ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2009

Vyhlásené: 8. 4. 2009 Vyhlásená verzia v Zbierke zákonov Slovenskej republiky

Obsah tohto dokumentu má informatívny charakter.

132

VYHLÁŠKA

Národného bezpečnostného úradu

z 26. marca 2009

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

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 audítorov 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 pravidlám[1]) 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 zaisťujú nepretržitú prevádzku akreditovanej certifikačnej autority aj v prípade zlyhania základnej technickej infraštruktúry najmenej na úrovni poskytovania služby registrácie požiadaviek u poskytovateľa akreditovanej certifikačnej služby

a) správy kvalifikovaných certifikátov podľa § 2 písm. l) prvého bodu zákona na poskytovanie zoznamu zrušených kvalifikovaných certifikátov,

b) dlhodobého uchovávania elektronických dokumentov podpísaných zaručeným elektronickým podpisom podľa § 2 písm. l) druhého bodu zákona na overenie a zobrazenie dokumentu,

c) vydávania časových pečiatok podľa § 2 písm. l) tretieho bodu zákona na registráciu požiadaviek na vydanie časovej pečiatky.

(5) Akreditovaná certifikačná autorita poskytujúca službu dlhodobého uchovávania elektronických dokumentov podpísaných zaručeným elektronickým podpisom zabezpečuje

a) zobrazenie elektronického dokumentu spôsobom umožňujúcim zistiť jeho obsah,

b) zachovanie integrity dokumentu – potvrdenie, že obsah dokumentu nebol zmenený a je dostupný v podobe, v akej bol do archívu uložený,

c) zachovanie autentickosti dokumentu – potvrdenie, že elektronický dokument bol vytvorený a podpísaný osobou, ktorá je uvedená ako podpisovateľ elektronického dokumentu,

d) evidenciu a uchovanie informácií dôležitých z hľadiska existencie elektronického dokumentu, údaje o prevzatí, o spôsobe uloženia, o prístupe k dokumentu, o type úložného média a iné,

e) výkon takých aktivít v rámci manipulácie s elektronickým dokumentom, ktoré umožnia uchovať nepopierateľnosť existencie a integritu údajov a zaistiť ich požadovanú dostupnosť.

(6) Pri vykonávaní činností podľa odseku 5 sa uplatňujú štandardy uvedené v medzinárodných normatívnych dokumentoch.[2])

(7) Aplikácie používané na poskytovanie služby dlhodobého uchovávania elektronických dokumentov podpísaných zaručeným elektronickým podpisom zabezpečujú, aby bolo možné overovať zaručený elektronický podpis aj po čase platnosti certifikátov použitých na overenie podpisu. Pre zabezpečenie možnosti overenia zaručeného elektronického podpisu aplikácie používajú formáty elektronického podpisu pre dlhodobé overovanie uvedené v európskych normatívnych dokumentoch[3]) a časové pečiatky, ktorých formát je uvedený v medzinárodných normatívnych dokumentoch.[4])

(8) Akreditovaná certifikačná autorita poskytujúca službu dlhodobého uchovávania elektronických dokumentov podpísaných zaručeným elektronickým podpisom zabezpečuje, aby dokumenty neboli poskytované tretej strane bez súhlasu vlastníka.

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

(10) Pri poskytovaní akreditovaných certifikačných služieb podľa § 2 písm. l) prvého bodu zákona poskytovateľ uplatňuje štandardy uvedené v európskych normatívnych dokumentoch.[5])

§ 4

Certifikačná autorita, ktorá žiada o akreditáciu, predloží okrem opisu a dokumentácie základných technických parametrov a dokumentácie prostriedkov podľa osobitného predpisu[6]) 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 webovej stránky.

§ 5

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

a) bezpečnostné pravidlá certifikačnej autority na bezpečný režim poskytovania akreditovaných 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 činnosti v prípade vzniku situácie ohrozujúcej poskytovanie akreditovaných certifikačných služieb,

c) organizačné rozčlenenie činností súvisiacich s poskytovaním akreditovaných 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]) primerane podľa druhu poskytovanej akreditovanej certifikačnej služby,

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 zaistiť spoľahlivosť a bezpečnosť 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 zo 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
Zrušovacie ustanovenie

Zrušuje sa vyhláška Národného bezpečnostného úradu č. 540/2002 Z. z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov.

§ 8
Záverečné ustanovenia

(1) Touto vyhláškou sa preberajú právne akty Európskych spoločenstiev a Európskej únie uvedené v prílohe.

(2) Táto vyhláška bola prijatá v súlade s príslušným právnym aktom Európskych spoločenstiev[7]) pod číslom notifikácie 2008/0531/SK.

§ 9
Účinnosť

Táto vyhláška nadobúda účinnosť dňom vyhlásenia.

František Blanárik v. r.

Príloha
k vyhláške č. 132/2009 Z. z.

ZOZNAM PREBERANÝCH PRÁVNYCH AKTOV EURÓPSKYCH SPOLOČENSTIEV A EURÓPSKEJ ÚNIE

Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy (Ú. v. ES L 13, 19. 1. 2000; Mimoriadne vydanie Ú. v. EÚ, kap. 13/zv. 24).

1) Vyhláška Národného bezpečnostného úradu č. 133/2009 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností.

2) ISO/TR 15801: Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability (ISO/TR 15801 Elektronické zobrazovanie. Informácie uchovávané elektronicky. Odporúčania pre dôveryhodnosť a spoľahlivosť), ISO/TR 18492: Long – term preservation of electronic document – based information (ISO/TR 18492 Dlhodobé uchovávanie informácií založených na elektronických dokumentoch).

3) ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI). CMS Advanced Electronic Signatures (CAdES) [Elektronické podpisy a infraštruktúry (ESI). CMS zaručené elektronické podpisy (CAdES)]. ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES) [XML zaručené elektronické podpisy (XAdES)]. RFC 5126 Electronic Signature Formats for Long Term Electronic Signatures (Formáty elektronického podpisu pre dlhodobé elektronické podpisy).

4) RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) (Protokol časovej pečiatky).

5) ETSI TS 101 456 Electronic signatures and Infrastructures (ESI): Policy requirements for certification autorities issuing qualified certificates [ETSI TS 101 456 Elektronické podpisy a infraštruktúry (ESI). Požiadavky na politiky certifikačných autorít vydávajúcich kvalifikované certifikáty], CWA 14172-2 EESSI Conformity Assessment Guidance – Part 2: Certification Authority services and processes (Návod EESSI na posúdenie zhody. Časť 2: Služby a procesy certifikačných autorít).

6) Vyhláška Národného bezpečnostného úradu č. 134/2009 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).

7) Smernica Európskeho parlamentu a Rady 98/34/ES o postupe pri poskytovaní informácií v oblasti technických noriem a predpisov (Ú. v. ES L 204, 21. 7. 1998; Mimoriadne vydanie Ú. v. EÚ, kap. 3/zv. 20) v platnom znení.

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Ministerstvo spravodlivosti Slovenskej republiky, Župné námestie 13, 813 11 Bratislava,
tel.: 02 888 91 137, fax: 02/52442853, e-mail: helpdesk@slov-lex.sk.