Vyhláška Úradu pre elektronický podpis č. ..../200. z ....., ktorou sa stanovujú podmienky vytváranie a používanie zaručeného elektronického podpisu

Predmet vyhlášky:

a. Postup fyzickej osoby pri vytváraní zaručeného elektronického podpisu a jeho používaní.

b. Definovanie formátu zaručeného elektronického podpisu.

c. Definovanie formátu časovej pečiatky a spôsob jej vytvárania.

d. Spôsob použitia zaručeného elektronického podpisu vo verejnej správe Slovenskej republiky a v styku verejná správa - občan.

e. Postup pri overovaní a podmienky overenia alebo odmietnutia zaručeného elektronického podpisu overovateľom

f. Spôsoby a podmienky zverejňovania verejných kľúčov, prislúchajúcich k súkromným kľúčom určeným na vytváranie zaručeného elektronického podpisu úradom.

4. Vyhláška Úradu pre elektronický podpis č. ..../200. z ....., o správe a používaní kvalifikovaných certifikátov

Predmet vyhlášky:

a. Stanovuje formát a obsah jednotlivých druhov kvalifikovaných certifikátov podľa §9 zuákona o EP.

b. Definuje formát, frekvenciu vydávania a spôsob vydávania zoznamov zrušených kvalifikovaných certifikátov.

c. Stanovuje podmienky a postup zrušenia kvalifikovaných certifikátov úradom.

5. Vyhláška Úradu pre elektronický podpis č. ..../200. z ....., o vzájomnom uznávaní certifikátov medzi Slovenskou republikou a inými krajinami

Predmet vyhlášky:

a. Konkretizuje podmienky uznávania certifikátov alebo kvalifikovaných certifikátov medzi Slovenskou republikou a inými krajinami,

b. Stanovuje spôsob zverejňovania krížového zoznamu uznaných zahraničných certifikátov t.j. zahraničných certifikátov uznaných v Slovenskej republike a certifikátov, vydaných poskytovateľom certifikačných služieb v Slovenskej republike, uznaných v zahraničí

Národná rada Slovenskej republiky

II. volebné obdobie

Číslo: 928/2001

984a

Spoločná správa

výborov Národnej rady Slovenskej republiky o výsledku prerokovania návrhu skupiny poslancov Národnej rady Slovenskej republiky na vydanie zákona o elektronickom podpise (tlač **984**) v druhom čítaní

Výbor Národnej rady Slovenskej republiky pre hospodárstvo, privatizáciu a podnikanie v súlade s § 78 zákona NR SR č. 350/1996 Z. z. o rokovacom poriadku Národnej rady Slovenskej republiky (ďalej len „rokovací poriadok") predkladá Národnej rade Slovenskej republiky ako gestorský výbor (ďalej len „gestorský výbor") spoločnú správu výborov NR SR k návrhu skupiny poslancov Národnej rady Slovenskej republiky na vydanie zákona o elektronickom podpise (tlač **984**) v druhom čítaní.

I.

Národná rada Slovenskej republiky uznesením č. 1555 zo 6. septembra 2001 pridelila návrh zákona na prerokovanie s termínom do 11. októbra 2001 výborom:

Ústavnoprávnemu výboru NR SR
Výboru NR SR pre financie, rozpočet a menu
Výboru NR SR pre verejnú správu
Výboru NR SR pre obranu a bezpečnosť
Výboru NR SR pre európsku integráciu
Výboru NR SR pre hospodárstvo, privatizáciu a podnikanie.

Ako gestorský výbor určila Výbor NR SR pre hospodárstvo, privatizáciu a podnikanie na vypracovanie spoločnej správy o výsledku prerokovania v lehote do 16. októbra 2001.

Uvedené výbory prerokovali pridelený návrh a gestorský výbor prerokoval a schválil podľa § 79 ods. 4 rokovacieho poriadku spoločnú správu výborov NR SR uznesením č. 637 z 26. októbra 2001.

Iné výbory NR SR návrh neprerokovali.

II.

Gestorskému výboru do začatia jeho rokovania neoznámili poslanci, ktorí nie sú členmi výborov NR SR, uvedených v uznesení NR SR, svoje stanoviská podľa § 75 ods. 2 rokovacieho poriadku.

III.

