

540

VYHLÁŠKA
Národného bezpečnostného úradu

z 9. septembra 2002

**o podmienkach na poskytovanie akreditovaných certifikačných služieb
a o požiadavkách na audit, rozsah auditu a kvalifikáciu auditorov**

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 13 ods. 2 a § 25 ods. 1 zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1

Predmet úpravy

Táto vyhláška upravuje podrobnosti o

- a) materiálnych, priestorových, technických, organizačných a právnych podmienkach na poskytovanie akreditovaných certifikačných služieb,
- b) požiadavkách na audit, rozsah auditu a kvalifikáciu auditorov a o výkone auditu akreditovanej certifikačnej autority.

Podrobnosti o podmienkach
na poskytovanie akreditovaných
certifikačných služieb

§ 2

Certifikačná autorita, ktorá chce poskytovať akreditované certifikačné služby,

- a) doručí úradu žiadosť o akreditáciu; k žiadosti o akreditáciu certifikačná autorita predloží náležitosti podľa § 13 ods. 3 zákona,
- b) preukáže úradu splnenie podmienok podľa § 3 až 5 na poskytovanie akreditovaných certifikačných služieb.

§ 3

(1) Certifikačná autorita, ktorá žiada o akreditáciu, musí vlastniť alebo mať zmluvne zabezpečený prenájom priestorov na poskytovanie akreditovaných certifikačných služieb, ktoré vyhovujú bezpečnostným pravidlám¹⁾ a podmienkam podľa odsekov 2 až 5.

(2) V prípade poskytovania akreditovaných certifikačných služieb v prenajatých priestoroch musí byť samostatný vstup majiteľa objektu do chránených priestorov zmluvne obmedzený len na nevyhnutné a okamžité riešenie havarijných stavov budovy.

(3) Okrem prevádzkových priestorov musí akreditovaná certifikačná autorita zabezpečiť ďalšie chránené priestory na bezpečné skladovanie archívnych dokumentov a údajov a mesačných záložných kópií údajov systému akreditovanej certifikačnej autority; tieto priestory musia byť umiestnené v objekte, ktorý nie je fyzicky spojený s objektom, v ktorom sa realizuje poskytovanie akreditovaných certifikačných služieb.

(4) Technické a organizačné opatrenia musia zaistiť nepretržitú prevádzku akreditovanej certifikačnej autority aj v prípade zlyhania základnej technickej infraštruktúry minimálne na úrovni poskytovania služby registrácie požiadaviek na funkciu časovej pečiatky.

(5) Certifikačná autorita musí mať vypracovaný vlastný systém priebežnej kontroly funkčnosti a bezpečnosti používaných bezpečnostných prostriedkov a opatrení.

§ 4

Certifikačná autorita, ktorá žiada o akreditáciu, predloží okrem základných technických parametrov a dokumentácie prostriedkov podľa osobitného predpisu²⁾ aj dokumentáciu prostriedkov, ktoré plánuje použiť na podporu poskytovania certifikačných služieb na

- a) vedenie a zabezpečenie archívu dokumentov podľa § 18 zákona,
- b) prevádzku a zabezpečenie svojej internetovej stránky.

§ 5

Akreditovaná certifikačná autorita musí mať vytvorené organizačné podmienky v tomto rozsahu:

- a) bezpečnostné pravidlá certifikačnej autority na bezpečný režim poskytovania certifikačných služieb a na výkony certifikačných činností,
- b) opatrenia určujúce podmienky vstupu osôb do chráneného priestoru, podmienky na prácu s produktom pre elektronický podpis a opatrenia určujúce

¹⁾ Vyhláška Národného bezpečnostného úradu č. 541/2002 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností.

²⁾ Vyhláška Národného bezpečnostného úradu č. 539/2002 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis (o produktoch elektronického podpisu).

- júce činnosti v prípade vzniku situácie ohrozujúcej poskytovanie certifikačných služieb,
- c) organizačné rozčlenenie činností súvisiacich s poskytovaním certifikačných služieb medzi rôzne osoby a útvary tak, aby bola umožnená vzájomná kontrola, ako aj nezávislá kontrola vykonávaných činností,
 - d) vedenie prevádzkovej dokumentácie certifikačnej autority podľa osobitného predpisu,¹⁾
 - e) zásady na výkon personálnej práce v rámci certifikačnej autority,
 - f) zásady na výkon vnútornej kontroly v rámci certifikačnej autority,
 - g) zásady na zaistenie bezpečnosti pri uzatváraní zmluvných vzťahov s právnickými osobami alebo s fyzickými osobami o poskytovaní služieb podporujúcich poskytovanie služieb certifikačnou autoritou.

§ 6

Podrobnosti o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov

(1) Audit bezpečnosti poskytovania certifikačných činností môže vykonať len oprávnená fyzická osoba alebo právnická osoba.

(2) Fyzická osoba alebo právnická osoba môže byť oprávnená na výkon auditu bezpečnosti certifikačných činností, ak

- a) je držiteľkou platného medzinárodného alebo slovenského osvedčenia na výkon auditu informačných systémov,
- b) má preukázateľnú odbornú prax v oblasti auditu informačných systémov nie kratšiu ako päť rokov.

(3) Výkon auditu pozostáva z overenia

- a) bezpečnostných vlastností produktu pre elektronický podpis a bezpečnostných vlastností prostredia, v ktorom sa produkt pre elektronický podpis prevádzkuje,
- b) bezpečnosti šifrovacích prostriedkov a režimu práce s nimi,

- c) ochrany produktu pre elektronický podpis pred neautorizovanou manipuláciou, zneužitím a zlyhaním,
- d) bezpečnosti procesov výkonu certifikačných činností,
- e) ochrany komunikačnej infraštruktúry pred útokmi a zlyhaniami,
- f) súladu položiek v papierových a elektronických záznamoch výkonu certifikačných činností,
- g) vhodnosti a dostatočnosti bezpečnostného zámeru, projektu a bezpečnostných smerníc,
- h) vhodnosti a dostatočnosti bezpečnostných opatrení a prostriedkov, ktoré sú špecifikované v bezpečnostných smerniciach,
- i) bezpečnostných opatrení súvisiacich s poskytovaním činností inými právnickými osobami alebo fyzickými osobami,
- j) iných bezpečnostných opatrení a prostriedkov, ktoré certifikačná autorita prijala s cieľom zaistenia spoľahlivosti a bezpečnosti poskytovania certifikačných služieb,
- k) pripravenosti certifikačnej autority pri výskyte udalostí ohrozujúcich jej prevádzku – plánov pre prípad havárií a plánov obnovy činnosti certifikačnej autority,
- l) ostatných požadovaných bezpečnostných požiadaviek na výkon certifikačných činností podľa zákona.

(4) Výkon auditu sa končí záverečnou správou, ktorá pozostáva z

- a) výroku audítora a zhodnotenia celkového stavu bezpečnosti certifikačnej autority v čase výkonu bezpečnostného auditu,
- b) popisu zistení o nedostatkoch bezpečnostného charakteru,
- c) odporúčaní na odstránenie zistených nedostatkov.

§ 7

Účinnosť

Táto vyhláška nadobúda účinnosť 1. októbra 2002.

Ján Mojžiš v. r.