Výbory NR SR, ktorým bol pridelený návrh zákona na prerokovanie, zaujali tieto stanoviská:

Ústavnoprávny výbor NR SR prerokoval návrh 10. októbra 2001 a uznesením č. 697 prerušil rokovanie a vracia poslanecký návrh predkladateľom návrhu na dopracovanie.

Výbor NR SR pre financie, rozpočet a menu prerokoval návrh 17. októbra 2001 a neprijal platné uznesenie, lebo podľa § 52 ods. 4 rokovacieho poriadku národnej rady nehlasovala za navrhnuté uznesenie nadpolovičná väčšina prítomných členov výboru (z 12 členov výboru prítomných 8, za nikto, proti nikto, zdržali sa 8 poslanci).

Výbor NR SR pre verejnú správu prerokoval návrh 15. októbra 2001 a uznesením č. 343 prerušil rokovanie a neodporúča národnej rade návrh schváliť v predloženom znení.

Výbor NR SR pre obranu a bezpečnosť prerokoval návrh 9. októbra 2001 a uznesením č. 417 odporučil Národnej rade Slovenskej republiky návrh schváliť s pripomienkami.

Výbor NR SR pre európsku integráciu rokoval o návrhu 2. októbra 2001, nebol uznášaniaschopný a neprijal platné uznesenie.

Výbor NR SR pre hospodárstvo, privatizáciu a podnikanie prerokoval návrh 15. októbra 2001 a uznesením č. 626 odporučil Národnej rade Slovenskej republiky návrh podľa § 79 ods. 4 písm. f) rokovacieho poriadku národnej rady návrh zákona vrátiť navrhovateľovi zákona na dopracovanie.

IV.

Z uznesení výborov NR SR, uvedených v bode III. tejto správy, vyplývajú tieto závery:

a) Výbor NR SR pre obranu a bezpečnosť odporučil schváliť s týmito pripomienkami:

1. Návrh zákona označiť ako čl. I a zákony uvedené v § 34 ako odseky označiť ako články. Ako posledný článok označiť doterajší § 35.

2. K čl. I § 1 nový text poznámky pod čiarou k odkazu [1] znie:
„[1] Zákon Národnej rady Slovenskej republiky č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.“.

   Pôvodná poznámka sa vzťahovala k už neplatnému zákonu č. 100/1996 Z. z.

3. K čl. 8 doterajší § 35 novooznačený ako čl. VIII. znie:

„Tento zákon nadobúda účinnosť 1. januára 2002 okrem § 6, 7, 14 až 17, 23 ods. 5, 25, 27 ods. 7, 28 až 31, ktoré nadobúdajú účinnosť 1. júla 2002.“.

   Táto úprava sa týka vytvorenia dostatočného časového priestoru pre naštartovanie Úradu pre elektronický

podpis.

b) Ústavnoprávny výbor NR SR, Výbor NR SR pre financie, rozpočet a menu, Výbor NR SR pre verejnú správu a Výbor NR SR pre hospodárstvo, privatizáciu a podnikanie odporučili Národnej rade Slovenskej republiky podľa § 79 ods. 4 písm. f) rokovacieho poriadku národnej rady návrh zákona vrátiť navrhovateľovi zákona na dopracovanie. Toto stanovisko zobrali súhlasne na vedomie aj predkladatelia poslaneckého návrhu zákona.

V.

Gestorský výbor neodporúča o návrhoch výboru NR SR pre obranu a bezpečnosť hlasovať.

VI.

Gestorský výbor na základe rokovaní výborov NR SR v súlade s § 79 ods. 4 písm. f) rokovacieho poriadku

odporúča Národnej rade Slovenskej republiky

návrh skupiny poslancov Národnej rady Slovenskej republiky na vydanie zákona o elektronickom podpise (tlač **984**)

podľa § 79 ods. 4 písm. f) rokovacieho poriadku národnej rady návrh zákona vrátiť navrhovateľovi zákona na dopracovanie.

Súčasne poveril uznesením výboru č. 637 z 26. októbra 2001 spoločného spravodajcu výborov predložiť Národnej rade Slovenskej republiky spoločnú správu výborov o výsledku prerokovania vládneho návrhu zákona a poveril ho oprávneniami podľa § 79 ods. 5 rokovacieho poriadku Národnej rady Slovenskej republiky.

Bratislava, 26. októbra 2001

Jaroslav **V o l f** v. r.
predseda Výboru NR SR pre
hospodárstvo, privatizáciu
a podnikanie